Contributions to Security and Defence Studies

Heiko Borchert
Torben Schütz
Joseph Verbovszky *Editors*

The Very Long Game

25 Case Studies on the Global State of Defense AI

OPEN ACCESS

Springer

Contributions to Security and Defence Studies

This book series offers an outlet for cutting-edge research on all areas of security and defence studies. Contributions to Security and Defence Studies (CSDS) welcomes theoretically sound and empirically robust monographs, edited volumes and handbooks from various disciplines and approaches on topics such as international security studies, securitization, proliferation and arms control, military studies, strategic studies, terrorism and counter-terrorism, defence and military economics, economic security, defence technologies, cyber-warfare, cyberdefence, military applications of artificial intelligence, security policies, policing and security, political violence, and crisis and disaster management.

All titles in this series are peer-reviewed.

Heiko Borchert • Torben Schütz •
Joseph Verbovszky
Editors

The Very Long Game

25 Case Studies on the Global State of Defense AI

Springer

Editors
Heiko Borchert
Defense AI Observatory
Helmut Schmidt University
Hamburg, Germany

Torben Schütz
Defense AI Observatory
Helmut Schmidt University
Hamburg, Germany

Joseph Verbovszky
Defense AI Observatory
Helmut Schmidt University
Hamburg, Germany

ISSN 2948-2283 ISSN 2948-2291 (electronic)
Contributions to Security and Defence Studies
ISBN 978-3-031-58648-4 ISBN 978-3-031-58649-1 (eBook)
https://doi.org/10.1007/978-3-031-58649-1

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

"*The Very Long Game* is an eye-opening book. AI has the potential to be the single greatest force multiplier for armed forces in human history. But how to prepare armed forces to successfully leverage AI? This is the key question at the core of *The Very Long Game*. An impressive selection of 25 international case studies convincingly illustrates that conceptual, cultural, organizational, and operational transformation need to go hand in hand with technological innovation for AI to make a difference. Written by expert analysts and practitioners, *The Very Long Game* compellingly blends theoretical with practical insight and sets the standard for comparative defense AI analyses. Military leaders, industry experts, and scholars will greatly benefit from reading this book".

—Gen (ret) John Allen, *Former Commander of the NATO International Security Assistance Force, and US Forces in Afghanistan, past President of The Brookings Institution, and Strategic Advisor to the Microsoft Corporation*

"A most timely comparative study, rich in empirical analysis, that examines the "drivers, pace, and priorities" of defense AI across 25 nations. This volume is a vital resource for anyone interested in military innovation and defense transformation".

—Prof. Theo Farrell, PhD, *President and Vice-Chancellor, La Trobe University*

"The Very Long Game is an absolute must-have for everyone interested in defense AI! 25 case studies provide a comprehensive in-depth look at the current practice and future trajectories of defense AI across different regions. One of the book's key strengths is the unitary analytical framework, which makes the detailed case studies easily accessible and provides insightful findings on cross-regional commonalities and differences".

—Joonsoo Park*, Director, Defense Acquisition and Industries Division, Korea Institute for Defense Analyses*

"*The Very Long Game* is an excellent and timely volume, bringing out comparative strengths and weaknesses of over two dozen countries who are interested and invested in AI. That the volume dwells into details on how each of the nations is preparing for AI adoption in military and defense strategies is particularly relevant. *The Very Long Game* is a must-read for policy makers, practitioners, as well as academia, who are interested in technologies and future warfare".

—Dr. Rajeswari Pillai Rajagopalan, *Director, Center for Security, Strategy and Technology, Observer Research Foundation*

"The use of AI by the armed forces is a major issue for the development of national military power and the shape of geopolitical competition. Indeed, military AI is the subject of many speculations regarding the future character of warfare, as well as ethical concerns about the proper interactions between human decision-makers and AI-enabled weapons systems. This book provides the reader with a

much-needed overview of what different military organizations around the world actually do to implement AI in the conduct of their daily operations. Looking at countries varying in size, resources, or strategic priorities, it gives a solid conceptual and empirical foundation to analyze the current and future developments in the military use of AI".

—Prof. Dr. Olivier Schmitt, *Center for War Studies, University of Southern Denmark*

Acknowledgments

The Very Long Game is the product of the "Joint Force" in action. 34 scholars and practitioners engaged in assessing the use of artificial intelligence (AI) for defense in 25 nations. Our analysis appears at a time of fundamental strategic change. 24 February 2022 marks Russia's invasion of Ukraine, and 7 October 2023 marks the attack of Hamas on Israel. Both conflicts have triggered vigorous debate about the current (and future) interplay of legacy systems with emerging technologies like AI and the setup required for armed forces to generate and adopt novel ways of warfighting. These geopolitical changes are paired with a fundamentally new geoeconomic environment. 7 October 2022 marks the adoption of the hitherto most far-reaching export and technology restrictions the USA has adopted in its techno-economic competition with China. These restrictions have been justified on the grounds of reining in China's ability to exploit technologies like AI to advance its strategic goals. Thus, defense AI sits at the center of geopolitical and geoeconomic competition.

The chapters published in *The Very Long Game* reflect this duality and put it in context with strategic culture, long-term force development needs, urgent operational requirements, and defense/commercial ecosystem developments across the North Atlantic Community, Eurasia, the Greater Middle East, and the Asia-Pacific region. Each of these regions is home to different drivers of strategic change that affect how armed forces think about defense AI and how they prioritize its use for current and future missions. The following chapters illustrate the respective consequences and challenges.

Our volume grew out of a collection of country case studies that the Defense AI Observatory (DAIO) started publishing in early 2022. DAIO has been established within the framework of GhostPlay, a capability and technology development project funded by dtec.bw—Digitalization and Technology Research Center of the German Bundeswehr, whose support we gratefully acknowledge. dtec.bw is funded by the European Union—NextGenerationEU. Being part of an ongoing defense project offers the opportunity to focus our analytical work on what is practically needed to advance defense capabilities while at the same time reflecting upon the

broader context of defense innovation. Consequently, we wanted to better understand how armed forces conceive defense AI.

The need to separate rhetoric from reality prompted us to reach out subject matter experts across 25 countries to produce the *The Very Long Game.* We are immensely grateful that our co-authors accepted our invitation to scrutinize the current international practice of defense AI and attended the September 2023 authors' workshop in Berlin. The "Joint Force" helped us understand where the defense AI journey is heading, which parts of the journey might constitute a break with the past, and when and where caution is at place to see through the "fog of hype" encapsulating defense AI. This volume is a starting point that offers a conceptual reference framework to analyze the contribution of AI in shaping the demanding transition from warfighting as a human endeavor to a future of collaborative human–machine interaction. Given the need for a comprehensive rethink of the intellectual, cultural, organizational, and technological underpinnings of military power, this is indeed going to be a very long game.

Hamburg, 15 February 2024

Heiko Borchert
Torben Schütz
Joseph Verbovszky

The publication of this book is funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr, which we gratefully acknowledge. dtec.bw is funded by the European Union – NextGenerationEU.

Contents

Contributors

Liran Antebi Advanced Technologies and National Security Program, Institute of National Security Studies, Tel Aviv, Israel

Heiko Borchert Defense AI Observatory, Helmut Schmidt University, Hamburg, Germany

Inbar Dolinko Independent Researcher and Consultant, Tel Aviv, Israel

Robert C. Engen Australian Defence College, Canberra, Australia

Alastair Finlan Swedish Defence University, Stockholm, Sweden

Andrea Gilli University of St Andrews, St Andrews, Scotland

Mauro Gilli Center for Security Studies, Swiss Federal Institute of Technology, Zurich, Switzerland

Vitaliy Goncharuk AI Committee of Ukraine, Kyiv, Ukraine

TechWise Society Foundation, Washington, DC, USA

Andreas Immanuel Graae Department of Military Technology, Royal Danish Defence Academy, Copenhagen, Denmark

Marierose M. M. Heineken-van Dooren Netherlands Defence Academy, Breda, The Netherlands

Sami O. Järvinen Defence Command Finland, Helsinki, Finland

Mahmoud Javadi Erasmus School of Social and Behavioral Sciences, Erasmus University Rotterdam, Rotterdam, The Netherlands

Tomas Jermalavičius International Center for Defence and Security, Tallinn, Estonia

Lauren Kahn Center for Security and Emerging Technology, Washington, DC, USA

Nikolaos Karampekios Innovation and Networking Unit, National Documentation Center (EKT), Athens, Greece

Çağlar Kurç Political Science and International Relations, Abdullah Gül University, Kayseri, Turkey

Peter Layton Griffith Asia Institute, Brisbane, QLD, Australia

John Lee Leiden Asia Centre, Leiden, The Netherlands

East West Futures Consulting, Berlin, Germany

Kitsch Liao Atlantic Council Global China Hub, Washington, DC, USA

Roy Lindelauf Netherlands Defence Academy, Faculty of Military Sciences, Breda, The Netherlands

Tilburg University, Tilburg, The Netherlands

Data Science Center of Excellence, Ministry of Defence, The Hague, The Netherlands

Lucie Liversain Management Research Center, Ecole Polytechnique (I3-CRG*), Paris, France

Kevin Martin Fondation pour la Recherche Stratégique, Paris, France

Shimona Mohan United Nations Institute for Disarmament Research (UNIDIR), Geneva, Switzerland

Iraklis Oikonomou Independent Researcher, Athens, Greece

Youngwook Park The Korea Institute of Defence Technology, Seoul, South Korea

Myongji University, Youngin-si, South Korea

Woosuk University, Wanju-gun, South Korea

Kenneth Payne King's College, London, UK

Michael Raska S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Nanyang, Singapore

Raquel Jorge Ricart Technology and International Affairs, Elcano Royal Institute, Madrid, Spain

Konstantinos Sakkonos National and Kapodistrian University of Athens, Athens, Greece

Hellenic Air Force, Athens, Greece

Torben Schütz Defense AI Observatory, Helmut Schmidt University, Hamburg, Germany

German Council on Foreign Policy, Berlin, Germany

Motohiro Tshuchiya Graduate School of Media and Governance, Keio University, Tokyo, Japan

Keio University Global Research Institute, Tokyo, Japan

Joseph Verbovszky Defense AI Observatory, Helmut Schmidt University, Hamburg, Germany

Ivan Zaccagnini Department of Political Science, LUISS University, Rome, Italy

Center for Security, Diplomacy, and Strategy (CSDS), Vrije Universiteit Brussels (VUB), Brussels, Belgium

Katarzyna Zysk Norwegian Institute for Defence Studies, Oslo, Norway

Abbreviations

3D	Dull, Dirty, or Dangerous
4IRC	4th Industrial Revolution Committee
A2/AD	Anti-Access/Area Denial
AAPS UCU	Ukrainian Catholic University's Faculty of Applied Sciences
ACCESS	Arctic Command and Control Effector and Sensor System
ACINT	Acoustic Intelligence
ADD	Agency for Defense Development
ADF	Australian Defence Force
ADIA	Abu Dhabi Investment Authority
ADM(DIA)	Assistant Deputy Minister (Data, Innovation, Analytics)
ADM(IM)	Assistant Deputy Minister (Information Management)
AED	Automated External Defibrillator
AEPL	Aerospace Engineering Private Limited
AFIB	Autonomous Fast Intercept Boat
AI	Artificial Intelligence
AI4DEF	Artificial Intelligence for Defence
AIA	Algorithmic Impact Assessment
AIDA	Artificial Intelligence Deployable Agent (Estonia)
AIDA	Artificial Intelligence and Data Accelerator (United States)
AIDef	AI in Defense
AIE	Artificial Intelligence Exploration
AIM	Atal Innovation Mission
AIMA	AI-Based Multifunctional Aperture
AIO	Aerospace Industries Organization
AIoT	Artificial Intelligence of Things
AIP	Center for Advanced Intelligence Project
AIPfD	AI Partnership for Defence
AIRC	Artificial Intelligence Research Center
AIST	National Institute of Advanced Industrial Science and Technology
AJP	Allied Joint Publication

AMRAAM	Advanced Medium-Range Air-to-Air Missile
AND	Defense Digital Agency
ANSSI	National Agency for Information Systems Security
APC	Armoured Personnel Carrier
AR	Augmented Reality
ARES	Advanced Recognition and Exploitation System
ARIA	Advanced Research and Invention Agency
ARTEMIS	Army Tactical Engagement and Information System
ASCA	Advanced Strategic Capabilities Accelerator
ASEAN	Association of Southeast Asian Nations
ATGM	Guided Anti-Tank Missiles
ATLA	Acquisition, Technology & Logistics Agency
ATP	Allied Tactical Publication
ATR	Advanced Telecommunications Research Institute International
ATRDC	Aerospace Technology Research and Development Center
AUKUS	Australia, the United Kingdom, and the United States
AUV	Autonomous Underwater Vehicle
AW	Autonomous Warrior
BAES	BAE Systems
BLOS	Beyond Line of Sight
BMD	Ballistic Missile Defense
BMS	Battlefield Management Systems
BMVg	Bundesministerium der Verteidigung
BVLOS	Beyond Visual Line of Sight
BVR	Beyond Visual Range
C2	Command and Control
C3I	Command, Control, Communications and Intelligence
C4/5	Command, Control, Computers, Communications, and Cyber
C4I	Command, Control, Computers, Communications, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance
CAD	Canadian Dollar
CAF	Canadian Armed Forces
CAIR	Centre for Artificial Intelligence and Robotics
CAPE	Office of Cost Assessment and Program Evaluation
CAS	Chinese Academy of Sciences
CAS IoA	Chinese Academy of Science's Institute of Automation
CASC	China Aerospace Science and Technology Corporation
CASG	Capability Acquisition and Sustainment Group
CBRN	Chemical, Biological, Radiological, and Nuclear
CCCI	Central Commission for Cybersecurity and Informatization
CCDCOE	Cooperative Cyber Defense Centre of Excellence
CCIAD	Defense Artificial Intelligence Coordination Unit
CCIS	Command and Control Information System

CCIT	Chung Cheng Institute of Technology
CCW GGE	United Nations Convention on Certain Conventional Weapons and its Group of Governmental Experts
CD&E	Concept Development and Experimentation
CDAO	Chief Digital and Artificial Intelligence Office
CDF	Chief of the Defense Force
CDO	Office of the Chief Data Officer
CDS	Chief of the Defense Staff
CDTI	Center for Technological and Innovation Development
CEA	French Alternative Energies and Atomic Energy Commission
CEPN	Naval Programs Expertise Center
CESEDEN	Research Centre for High Studies on National Defense
CESIVA	Army Simulation and Validation Center
CESTIC	Center for Information and Communications Systems and Technologies
CETC	China Electronics Technology Group Corporation
CFSP	Common Foreign and Security Policy
CHOD	Chief of Defense
CIO	Chief Information Officer
CIR	Cyber- und Informationsraum
CIT	Cyber- und Informationstechnik
CIWS	Close-In Weapon System
CMC	Central Military Commission
CMS	Combat Management System
CNAD	Conference of National Armaments Directors
CNASOFCOM	Canadian Special Operations Forces Command
CNKI	China National Knowledge Infrastructure
CNO	Computer Network Operations
CNR	National Research Council
CNRS	National Center for Scientific Research
COINCIDENTE	Program for Cooperation in Scientific Research and Strategic Technologies Development
COMINT	Communication Intelligence
COMMANDS	Convoy Operations with Manned-unManneD Systems
CONOPS	Concept of Operations
COP	Common Operational Picture
COPD	Comprehensive Operations Planning Directive
CP	Command Post
CPAS	Campaign Planning and Analysis System
CPC	Communist Party of China
CPR	Cardiopulmonary Resuscitation
CSC	Concept to Sovereign Capability
CSD-M	Naval Data Service Center
CSIC	China Shipbuilding Industry Corporation
CSIRO	Commonwealth Scientific and Industrial Research Organization

CSIT	Centre for Strategic Infocomm Technologies
CSO	Composante Spatiale Optique
CTO	Chief Technology Officer
D-LBO	Digitalized Land-Based Operations
D&D	Denial and Deception
DACOIE	Danish Common Operational Information Environment
DAIC	Defense Artificial Intelligence Center (United Kingdom)
DAIC	Defense Artificial Intelligence Council (India)
DAIC	Defense Artificial Intelligence Council (South Korea)
DAICoE	Defense AI Center of Excellence
DAIPA	Defense AI Projects Agency
DAIRNet	Defense AI Research Network
DALO	Defense Acquisition and Logistics Organization
DAPA	Defense Acquisition Program Administration
DARB	NATO Data and Artificial Intelligence Review Board
DARPA	Defense Advanced Research Projects Agency
DASA	Defense and Security Accelerator
DATDP	Defense Advanced Technology Development Program
DAU	Defense AI and Autonomy Unit
DCAR	Defense Centre for AI Research
DCC	Digital Capability Centre
DCS	Data-Centric Security
DDE	Digital Defense Ecosystem
DDITR	Directorate for Defense Investments and Technological Research
DDP	Directive on Defense Policy (Spain)
DDP	Department of Defense Production (India)
DDS	Defense Digital Service
DEFIC	Defense Information Cloud
DEMA	Danish Emergency Management Agency
DFKI	German Research Center for Artificial Intelligence
DGA	French General Directorate for Armament
DGA TA	French General Directorate for Armament expertise center on aeronautical techniques
DGAM	Directorate General for Armament and Materials
DGNUM	French MoD's Digital Directorate
DIA	Defense Innovation Agency
DIANA	Defense Innovation Accelerator for the North Atlantic
DIGENIN	Directorate General for Infrastructure
DINUM	French Interministerial Digital Department
DIO	Defense Innovation Organization
DIRISI	Joint Directorate of Infrastructure Networks and Information Systems
DIRO	Defensive Innovation and Research Organization
DIS	Defense Industry Strategy (Netherlands)

DIS	Digital and Intelligence Service (Singapore)
DITRI	Defense Industries Training and Research Institute
DIU	Defense Innovation Unit
DKIM	Directorate of Knowledge and Information Management
DM	Deputy Minister
DMAé	Directorate of Aeronautical Maintenance
DMG	Defense Management Group
DND	Department of National Defense (Canada)
DND	Directive on National Defense (Spain)
DoD	Department of Defense
DOTC	Digital Ops-Tech Centre
DOTLMPFI	Doctrine, Organization, Training, Material, Leadership/ Education, Personnel, Facilities, Interoperability
DPG	Defense Policy Group
DPI	Digital Public Infrastructure
DPO	Defense Policy Office
DRDC	Defense Research and Development Canada
DRDO	Defense Research & Development Organization
DRM	Directorate of Military Intelligence
DSCE	Data Science Centre of Excellence
DSO Labs	Defense Science Organization Labs
DSTA	Defense Science and Technology Agency
DSTG	Defense Science and Technology Group
Dstl	Defense Science and Technology Laboratory
DTC	Defense Technology Community
DTCO	Defense Technology Collaboration Office
DTDM	Defense Technology Development Mechanism
DTEP	Defense Technology Exploration Program
DTG	Defense Tech Group
dTHOR	Digital Ship Structural Health Monitoring
DTIB	Defense Industrial and Technology Base
DTO	Digital Transformation Office
DTU	Technical University of Denmark
DWP	Defense White Paper
DYSL	DRDO Young Scientist Laboratories
E-NASCOS	Naval Collaborate Surveillance
ECG	AI-based Electrocardiogram Analysis Platform
ECM	Electronic Countermeasures
EDA	European Defense Agency
EDAM	Center for Economics and Foreign Policy Studies
EDF	European Defense Fund
EDF	Estonian Defense Forces
EDIDP	European Defense Industrial Development Program
EDINAF	European Digital Naval Foundation
EDL	Estonian Defense League

EDT	Emerging and Disruptive Technologies
EEZ	Exclusive Economic Zone
eFP	enhanced Forward Presence
EIFO	Export and Investment Fund
ELINT	Electronic Intelligence
ELSA	Ethical, Legal, Societal Aspects
EM	Electromagnetic
EMSM	Electromagnetic Spectrum Management
ENISA	European Network and Information Security Agency
EOB	Electronic Order of Battle
EPC	European Patrol Corvette
ESA	European Space Agency
ESDC	European Security and Defense College
ESM	Electronic Support Measures
ESTDIV	Estonian Division
ETID	Defense Technology and Innovation Strategy
ETRI	Electronics & Telecommunications Research Institute
EU	European Union
EU-GUARDIAN	European frameworks and proofs-of-concept for the intelligent automation of cyber defense incident management
EUCINF	Cyber and Information Warfare Toolbox
EW	Electronic Warfare
FAIA	Finland's Artificial Intelligence Accelerator
FaRADAI	Frugal and Robust AI for Defence Advanced Technology
FCAI	Finnish Centre for Artificial Intelligence
FCAS	Future Combat Air System
FDF	Finnish Defence Forces
FID	Fonds Innovation Défense
FIMI	Foreign Influence Operations
FKIE	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (Fraunhofer Institute for Communication, Information Processing and Ergonomics)
FOI	Swedish Defense Research Agency
FOMO	Fear of Missing Out
FoT	Forskning och Teknikutveckling (Research and Technology Development)
FoU	Forskning och Utveckling (Research and Development)
FPI	Fond perspektivnykh issledovanii (Advanced Research Foundation)
FPV	First-Person View
FRACAS	Failure, Reporting, Analysis, and Corrective Action
FRP	Forces Reduction Program
FRSD	Recognition System Under Disguise
FRT	Facial Recognition Technology

FSB	Federal Security Service
FSTD	Future Systems & Technology Directorate
FTC	Flight Training Center
FY	Fiscal Year
GAO	General Accountability Office
GCAP	Global Combat Air Program
GCHQ	Government Communications Headquarters
GCV	Ground Combat Vehicle
GDDIA	General Directorate for Defense Investments and Armaments
GDNDPIR	General Directorate of National Defense Policy and International Relations
GDP	Gross Domestic Product
GHQ	General Headquarters of the Allied Forces
GIS	Geographic Information Systems
GIUK	Greenland, Iceland, United Kingdom
GNSS	Global Navigation Satellite Systems
GÖRÜ	Identification and Classification of Radar-Identified Surface Targets Project
GPDPO	Italian Army General Plans Department Plans Office
GPS	Global Positioning System
GRSE	Garden Reach Shipbuilders and Engineers
GSAF	Islamic Republic's General Staff of the Armed Forces
GUIR	Main Directorate of Innovative Development
HAL	Hindustan Aeronautics Ltd.
HAMLE	AI Commander Assistant Developing Course of Action Project
HARMSPRO	Harbor and Maritime Surveillance & Protection
HASAT	Image Analysis and Automatic Target Recognition System Project
HEU	Harbin Engineering University
HIMARS	High Mobility Artillery Rocket System
HMT	Human-Machine Teaming
HPC	High-Performance Computing
HQ	Headquarters
IADS	Integrated Air Defense System
IAF	Indian Air Force
IAI	Israel Aerospace Industries
IC	Intelligence Community
ICE	Information, Communication, Electronics
ICEF	Information Communication Electronic Force
iCET	U.S.-India initiative on Critical and Emerging Technology
ICT	Information and Communications Technology
IDEA	Innovation, Digitalization, Empowerment, and Agility
IDEaS	Innovation for Defense Excellence and Security
iDEX	Innovations for Defense Excellence
IDF	Israeli Defense Forces

IDSS	Intelligent Decision Support System
IEC	International Electrotechnical Commission
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
IFC	Intelligence Fusion Cell
IFCS	Intelligent Fire Control System
IFF	Identification Friend or Foe
IFV	Infantry Fighting Vehicle
IHL	International Humanitarian Law
IHU	Imam Hossein University
IKUMUT	Imam Khamenei University of Marine University and Technology
IM	Information Management
IMINT	Image Intelligence
IMOD	Israel Ministry of Defense
IMOD DDR&D	Israel Ministry of Defense Directorate of Defense Research & Development
iMUGS	Integrated Modular Unmanned Ground Systems
INRIA	National Institute for Research in Digital Science and Technology
IntSen2	Proactive automatic imagery intelligence powered by artificial intelligence exploiting European space assets
IoBT	Internet of Battlefield Things
IoT	Internet of Things
IR	Infrared
IRCC	Immigration, Refugees and Citizenship Canada
IRGC	Islamic Revolutionary Guard Corps
IRPO	Industry & Resources Policy Office
IRSA	Integrated Remote Sensing in the Arctic
ISIS	Islamic State of Iraq and Syria
ISO	International Organization for Standardization
ISR	Intelligence, Surveillance, Reconnaissance
ISTAR	Intelligence, surveillance, target acquisition and reconnaissance
IT	Information Technology
IWI	Israel Weapon Industries
J3MS	Joint Maritime Multimission System
JABMS	Joint Air Battle Management System
JADC2	Joint All-Domain Command and Control
JAIC	Joint Artificial Intelligence Center
JASSM-ER	Joint Air-to-Surface Standoff Missile-Extended Range
JCOP	Joint Common Operational Picture
JCS	Joint Chief of Staff
JDAM	Joint Direct Attack Munition
JDCD	Joint Digital and C4 Department

JEF	Joint Expeditionary Force
JPY	Japanese Yen
JSM	Joint Strike Missile
KERKES	Global Positioning System Independent Autonomous Navigation System Project
KETAK	Hellenic Center for Defense Research and Innovation Development
KIDA	Korea Institute for Defense Analysis
KIDET	Korea Institute of Defense Technology
KMT	Nationalist Kuomintang
KOIOS	Knowledge Extraction, Machine Learning and other AI approaches for secure, robust, frugal, resilient and explainable solutions in Defence Applications
KOLT	Kaitseväe olukorra ja lahinguteadlikkuse süsteem (Defence Forces Situational and Combat Awareness System)
KRW	Korean Won
LATACC	Collaborative Combat for Land Forces
LAUV	Light Autonomous Underwater Vehicle
LAWS	Lethal Autonomous Weapon Systems
LLM	Large Language Models
LM	Loitering Munition
LTC	Lieutenant Colonel
M&A	Mergers and Acquisitions
M&S	Modeling and Simulation
MANPADS	Man-Portable Air-Defense Systems
MARIN	Maritime Research Institute Netherlands
MAVs	Micro Air Vehicles
MCF	Military-Civil Fusion
MCM	Mine-Countermeasures
MDO	Multi-Domain Operations
MDPW	Multi-Domain Precision Warfare
MeitY	Ministry of Electronics and Information Technology
MFA	Ministry of Foreign Affairs
MG	Major General
MGCS	Main Ground Combat System
MGF-GenAI	Model AI Governance Framework for Generative AI
MIC	Ministry of Internal Affairs and Communications
MICI	Ministry of Science and Innovation
MIIT	Ministry of Industry and Information Technology
MINCOTUR	Ministry of Industry, Trade and Tourism
MINDEF	Ministry of Defense
MINDS	Mobilizing Insights in Defense and Security
MINHAP	Ministry of Finance and Public Administrations
MINT	Mathematics, Informatics, Natural Science, and Technology
MITA	Military Internet of Things für taktische Aufklärung

ML	Machine Learning
MNC	Multinational Corporation
MND	Korean Ministry of National Defense | Taiwanese Ministry of National Defense
MoD	Ministry of Defense
MoD	Ministry of National Defense (Greece)
MoU	Memorandum of Understanding
MRO	Maintenance, Repair, and Overhaul
MSD	Mine Sweeping Drone
MSIT	Ministry of Science and Information and Communications Technology
MTTR	Mean Time Between Repairs
MUM-CS	Complex Manned-Unmanned Combat System
MUM-T	Manned-Unmanned Teaming
MUT	Malek Ashtar University of Technology
NAIS	National Artificial Intelligence Strategy
NATO	North Atlantic Treaty Organization
NCO	Non-Commissioned officers
NCSIST	National Chungshan Institute of Science and Technology
NDA	National Defense Academy (Estonia)
NDA	National Armaments Directorate
NDAA	National Defense Authorization Act
NDAIC	National Defense AI Center
NDIDF	National Defense Industry Development Foundation
NDPG	National Defense Program Guidelines
NDR	National Defense Review
NDU	National Defense University
NEC	Network Enabled Capabilities
NFC	National Defense Technology Center
NGWS	Next Generation Weapon System
NIA	National Information Society Agency
NICT	Institute of Information and Communications Technology
NIDV	Netherlands Industries for Defense and Security
NIF	NATO Innovation Fund
NL AIC	Netherlands AI Coalition
NLAW	Next Generation Light Anti-Tank Weapon
NLDA	Netherlands Defense Academy
NLOS	Non-line of sight
NLP	Natural Language Processing
NLR	Royal Netherlands Aerospace Centre
NLTIB	Dutch Defense Technological and Industrial Base
NMI	National Mission Initiatives
NPDO	National Passive Defense Organization
NPT	Non-Proliferation Treaty
NPU	Northwest Polytechnic University

NS	National Service
NSA	National Security Agency
NSC	National Security Council
NSCAI	National Security Commission on Artificial Intelligence
NSCS	National Security Council Secretariat
NSDC	Naval Ship Development Center
NSonAI	National Strategy on Artificial Intelligence
NSS	National Security Strategy
NSSTC	National Security Science and Technology Centre
NWA	Dutch Research Agenda
NWCC	NATO Warfighting Capstone Concept
NWO	Dutch Science Organization
OA/OR	Operational Analysis/Operations Research
OCCV	Optionally Crewed Combat Vehicles
ODC	Overall Defense Concept
ONR	Office of Naval Research
OODA	Orient, Observe, Decide, Act
OPFOR	Opposing Forces
ORDC	Ordnance Readiness Development Center
OTAĞ	Odak Teknoloji Ağı (Focus Technology Report)
OTAs	Other transaction authorities
OTI	Operational Training Infrastructure
OUSD(R&D)	Office of the Under Secretary of Defense for Research and Engineering
PAD	Project Approval Directive
PEGEL	Social Media Analysis Performance Development Project
PEICTI	National Plans of Scientific, Technical and Innovation Research
PESCO	Permanent Structured Cooperation
PIA	Investment for the Future Program
PLA	People's Liberation Army
PMCs	Private Military Contractors
PME	Professional Military Education
PRISM	Proactive Real-time Intelligence and Surveillance Monitoring
QDR	Quadrennial Defense Review
R&D	Research and Development
RAAF	Royal Australian Air Force
RADM	Rear Admiral
RAF	Royal Air Force
RAI	Responsible Artificial Intelligence
RAISE	Responsible AI for Social Empowerment
RAN	Royal Australian Navy
RAS	Robotic and Autonomous Systems
RCAF	Royal Canadian Air Force
RCN	Royal Canadian Navy
RCO	Rapid Capabilities Office

RD&I	Research, Development, and Innovation
RDI	Research, Development, and Innovation
RDT&E	Research, Development, Technology, and Experimentation
REAIM	Responsible Use of Artificial Intelligence in the Military Domain
REPMUS	Robotic Experimentation and Prototyping Exercise by Maritime Uncrewed Systems
RICO	Robotic and Autonomous Systems Implementation and Coordination Office
RIKEN	National Institute of Physical and Chemical Research
RM	Royal Marines
RN	Royal Navy
RNLM	Royal Netherlands Marechaussee
ROCC	Regional Operation Control Center
ROK	Republic of Korea
RPA	Robotic Process Automation (Denmark)
RPA	Remotely Piloted Aerial Vehicles
RPAS	Remotely Piloted Air Systems
RSAF	Republic of Singapore Air Force
RSSJO	Research and Self-Sufficiency Jihad Organization
RTO	Research and Technology Organization
RWMTC	Rotary Wing Mission Training Center
S&I	Strategy and Implementation
S&T	Science and Technology
S3	Survival, Security, Stability
SaaS	Software as a Service
SAF	Spanish Armed Forces (Spain)
SAF	Singapore Armed Forces (Singapore)
SAGA	Savunma Sanayi Ar-Ge Geniş Alan (Defense Industry R&D Broad Topic Calls)
SAR	Search and Rescue
SAR	Synthetic Aperture Radar
SAS	Synthetic Aperture Sonar
SAYZEK	Savunma Sanayii Yapay Zeka Yetenek Kümelenmesi (Artificial Intelligence Talent Cluster of Defence Industry)
SBIR	Small Business Innovation Research
SCAF/FCAS	Future Combat Air System
SCCOA	Command and Control System for Aerospace Operations
SCCR	Supreme Council of the Cultural Revolution
SCP	Strategic Computing Program
SDB	Small Diameter Bomb
SDF	Self-Defense Forces
SDG PLATIN	Sub-Directorate General for Planning, Technology and Innovation
SDN	Software-Defined Networking
SEAD	Suppression of Enemy Air Defense

SEKPY	Hellenic Manufacturers of Defense Material Association
SFG	Strategy and Futures Group
SGD	Directorate of the Secretariat General
SGPI	General Secretary for Investment
SIPRI	Stockholm International Peace Research Institute
SKIA	Strategic Knowledge and Innovation Agenda
SLOCs	Sea Lines of Communication
SME	Small and Medium-Sized Enterprise
SOE	State-Owned Enterprise
SOF	Special Operations Forces
SOIC	Ship and Ocean Industries R&D Center
SPNET	Security-Policy Nexus of Emerging Technology
SSB	Savunma Sanayii Başkanlığı (Defence Industry Agency)
SSE	Strong, Secure, Engaged (2017 Canadian Defence Policy Paper)
SSF	Strategic Support Force
STANAG	Standardization Agreement
STaR	Science, Technology and Research
STEM	Science, Technology, Engineering, and Mathematics
STTR	Small Business Technology Transfer Programs
SwAF	Swedish Armed Forces
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TAF	Taiwan Air Force
TAIIA	"Traitement et Analyse d'Images par Intelligence Artificielle" or Image Processing and Analysis by Artificial Intelligence
TAS	Trusted Autonomous Systems
TD	Total Defense
TEDBF	Twin Engine Deck Based Fighter
TEV&V	Testing, Evaluation, Validation & Verification
TNO	Netherlands Organisation for Applied Scientific Research
ToT	Transfer of Technology
TRAI	Turkish AI Initiative
TRL	Technology Readiness Level
TSK	Türk Silahlı Kuvvetleri (Turkish Armed Forces)
TSPO	Technology Strategy & Policy Office
TTP	Tactics, Techniques, and Procedures
TUYGUN	Advanced Imagining Technologies Project
TWD	Taiwan Dollar
UAS	Uncrewed Aerial System
UAV	Uncrewed (or Uninhabited) Air Vehicle
UDAAN	Unit for Digitisation, Automation, Artificial Intelligence and Application Networking
UK	United Kingdom
UKRI	UK Research and Innovation
UMVs	Uncrewed Marine Vehicles
UOR	Urgent Operational Requirement

USAF	US Air Force
USIAI	U.S.-India Artificial Intelligence Initiative
USMC	United States Marine Corps
USV	Uncrewed Surface Vehicle
UUV	Uncrewed Underwater Vehicle
UVs	Unmanned Vehicles
UXV	Uncrewed Vehicle
VACS	Voice Activated Command System
VDE	German Association for Electrical, Electronic, and Information Technologies
VMS	Vehicle Management System
VR	Virtual Reality
VSHORAD	Very Short-Range Air Defense
VTOL	Vertical Take Off and Landing
WASP	Wallenberg AI, Autonomous Systems, and Software Program
WIN	Warfare Innovation Navy
WVR	Within Visual Range
WWII	World War Two
XLUUV	Extra-Large Uninhabited Underwater Vehicles
YETEN	Defense Industry Capability Inventory
μE	Microsystems Exploration

The Very Long Game of Defense AI Adoption: Introduction

Heiko Borchert

> *I don't need this "AI nonsense."* (Probasco 2023)
> *Adopting processes that exploit AI-enabled autonomy across the battle network is the path to achieving a higher relative system operating tempo than US competitors.* (Work 2020)

What is France's, Germany's, or Russia's approach to defense artificial intelligence (AI)? How does India or Iran think about defense AI? What are the defense AI development priorities of the United States, Israel, South Korea, or Singapore? Is the defense AI approach of authoritarian countries distinctively different from the practice in democratic countries? How do ongoing conflicts shape the defense AI trajectory?

Analysts interested in answering these questions fight a steep uphill battle as information is scattered across a rapidly growing body of literature looking at the way AI is likely to shape military thinking and warfighting practice. To solve this problem and advance the international understanding of how nations approach and implement defense AI, *The Very Long Game* provides the first collective in-depth analysis of 25 nations that is both comprehensive and comparative, as well as easily accessible. Rather than speculating about how AI could contribute to military power and change warfighting, this book focuses on what nations do now to use defense AI today and in the future. This approach, the current chapter will show, tames hyperbolic imaginaries that range from ascribing superhuman powers to defense AI to portraying the technology as the harbinger of dystopian war scenarios.

By focusing on the current state of play related to defense AI, this volume sits at the intersection of strategic affairs, military innovation, organizational change, emerging technologies, and future force development trajectories. It brings together a diverse set of authors and sheds light on cross-regional commonalities and regional specifics that need to be considered when reflecting upon the interplay between military power and technology. The selected case studies look beyond Canada,

H. Borchert (✉)
Defense AI Observatory, Helmut Schmidt University, Hamburg, Germany
e-mail: hb@defenseai.eu

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_1

Denmark, Estonia, Finland, France, Germany, Greece, Italy, the Netherlands, Spain, Sweden, Turkey, the United Kingdom and the United States as member states of the European Union (EU) and/or the North Atlantic Treaty Organization (NATO) and also cover Australia, China, India, Iran, Israel, Japan, South Korea, Russia, Singapore, Taiwan, and Ukraine to capture the dynamics in different strategic theaters. These 25 country studies look at well-established as well as ambitious new defense exporters to get a better understanding of how defense AI could influence future defense export prospects and provide inroads for newcomers to unlock mature markets. This volume also considers military thought leaders and countries that aspire to become role models for other nations, thus tracking the defense angle of an increasingly "multiplex" world order characterized by the absence of global hegemony through any single nation, broader patterns of interdependence, and intellectual and political diversity sketching out different ways to ensure peace and stability (Acharya et al. 2023: 2341). Furthermore, this volume presents case studies on the use of defense AI in war zones as well as the strategically contested regions of North-East Asia, the Eastern Mediterranean and wider Arab Gulf.

In all the countries selected for this volume, AI and other emerging technologies rank high on the agenda. The assumptions underpinning these agendas are diverse, as the two introductory quotations make clear. In general, there is a growing belief that AI is likely to change future warfare and could also tip the strategic balance. Warfighters, as the Ukrainian voice cited in Probasco's opening quotation, may beg to disagree. They have a point. Despite the hype around emerging technologies, technology alone is insufficient to modify the way armed forces operate and drive change. Rather, technology needs to be embedded in the broader cultural, conceptual, and organizational context.

This understanding is in line with a growing body of literature on military innovation and the role of defense AI. Focusing on a selection of publications that appeared within the last three to five years, three groups can be identified. First, the number of texts making general assumptions about the military impact of defense AI is growing quickly. This group includes books like *Army of None* and *Four Battlegrounds* by Paul Scharre (Scharre 2019; Scharre 2023), Johnson's analysis of the interplay between defense AI, future wars, and strategic stability (Johnson 2021), and Kenneth Payne's *I, Warbot* (Payne 2021). Reflections on the possible impact of AI on international stability and the role of arms control in preventing an AI "arms race" also belong to this group (Cummings 2018; Diehl and Lambach 2022; Horowitz 2018; Horowitz et al. 2018; Horowitz and Scharre 2021; Scharre and Lamberth 2022; Scharre 2021). While primarily interested in the interplay between defense AI and strategic affairs, most of these texts only look at a limited number of countries and combine examples of the current use of defense AI with speculations about its future impact. A combination of AI with uncrewed systems as well as ethical and regulatory considerations is commonplace as well.

In addition to these broad treatises, a second group of authors tries to understand how AI might affect military power with a focus on specific military domains and what factors enable or block the diffusion of AI and information-driven ideas of change. This body of literature includes, for example, Sam Tangredi's and George V. Galdorisi's book

on AI and naval warfare (Tangredi and Galdorisi 2021) and the analysis of defense innovation in the information age by Jensen et al. (2022). These texts focus on understanding AI's added value for operators and/or theoretical advancements. Along these lines, Lin-Greenberg (Lin-Greenberg 2020) scrutinize the impact of AI on coalition decision-making, while Lindsay (Lindsay 2023/2024) sheds light on the institutional context for AI-enhanced military innovation. Analyses of the risks posed by defense AI form a prominent sub-group inside this specialized impact literature, for example, with papers focusing on countering intelligence algorithms (Phillips and Pohl 2021) or the use of AI in wargames (Barzhaskha 2023). This literature is also linked to the prominent discourse on the ethics of defense AI (CIGI Undated; Hofstetter and Verbovzsky 2023; Galliott and Scholz 2020; Stanley-Lockman 2021; Rowe 2022).

The third group of publications takes a more comparative approach by focusing on the specific approaches undertaken in different countries. *Artificial Intelligence, China, Russia, and the Global Order,* edited by Nicholas D. Wright (Wright 2019), for example, covers different aspects of defense AI in the two countries mentioned but does not adopt a comprehensive analytical approach to provide cross country assessments. By contrast, *The AI Wave in Defense Innovation. Assessing Military Artificial Intelligence, Strategic Capabilities and Trajectories,* edited by Raska and Bitzinger (Raska and Bitzinger 2023), presents case studies on defense AI in the US, China, Russia, Japan, and South Korea as well as Australia. Moreover, one chapter looks at the use of military AI in Europe with an EU/NATO focus.

As this short overview illustrates, most of the literature is focusing on broad questions while somewhat pushing aside the more complex and protracted issues of how countries specifically think about defense AI, how they prepare for its adoption, and how they develop existing concepts, structures, processes and develop the respective capabilities (Goldfarb and Lindsay 2021/2022: 11). This is the gap that this volume is seeking to address. Therefore, the editors started in 2022 to commission the 25 case studies brought together in updated and abridged chapters for this volume.[1]

Together with other technologies like robotics and computing, AI is considered an emerging technology likely to prompt military innovation. As argued elsewhere (Borchert et al. 2021: 13–17), military innovation is a popular but controversial concept as it is challenging to gauge what constitutes innovation. For military innovation to occur, armed forces need to master the advent of new technology in tandem with conceptual, cultural, and organizational transformation. That's why the case studies understand defense AI as a socio-technological phenomenon that requires a broad analytical framework. Each chapter follows the same structure—inspired by the DOTLMPFI[2] lines of effort—to discuss how nations:

- think about defense AI to illustrate how existing military concepts define and shape the use of defense AI;

[1] The original studies are available at https://defenseai.eu/. Accessed 15 February 2024.

[2] Doctrine, Organization, Training, Material, Leadership/Education, Personnel, Facilities, Interoperability.

- develop defense AI to outline existing defense research and development (R&D) priorities related to AI, highlight important research projects and priorities, and portray the national defense AI ecosystem;
- organize defense AI with a focus on specific structures and processes that have been put in place to advance organizational adaption of defense AI;
- fund defense AI to highlight spending priorities;
- field and operate defense AI to give an overview to what extent AI is already used to support existing military missions;
- train for defense AI to analyze how armed forces prepare for a future in which they cooperate with cognitive machine intelligence.

In so doing, each chapter looks at the interplay of four critical elements relevant for capability development and force adaption: First, there are ideas, concepts, and policies that underpin military power. As the case studies highlight, most nations understand defense AI as a means to improve existing practice, rather than to embark on exploring new ways of applying military power. This serves as a cautionary tale and deflates much of the rhetoric about the "disruptive" power of defense AI.

Second, novel ideas need champions to diffuse them within and across hierarchies. In addition to intra- and interservice rivalries that the military innovation literature has identified as stimuli for change (Mansoor and Murray 2019: 11–14), or the idea that software-driven modernization can enable military powers to leapfrog on capability growth (Soare 2023), the following case studies identify incumbent and emerging new defense companies as important technology bridges to induce change. This, however, raises thorny questions related to controlling the exports of companies that serve military and commercial clients, the relationship between sovereign and private algorithm development, and the acceptance of "black boxes" when defense AI solutions are embedded in foreign weapons supplies.

The rise of the "new kids on the defense block" is closely related to each country's institutional setup as the third important aspect to consider. Institutional maturity and complexity can create market barriers for new defense suppliers and cause organizational pathologies that render the successful application of defense AI almost impossible, as the case study on defense AI in Canada makes clear. Most nations play around with new organizational elements and enhance cross-institutional coordination for defense AI. As the case studies show, military organizational change in the US receives a lot of attention as many nations seek to emulate what the US Department of Defense is doing.

Finally, change will never materialize without resources. As argued below, adapting the business models of digital platform providers that are awash in data that consumers share freely in return for products and services, is of limited use for defense AI. The consumer data reality has nothing in common with the defense data reality. Adhering to data-centricity, although popular among all armed forces discussed in this volume, is likely to slow down, rather than boost the military's use of AI.

Against this background, the remainder of this chapter will first provide a quick introduction into the technicalities of AI. A summary of the main findings of all case

studies follows second. Rather than providing country-specific abstracts, I use the six lines of effort discussed above to advance a cross-country understanding of who is doing what, why and how concerning defense AI. Third, the chapter will interpret these findings and suggest that some of them confirm existing expectations, whereas others are surprising and tell uncomfortable truths. Concluding remarks related to contemporary imaginaries underpinning the defense AI discourse round off the chapter.

1 Defense AI: What's in a Word

AI is popular, but challenging as there is no unifying definition. In one way or another most definitions used by the armed forces analyzed in this volume coalesce around the notion—put forward in the AI strategy of the US Department of Defense (Department of Defense 2018: 4)—that AI "refers to the ability of machines to perform tasks that normally require human intelligence." This definition is straightforward but can cause controversy as it challenges the notion—underpinning the thinking on defense AI prevalent in almost all nations analyzed in this volume—that humans must always control machine intelligence and action. According to Brandlhuber (Brandlhuber 2021: 6), a less contentious understanding of AI would thus emphasize the role of hardware and software systems in implementing reasoning mechanisms without the need to pre-program the solutions that these systems are expected to accomplish.

In so doing, AI uses and depends on different methods with much of the literature focusing on machine learning (ML). ML posits that "knowledge is learned from data" and that the respective algorithms run "on a training dataset and produce an AI model" (Allen 2020: 3). This notion has become very popular due to the prevalence of digital commercial business models that seek to leverage (consumer) data as well as the rapid improvement of computing resources to handle large volumes of data. The ML focus, however, has created a narrow perspective on AI.

The problem stems from overemphasizing the role of data. Digital business models for consumer markets constitute the implicit reference point. These are data-centric because users provide their data in exchange for digital products and services. In addition, digital companies want to work "model-free" as AI systems should replace and scale the steps that were previously developed using specialist expertise and engineering skills. To this end, ML systems should process large amounts of data to reproduce a desired behavioral pattern.

This data-centric logic has also captured military thinking. All the countries surveyed describe data as their most important strategic asset and are gearing data strategies towards exploiting this "data treasure," also by investing in powerful hardware. But armed forces do not operate in a consumer environment with abundant data;

rather they struggle with data scarcity.[3] Data-centric approaches are resource-intensive and require personnel, computing power, energy, infrastructure, bandwidth and recording time, which become even scarcer in the event of war (Chahal et al. 2020: 10–13; Michel 2023: 16–21). Paradoxically, they are also past-oriented, i.e., armed forces can only evaluate what has been collected. While collected data can describe the dynamics of the past, it cannot describe dynamic operating principles of the physical environment in which armed forces operate (Borchert et al. 2023a: 47).

In contrast to this prominent view, military users should be cognizant of the fact that AI may be a general-purpose technology (Horowitz 2018: 39–41; Scharre 2023: 3), but it also is a "bag full of methods" (Hofstetter 2014: 136–142). Some AI methods are better suited than others to address different military tasks. Being precise about which method best suits what task is important to set the goals for defense AI to achieve. Four general approaches are important to distinguish (Brandlhuber 2021: 14; Allen 2020: 4):

- Unsupervised learning, which does not require labels for data used, is helpful for data analytics, anomaly detection or auto-coding.
- Supervised learning, which uses data labelled by human operators, is used for speech or image recognition, video analysis, auto translation, and to classify signals.
- Reinforcement learning, which allows for AI agents to generate their own data based on interacting with the relevant environment, in which they operate, is instrumental for optimal sequencing of actions over several iterations, hedging strategies to support risk management or strategic decision-making.
- Finally, cooperation and emergence result from AI agents that interact with their environment and are useful for dynamic resource management (e.g., to improve sensor capabilities), optimal resource sharing (e.g., optimal allocation of sensors and effectors to engage targets), or efficient routing.

Against this background, the US Defense Advanced Research Projects Agency (DARPA) has proposed differentiating three waves of AI (DARPA Undated; Borchert et al. 2023b: 27):

- First wave AI leverages handcrafted knowledge. Human experts construct expert systems that capture the specialized knowledge of human experts in rules that systems can apply.
- Second wave AI focuses on correlational learning. Statistical and probabilistic methods are used to train neural networks to perform classification and prediction tasks.
- Third wave AI emphasizes contextual reasoning. Here, computing systems have full situational awareness, which means that these systems reason in context and understand the consequences of their action and actions undertaken by third parties like adversaries, for example.

[3] The US Department of Defense is said to collect around 22 terabytes of data per day (Mehta 2017), but Google handles around 20 Petabyte (or 20,000 terabytes) per day (Skill-Lync 2023).

The transition from second to third wave AI is essential to understand given the latter's ability to self-learn. First and second wave AI focus on extracting patterns from (big) data by using classification and regression. Third wave AI, in contrast, strives to develop solutions that learn how best to learn by using context-aware, complex, and multi-stage decision-making commensurate with the relevant operational environment, mission tasks, and overall rules of engagement. This is pivotal for defense AI, because reinforcement learning, which is important for ML, has yielded impressive performance results in ideal-type games with perfect information (Silver et al. 2017; Vinyals et al. 2019). Imperfect information and uncertainty, however, are typical for military operations. That's why third wave AI needs to address, for example, the fact that tactical military decisions occur along a decision sequence in which prior decisions are contingent for later decisions, non-decisions may significantly limit a commander's future freedom of action, and adversarial operations in the electromagnetic spectrum may jam or even neutralize sensors and thus hamper situational awareness and situational understanding. Third wave AI thus needs to be able to interpret this mission-relevant context to avoid prejudicing decisions to hamper mission success at later stages.

Markov-Decision-Processes constitute one mathematical approach relevant to tackle these challenges as they model decision-making in an environment, "which changes state randomly in response to action choices made by the decision maker" (Littman 2001). Additional methods include adversarial learning to advance the robustness of ML (Bai et al. 2021), transfer learning (Zhuang et al. 2019) to develop defense AI solutions that can be transposed from the defense metaverse—that digitally mimics key parameters of the battlefield (Borchert et al. 2023b)—into physical reality, as well as meta learning (Vettoruzzo et al. 2023) to enable decision-making policies to evolve commensurate with a non-stationary mission environment that changes over time. As a result, third wave AI addresses uncertainty by emphasizing emergence, not linearity or regularity, as the key principle and posits that formation, rather than formulation, matters for successful adaption (Mintzberg et al. 2005: 177; Popescu 2018). Essentially, emergence also emphasizes the "capacity to experiment" (Mintzberg et al. 2005: 189) to explore new avenues and exploit existing avenues at the same time (Reeves et al. 2013).

Distinguishing between three waves of AI is useful to consider what defense AI can accomplish. As Table 1 illustrates, the contribution of defense AI to implement the principles of war that describe how to use military power, becomes more significant the more military users envision employing third wave AI. So far, however, almost all nations portrayed in this volume focus on second wave AI that emphasizes the central role of data exchange via digital platforms. This "hub and spoke" logic works for benign environments, in which centralizing is efficient and provides scale. The military combat environment, however, is non-benign and requires AI solutions that operate under uncertainty. That's why successfully using defense AI on the battlefield will require armed forces to transition to decentralized, self-learning solutions that third wave AI empowers (Bousquet 2022: 210–211).

Table 1 Contribution of three waves of defense AI to the principles of war

		1st wave AI	2nd wave AI	3rd wave AI
	Core idea	Handcrafted knowledge	Correlational learning	Contextual reasoning
	Main goal	Efficiency	Efficiency and effectiveness	Emergence
Contribution to selected principles of war	*Concentration:* Concentration is not synonymous with the physical massing of forces for a decisive action, but concentration of effects created from a dispersed force.	Indirectly by data analytics	Directly by data analytics	Directly by self-learning
	Definition of objectives: Operations must be focused towards clearly defined and commonly understood objectives that contribute to attain the end state.	Technical objectives set and pre-programmed	Technical objectives defined by error function, tutorial guidelines and supported by data analytics	Tactical objectives directly addressed by objective/utility function (per design). System may learn to create sub-goals automatically
	Economy of effort: Concentration must be delivered economically and precisely, targeting the right objects in the right space at the right time with the appropriate resources.	No direct contribution	Directly by data analytics and operations research	Directly by self-learned tactics
	Flexibility: A flexible force is one that has the ability to be highly responsive to changing circumstances	No direct contribution	Indirectly by data analytics	Directly by self-organization and emergent coordination
	Initiative: To hold the initiative is the ability to set or dictate the terms of action throughout the operation.	No direct contribution	No direct contribution	Directly by self-learned tactics
	Security: Security limits vulnerability to hostile activities, threats and surprise. It is a shield that can help conserve fighting power and affords the initiative and freedom of action, when and where required, to achieve objectives.	No direct contribution	No direct contribution	Directly by decision policies that operate under electromagnetic emission control
	Surprise: Surprise, achieved through unexpected actions, achieves a cognitive effect—a feeling of relative confusion, or perhaps shock—that can undermine the adversary's cohesion and morale.	No direct contribution	Indirectly by data analytics, analysis of courses of action, and operations research	Directly by self-learned tactics and emergent coordination
	Sustainment: The ability to generate and re-generate, avoiding shortages and waste, maintains a commander's flexibility and freedom of action (…).	Directly by data analytics	Directly by data analytics	Directly by supporting planning in the (real-time) defense metaverse

Source: Author's Overview with NATO principles of war based on NATO 2022: 74–76.

2 Who Does What, Why, and How?

This section provides a comparative summary of the 25 case studies along the six lines of effort discussed above. Before moving on, a word of caution is needed. Although detailed, the case studies, which are based on open-source information and expert interviews, only provide a snapshot of the national defense AI endeavors in late 2023 and early 2024. Based on the case studies, the summary is selective. In addition, the summary also simplifies, for example, by equating a single project with a national focus on developing or deploying defense AI. This, in turn, might not always adequately describe the respective levels of maturity and could inflate the importance of individual projects or initiatives.

2.1 Thinking About Defense AI

The countries analyzed are not very specific about the concrete goals defense AI is meant to accomplish. Most descriptions remain generic referring to potential gains such as being able to analyze ever-growing datasets, sneak into the enemy's OODA loop (Orient, Observe, Decide, Act), or accelerate decision-making. Overall, most armed forces want to improve and optimize what they are doing today, rather than exploring how using defense AI might empower them to accomplish new tasks and missions. What may surprise at first sight, becomes less puzzling when looking at the underlying drivers shaping national defense AI perspectives.

2.1.1 Strategic Motives

Three strategic motives are at play (Table 2). The first group of nations has adopted a threat-based approach. In this case, one strategic challenger or a complex set of regional challenges has been identified, and defense AI is seen as a key solution. The textbook example are China and the United States, which see each other as prime challengers and focus on defense AI to contain the other. The same logic applies to Russia and to neighboring pairs of countries like Greece and Turkey, South Korea and Japan (vs. China and North Korea), as well as Ukraine and Russia. Israel and India also operate under this perspective, but with additional regional drivers shaping their view. India, for example, is also concerned that defense AI might empower other nations to dominate the country, which prompts New Delhi to invest in indigenous solutions. A similar logic is at play in Iran, which considers Israel, the United States, and their allies in the region as an existential threat shaping its approach to defense AI. Finally, Taiwan is a special case as all three strategic motives are at play with the threat from China as the key driver.

The second group of countries fears missing out (FOMO) or falling behind. This is a different threat-based perspective that emphasizes the competitive disadvantage

Table 2 Three strategic drivers of defense AI

Fear of missing out (FOMO)	AI as a capability multiplier	Threat-based thinking
DNK, FRA, GRE, ITA, TWN	AUS, CAN, DEU, DNK, ESP, EST, FIN, FRA, GBR, GRE, IRN, ISR, ITA, JPN, KOR, NLD, RUS, SGP, SWE, TUR, TWN, USA	CHN, GRE, IND, IRN, ISR, JPN, KOR, RUS, TWN, UKR, USA

Country Code: AUS Australia, CAN Canada, CHN China, DEU Germany, DNK Denmark, ESP Spain, EST Estonia, FIN Finland, FRA France, GBR United Kingdom, GRE Greece, IND India, IRN Iran, ISR Israel, ITA Italy, JPN Japan, KOR South Korea, NLD The Netherlands, RUS Russia, SGP Singapore, SWE Sweden, TUR Turkey, TWN Taiwan, UKR Ukraine, USA United States

that could result from the inability to embrace defense AI. This includes well-established defense exporters like France and Italy, transatlanticist Denmark, as well as Greece, whose armed forces went through several years of underfunding after the international financial crisis in 2008/2009. In Athens' case, the fear of missing out is also directly linked to the threats the country sees originating from Turkey.

Most of the countries belong to the third group, which takes a less pronounced position and interprets AI primarily as a capability multiplier. Members of the other two groups also share this perspective but drive defense AI development via threat or FOMO-based foci. Adherents of the capability multiplier perspective, by contrast, tend to have less well-defined development and deployment priorities as they put more emphasis on exploring various defense AI use cases.

2.1.2 Who Shapes Whom?

These strategic motives also play a role when asking if and to what extent others are shaping national defense AI perspectives. Partners, Table 3 illustrates, play a foundational role. Here, the United States remains the pivotal player, particularly for its allies in the Asia-Pacific region. European partners of the United States also look to other members of NATO and the EU for inspiration. In this context, inspiration implies that partners adjust their defense capstone documents within the context of US thinking, for example by emphasizing the role of AI in Multi-Domain Operations, mimic US organizational reforms, and emulate US defense systems concepts and architectures, like the Joint All-Domain Command and Control (JADC2) concept, to remain interoperable with the US. Emulation, however, also comes with risks. Taiwan's AI-pilot project—modelled after DARPA's Alpha Dogfight—illustrates these risks by proving to be "far-reaching but conceptually ill-informed," as the chapter notes.

Strategic challengers are as powerful as partners and allies in shaping defense AI perspectives. Again, the case studies on China and the United States highlight how closely both nations monitor each other's defense AI moves. In addition, the threat-based perspective discussed above also shapes the perspectives of those countries that feel existentially threatened by neighbors or a cocktail of different risks.

Table 3 Who shapes the thinking on defense AI?

Challengers shape thinking	Agnostic	Partners shape thinking
CHN: USA *USA:* CHN *Multiple:* IND (CHN, PAK), IRN (USA, ISR), ISR, RUS *Neighbor:* GRE (TUR), UKR (RUS)	EST, FRA, SWE	*USA:* AUS, CAN, DEU, DNK, FIN, GBR, JPN, KOR, TUR, TWN *Several:* EST (USA, UK, FRA, NATO), GRE (USA, ISR), ESP (NATO, EU), ITA (NATO, US), NLD (USA, NATO, EU), SGP

Interestingly, the match is not always perfect. While Greece's thinking on defense AI is motivated by the military and defense industrial challenges posed by Turkey, the latter is more and more replacing its traditional focus on the US by emphasizing its own foreign policy and indigenous defense industrial ambitions.

Between these two poles, only few countries remain. France traditionally emphasizes its role as a self-determined nuclear power and tries to chart its own course regarding defense AI. Sweden and Spain, by contrast, are a bit more difficult to locate. Spain's national security strategy talks about the China challenge, but it is not much of a strategic driver for its thinking on defense AI, which seems more influenced by initiatives driven from inside NATO and the EU. Sweden, traditionally very close the US, takes an agnostic perspective as its thinking is shaped by internal drivers like total defense and NATO.

2.1.3 Human or Tech-Centric Understanding

Whether countries adopt a human or a technology-centric approach to defense AI is important to understand the relationship between human operators and machines. The human-centric approach builds on the idea that AI is to complement, not replace human beings. By contrast, a technology-centric approach posits that AI shall facilitate and accelerate full technical autonomy and machine-machine interaction, as illustrated in the quotation by Bob Work, former US Deputy Secretary of Defense, at the beginning of this chapter.

Table 4 illustrates that most of the 25 nations adopt a human-centric approach, but with notable nuances. Estonia, for example, supports a human-centric approach but is not a "normative hawk" on regulation, as discussed below. South Korea belongs to this group as well but demographic aging and a dramatically shrinking personnel basis of the armed forces could become drivers for a more technology-centric view in the future. The US, for the time being, is also clearly human-centric but the most recent Replicator initiative announced by the Department of Defense envisions a future with swarms of uncrewed assets to overwhelm adversaries that is firmly anchored in the technology-centric perspective (Hicks 2023; Tucker 2024).

Already today, two countries edge towards the technology-centric approach. Turkey wants to leverage AI in tandem with the country's expertise on uncrewed assets to advance autonomous operations across domains. Turkish defense company

Table 4 Human or tech-centric understanding of defense AI

Tech-centric approach	Agnostic	Human-centric approach
UKR, TUR	DNK, EST, GRE, IRN, RUS, SWE	AUS, CAN, CHN, DEU, DNK, ESP, EST, FIN, FRA, GBR, IND, ISR, ITA, JPN, KOR, NLD, SGP, TUR, TWN, UKR, USA

Havelsan has been championing the "Digital Troops" concept that reflects this idea and is building a product portfolio around it. In addition, the country's defense engineers posit that it is more difficult to arrange for man-machine integration than to enable machine-machine interaction, which adds to the country's edge towards a technology-centric approach. Ukraine follows a similar idea borne out of the current war. Achieving machine autonomy with defense AI is one of the country's declared development priorities for the near future, also because the war shows that connectivity that provides one option for human operators to continue piloting uncrewed assets, is brittle in combat.

Finally, there are several nations that take an agnostic view, but across this group there are strong drivers that point towards the likelihood of a more technology-centric stance in the future. Denmark's need for wide area surveillance with uncrewed assets and defense AI could entice a more technology-centric approach. Estonia, Iran, Singapore, and Taiwan see the option to free up scarce manpower with the help of AI and uncrewed systems. Greece is still agnostic, but strategic rivalry with Turkey could tilt the balance depending on where Turkey is heading. Russia's position is moving between both poles, in particular regarding the interplay between defense AI and lethal autonomous weapon systems (LAWS). Finally, Sweden, like Denmark, sees a need for wide area surveillance, for which defense AI could augment uncrewed assets. In addition, the need to counter hypersonic weapons could prompt a more technology-centric stance with defense AI playing a prominent role in analyzing data related to this specific threat.

2.2 Developing Defense AI

Before addressing current defense AI development priorities in detail, it is worth asking which of the three waves of defense AI shapes national mindsets. As argued above, this differentiation serves as an indicator for defense AI applications that are aligned with the status quo (second wave AI) or illustrate potential "breakout" solutions (third wave AI).

The overwhelming majority of the countries (Table 5) follows a data-focused understanding of defense AI, whereas the United States is the only nation that has so far officially discussed and explored the military benefits of third wave AI thanks to dedicated programs managed by DARPA. Few countries hold an agnostic position. Estonia, Iran, and Spain are in the process of establishing defense AI practices and might still need to mature their respective thoughts and concepts. Turkey's

Table 5 Data or emergence-based defense AI development

Focus on data	Agnostic	Focus on emergence
AUS, CHN, DEU, DNK, FIN, FRA, GBR, GRE, IND, ISR, ITA, JPN, KOR, NLD, RUS, SGP, SWE, TWN, UKR, USA	CAN, EST, ESP, IRN, TUR	USA

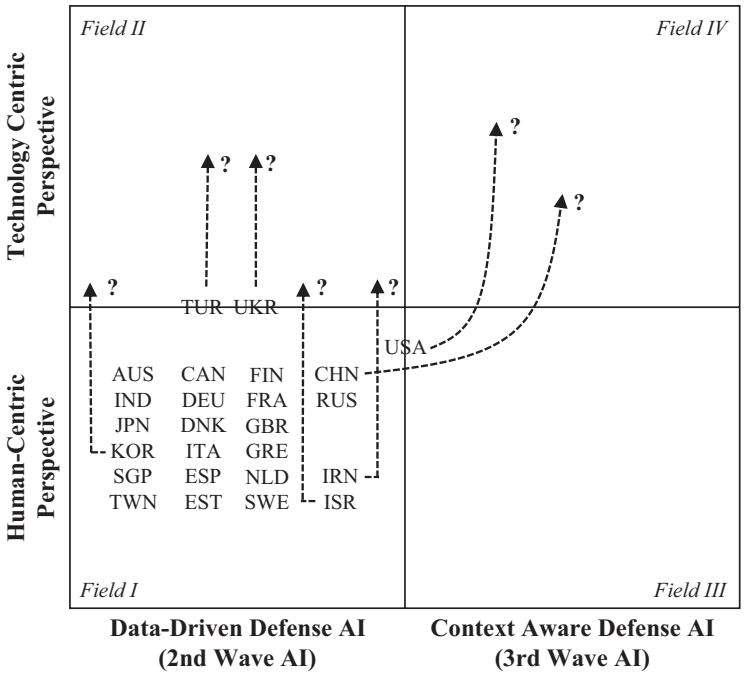


Fig. 1 Four paradigms to develop defense AI

development priorities indicate a weak tilt towards emergence in combination with uncrewed systems. Canada's approach to defense AI suffers from current organizational stovepipes.

Combining the data vs emergence perspective with technology and human-centric approaches to defense AI produces a most interesting 2x2 matrix depicted in Fig. 1. This chart clearly underlines that for the time being all 25 nations operate within the same data and human-centric paradigm. When challengers and incumbents operate along the same mindset, surprise will hardly manifest. But the matrix also clearly suggests that there are different breakout trajectories that could materialize in the near future:

- The United States is the most prominent candidate to embrace emergence for future operations, as the recent Replicator initiative illustrates. US concepts like JADC2 would also greatly benefit from a move towards decentralized and hori-

zontal, rather than vertical, command and control (C2) approaches, but current service preference seem to stand in the way of fully leveraging this idea.
- Once the United States move towards emergence, China is likely to follow suit as it wants to play on par. Whether China would move towards emergence via emphasizing machine autonomy before embracing context-aware defense AI solutions is hard to say right now. The country's most recent experiments with large language models (LLM) to support swarm C2 could be seen as an early indicator towards this direction. However, if an LLM-based swarm of autonomous systems would withstand battlefield realities is doubtful as its ability to generate forward-looking tactics that are difficult for adversaries to mimic is likely limited.
- Ukraine, which recently decided to set up a new unmanned systems branch (President of Ukraine 2024), and Israel also constitute two obvious candidates for change as both see value in advancing machine autonomy with AI given current battlefield realities. The same is true for Turkey, which is leveraging defense AI in tandem with the country's broad portfolio of uncrewed systems across all domains.
- Finally, Iran and South Korea both qualify as potential adopters of a more pronounced machine autonomy paradigm. Both see value in compensating demographic aging and shrinking armed forces with more technical autonomy. And Iran, given the erroneous downing of Ukrainian International Airline flight 572 in 2020 by a ground-based air defense battery, considers more autonomy to avoid human errors.

Against this background, Table 6 summarizes today's key defense AI development use cases across all case studies. The table shows interesting priority clusters. First, a regional perspective suggests that defense AI priorities play a prominent role in EU and NATO countries. This may be related to the technological maturity of the armed forces as well as current and most recent wars in Europe and adjacent regions. Defense AI development priorities are less pronounced across the Greater Middle East. China, Russia, and Turkey have ambitious defense export plans for the region and could thus set the pace regarding diffusing defense AI across the respective countries. Israel's opportunities to shape regional defense AI capabilities, however, seem much more muted as a fallout of the Gaza war that questions the efforts to normalize relations with the country, particularly among the Gulf states. Apart from Australia and China, defense AI development priorities remain nascent across the Asia-Pacific countries analyzed. The fact that Japan, South Korea, Taiwan, and Singapore maintain close relations with the United States is important as these nations will want to develop their defense AI capabilities in tandem with the US and reach out to US defense AI suppliers for help, as developments in Australia illustrate.

Second, current defense AI development priorities underpin several capability categories:

- The combination of AI with uncrewed systems is the most prevalent area of application. Here, quality differences stem from the portfolio of uncrewed assets maintained today (domain specific or multi-domain preferences) and the tasks these systems are expected to perform. Most often, these tasks focus on intelligence, surveillance, and reconnaissance (ISR) either to improve common operational pictures (situational awareness and situational understanding) or support targeting and strike. In this regard, manned-unmanned teaming is relevant as well.

Table 6 International defense AI development use cases

Use case	USA	CAN	GBR	SWE	FIN	EST	DNK	DEU	NLD	FRA	ESP	ITA	GRE	TUR	RUS	UKR	ISR	IRN	IND	CHN	JPN	KOR	TWN	SGP	AUS
Air defense			■				■	■		■					■			■					■	■	
Battle/combat management																■								■	
Command and control	■		■		■	■		■	■	■		■			■		■	■		■	■	■		■	
Common operational picture			■		■	■	■	■		■	■		■		■					■			■	■	■
Cyber/CNO	■	■			■	■				■			■		■	■	■	■		■	■		■	■	
Data analytics/ management		■	■	■			■	■	■		■		■	■	■	■		■	■				■	■	
Decision and planning support		■			■				■	■		■		■	■				■		■	■		■	■
Disaster relief	■																							■	
Electronic warfare (EMSO)					■			■	■					■	■	■		■		■					
Encryption			■			■							■												
Enterprise services			■					■	■	■									■				■	■	■
Fire support (e.g., artillery)						■								■	■									■	
Force protection (incl. CBRN)					■					■	■	■												■	■
Intelligence, surveillance, reconnaissance	■		■	■	■	■		■	■	■		■	■		■		■	■	■	■	■	■	■	■	■
Influence/ information operations			■							■					■	■				■				■	■
IOD/MCM/mine clearance/UXO			■							■		■	■		■	■									

(continued)

Table 6 (continued)

Use case	USA	CAN	GBR	SWE	FIN	EST	DNK	DEU	NLD	FRA	ESP	ITA	GRE	TUR	RUS	UKR	ISR	IRN	IND	CHN	JPN	KOR	TWN	SGP	AUS
Manned-unmanned teaming			■	■	■	■		■	■	■		■		■					■	■		■		■	■
Medical services			■							■												■	■		
(Mission) planning			■			■	■	■															■	■	
Modelling, simulation, red teaming, Wargaming			■					■					■	■	■	■			■	■			■	■	
Precision effects (e.g., missiles, torpedoes)								■		■	■				■			■							
Predictive maintenance, logistics, MRO	■		■	■	■			■	■	■	■		■		■	■	■			■		■	■	■	■
Safety									■																
Space and space-based assets			■					■							■										
Swarming			■		■			■		■				■	■	■			■	■					
Training (incl. Simulation-based training)			■					■				■	■	■	■				■	■	■	■	■	■	
Tactics development								■																	
Target detection, classification, identification			■					■		■	■	■		■	■	■			■	■	■		■	■	■
Uncrewed systems	■	■	■	■	■	■		■	■	■		■	■	■	■	■	■		■	■	■	■		■	■
Uncrewed systems: Counter solutions			■											■		■								■	

- Predictive maintenance, logistics, as well as cyber operations constitute a second group that is directly related to the prevailing preference for data-driven AI solutions, which is also reflected in the focus on data analytics and data management.
- C2 in combination with data analytics and data management forms a third priority capability cluster as many nations look at AI for help in assessing growing data volumes. Few countries, by contrast, want to use AI to develop new C2 approaches.
- While AI for electronic warfare (EW) and to counter adversarial EW plays a role for around a third of the countries, AI for use in missiles, torpedoes, fire support and air defense rank lower on the development agendas. It will be interesting to see to what extent the Russia-Ukraine war and current missile attacks against Israel will shift these priorities.
- While around a third of the countries consider defense AI for red teaming and wargaming, far fewer countries develop defense AI for (mission) planning and tactics development. Interestingly, Germany has paved the ground for exactly these types of future applications, which may be a harbinger of significant change if the German Ministry of Defense (MoD) were to succeed in transitioning development results into mature defense systems and capabilities. Here, lessons from the war in Ukraine could serve as an accelerator, in particular, for future German air/missile defense solutions.
- Finally, the significant congruence between Russian and Chinese defense AI development priorities is noteworthy. Among other aspects, both nations share an interest in defense AI for target identification, EW, and swarming, which could, in combination with the focus on uncrewed systems, point towards fully autonomous reconnaissance-strike complexes able to operate under adversarial electromagnetic spectrum dominance in the future.

Reference to congruent defense AI priorities highlights the fact that more and more countries look at opportunities to co-develop defense AI capabilities with partners.[4] Pillar two cooperation among Australia, the United Kingdom, and the United States (AUKUS) is one example illustrating a multinational capability development strand. Cooperation between the United Kingdom, Italy, and Japan in the Global Combat Air Program (GCAP) could also address defense AI in the future. And multinational development projects that receive co-funding via the European Defense Fund (EDF) play a key role for defense AI development in Estonia, Finland, Italy, Greece, and Spain.

As attractive as multinational defense cooperation may be it will raise thorny questions regarding the future (national) ownership of (multinational) defense AI efforts and the interoperability between AI building blocks originating from different countries operating under heterogeneous data protection/sharing regimes. Even more importantly, multinational defense AI efforts are likely to run into national

[4] Turkey is the outlier in this regard. Although the country does not seek international partnerships to develop defense AI, it is ready to participate in NATO initiatives and standardize its defense AI solutions accordingly to improve export prospects.

interests, as, for example, Australia, Germany, France, the Netherlands, and the United Kingdom consider defense AI a sovereign defense industrial capability—which in turn might limit multinational cooperation. The Netherlands, for example, have only tasked TNO, the government-owned research entity, not industry, to develop defense AI algorithms that are intimately related to the way its armed forces plan and execute certain military operations.

A final note is due on the question of who adopts from whom, which matters for national and multinational development efforts. Developing AI against the background of an already existing system or platform will always shape AI in line with the prime tasks of the respective system. By contrast, enabling new behavior on the battlefield by developing AI tactics, would reshape the design and performance parameters of these systems and platforms in line with tactics—but might be less palatable because of this. There is no right or wrong on this question but given the congruence in defense AI development priorities to improve existing solutions discussed above, the latter will likely become more important in the future to achieve and sustain a competitive edge.

2.3 Organizing Defense AI

According to Jensen et al. (2022: 3), structure is one of two key factors determining if and to what extent the use of information technology will lead to military innovation, because the "structure of institutions channels the flow and interchange of information across the formation."[5] Whether nations undergo organizational reform to prepare for the use of defense AI is thus an important question. The case studies send mixed signals on how reform could or should look like (Table 7).

The United States and France are among the few countries that have set up new project-specific organizations to advance defense AI. Project Maven in the US explored the use of defense AI for ISR and made progress thanks to the new, small, dedicated project structure—but later faced organizational challenges and resistance upon transitioning into the prevailing functional organization. France set up ARTEMIS.IA as a public-private partnership to provide the armed forces with a set of different applications to analyze big defense data volumes but was not able to

Table 7 How to organize defense AI

Project-based approach	Entrusting existing organizations with defense AI	Creating new organizations to deal with defense AI
FRA, USA	AUS, CAN, CHN, DEU, DNK, ESP, EST, FIN, GRE, IRN, ITA, JPN, SGP, SWE, TUR, TWN	CAN, FRA, GBR, IND, ISR, KOR, NLD, RUS, UKR, USA

[5] The other factor is resonance understood as the "degree to which prevailing ideas about how war is fought and problem-solving routines accommodate new information flows" (Jensen et al. 2022: 3).

deliver the key goal of identifying and selecting best-in-class proposals because loopholes in the design provided options for circumventing the setup's competitive nature.

Several countries decided to set up new defense AI units mostly at the level of the MoD, while others also established new research and development (R&D) entities to drive defense AI forward. The list of newly created defense AI units includes.

- France's Defense AI Coordination Unit (CCIAD);
- Plans for a new unit focusing on developing future technologies in the R&D directorate of Israel's MoD;
- India's Defense AI Council (DAIC) and Defense AI Projects Agency (DAIPA);
- South Korean plans for a National Defense AI Center, explicitly modeled on the basis of new units established in the United States and the United Kingdom;
- The Netherlands' appointment of a Chief Information Officer and the establishment of the Data Science Center of Excellence;
- Russia's new special department on developing AI technologies in the MoD;
- UK's Defense AI Center (DAIC);
- The Pentagon's new Chief Digital and AI Office (CDAO);
- Ukraine's Brave1 and the Innovation Development Accelerator.

Canada, which is also listed in this group of countries, holds a special place as its current organizational setup is so dysfunctional that it almost prevents the armed forces from using AI properly. The Defense AI Center of Excellence (DAICoE) has thus been proposed as an institutional solution to overcome an excessively siloed organization. Like the other new organizations mentioned, this unit would be tasked with horizontal coordination of different stakeholders, which can create conflicts given different functional tasks and organizational interests. Thus, the jury is still out whether these new units will facilitate defense AI advancement and synchronization.

This uncertainty is also the reason why several other countries entrusted existing organizations with the task of bringing defense AI into the armed forces. Turkey, for example, has added the task of coordinating defense AI stakeholders to the portfolio of the State Secretariat for the Defense Industry (SSB). Finland rejected the idea of setting up a new unit to deal with defense AI and instead chose a cross-organizational matrix approach. Estonia created a new position inside the MoD and uses the Cyber Command as a transmission mechanism to reach out to industry and involve the military services. Australia does not foresee big organizational implications of defense AI but has rather changed its overall innovation pathway to expedite the transfer of new ideas to in-service solutions.

In addition to organizational change at ministerial levels, several countries also introduced novel elements at service and command levels. The United States launched the AI and Data Accelerator (AIDA) initiative to "embed teams of data experts within combatant commands" (Barnett 2021). France uses AI coordinators at service levels in a similar way. The Netherlands involves experts of the Data Science Center of Excellence as defense AI advisors to cooperate with specific warfare centers to formulate doctrine and set up projects. Australia has established a

central organization within the Joint Capabilities Group to coordinate efforts among the services. India has adopted a similar approach with setting up a new AI Subcommittee and a Joint Working Group on AI for the services. Singapore has set up the Digital Ops-Tech Center at the new Digital and Intelligence Service for the same purpose. South Korea goes furthest with designating dedicated experimental units for each service to advance defense AI adoption.

2.4 Funding Defense AI

Sustained funding is essential for defense capability development. Defense AI is no exception to this rule. But funding has presented the biggest analytical challenges across all case studies. The significant spread in funding, that ranges from a few hundred thousand euros or dollars per annum in some countries to close to USD5bn in the United States, makes a volume-based comparison useless. In addition, national budgetary laws and diverging definitions of funding categories move cross-country analyses close to comparing apples with peaches. Therefore, the findings depicted in Table 8 need to be interpreted with care.

Starting from left to right, the category "somehow financed" suggests that it is not clear, what the respective countries spend on defense AI because budgets are not disclosed. While money is available, different defense budget lines are tapped to fund the respective projects. If funding is sustainable, is hard to say in these cases. The second category "dedicated AI budget line" suggests that defense AI officially appears in the defense budget, most often in the form of R&D projects that are either listed at aggregate levels or with respect to different R&D priorities, use cases, or technology fields. Italy's spending, for example, also includes funds to advance the networking of ecosystem partners to include specialized civilian AI research institutes. When defense AI is mentioned, like in Australia, France, and Iran, as a program of record, it signifies that procurement activities are ongoing, which also suggests multi-year funding. The final two categories in Table 8 show that the listed countries budget defense AI as part of ongoing defense R&D efforts as well as procurement projects. While this sounds like good news at first, integrating defense AI into procurement projects also implies that it is—absent access to more classified budgetary material—close to impossible to gauge the true level of defense AI spending related to the respective procurement project.

Table 8 How to fund defense AI

Somehow financed	Dedicated AI budget line	Program of record	Dedicated AI budget line and program of record	Dedicated AI budget line, program of record and interagency funding
DNK, EST, ESP, GBR, GRE, ISR, NLD, SGP, SWE, TWN	FIN, IND, ITA, ISR, JPN	AUS, FRA, IRN	CAN, CHN, DEU, RUS, TUR, UKR, USA	KOR

Ensuring funding, however, is only one element. Even more important is the question how funds are made available. This question poses challenges as information is sparse. However, the case studies on France and Germany, for example, clearly illustrate that traditional funding mechanisms set up for hardware development might reach their limit when considering software-enabled AI. In France, traditional hardware-focused procurement projects have separated R&D from equipment budgets. And Germany, apart from basic defense research funding, is integrating defense R&D into defense procurement programs without properly disclosing specific R&D amounts. South Korea, by contrast, is the only country in this volume that has engaged civilian ministries, primarily the Ministry of Science and Information and Communications Technology, in co-funding the development of defense AI.

The prevailing opaqueness of defense AI funding is a problem as it hampers informed debate on what is being spent and how effectively money has been invested. Overcoming the situation is challenging, as an internationally accepted taxonomy on defense AI spending is missing. In view of developing such a taxonomy, it will be important to combine input and output/outcome perspectives to assess what has been made available and what has been achieved. In this regards, three aspects are key. First, a spending taxonomy could create transparency regarding the input factors needed to produce defense AI solutions such as hardware (e.g., edge computing, high-performance computing), data management and data curation, data analytics, digital models of physical assets (e.g., missiles, radars, vehicles), mathematical models, advanced simulation environments, and software development. Second, the taxonomy needs to consider the performance of AI models and approaches commensurate with the tasks to be fulfilled. The metrics for this category should vary as second wave AI, for example, focusing on classification or pattern recognition, would need benchmarks like accuracy or false positive rates, whereas third wave AI, that can be used to develop AI tactics, will need benchmarks like exploitability, defined as the ability of one player to take advantage of a suboptimal adversarial move. Finally, the taxonomy needs to look at effectiveness and focus on outcome and impact generated by defense AI. Benchmarks could ask if an AI-enhanced ground-based air defense system engaged more adversarial targets with less munition and in shorter time or what the minimum size of an AI-empowered swarm that successfully neutralizes or destroy an adversarial tank formation would need to be.

2.5 Fielding and Operating Defense AI

Armed forces are using defense AI applications, but it is challenging to gauge the true level of contemporary defense AI diffusion. The picture presented in Table 9 is markedly different from the defense AI development priorities (Table 6) discussed above.

Form a regional perspective, current use cases for fielded defense AI solutions seem more prevalent in EU and NATO countries, but the differences to other regions are less stark. The most illuminating regional cluster emerges from the current war

between Russia and Ukraine, which reflects an almost identical tit-for-tat use of defense AI among the warring parties. Absent conceptual novelties and tactical surprises, it is difficult to see how defense AI could benefit one of the two sides when both focus on fielding defense AI to advance situational understanding, data analytics, decision and planning support, fire support, ISR, influence operations, precision effects, and uncrewed systems.

Combining defense AI with uncrewed systems and ISR is also the most prominent use case across all 25 nations followed by target detection and data analytics. Tellingly, more countries have already deployed defense AI solutions for precision effects than identified this use case as a development priority. Among other countries, France, Germany, Iran, Russia, and the United Kingdom consider developing and fielding defense AI for precision effects among their priorities, which is in line with their well-established missile portfolios.

Almost every second country currently uses defense AI for predictive maintenance and logistics as well as simulation-based training. Around one third of the countries use it to conduct cyber network operations and improve air defense. Interestingly, fewer countries use, rather than develop, defense AI to augment situational awareness and situational understanding and for C2. Battle or Combat Management Systems are closely related to both functions. This application is interesting as Denmark has placed itself in a prominent position due to the SitaWare software suite developed by Systematic, which is used by Australia, Denmark, Finland, Germany, Sweden, the United Kingdom, the US, and other countries (Systematic 2023).

Fielding defense AI solutions for border security is relevant for Greece and Turkey, Iran, and India, as well as the United Kingdom, but no country counts border security as a development priority. This could suggest that using AI for surveillance, video and image analysis or in combination with biometrics is already rather mature. By contrast, tactics development and safety drop from the list of current deployment use cases. Defense AI to counter uncrewed assets, in support of swarming, loitering munition, and mission planning are also not yet well-established fielding priorities, suggesting that defense AI for these use cases is still at a lower level of technological readiness.

While Table 9 illustrates current use cases for defense AI, it does not yet indicate how nations roll out defense AI. In this regard Table 10 offers interesting insights. Right now, most of the countries use experiments and/or single projects to field specific defense AI solutions, but very few of these projects make it into official programs of record. This suggest that there are two "valleys of death." The first, well-known, describes the challenge of transforming ideas into market ready products; the second is more "internal" and captures the transition from R&D to procurement. The US experience is particularly enlightening as both valleys of death are very pronounced here despite launching different AI-focused programs like Maven, which uses AI for video and image analysis, and Scarlet Dragon, which builds on results from Maven for AI-enhanced targeting assistance and setting up JADC2 as a proper program of record involving defense AI applications.

Table 9 International defense AI fielding use cases

Use case	USA	CAN	GBR	SWE	FIN	EST	DNK	DEU	NLD	FRA	ESP	ITA	GRE	TUR	RUS	UKR	ISR	IRN	IND	CHN	JPN	KOR	TWN	SGP	AUS
Air/missile defense			■				■	■		■							■	■	■				■	■	
Air traffic management							■			■															
Battle/combat management			■		■		■	■		■									■					■	
Border security			■										■	■				■	■					■	
Close-in weapon systems			■				■																		
Command and control							■					■			■		■			■	■			■	
Common operational picture	■							■		■			■		■	■			■					■	
Cyber/CNO	■		■				■			■					■	■	■				■			■	
Data analytics and data management		■		■	■		■	■	■	■	■			■		■	■					■	■	■	■
Decision and planning support											■			■	■	■			■					■	
Defense industrial production														■	■										
Disaster relief	■																							■	
Electronic warfare			■								■				■					■					
Encryption			■												■									■	
Enterprise services					■		■	■											■			■	■	■	

(continued)

Table 9 (continued)

Use case	USA	CAN	GBR	SWE	FIN	EST	DNK	DEU	NLD	FRA	ESP	ITA	GRE	TUR	RUS	UKR	ISR	IRN	IND	CHN	JPN	KOR	TWN	SGP	AUS
Fire support (e.g., artillery)															■	■								■	
Force protection								■									■					■		■	
Human performance modification											■														
Intelligence, surveillance, reconnaissance	■	■	■	■		■	■	■		■				■	■	■	■		■	■	■	■		■	
Influence/ information operations			■							■	■				■	■				■				■	
IOD/MCM/mine clearance/UXO		■			■		■												■					■	
Loitering munition			■											■											
Manned-unmanned teaming			■									■		■	■				■			■		■	
Medical services		■						■														■	■		
Mission planning					■		■																	■	
Modelling, simulation, red teaming, Wargaming			■																					■	■
Precision effects			■		■			■		■			■		■	■		■							
Predictive maintenance, logistics, MRO	■				■		■	■		■							■		■	■			■	■	■

Swarming	■		■																					
Training (incl. Simulation-based training)			■										■		■	■				■	■	■		
Target detection, classification, identification	■	■	■						■	■		■	■	■	■	■	■	■	■	■	■	■	■	
Uncrewed systems	■		■		■	■		■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Uncrewed systems: Counter solutions																								

Table 10 Modes of fielding defense AI solutions

Not yet fielded	Experiments and projects involving AI	AI-focused experiments and projects	Programs of record involving AI	AI-focused programs of record	AI part of foreign procured systems	Battlefield use
JPN	AUS, CHN, DEU, DNK, ESP, EST, GBR, FIN, FRA, ITA, KOR, NLD, RUS, SGP, TUR, TWN	CAN, DEU, IRN, NLD, RUS, SGP, TWN, USA	FRA, ISR, IND, RUS, USA	FRA	DEU, DNK, EST, FIN, GRE, IND, ITA, NLD, UK, UKR	ISR, RUS, UKR

Finally, "learning by procuring" is a prominent inroad for defense AI to enter a foreign market via the defense solutions procured from a partner. As the overview illustrates, this avenue is not only relevant for countries with less advanced national defense industrial bases but also for defense industrial heavyweights like Germany, Italy, the Netherlands, and the United Kingdom. In all four countries defense AI solutions enter the national defense ecosystem via purchases from the US and/or Israel. In fact, a modern fifth generation fighter jet like Lockheed-Martin's F-35, advanced uncrewed systems like the Reaper or air defense solutions like Arrow need to be considered as pivotal defense AI transmission mechanism.

While using these systems can solidify the advancement of defense AI, this option also comes with challenges. A first challenge stems from the inevitable crowding-out effect that defense AI embedded with these systems might produce vis-à-vis indigenous defense AI applications. The second stems from properly understanding what kind of defense AI you get when importing foreign systems. In this regard, Moshe Patel, Director of the Israel Missile Defense Organization, made a telling statement at a May 2023 event at the Center for Strategic and International Studies in Washington, DC, when he argued that Israel would be integrating its air defense algorithms "inside the Finnish command and control" (CSIS 2023). How deep, one may ask, will nations be willing to integrate "foreign algorithms" into national sovereign systems and to what extent will the buyer have a say in calibrating and adjusting these "foreign algorithms?"

2.6 Training for Defense AI

AI needs talents but competition for talents is fierce as armed forces, defense companies, and commercial industries vie for key experts.[6] Given the financial power of big tech, for example, Marie Louise Cummings already speculated years ago, that

[6] Specific data training initiatives are discussed in the country chapters on Germany, Israel, the Netherlands, Spain, and Ukraine.

the defense community's relative "AI illiteracy" could tilt the balance towards big private interests (Cummings 2018: 17). This, and the conviction, explicitly expressed in countries like Denmark, Estonia, and Finland, that armed forces should only operate AI systems they truly understand, has prompted many nations to step up training efforts.

Given the fact that most nations acknowledge the general-purpose character of AI and its broad impact on all facets of private and corporate life, the limitedness of existing training efforts is puzzling. Most of the countries concentrate on making sure that soldiers understand and handle AI properly, Table 11 reveals. Updating the curricula of defense academies, setting up new courses, and advancing wargaming with AI are some of the initiatives undertaken by these countries.

A second group looks at the workforce more broadly and includes civilian defense personnel as well. In this regard, Greece and South Korea are of particular interest. Greece has been setting up comprehensive training programs at the military academies, while in South Korea the Ministry of Defense is cooperating with the Ministry of Science and Information and Communications Technology to educate AI literate soldiers and officers. Both countries emphasize that significant training efforts also of the civilian defense personnel are needed to make sure that defense talents are well prepared should they transit over to the civilian labor market. Similar drivers are at work in Israel, where the armed forces also use AI to early identify potentially outstanding future commanders, personalize training programs, and identify soldiers likely to extend their service. Similar initiatives are also being launched in the United Kingdom.

The third group of nations includes countries that look at training the military service and defense industrial workforces. This is the case in Spain and France, where industry plays an active role in advancing corporate AI training programs also in view of better integrating small and medium-sized enterprises into the AI-relevant supply chains of leading defense players. Turkey also belongs to this group, with the YETEN project playing a special role in AI-enhanced corporate matchmaking to identify the defense company best suited to develop specific technologies indigenously, which also includes a skills aspect.

Finally, Russia is for the time being the only country reviewed in this volume that sets its focus on expanding the AI expertise of its civilian defense, defense industrial, and military services workforce. While also using AI for training purposes, Russia uses "military scientific units." The conscripts, with whom these units are staffed, are expected to follow a military-scientific carrier that could either lead

Table 11 Who is trained for defense AI?

Unclear	Military service workforce	Civilian defense and military service workforce	Defense industrial and military service workforce	Civilian defense, defense industrial, and military service workforce
CAN, DNK, JPN	AUS, CHN, DEU, EST, FIN, IND, ITA, SWE	GRE, IRN, ISR, KOR, NLD, SGP, UKR, USA, TWN	ESP, FRA, GBR, TUR	RUS

them to work for military institutes or as experts of the armed forces. Like this idea, but with a different focus, France and Israel pool local expertise via "digital reserve elements," that can be activated in times of need.

An interesting new angle comes into play when considering the growing importance of mini- or multilateral frameworks to develop defense AI, as discussed above. In view of co-developing defense AI, the "ability to move talent between partner countries to improve the speed of technology innovation is vital" (Cohen and Nott 2023: 9) to advance the human skillset required for defense AI. The problem, however, is that defense AI experts are on short supply everywhere. This prompts the need rethink how talents can be attracted and retained. Like jointly funding sovereign technology development via the NATO Innovation Fund, a new initiative could champion the idea of establishing a defense-focused sovereign talent management regime. Most importantly, the regime would clear experts for sensitive work on defense AI and thus facilitate, like the Schengen Agreement in Europe, free movement among its members. This idea might be particularly appealing to retain and bring back reservists that have embarked on a civil career track relevant for defense AI. In addition, national defense academies could be tasked to offer dedicated programs that ensure knowledge transmission among national and international experts. Furthermore, innovation and startup hubs could be brought in to make sure that defense industrial newcomers also benefit from knowledge transfers.

3 Interpreting the Findings

Operational requirements, technological readiness, and conceptual maturity need to come together for armed forces to innovate. The above discussion underlined that the adoption of defense AI along these three trajectories is very uneven. Consequently, some of the findings produced by this collection of case studies are confirming elements of the defense innovation literature and practices, whereas others are surprising and some even tell uncomfortable truths.

3.1 Confirming Expectations

New military ideas, concepts, and technologies diffuse in a multi-stage process. As Raska (Raska 2016: 168–169) has argued, this process ranges from emulating what others have been doing, via adopting existing practices to developing novel concepts and tactics. Right now, defense AI emulation is prevalent. First, challengers and partners look at how the United States is handling the integration of AI into military concepts and capabilities. China, Russia, and Iran scrutinize the US practice in view of better understanding how to prepare against the US use of defense AI and identifying possible weak spots that might be exploited for their own use of AI on the battlefield. The same is true for US allies and partners in Europe and the

Asia-Pacific region. In this case emulating US practice signals "closeness" meant to facilitate interoperability and thus also cooperation.

Second, nations well versed in handling new technologies like AI also look at others in a process of "reverse emulation." On the one hand, these nations look at challengers to understand if their own processes are fit enough to avoid being surprised by challengers. This becomes most obvious regarding the need to create a holistic defense AI ecosystem bringing together defense end users, research institutes, established defense and new non-defense companies, as well as investors. While most nations have adopted this idea and struggle with its proper implementation given high market entry barriers for non-defense companies and startups, China's seemingly perfect mastering of military-civil fusion creates an implicit international benchmark. This perspective, however, overlooks the difficulties even the Chinese leadership has in implementing its top-down approach to driving technology-induced defense modernization.

On the other hand, established players and ambitious newcomers look at current wars to assess how defense AI might affect warfighting and what needs to be adapted to incorporate initial lessons identified. Volunteer-led software driven novelties that originate from Ukraine are catching the eye of many observes in EU and NATO countries. This view, however, tends to ignore that Ukraine's all-source data and information fusion would be impossible to implement in most EU and NATO countries given current privacy protection and data sharing regulations. The prominent role of Western defense AI solution providers in Ukraine should also serve as cautionary warning not to become victim of false mirror imaging that emerges from the fact that the use of Western technology by Ukrainian forces is considered a true indigenous innovation that would, in turn, be impossible at home given the broader regulatory leeway these companies enjoy in Ukraine. In addition, war zone analyses tend to overemphasize the contribution of single assets or applications thus neglecting the need for a more systemic view (Borchert et al. 2021: 37–52).

3.2 Surprises

One of the most counter-intuitive findings of this volume is that there is no real disruptor when it comes to defense AI. One reason is conceptual and stems from the fact that disruption in military terms is hard to define. Change in the use of military power, that could lead to disruptive outcomes, can result from conceptual, organizational, technological, or operational modifications and will most often only become visible in retrospect. A second reason stems from the fact that despite the rhetoric about thinking and acting out of the box, no nation seems willing to break out as it is unclear if the "first mover advantage" will incur strategic benefits that outweigh the risks. Yet the case studies also make it amply clear that there are two thresholds that—if passed in the long-run—could constitute game-changing impacts: The move from second to third-wave defense AI that emphasizes context and consequence awareness and a relaxation of the "human in the loop" principle to advance

machine autonomy. But as long as no nation is crossing these thresholds, data-driven AI in combination with the "human in the loop" principle continues to be the prevailing paradigm (Fig. 1).

A second surprise stems from the fact that digitalization is a misleading indicator for a nation's defense AI prowess. All countries considered leaders in digitally modernizing the public sector, for example, have a hard time pulling through this edge into the military domain. Estonia, considered a thought and practice leader on e-government and cybersecurity, faces the challenge of a conservative military and a clear focus on meeting current capability needs; both forces prevent the country from quickly adopting defense AI. The same is true for Israel (Adamsky 2010: 132–133) whose "organized mess" in defense AI produces results but is far from providing optimal inroads for the country to leverage the technology base it has. A similar industrial-military dysfunction is at play in Taiwan, where commercial and defense industrial players operate in their own silos thus depriving the country's armed forces of access to commercial talent and technology. The very same problem also hampers defense AI in South Korea, where the defense industry is considered unattractive to work with. And while India might be considered an "AI talent hotbed, it is not an AI innovation one," the case study argues. All these countries thus serve as a cautionary tale that public (and private) sector digitalization does not easily transfer into the armed forces to create added value. This finding is even more relevant as most of the countries analyzed in this volume consider defense digitalization a prerequisite for the successful use of defense AI.

Combining this finding with the above discussion about the struggle to build adequate ecosystems leads to a third surprising insight: Irrespective of the industrial level of maturity, defense industrial innovation is the often-neglected sibling of defense and military innovation. Novel modes of defense industrial cooperation including big tech companies or smaller startups from the commercial world do not happen overnight. Rather, there is a growing need for dedicated defense industrial transformation management that very few governments have on their agenda.

South Korea, for example, is a textbook example of synchronizing the activities of many different ministries to advance defense capabilities. But interagency jointness meets a completely bifurcated industrial ecosystem. In Germany and Spain, industrial bifurcation is in full swing as well, but without a common understanding of several ministries to join forces in augmenting defense. And while France invests a lot of effort in designing a sovereign ecosystem for defense AI, the country's leading defense companies have embarked on very different digital modernization journeys thus rendering synchronization with non-defense companies challenging. This is also the case in the United States, despite the efforts of the Department of Defense to set up defense innovation units with outreach offices in the country's technology hotspots. In slight contrast, the case studies on Russia and Turkey suggest that both countries explore using AI to advance indigenous defense industrial capacities. Although it is unclear, yet, if the respective initiatives hold up to the announced promises, Moscow's approach deserves attention given the country's "continually improving adaptation cycle that links battlefield lessons to Russia's industry and strategies" (Ryan 2024).

While this volume focuses on defense AI, the ecosystem challenge is also relevant for successfully bringing other emerging technologies into the defense sector. Defense industrial innovation and defense ecosystem management should thus be considered strategic tasks that require more government attention, because governments set the overall regulatory framework and incentives. Industrial innovation also needs more corporate efforts, because ecosystem design is all about appropriately readjusting corporate supply chains considering the need to sustain defense industrial capacities for periods of long and protracted warfighting.

3.3 Uncomfortable Truths

Some of this volume's findings do not sit easily with prevailing assumptions underpinning the current discourse on defense AI ethics. First, defense AI ethics matters, but is more pronounced in some countries than in others and shaped by very different motives. France and the United Kingdom have established special MoD committees to oversee development of reliable AI for defense. Russia and China do see the need for defense AI regulation at the global level, but primarily as an instrument to contain the strategic leeway of the United States and to avoid US leapfrogging that would prevent both nations from overcoming existing gaps. The United States, in turn, might have a similar interest in using international regulation to prescribe a certain use of defense AI that does not create surprises on the battlefield. Spain, in contrast, has mainly focused its efforts during the EU Presidency in the second half of 2023 on advancing AI regulation irrespective of the country's defense needs, which prompted the defense community to develop its thinking via the military channels in the EU and NATO. Thus, analysts need to put more light on the motives that prompt countries to engage on defense AI ethics at all. India, for example, sends very mixed signals when arguing in favor of the responsible use of defense AI but abstaining from signing, for example, the 2023 REAIM Summit's Call for Action on exactly this principle. The Netherlands have established a national ELSA Lab Defense to assess the ethical, legal, and societal consequences of defense AI also in view of leveraging this approach to co-shape international norm-building. Singapore follows a similar understanding and considers military AI governance an important element of its defense diplomacy outreach, which led the city-state to publish its own guiding principles for defense AI in 2019. While consenting with the need for responsible defense AI, Estonia and Finland, for example, are concerned that an overemphasis on regulation might hamper ethically justified technology development and thus also business interests. And in Greece decades of underinvestment and strategic rivalry with Turkey have pushed the defense AI ethics discourse to the backburner.

Second, the case study on Ukraine—as well as current developments in Israel—illustrate that war readjusts normative preferences. Under threat, both nations recalibrate the rules of engagement for AI on the battlefield. When "the emphasis is on damage and not on accuracy," as a spokesperson of the Israel Defense Forces said

on 9 October 2023 (Abraham 2023), the threshold for the use of AI in military operations is lowered—by the "human in the loop," and not by technology. Adversarial electromagnetic spectrum dominance, that makes it more difficult to provide connectivity to remotely operate assets using AI, can render fail-safe provisions to keep AI under human control more challenging, as the Ukrainian case study shows. Therefore, both case studies serve as powerful reminders that norm preferences are context-driven since war can entice governments to "embrace once-controversial technologies with gusto" (O'Brien 2024). An in-depth discussion of this topic goes beyond the scope of this volume, but future research on defense AI ethics could provide added value by analyzing, if and how norm adjustments, that occurred under war, "survive" the transition to peace, how war-torn societies use their own experience in shaping international norm discussions, and what role other factors like Ukraine's new status as an EU admission candidate play in this regard.

Finally, the findings of this volume cautiously warn against making non-democratic nations nine feet tall when it comes to implementing defense AI. Rather, the China, Iran, and Russia chapters show, that these countries suffer from the same pathologies that hinder defense innovation in democratic nations. The idea that individuals or leading party-affiliated groups have a completely free hand in autopiloting their defense establishment towards AI-enhanced military superiority is a caricature of reality. Yes, civil-military relations differ from a democratic and rules-based approach prevalent in democratic nations. This, however, does not yet suggest that military-civil fusion is easier to achieve as it depends if and to what extent novel ideas and technologies of non-military origin can penetrate the military industrial complex, which is an important power player in these countries, to yield military advantages (Evron and Bitzinger 2023; Scharre 2023: 21). Second, non-democratic governments may have a different risk calculus, but most of them do not gamble regime survival for novel, but immature ideas, concepts and, technologies. This illustrates that strategic competition can produce lookalikes, if challengers believe that "the perceived risks of failing to imitate another state outweigh the perceived benefits of pursuing a novel but risky new technology" (Liou et al. 2015: 159).

At the same time, however, there is reason to stay vigilant about how defense AI will evolve in these three countries. Two aspects deserve special attention. First, more research is needed on emulation among non-democracies that have learned to cope with sanctions targeting their economies, strategic industries, and critical technologies. China, Iran, and Russia are convinced that the global influence of the United States is waning. And this might prompt them to test the resolve of Washington and its allies also by using defense AI. In this regard the use of defense AI in the context of the respective nuclear arsenals and to exert domestic control are two important topics to monitor closely.

Second, Russia is a well-established defense exporter, China is ramping up defense exports into the Greater Middle East, Africa, and Latin America, and Iran is maintaining a pan-regional network of proxy forces. While it is too early to tell, to what extent all three nations are willing to export defense AI and engage in knowledge and technology transfer with recipients, these development vectors also need more attention. On the one hand, AI could shift the intra-power balance between the

three since Iranian military capabilities empowered with AI could directly threaten Russia and endanger Chinese interests in the Middle East. On the other hand—and building on the often-overlooked aspect of innovation driven by violent non-state actors (Veilleux-Lepage and Archambault 2022)—countries like Iran could use proxy forces like Hezbollah or Hamas as "battle lab assistants" that evaluate and test the benefits of new AI-related concepts and technologies in different theaters of operation before fielding them on their own.

4 Conclusion

Defense AI is advancing across the 25 countries analyzed in this volume, but motives, drivers, pace, and priorities differ. The paradigm that is underpinning defense AI, however, is surprisingly stable irrespective of a country's overall strategic ambition, its technological and industrial maturity, or the character of its domestic political system: data and human-centric defense AI describe today's dominating focus and understanding of defense AI. This prompts two final remarks related to the prevailing imaginaries about defense AI.

First, what do we (believe to) see when we talk about defense AI? This question addresses the boundaries of the prevalent socio-technical defense AI imaginaries (Jasanoff and Kim 2015). Currently, the dominant body of literature, briefly discussed at the beginning of this chapter, is fixated on data-centricity and thus second wave AI. Current analyses predominantly ascribe limitations and opportunities to defense AI that are true for traditional machine learning, but do not apply in the same way for third wave AI. Understanding the limits of this analytical perspective is important as it can lead to inadequate assumptions about the overall impact of defense AI. The often-discussed idea of so-called "flash wars" (Scharre 2018), analogous to stock market flash crashes caused by technology glitches, builds on the erroneous idea that AI will unstoppably pursue its path in a certain direction creating an escalatory dynamic. Third wave AI, by contrast, knows when "going out of action" due to confusing signals from the battlefield would be needed or when de-escalation would be more beneficial than aggressively staying the course (Hofstetter 2014).

Therefore, the rise of third wave AI has significant consequences for the regulation of defense AI, as the respective technologies are subject to fierce geoeconomic competition among nations aiming at containing raising challengers to maintain their own edge. In view of containment, third wave AI is ambivalent. The fact that it is less data hungry will make it less prone to data-induced restrictions. But third wave AI still requires significant computing power opening the door for regulation to target this angle to limit adversarial capacities. This, however, is easier said than done as sophisticated mathematical effort goes into applying methods that reduce third wave AI's need for computing power. In sum, as mathematical modelling and theoretical as well as conceptual sophistication are more important for third wave defense AI, the diffusion of these solutions is very likely

harder to control and contain but will likely also occur at slower pace given more demanding requirements.

This is, perhaps, also the reason why third wave AI remains still difficult to understand and requires a more nuanced vocabulary to describe its outcomes. Eric Lipton's August 2023 story about Valkyrie, an experimental pilotless aircraft of the US Air Force using AI, serves as a telling example. He wrote:

> One of the things Major Elder watches for is any discrepancies between simulations run by computer before the flight and the actions by the drone when it is actually in the air (…) or *even more worrisome, any sign of 'emergent behavior,' where the robot drone is acting in a potentially harmful way*. (Lipton 2023, emphasis added)

Emergence, in the context of this quotation, meant that the AI-enhanced Valkyrie went into a series of rolls to make optimal use of the infrared sensors on board. Human operators were not expecting AI to perform these moves, but these moves yielded better performance. So, the pure fact that emergence might imply tactical behavior that human operators did not expect does not make this kind of behavior "potentially harmful." Or, to put it differently: Equating emergence with wrongful behavior will deprive armed forces of the added value third wave AI can deliver, for example, by creating surprise, a core principle of war, in a way "differently than a human" would act (Demarest 2024). The more important question is if the system, that is producing AI-driven emergent behavior, is producing it in an explainable and verifiable way as this will be needed for third wave AI solutions to be certified for military use.

Second, when do we know that AI has been used on the battlefield? This question is anything but easy to answer because AI, as software, mostly eludes our sensory perception. In fact, to be effective, AI needs to be embedded in sensors, missiles, platforms, decision-making procedures or other assets and technologies. Thus, the true impact of AI can only be evaluated in tandem with them—and it is this dependence that also shapes the performance of AI.

This, in turn, reinforces the need to be much more precise about the ultimate goals defense AI is expected to accomplish, the roadmap needed to deliver AI-induced capability growth, and the metric needed for performance measurement. Going back to the principles of war, defense planners need to consider what benchmarks they use, for example, to assess the contribution of AI in creating surprise, advancing flexibility, or enabling the initiative. In so doing, it becomes obvious that asking which nation is leading is popular, but quite misleading. There is no aggregate benchmark that would capture the state of transformation regarding conceptual, organizational, technological, and operational maturity in adopting defense AI. Rather each country's progress needs to be analyzed in view of its own level of ambition, the contextual challenges it faces, the sophistication of it defense-industrial technology base, and the savviness of its armed forces. Consequently, countries that look for inspiration when exploring defense AI can choose from a continually growing number of role models. Whether this accelerates instability or reinforces stability very much depends, to paraphrase Alexander Wendt (Wendt 1992), on what military users of AI make of it.

References

Abraham, Yuval. 2023. "A Mass Assassination Factory:" Inside Israel's Calculated Bombing of Gaza. +972 Magazine. https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/. Accessed 15 Feb 2024.

Acharya, Amitav, Antoni Estevadeordal, and Louis W. Goodman. 2023. Multipolar or Multiplex? Interaction Capacity, Global Cooperation and World Order. *International Affairs* 6: 2339–2365. https://academic.oup.com/ia/article/99/6/2339/7337131. Accessed 15 Feb 2024.

Adamsky, Dima. 2010. *The Culture of Military Innovation. The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*. Stanford: Stanford University Press.

Allen, Gregory C. 2020. Understanding AI Technology. Joint Artificial Intelligence Center/ Department of Defense. https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf. Accessed 15 Feb 2024.

Bai, Tao et al. 2021. Recent Advances in Adversarial Training for Adversarial Robustness. arXiv:2102.01356. https://arxiv.org/abs/2102.01356. Accessed 6 Feb 2024.

Barnett, Jackson. 2021. DOD to Embed Data Experts within Combatant Commands. Workscoop. https://workscoop.com/2021/06/22/dod-new-data-and-ai-initiative-for-combatant-commands-jadc2. Accessed 15 Feb 2024.

Barzhaskha, Ivanka. 2023. Wargames and AI. A Dangerous Mix that Needs Ethical Oversight. Bulletin of the Atomic Scientists. https://thebulletin.org/2023/12/wargames-and-ai-a-dangerous-mix-that-needs-ethical-oversight/. Accessed 30 Jan 2024.

Borchert, Heiko, Torben Schütz, and Joseph Verbovszky. 2021. Beware the Hype. What Conflicts in Ukraine, Syria, Libya, and Nagorno-Karabakh (Don't) Tell Us About the Future of War. Defense AI Observatory. https://defenseai.eu/daio_beware_the_hype. Accessed 15 Feb 2024.

Borchert, Heiko, Torben Schütz, and Joseph Verbovzsky. 2023a. Weiter denken! *Internationale Politik* 6: 49–49. https://internationalepolitik.de/de/weiter-denken. Accessed 15 Feb 2024.

Borchert, Heiko, Torben Schütz, and Christian Brandlhuber. 2023b. Leveraging the Defense Metaverse. Unlocking the Power of AI for Force Development. *The Air Power Journal* 3: 23–32. https://www.diacc.ae/wp-content/uploads/2023/10/P3-Dr.-Heiko-Borchert-Leveraging-the-Defense-Metaverse-Defense-AI-Observatory-www.diacc_.ae-www.theairpowerjournal.com-www.spps_.se_.pdf. Accessed 15 Feb 2024.

Bousquet, Antonie. 2022. *The Scientific Way of Warfare. Order and Chaos on the Battlefield of Modernity*. London: Hurst.

Brandlhuber, Christian. 2021. GhostPlay: AI-Enhanced Decision Support for Military Operations. Lecture at the Helmut-Schmidt-University. Hamburg. 3 December. Unpublished.

Chahal, Husanjot, Ryan Fedasiuk, and Carrick Flynn. 2020. Messier than Oil. Assessing Data Advantage of Military AI. Center for Security and Technology. https://cset.georgetown.edu/wp-content/uploads/Messier-than-Oil-Brief-1.pdf. Accessed 15 Feb 2024.

CIGI. Undated. The Ethics of Automated Warfare and Artificial Intelligence. Webinar Series. https://www.cigionline.org/the-ethics-of-automated-warfare-and-artificial-intelligence/. Accessed 15 Feb 2024.

Cohen, Michael, and Chris Nott. 2023. Strengthening the Future of the AUKUS Partnership. IBM Center for the Business of Government. https://www.businessofgovernment.org/report/strengthening-future-aukus-partnership. Accessed 30 Jan 2024.

CSIS. 2023. Missile Defense in Israel. A Conversation with Moshe Patel. https://www.csis.org/analysis/missile-defense-israel-conversation-moshe-patel. Accessed 15 Feb 2024.

Cummings, M.L. 2018. Artificial Intelligence and the Future of Warfare. In *Artificial Intelligence and International Affairs. Disruption Anticipated*, ed. M.L. Cummings et al., 7–18. London: Chatham House. https://www.chathamhouse.org/2018/06/artificial-intelligence-and-international-affairs. Accessed 15 Feb 2024.

DARPA. Undated. AI Next Campaign (Archived). https://www.darpa.mil/work-with-us/ai-next-campaign. Accessed 15 Feb 2024.

Demarest, Colin. 2024. AI-enabled Valkyrie Drone Teases Future of US Air Force Fleet. Defense News. https://www.defensenews.com/unmanned/uas/2024/01/18/ai-enabled-valkyrie-drone-teases-future-of-us-air-force-fleet/. Accessed 30 Jan 2024.

Department of Defense. 2018. Summary of the 2018 Department of Defense AI Strategy. Department of Defense. https://apps.dtic.mil/sti/pdfs/AD1114486.pdf. Accessed 15 Feb 2024.

Diehl, Carlo, and Daniel Lambach. 2022. (K)ein 'AI Arms Race'? Technologieführerschaft im Verhältnis der Grossmächte. *Zeitschrift für Aussen- und Sicherheitspolitik* 15: 263–282. https://link.springer.com/article/10.1007/s12399-022-00915-7. Accessed 6 Feb 2024.

Evron, Yoram, and Richard A. Bitzinger. 2023. *The Fourth Industrial Revolution and Military-Civil Fusion. A New Paradigm for Military Innovation?* Cambridge: Cambridge University Press.

Galliott, Jai, and Jason Scholz. 2020. The Case for Ethical AI in the Military. In *The Oxford Handbook of Ethics and AI*, ed. Markus D. Dubber, Frank Pasquale, and Sunit Das, 684–702. Oxford: Oxford University Press.

Goldfarb, Avi, and Jon R. Lindsay. 2021/2022. Prediction and Judgment. Why Artificial Intelligence Increases the Importance of Humans in War. *International Security* 3: 77–50.

Hicks, Kathleen. 2023. Deputy Secretary of Defense Kathleen Hicks' Remarks: "Unpacking the Replicator Initiative" at the Defense News Conference (As Delivered). https://www.defense.gov/News/Speeches/Speech/Article/3517213/deputy-secretary-of-defense-kathleen-hicks-remarks-unpacking-the-replicator-ini/. Accessed 15 Feb 2024.

Hofstetter, Yvonne. 2014. *Sie wissen alles*. München: C. Bertelsmann.

Hofstetter, Yvonne and Joseph Verbovzsky. 2023. How AI Learns the Bundeswehr's 'Innere Führung.' Defense AI Observatory. https://defenseai.eu/daio_study2310. Accessed 15 Feb 2024.

Horowitz, Michael C. 2018. Artificial Intelligence, International Competition, and the Balance of Power. *Texas National Security Review* 1: 36–57. https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/. Accessed 6 Feb 2024.

Horowitz, Michael C., and Paul Scharre. 2021. *AI and International Stability. Risks and Confidence-Building Measures*. Center for New American Security. https://www.cnas.org/publications/reports/ai-and-international-stability-risks-and-confidence-building-measures. Accessed 15 Feb 2024.

Horowitz, Michael C. et al. 2018. *Strategic Competition in an Era of Artificial Intelligence.* Center for New American Security. https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence. Accessed 6 Feb 2024.

Jasanoff, Sheila, and Sang-Hyun Kim, eds. 2015. *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power*. Chicago, IL/London: The University of Chicago Press.

Jensen, Benjamin M., Christopher Whyte, and Scott Cuomo. 2022. *Information in War. Military Innovation, Battle Networks, and the Future of Artificial Intelligence*. Washington, DC: Georgetown University Press.

Johnson, James. 2021. *Artificial Intelligence and the Future of War: The US, China, and Strategic Stability*. Manchester: Manchester University Press.

Lindsay, Jon R. 2023/24. War Is from Mars, AI Is from Venus: Rediscovering the Institutional Context of Military Automation. *Texas National Security Review*. https://tnsr.org/2023/11/war-is-from-mars-ai-is-from-venus-rediscovering-the-institutional-context-of-military-automation/. Accessed 15 Feb 2024.

Lin-Greenberg, Erik. 2020. Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making. *Texas National Security Review* 3: 56–76. https://doi.org/10.26153/tsw/8866. Accessed 15 Feb 2024.

Liou, Yu-Ming, Paul Musgrave, and J. Furman Daniel. 2015. The Imitation Game: Why Don't Rising Powers Innovate Their Militaries More. *The Washington Quarterly* 38: 157–174. https://doi.org/10.1080/0163660X.2015.1099030. Accessed 6 Feb 2024.

Lipton, Eric. 2023. AI Brings the Robot Wingman to Aerial Combat. New York Times. https://www.nytimes.com/2023/08/27/us/politics/ai-air-force.html. Accessed 15 Feb 2024.

Littman, M.L. 2001. Markov Decision Processes. In *International Encyclopedia of the Social and Behavioral Sciences*, ed. Neil J. Smelser and Paul B. Baltes, 9240–9242. Amsterdam: Elsevier. https://doi.org/10.1016/B0-08-043076-7/00614-8. Accessed 15 Feb 2024.

Mansoor, Peter R., and Williamson Murray. 2019. Introduction. In *The Culture of Military Organizations*, ed. Peter R. Mansoor and Williamson Murray, 1–14. Cambridge: Cambridge University Press.

Mehta, Aaron. 2017. Pentagon Tech Advisers Target How the Military Digests Data. Defense News. https://www.defensenews.com/pentagon/2017/04/06/pentagon-tech-advisers-target-how-the-military-digests-data/. Accessed 15 Feb 2024.

Michel, Arthur Holland. 2023. Recalibrating Assumptions on AI. Towards an Evidence-based and Inclusive AI Policy Discourse. Chatham House. https://www.chathamhouse.org/2023/04/recalibrating-assumptions-ai. Accessed 15 Feb 2024.

Mintzberg, Henry, Bruce Ahlstrand, and Joseph Lampel. 2005. *Strategy Safari. A Guided Tour Through the Wilds of Strategic Management*. New York: Free Press.

NATO. 2022. Allied Joint Doctrine AJP-01. North Atlantic Treaty Organization. https://www.cimic-coe.org/resources/external-publications/ajp-01-edf-v1-f.pdf. Accessed 15 Feb 2024.

O'Brien, Phillips Payson. 2024. The Real AI Weapons Are Drones, Not Nukes. The Atlantic. https://www.theatlantic.com/ideas/archive/2024/02/artificial-intelligence-war-autonomous-weapons/677306/. Accessed 15 Feb 2024.

Payne, Kenneth. 2021. *I, Warbot. The Dawn of Artificially Intelligent Conflict*. London: Hurst & Company.

Phillips, Peter J., and Gabriela Pohl. 2021. Countering Intelligence Algorithms. *The RUSI Journal* 165: 22–32. https://doi.org/10.1080/03071847.2021.1893126. Accessed 15 Feb 2024.

Popescu, Ionut C. 2018. Grand Strategy vs Emergent Strategy in the conduct of foreign policy. *Journal of Strategic Studies* 41: 438–460.

President of Ukraine. 2024. I Signed a Decree Initiating the Establishment of a Separate Branch Forces—The Unmanned Systems Forces—Address by the President of Ukraine. https://www.president.gov.ua/en/news/pidpisav-ukaz-yakij-rozpochinaye-stvorennya-okremogo-rodu-si-88817. Accessed 15 Feb 2024.

Probasco, Emelia. 2023. The Future of Drones in Ukraine: A Report from the DIU-Brave1 Warsaw Conference. Center for Security and Emerging Technology Blog. https://cset.georgetown.edu/article/the-future-of-drones-in-ukraine-a-report-from-the-diu-brave1-warsaw-conference/. Accessed 15 Feb 2024.

Raska, Michael. 2016. *Military Innovation in Small States. Creating a Reverse Asymmetry*. London: Routledge.

Raska, Michael, and Richard Bitzinger. 2023. *The AI Wave in Defense Innovation. Assessing Military Artificial Intelligence, Strategic Capabilities and Trajectories*. London: Routledge.

Reeves, Martin et al. 2013. Ambidexterity. The Art of Thriving in Complex Environments. Boston Consulting Group. https://www.bcg.com/publications/2013/strategy-growth-ambidexterity-art-thriving-complex-environments. Accessed 15 Feb 2024.

Rowe, Neil C. 2022. The Comparative Ethics of Artificial Intelligence Methods for Military Applications. *Frontiers* 5: 991759. https://www.frontiersin.org/articles/10.3389/fdata.2022.991759/full. Accessed 15 Feb 2024.

Ryan, Mick. 2024. Russia's Adaptation Advantage. Foreign Affairs. https://www.foreignaffairs.com/ukraine/russias-adaptation-advantage. Accessed 15 Feb 2024.

Scharre, Paul. 2018. A Million Mistakes a Second. Foreign Policy. https://foreignpolicy.com/2018/09/12/a-million-mistakes-a-second-future-of-war/. Accessed 15 Feb 2024.

———. 2019. *Army of None*. New York/London: W. W. Norton & Company.

———. 2021. Debunking the AI Arms Race Theory. *Texas National Security Review* 4: 121–132. https://tnsr.org/2021/06/debunking-the-ai-arms-race-theory/. Accessed 15 Feb 2024.

———. 2023. *Four Battlegrounds*. New York/London: W. W. Norton & Company.

Scharre, Paul, and Megan Lamberth. 2022. Artificial Intelligence and Arms Control. Center for New American Security. https://www.cnas.org/publications/reports/artificial-intelligence-and-arms-control. Accessed 15 Feb 2024.

Silver, David, et al. 2017. Mastering the Game of Go without Human Knowledge. *Nature* 550: 354–359. https://www.nature.com/articles/nature24270. Accessed 15 Feb 2024.
Skill-Lync. 2023. How Google Handles over 40,000 Petabytes of Data on a Daily Basis. https://skill-lync.com/blogs/how-google-handles-over-40000-petabytes-of-data-on-a-daily-basis. Accessed 15 Feb 2024.
Soare, Simona R. 2023. Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age. IISS. https://www.iiss.org/research-paper/2023/08/digitalisation-of-defence%2D%2Din-nato-and-the-eu/. Accessed 15 Feb 2024.
Stanley-Lockman, Zoe. 2021. Responsible and Ethical Military AI. Allies and Allied Perspectives. Center for Security and Emerging Technologies. https://cset.georgetown.edu/publication/responsible-and-ethical-military-ai/. Accessed 15 Feb 2024.
Systematic. 2023. Systematic Lands a Multi-million Euro Contract with the British Army. https://systematic.com/en-gb/newsroom/corporate-news/systematic-lands-a-multi-million-euro-contract-with-the-british-army/. Accessed 15 Feb 2024.
Tangredi, Sam, and George V. Galdorisi. 2021. *AI at War. How Big Data Artificial Intelligence and Machine Learning Are Changing Naval Warfare*. Annapolis: Naval Institute Press.
Tucker, Patrick. 2024. The Pentagon Is Already Testing Tomorrow's AI-powered Swarm Drones, Ships. Defense One. https://www.defenseone.com/technology/2024/01/pentagon-already-testing-tomorrows-ai-powered-swarm-drones-ships/393528/. Accessed 15 Feb 2024.
Veilleux-Lepage, Yannick, and Emil Archambault. 2022. *A Comparative Study of Non-State Violent Drone Use in the Middle East*. The Hague: International Centre for Counter-Terrorism. https://www.icct.nl/publication/comparative-study-non-state-violent-drone-use-middle-east. Accessed 15 Feb 2024.
Vettoruzzo, Anna et al. 2023. Advances and Challenges in Meta-Learning: A Technical Review. arXiv:2307.04722. https://doi.org/10.48550/arXiv.2307.04722. Accessed 15 Feb 2024.
Vinyals, Oriol, et al. 2019. Grandmaster Level in StarCraft II Suing Multi-agent Reinforcement Learning. *Nature* 575: 350–354. https://www.nature.com/articles/s41586-019-1724-z. Accessed 15 Feb 2024.
Wendt, Alexander. 1992. Anarchy Is What States Make of it: The Social Construction of Power Politics. *International Organization* 46: 391–425.
Work, Bob. 2020. A Joint Warfighting Concept for Systems Warfare. Center for a New American Security. https://www.cnas.org/publications/commentary/a-joint-warfighting-concept-for-systems-warfare. Accessed 15 Feb 2024.
Wright, Nicholas D. 2019. *Artificial Intelligence, China, Russia, and the Global Order*. Maxwell Air Force Base: Air University Press.
Zhuang, Fuzhen et al. 2019. A Comprehensive Survey on Transfer Learning. arXiv:1911.02685. https://doi.org/10.48550/arXiv.1911.02685. Accessed 15 Feb 2024.

Risky Incrementalism: Defense AI in the United States

Lauren A. Kahn

The United States remains the world's preeminent military and technological power. Over the last decade, the United States has increasingly viewed artificial intelligence (AI) proficiency as a vital U.S. interest and mechanism for assuring U.S. military and economic power, recognizing its potential as a force multiplier. Over the last decade, artificial intelligence has become a critical capability for U.S. national defense, especially given the focus of the 2022 U.S. National Defense Strategy on the Indo-Pacific region and the pacing challenge of China (DoD 2022b).

As a result, the U.S. Department of Defense (DoD) has shown growing enthusiasm for AI and related emerging technologies. However, while the United States is currently making advances in AI research and development in both academia and the private sector, the Department of Defense has yet to successfully, on a broad scale, translate commercial AI developments into real military capabilities.

The United States government is generally well-placed to leverage defense AI and AI-enabled systems. However, various bureaucratic, organizational, and procedural hurdles have slowed down progress on defense AI adoption and technology-based innovation within the Defense Department over the last few years. Critically, DoD suffers from a complex acquisition process and a widespread shortfall of data, talent in Science, Technology, Engineering, Mathematics (STEM), and AI and training. Organizations working on AI and AI-related technologies and projects are often siloed, separated not only from each other but also from necessary data and other resources, and there exists within the department a culture that favors tried-and-true methods and systems, sometimes trending towards Luddism. These factors have contributed to a surprisingly slow pace of AI adoption. The National Security Commission's 2021 Final Report to Congress summarized, "despite exciting experimentation and a few small AI programs, the U.S. government is a long way from being AI-ready" (NSCAI 2021: 2).

L. A. Kahn (✉)
Center for Security and Emerging Technology, Washington, DC, USA
e-mail: lauren.kahn@georgetown.edu

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_2

Thus, despite its potential to enhance U.S. national security and be an area of strength, and given the long U.S. tradition of military, innovation, and technological leadership, AI risks becoming a point of weakness, expanding "the window of vulnerability the United States has already entered" (NSCAI 2021: 7). AI will continue to be a point of insecurity if the United States does not pick up the pace of innovation to reach responsible speed and lay the institutional foundations necessary to support an AI-savvy military.

In the last few years (this report is current as of December 2023); however, the Defense Department has made substantial headway on some of these challenges, restructuring its approach to defense AI. In November 2023, the Department of Defense published a new Data, Analytics, and AI Adoption Strategy and has since begun to execute it. Most significantly, the DoD has completed a significant overhaul of its AI organizational structure, creating a new Chief Digital and Artificial Intelligence Office (CDAO) to consolidate its disparate AI projects and stakeholders and better align them with the department's data streams. It has also since established the Generative AI Task Force Lima to assess, synchronize, and employ generative AI capabilities across the Department, updated the Autonomy in Weapons System Directive 3000.09, and launched the Replicator Initiative, which seeks to have DoD fielding thousands of all-domain attritable autonomous systems within the next 18–24 months. Notably, the United States DoD is undergoing significant changes and revitalization of its overall approach to defense AI. However, whether these new AI efforts will be sufficient to allow the U.S. to make up for time lost remains to be seen.

1 Thinking About Defense AI

The United States and other countries have recognized the potential power and efficiencies AI can generate, especially in military contexts. China has famously declared its plan to become the world leader in AI by 2030, while Putin has argued the state that becomes the first to conquer AI will become the "ruler of the world" (Vincent 2017).

The use of cutting-edge, emerging technologies—including AI—in the Russian-Ukraine conflict has made the potential applications of these capabilities much more tangible for states and has piqued interest in everything from drones to Ukraine's so-called "Uber for Artillery" (Kahn 2022; Cooper 2022). Consequently, it has also made evident the condensed timeline militaries face to have these capabilities operational and deployed on the battlefields if they wish to remain competitive.

In line with this global trend, the United States views artificial intelligence as an enabling technology and force multiplier that will generate efficiencies and, if leveraged successfully, will reinforce (or arguably renew) U.S. competitiveness and global technological and military dominance. Along with recent shifts in U.S. defense

and security strategy to address China's pacing challenge, defense AI is considered essential for U.S. military capabilities worldwide.

1.1 What Is the U.S. Understanding of Defense AI?

In 2018, with the release of the first U.S. Department of Defense Artificial Intelligence Strategy, there was a formalized definition of what AI means in U.S. defense contexts. The strategy concisely defined AI as "the ability of machines to perform tasks that normally require human intelligence" (DoD 2018b). Until that point, much of the rhetoric of the U.S. defense community sometimes—inaccurately—made "artificial intelligence seem like a munition" rather than an enabler (Horowitz 2018). Therefore, the 2018 formalization of the definition of AI was a significant step forward in getting the defense establishment closer to the mark when it came to AI. However, defining AI in this manner has been challenging for many in the national security enterprise to grasp. This definition encompasses decades-old technologies dating back to WWII, such as autopilot on aircraft, automated warning systems, and missile guidance, to more recent breakthroughs, such as facial recognition technology, autonomous vehicles, and machine and deep learning algorithms. These definitional lines are further blurred when distinguishing between artificial intelligence, automated/automatic systems (which respond mechanically to inputs), and autonomous systems (which operate on preprogrammed instructions), which may or may not be AI-enabled.

1.2 Why Does the United States Want AI?

AI has become a key pillar in national strategies to achieve U.S. interests, from the Trump Administration to the Biden Administration. When addressing national security challenges and the balance of power, progress in defense AI is often used as a heuristic metric for assessing U.S. military and technology leadership.

The Biden administration has identified China as the pacing challenge shaping current U.S. national defense and security strategy, as well as future military planning (Horowitz 2021). The White House, in its national security strategy, explained this shift in strategy to meet a shifting global balance in power, as China has steadily become the "only competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system" (White House 2022c: 8). As a result, a unique emphasis has been placed on the Chinese threat to U.S. technological dominance.

As a result, much of the U.S. effort on defense AI and other emerging technologies has been contextualized concerning competition with China. Worrying about Chinese AI advancements creates a sense of urgency and a need to advocate for the United States to pick up the pace with responsible speed regarding AI investment,

research, development, acquisition, and deployment. The U.S. military believes AI investments could generate essential capabilities in several areas, with some closer to fielding and others still in the early stages of Research, Development, Testing and Evaluation (RDT&E).

2 Developing Defense AI

The previous sections outline how the United States thinks about defense AI in terms of its national interests, goals, and security. Over the past 5 years, AI has become an ascendant capability in defining U.S. technological leadership. This section will measure the United States' progress in successfully developing, adopting, and leveraging AI capabilities for defense. Subsequent sections will discuss the mechanisms for executing defense AI policy within the United States.

2.1 U.S. AI Strategy and its Evolution

In 2018, the Department of Defense published its first-ever AI strategy, Harnessing AI to Advance Our Security and Prosperity. It emerged from the recognition that technological advances have always been at the forefront to ensure the United States had an enduring "competitive and military advantage" and other states (namely U.S. competitors) were already making significant military investments in AI. The strategy accompanied the newly created Joint Artificial Intelligence Center (JAIC), which was mandated to execute much of the DoD's vision and "synchronize DoD AI activities to expand Joint Force advantages" (DoD 2018b: 5, 9). The strategy positioned AI as a human-centered tool that would help the DoD better support and protect U.S. servicemembers and civilians, enhance national security, and create a more efficient and streamlined organization.

In June 2022, the office of the new CDAO published the Responsible Artificial Intelligence (RAI) Strategy and Implementation Pathway (RAI S&I Pathway) (DoD Responsible AI Working Council 2022). The RAI strategy acknowledges AI requires a more holistic and integrated approach and reinforces other DoD policies on AI and autonomous systems, such as Directive 3000.09—which established guardrails for autonomy in weapons systems (DoD 2012). The updated RAI strategy also formally enshrines DoD's AI ethical principles, which, since adoption in 2020, have become essential guardrails the department has used to shape its AI efforts, spanning everything from experimentation to use.

Finally, in November 2023, the CDAO released the updated Data, Analytics, and Artificial Intelligence Adoption Strategy to build upon and supersede the initial 2018 strategy (Clark 2023). While not a significant step-change in and of itself, the updated strategy more accurately reflects the current status of defense AI priorities,

efforts, and responsibilities in the Department, given the advancements, updates, and reorganizations undertaken in the past few years.

2.2 The United States: Falling Behind?

For decades, the United States has been the world's leading military power and the foremost technological innovator—two distinct yet mutually reinforcing designations. The United States military is uniquely positioned to capitalize on advances in artificial intelligence and other emerging technologies compared to other states. The academic and private sectors within the United States have become the preeminent contributors to furthering the field of AI. Whether in the form of AI conference citations or repository contributions, the weighted citation impact of corporate-academic publications, or attracting much of the world's AI and machine learning talent, the United States surpasses its peers (Zhang et al. 2021: 24; Zhang et al. 2022: 16–35; Zwetsloot et al. 2021a; Zwetsloot et al. 2021b). Despite having a rich AI ecosystem at its fingertips, the United States Department of Defense has failed to become a driving force of AI progress—less than 4% of all AI publications in the United States were government-sponsored in 2021 (Maslej et al. 2023: 27).

As Horowitz et al. (Horowitz et al. 2022: 158) put it, "Leading militaries often grow overconfident in their ability to win future wars, and there are signs that the U.S. Department of Defense could be falling victim to complacency. Although senior U.S. defense leaders have spent decades talking up the importance of emerging technologies, including AI and autonomous systems, action on the ground has been painfully slow." It is clear when it comes to successful defense AI adoption, let alone leadership, just having the technology is insufficient and must be accompanied by organizational and bureaucratic change and integration.

2.3 AI Backsliding, Luddism, and the "Valley of Death"

The 2018 National Defense Strategy noted, "success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting" (DoD 2018a: 10). Being slightly more realistic and acknowledging much of AI development is not being pioneered in government, the 2022 National Defense Strategy has promised that DoD will become a "fast-follower" of market- and commercially-driven technological capabilities with military relevance (DoD 2022b: 19). However, as of writing, the United States has yet to match its execution with its stated intentions and outlined AI strategies completely.

Implementation of this vision for AI leadership has been challenging for the U.S. defense establishment for several reasons:

- Difficulty in transitioning AI research into scalable programs of record supported by the services;
- Siloed research, AI programs, and data streams;
- Lack of STEM and AI talent and general technological literacy and training opportunities.

Like many other large, bureaucratic systems, the Department of Defense is often biased in favor of tried-and-true, existing capabilities over new tools and technologies (Horowitz et al. 2022: 160). Despite its recognized potential as a force multiplier and military innovation enabler, AI, in particular, has faced resistance within the DoD. This hesitancy might be due to perceptions that AI distances humans from decision-making on the battlefield by enabling systems to operate more autonomously. Some within the armed forces have noticed this trend of Luddism within the department, calling this "deliberate incrementalism," whereby AI projects that often meet set requirements and pass testing and verification procedures with flying colors are purposefully delayed when it comes to deployment with "cautious and lengthy feasibility studies," and sometimes cancellation (Spataro et al. 2022).

For example, in the early 2000s, the U.S. Air Force and Navy partnered to create a series of autonomous aircraft capable of conducting surveillance and military strikes, which have evolved into the X-45, the X-47A, and X-47B prototypes. Within two decades, the aircraft were already proving their mettle. Not only could they accomplish complex missions with little human oversight, such as landing on aircraft carriers and completing aerial refueling operations, but they often did so better than the crewed systems (Spataro et al. 2022). Despite the promise the prototypes demonstrated, in what some have called a "case of technological infanticide," the Air Force viewed the systems not as an improvement but as a threat to the F-35 fighter jet and dropped out of the joint program. The Navy continued with the program for a few more years until it canceled it due to internal debate (Osborn 2021). Other AI and autonomous experiments, such as Alpha Dogfight—DARPA's program to train AI algorithms to beat a human pilot in a simulated aerial dogfight—which has been touted as successes, have failed to lead to any actual implementations (Halpern 2022; Gould 2020).

The lofty promises of defense AI juxtaposed with the reality of the conservatism of the military services in AI adoption have contributed to a widening of the "valley of death"—the chasm a technology developed in the private sector must cross before its acquisition by the militaries. Whereas in the early 1960s, it might take a new technology 5 years on average to bridge the gap, today, it can take a decade or more for a capability to move from the lab to the battlefield (Greenwalt and Patt 2021). While some features of AI may have exacerbated the gap, it exists as the armed forces often require "a higher level of technology maturity than the science and technology community is willing to fund and develop" (GAO 2015: 4).

While the DoD may have been able to avoid the valley of death previously, this has become an incredibly sharp sticking point recently. AI and other newer technologies are increasingly software-based and originate almost entirely in the private and academic sectors. Historically, the Department of Defense has struggled with

"developing, procuring, and developing software-centric capabilities," with the acquisition process moving much slower for software-based systems than hardware and weapons systems (GAO 2022: 21). Thus, some institutions within the DoD, such as the Defense Innovation Unit, have taken on roles as an "accelerator" or "translator" of commercial technology for national security and circumvent some of the hurdles by providing funding and faster contract times (DIU 2023a). Nevertheless, such institutions still face challenges in gaining access to acquisition resources. Moreover, such efforts are merely stopgaps to a broader acquisition system problem.

Recognizing this, in August 2023, Deputy Secretary of Defense Kathleen Hicks announced an incredibly ambitious initiative, Replicator–a program focused on processes and ways to overcome some of these barriers to effectively scale technologies into real capabilities. The first big bet for the program would be to "field attritable autonomous systems at scale of multiple thousands, in multiple domains, within the next 18-to-24 months," and if the program successfully demonstrates a pathway to overcoming the valley of death, it will be replicated and inculcated for other capabilities across the department (DoD 2023). While the promise of Replicator is immense, and there has been some steady momentum, its success ultimately "hinges on overcoming a myriad of challenges, from production scalability to bureaucratic inertia, that have hindered previous similar innovation adoption efforts" (Kahn 2023).

There have been some early hints of progress in overcoming the difficulties described above. Some signposts include the U.S. Air Force fast-tracking development of the Phoenix Ghost loitering munition for almost immediate use in Ukraine, the Replicator Initiative, and indications that the Air Force is also considering a new program of record for a next-generation autonomous aircraft (Insinna 2022a; Insinna 2022b).

3 Organizing Defense AI

The United States defense establishment has had a rollercoaster relationship with AI. AI has had a history of sudden periods of progress and overhype—generating sudden boons in funding—followed by troughs of divestment when reality fails to match heightened expectations. The up-and-down has sometimes led to "backsliding" in defense AI progress (Ciocca et al. 2021).

In the very early days of the field, even before the term "artificial intelligence" was coined in 1956, AI research was heavily funded by organizations like the Office of Naval Research (ONR) and the Advanced Research Projects Agency (ARPA) (now known as the Defense Advanced Research Projects Agency, or DARPA) (Schuchmann 2019a). The hope was to use machine translation to aid the U.S. Navy during the Cold War by automatically translating Russian to English. However, stalls in progress in machine translation and slow-moving development in other related AI fields led DARPA and other organizations to fund less blue-skies and

fundamental research in favor of more applied projects. As a result, many refer to this period during the 1970s as the first "AI Winter."

In the 1980s, AI again captured the U.S. military's interest. DARPA invested USD1bn in a strategic computing initiative which hoped to reach a level of machine intelligence that would propel the United States ahead of competitors like Japan, which was experiencing an economic, industrial, and technological boom (Roland and Shiman 2014). The project ultimately over-promised, ushering in a second—much longer—AI Winter during which the U.S. military once again shied away from the field (Schuchmann 2019b).

It is only in the last decade—due to significant advances in machine learning, natural language processing, and computer vision—that AI has once again become a priority for the U.S. national security enterprise (Fig. 1). In 2014, the Department of Defense announced its Third Offset Strategy, the aim of which was "to draw on U.S. advanced technologies to offset China's and Russia's technological advances" (Gentile et al. 2021). One of the central tenets was to "find new ways to cultivate technological innovations and interact with the commercial world" to counter DoD's diminished role in driving innovation. While the Third Offset only lasted in an official capacity until 2018, it significantly influenced the 2018 National Defense Strategy, which argued a new cohort of technologies, including AI, autonomy, advanced computing, big data analytics, robotics, directed energy, hypersonics, and biotechnology would be the technologies to "ensure we will be able to fight and win the wars of the future" (Gentile et al. 2021: 72; DoD 2018a: 3).

Since 2018, AI has become a key pillar in U.S. defense and national security strategy. As technology has developed and progressed, and DoD's prioritization has shifted dramatically over the last 5 years, so has DoD's approach to organizing for AI. The progression of AI within the U.S. military can be divided into three distinct periods or eras, primarily differentiated by how defense AI has been organized within DoD. These include the Project Maven Era: 2017–2018, JAIC Era: 2018–2022, and the CDAO Era: 2022-present.

3.1 Project Maven Era (2017–2018)

Since its establishment in April 2017 as the Algorithmic Warfare Cross-Functional Team, Project Maven has become the most visible proof-of-concept for the application of AI for defense purposes in the United States (Office of the Deputy Secretary of Defense 2017). The idea behind the initiative was to relieve the burden on human operators tasked with analyzing video footage obtained from unmanned aerial systems (UAS). The Maven algorithms augmented or fully automated the object detection, classification, and alert tasks using computer vision supporting the Defeat-ISIS campaign.

Unlike previous DoD-funded AI projects, Maven was a resounding success and surpassed expectations. Even in the face of a public controversy early in its creation, by the end of its first year, Maven had its first models working directly in combat

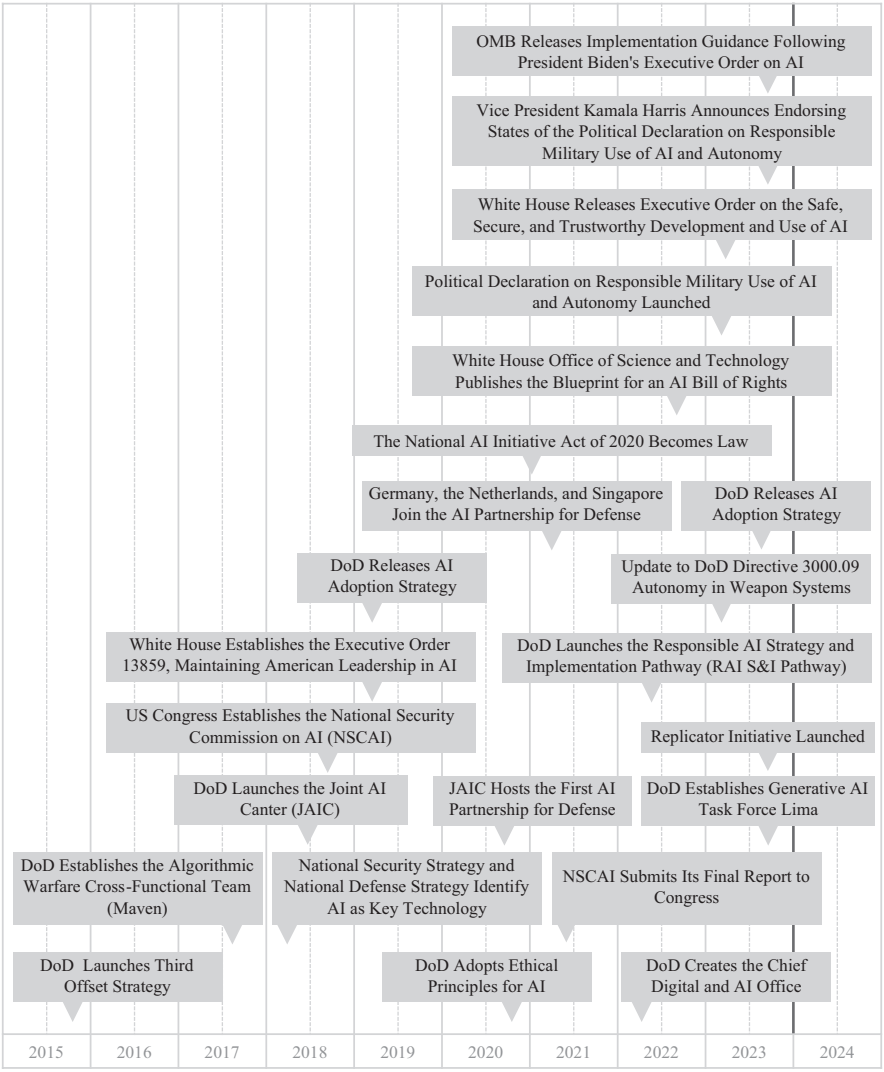


Fig. 1 Recent US policy developments related to defense AI. Source: Author's Chart

operations (Simonite 2021). By 2020, Maven was being applied across multiple conflicts, marking "a monumental early AI-driving win for DoD" (Vincent 2022).

Undoubtedly, Project Maven's swift and sweeping success was "enabled by its organizational structure: a small, operationally focused, cross-functional team that was empowered to develop external partnerships, leverage existing infrastructure and platforms, and engage with user communities iteratively during development" (Allen 2017). Maven was the first to set up to leverage AI effectively for a clear, well-defined purpose. In addition, there was an explicit data-labeling and cleaning

effort to ensure models were trained and applied to the best data, as well as a concerted emphasis on timeliness, with a requirement that algorithm-based technology would be integrated with Programs of Record in 90-day "sprints" (Office of the Deputy Secretary of Defense 2017). The launch of Project Maven was accompanied by the release of DoD's first-ever AI strategy, discussed above.

3.2 JAIC Era (2018–2022)

Emboldened by Project Maven's success, in 2018, the DoD established the Joint Artificial Intelligence Center (JAIC) as the centralized hub for AI within the Department to "seize upon the transformative potential of Artificial Intelligence technology for the benefit of America's national security" (JAIC 2020a). The creation of the JAIC marked a key inflection point in the U.S. approach to defense AI. It had significant funding and high internal and external visibility, which signaled a clear message: AI would be critical for the future of U.S. national security.

In the months following its establishment, in quick succession, Congress established the National Security Commission on Artificial Intelligence (NSCAI), the JAIC received its first director, the White House enacted Executive Order 13859 on Maintaining American Leadership in AI, and the DoD published its first-ever AI Strategy.

The JAIC's introduction marked the beginning of the AI spring within the defense enterprise, succeeding in elevating AI and laying the foundation for the widespread recognition of AI as critical for the future of U.S. national security and defense, which is bearing fruit today. In particular, the JAIC "made headway on AI adoption and data literacy, with initiatives like "AI 101," and on the data integration issue, as part of the Artificial Intelligence and Data Initiative (AIDA)" (Horowitz and Kahn 2022). AI R&D within the Defense Department has steadily grown, with the military services investing more in AI and related technologies, projects, and programs.

Ironically, as the JAIC succeeded in its original intent—as AI evolved and investment in the technology skyrocketed—it had become "torn between being a developer of algorithms itself and being an enabler that helps the military services figure out how to develop and implement algorithms within relevant military programs" (Horowitz and Kahn 2021). While the organization of the JAIC "followed best practices from military innovation and business innovation literature" at the time, "which advocated for surrounding the need to create a spinoff or separate sub-organizations to value the potential of emerging technologies" the institution had since outgrown itself, becoming less clear in its aim as it became the owner of an increasingly varied portfolio of projects, technologies, and responsibilities (Horowitz and Kahn 2021). Furthermore, while well-funded, it lacked the authority "to compel the military services and other institutions to collaborate" on AI and AI-related projects (Horowitz and Kahn 2021).

3.3 CDAO Era (2022-Present)

While the DoD created more and more separate projects and institutions like Maven and the JAIC (with varying degrees of success, funding, and support), the organizational and bureaucratic infrastructure were not well-suited to a technology that, by definition, was broad in its forms, applications, and use-cases. The defense AI enterprise within DoD remained siloed. As many as "fifteen separate departments and organizations funded and worked on AI and AI-adjacent technologies, often without formal coordination or throughlines," resulting in "redundancies, gaps, inconsistencies in application and access to data and resources" (Horowitz and Kahn 2022).

In recognition, the Department of Defense moved to reorganize its major institutional AI players in early 2022, restructuring the AI efforts it had built piecemeal from the ground up. Hoping to achieve a more integrated approach to defense AI, the Pentagon created a new office—the Chief Digital and Artificial Intelligence Office (CDAO), which would subsume the JAIC, the Defense Digital Service (DDS), and the Office of the Chief Data Officer (CDO).

For U.S. defense AI adoption, aligning these organizations could help to bridge the gaps between institutional players and better connect "DoD's AI efforts with data, the fuel AI requires" (Horowitz and Kahn 2022).

3.4 The Defense AI Ecosystem More Broadly

The defense AI ecosystem within DoD is encompassed, in part, by the broader Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&D)) organizations. This includes defense agencies and field activities such as the Defense Innovation Board, the Small Business Innovation Research and Small Business Technology Transfer Programs (SBIR/STTR), the Innovation Steering Group, Science and Technology Futures, the Offices of the Deputy Chief Technology Officer (CTO) for Science & Technology, and for Critical Technologies, DARPA, and more.

Since its early involvement in the 1950s, DARPA has continued to "lead innovation in AI research as it funds a broad portfolio of R&D programs, ranging from basic research to advance technology development" (DARPA 2023). As of writing, DARPA has over 50 currently ongoing AI-related projects on applications of AI ranging from making machine learning more explainable to using AI to assess better secures of critical mineral supplies. DARPA has its own streamlined contracting procedures and funding mechanisms, and because it is focused on R&D, it has had the flexibility to conduct more early-stage blue-skies research. While not all projects have translated into concrete capabilities or programs of record, DARPA is a consistent, key contributor to the overall defense AI ecosystem and the defense research and engineering ecosystem.

A few other cross-departmental specialty organizations designed to target AI and other emerging technologies have been established under this umbrella, which has helped direct funding and investment in capabilities. Namely, the Defense Innovation Board (DIB), established in 2016, was constructed to provide independent recommendations to the Secretary of Defense and other senior leaders within the DoD on emerging technologies the military should adopt. The Defense Innovation Unit (DIU) was stood up precisely to field and scale commercial emerging technologies across the military, and from June 2016 to September 2021, it leveraged USD20.1bn in private investment and awarded USD892.7M in contracts (DIU 2021: 7).

Outside DoD, some private sector initiatives have also emerged, attempting to facilitate the transition of commercial-sector emerging technologies into government and the Department of Defense and serve as essential connective tissue between Silicon Valley and the Pentagon.

3.5 Working with Allies and Partners

AI has also become a new binding mechanism between the United States and its allies and partners. As a significant component of the messaging and strategy surrounding the US approach to defense, AI has been used to counter China's growing technological primacy. Many of the DoD's efforts on AI have been folded into broader efforts to collaborate with regional partners.

For example, as a part of the Indo-Pacific Strategy released by the White House in February 2022, the Biden Administration announced the creation of a new Quad Fellowship which would recruit and financially support students from the United States, Japan, Australia, and India to pursue graduate degrees in STEM fields at U.S. institutions (White House 2022a: 10).

The trilateral security pact between Australia, the UK, and the US, known as AUKUS, created to deter China further, has revolved significantly around technology transfer and cooperation in developing emerging technologies, including AI and autonomy. As some have said, "AUKUS seeks to win the technology competition with China by pooling resources and integrating supply chains for defense-related science, industry, and supply chains. This will be the decades-long and multifaceted purpose of AUKUS—a transnational project racing to seize advantages in artificial intelligence, quantum computing, and cyber technology" (Tarapore 2021).

There has been more regular coordination on topics like AI governance and ethics with other states developing AI, including "academic conferences, Track II academic-to-academic exchanges, bilateral and multilateral dialogues, and discussions in various international forums," such as the DoD-hosted AI Partnership for Defense and the Political Declaration on Responsible Military Use of AI and Autonomy which has nearly 50 signatories (Scharre and Lamberth 2022; JAIC Public Affairs 2022; Department of State 2023).

4 Funding Defense AI

While complete details of the official Department of Defense budget and project spending are not publicly available, analysis of unclassified requests by the DoD paints a clear picture of a steady increase in the amount of funding designated for AI and other related and emerging technology research, development, testing, and evaluation (RDT&E) over the last few years. In Fiscal Year (FY) 2021, Stanford University's Institute for Human-Centered Artificial Intelligence estimated there were about 305 unclassified DoD RDT&E programs that specified the use of AI or machine learning technologies, comprising about USD5bn (Zhang et al. 2021: 168). Govini has estimated from FY17–FY21, the U.S. government spent about USD50bn on AI, machine learning, and autonomy technology (Govini 2022: 2). Approximately 84% of which was funded via direct contracts, 15% by grants, and the rest from other transaction authorities (OTAs) (Govini 2022: 24).

While the majority of these contracts and grants were awarded to the regular spread of large defense companies—Lockheed Martin, Northrop Grumman, General Dynamics, BAE, Raytheon, and Booz Allen Hamilton were all in the top 10 vendors —there have been "emergent" companies that have benefited from the work of the DIU and the other organizations that have made it their mission to facilitate collaboration between Silicon Valley and the Pentagon, such as Anduril, Applied Intuition, Databricks, ModalAI, Rebellion Defense, and ShieldAI (Govini 2022: 25). There are also stakeholders like Palantir, which recently received considerable media attention for the algorithmic power it has provided to Ukraine, that don't quite fit into either bucket but are increasingly becoming key players in developing AI for defense (Ignatius 2022a, 2022b).

In March 2022, the Biden Administration set a "record peacetime national defense budget of USD813bn, which earmarked USD773bn for the Pentagon" (Stone 2022). A staggering 17% of the funds directed towards the Pentagon are being allocated to research and development. In announcing the FY2023 budget request, the administration argued the "all-time high" of USD130.1bn for research and development reflected the understanding of the "need to sharpen our readiness in advanced technology, cyber, space, and artificial intelligence" in particular (White House 2022b). The budget builds on "DoD's progress to modernize and innovate," not only "including the largest investment ever in RDT&E—more than 9.5% over the FY 2022 enacted level," but also dedicated USD16.5bn to Science and Technology, USD3.3bn to microelectronics, and USD250M to 5G, and an undisclosed amount to artificial intelligence as a part of its efforts on "Advanced Capability Enablers" (White House 2022b).

5 Fielding and Operating Defense AI

Despite some of the difficulties discussed above, the United States has been actively prototyping, fielding, and operating applications of AI across the Department of Defense and the armed services. While the uses for AI in defense contexts are seemingly endless, from using AI to enhance the precision and accuracy of existing systems to generating simulation-based training initiatives and wargames, some of the more visible, established applications of AI the DoD has been pursuing are in the following areas:

- Intelligence, Surveillance, and Reconnaissance (ISR)
- Cyber
- Autonomous Systems and Vehicles
- Command and Control
- Disaster Relief
- Logistics

The below sections detail some examples of the more visible, mission-specific applications of AI the U.S. military has pursued.

5.1 Intelligence, Surveillance, and Reconnaissance (ISR)

AI is already demonstrating its dramatic impact on ISR capabilities due to its ability to recognize patterns quickly and analyze large swaths of disparate data from various sources. Project Maven, which used computer vision and algorithms to aid in video and image analysis, was the first AI project within DoD to be considered a resounding success. Other, more recent AI initiatives have emerged, including the Army's Scarlet Dragon which uses data from Maven to provide AI-augmented targeting assistance for large-scale combat operations, while the Marine Corps is working to "incorporate algorithms developed as part of Project Maven into their capabilities and to modernize legacy weapon systems" (Wasserbly 2021; GAO 2022). The Navy's Task Force 59 is working to create cost-effective, fully autonomous vehicles that also have AI-enabled surveillance capabilities to monitor threats ranging from "hostile Iranian drones to an aggressive Chinese posture to rogue pirates" (Barnett 2022a).

5.2 Cyber

Concerning how AI might impact cybersecurity and cyberoperations, much of the discourse within the United States has been about its disruptive potential. AI is expected to "make the work of cyber defenders more difficult over time, with faster

and faster computers enabling increasingly complex attacks and more rapid network intrusion" (Segal and Goldstein 2022: 31). The Navy and the Army both employ commercial machine learning algorithms, trained on commercial and government data, to better detect cyber threats (Kenyon 2022). The DoD has worked closely with Cyber Command to employ AI to enhance network protection tools.

5.3 Autonomous Systems and Vehicles

Advances in AI—and in particular, the integration of AI into piloting, guidance, navigation, and ISR and target acquisition systems on platforms—have enabled greater degrees of autonomy in everything from vehicles to munitions. R&D projects currently in development include the Navy's Ghost Fleet—the goal of which is to have nearly one in three warships be entirely autonomous, without any human crew aboard, by 2045— and the Air Force's Golden Horde experiments, which hope to develop swarming air-fired and air-dropped smart weapons that can autonomously share information, change course, and seek high-priority targets (Mizokami 2022; Insinna 2021). Most recently, the first effort under the Replicator Initiative is focused on attritable, all-domain, autonomous systems, with a goal of thousands of systems to be purchased in tranches within the next 2 years.

5.4 Command and Control

AI is also increasingly used to collect, identify, and synthesize multiple data streams to improve battlefield and situational awareness in real-time and better connect sensors with operators and decision-makers. Using AI to create a single source of information in this manner is sometimes referred to as a "common operating picture" (Barnett 2020). A Congressional Research Service report points out that "currently, information available to decision-makers comes in diverse formats from multiple platforms, often with redundancies or unresolved discrepancies" (Sayler 2020: 13). In this regard, AI is seen as the critical component to implementing the DoD vision of Joint All-Domain Command and Control (JADC2)— "which aims to centralize planning and execution of air-, space-, cyberspace-, sea-, and land-based operations" to create a wholly-connected and in-sync military. The DoD released its JADC2 Implementation Plan in March 2022, which elaborated that "JADC2 enables the Joint Force to 'sense,' 'make sense,' and 'act' on information across the battlespace quickly using automation, artificial intelligence, predictive analytics, and machine learning to deliver informed solutions via a resilient and robust network environment" (DoD 2022a). Data and AI have become so central that, moving forward, the CDAO will be heading up the strategy element of JADC2 (Pomerleau 2022).

All of the service's JADC2 projects—the Army's Project Convergence, the Navy's Project Overmatch, and the Air Force's Advanced Battle Management

System—have indicated the use of AI in some shape or form. The Army used its AI-powered network, Firestorm, to transmit intelligence directly from U.S. Army sensors to Australian and British forces in a recent Project Convergence experiment with allies (Feickert 2022; Hoehn 2022; Strout 2020; Lacdan 2022). The Air Force has also launched a series of Global Information Dominance Experiments to give more time to commanders to make decisions "by integrating more information from a global network of sensors and sources, using the power of AI and machine-learning techniques to identify the important trends within the data, and making both current and predictive information available" (Barnett 2021; U.S. Air Force 2021). DARPA has also launched programs to leverage AI to "network systems and sensors, prioritize incoming sensor data, and autonomously determine the optimal composition of forces" in the form of the Air Space Total Awareness for Rapid Tactical Execution project (Sayler 2020: 13; Barnett 2020).

5.5 Disaster Relief

The DoD also pursues AI for use cases with humanitarian goals. When the JAIC was first established in 2018, it had two initial capability delivery projects called National Mission Initiatives (NMIs) it was tasked with, one of which was Humanitarian Assistance and Disaster Relief (Cronk 2019). The idea behind the NMI is to use AI and machine learning to power "problem-solving prototypical applications to quickly identify and locate people and infrastructure impacted by natural and manmade disasters" (Esri 2019). Predictive geospatial intelligence and computer vision, for example, are both being developed for use in these situations (DIU 2023b).

5.6 Logistics

The second NMI the JAIC was initially tasked with was Predictive Maintenance. A significant component of logistics is ensuring materiel is up to standards and well-maintained. The idea behind the NMI was to use AI to generate efficiencies and reduce costs associated with maintenance by predicting in advance when a component might fail—a technique known as predictive maintenance (Department of Defense Office of Inspector General 2022: 2). In this way, AI could provide a unit-based, specially tailored recommendation instead of waiting for a system or part to fail before fixing it or relying on set force-wide maintenance schedules.

6 Training for Defense AI

One of the most widespread, recurring points of concern about U.S. defense AI adoption is the broad lack of STEM expertise and talent in government (Horowitz & Kahn 2020). In fact, according to the NSCAI's final report, it is the "alarming" deficient of diverse and tech-savvy talent within both the DoD and Intelligence Community that stands as the "greatest impediment to the United States being AI-ready by 2023" (NSCAI 2021: 121). The report continues, warning if the government fails to invest in building a digital workforce, the United States "will remain unprepared to buy, build, and use AI and its associated technologies" (NSCAI 2021: 121).

While the United States is attractive to global AI talent pool members, the public sector has failed to compete with academia and industry (Zwetsloot et al. 2021a). A survey of 254 U.S. AI Ph.D. graduates, for example, indicated only 31% would even consider a government role, citing a lack of access to both computing and data resources as well as growth opportunities and an inability to pursue research (Aiken et al. 2020: 2, 13).

Despite the blueprint provided by the NSCAI report and a congressional mandate to develop an AI workforce and education strategy in the 2020 National Defense Authorization Act (NDAA), there has not been any comprehensive effort to enact many of the recommendations outlined, nor to reform hiring, recruiting, and training processes in either the DoD or IC (U.S. Government Publishing Office 2019). However, the CDAO has begun to design and propagate a consistent AI education strategy and improve general understanding of AI across the department and the armed services through the launch of a series of "AI 101" educational pilot programs (JAIC 2020b; Barnett 2022b).

7 Conclusion

The United States has both the desire and means to achieve world leadership in defense applications of artificial intelligence. There is support from top leaders and policymakers across the government, and a rich AI research ecosystem exists across the private and academic spheres. Moreover, AI is increasingly viewed as critical in addressing national security concerns, particularly in capability-matching U.S. adversaries and addressing the pacing challenge with China that animates the 2022 National Defense Strategy.

Surprisingly, despite these stimuli, the U.S. government, particularly the Department of Defense, has yet to seriously, and on a broad scale, employ AI beyond one-off projects or initiatives. The lag is partly due to a predisposition to favoring and being more accustomed to hardware-based capabilities rather than software and momentum that biases the status quo. However, the most considerable obstacles slowing down U.S. defense innovation, and AI adoption especially, have

been (1) an organizational structure and acquisitions process that is not best suited to translating general-purpose technologies of commercial and civilian origins into fundamental capabilities to be used in national security and defense contexts, and (2) a significant AI/STEM talent deficit.

Significant geopolitical changes and events, including the Russia-Ukraine conflict and continuing evidence of China's technological rise, have crystallized the near-term military impact of emerging technologies, including AI. The United States Department of Defense has reacted by increasing the urgency with which it has pursued its AI goals by creating new organizations designed to improve DoD's AI adoption capacity, formalizing guiding ethical principles, increasing funding and support for projects and acquisitions mechanisms tailor-made for AI, and reorganizing its internal AI and data ecosystem.

There has been some early indication of progress due to these recent course-correction measures. After years of unmet potential, DoD is now more effectively moving forward towards creating a more AI-enabled US military, which is promising. However, only time will tell the long-term implications and whether recent efforts will be sufficient to launch a fully AI-enabled U.S. military.

References

Aiken, C., James Dunham, and Remco Zwetsloot. 2020. Career preferences of AI talent. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/career-preferences-of-ai-talent/. Accessed 30 Jan 2024.

Allen, Gregory. 2017. Project Maven brings AI to the fight against ISIS. Bulletin of the Atomic Scientists. https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/. Accessed 30 Jan 2024.

Barnett, Jackson. 2020. DARPA wants a common operating picture to 'complement' JADC2. FedScoop. https://www.fedscoop.com/darpa-jadc2-astarte-program/. Accessed 30 Jan 2024.

———. 2021. DOD tests new machine learning capabilities for JADC2. Fedscoop. https://www.fedscoop.com/dod-tests-new-machine-learning-capabilities-for-jadc2/. Accessed 30 Jan 2024.

——— 2022a. Task force 59: The future of the Navy's unmanned systems or a one-off win? FedScoop. https://www.fedscoop.com/task-force-59-the-future-of-the-navys-unmanned-systems-or-a-one-off-win/. Accessed 30 Jan 2024.

———. 2022b. JAIC piloting artificial intelligence education for DOD. Fedscoop. https://www.fedscoop.com/jaic-piloting-artificial-intelligence-education-for-dod/. Accessed 30 Jan 2024.

Ciocca, Julia, Michael C. Horowitz, and Lauren Kahn. 2021. The perils of overhyping artificial intelligence: For AI to succeed, it first must be able to fail. Foreign Affairs. https://www.foreignaffairs.com/united-states/perils-overhyping-artificial-intelligence. Accessed 30 Jan 2024.

Clark, Joseph. 2023. DOD releases AI adoption strategy. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/. Accessed 30 Jan 2024.

Cooper, Tom. 2022. Kropyva: Ukrainian artillery application. Medium. https://medium.com/@x_TomCooper_x/kropyva-ukrainian-artillery-application-e5c6161b6c0a. Accessed 30 Jan 2024.

Cronk, Terri Moon. 2019. DOD's Artificial Intelligence initiatives outlined before senate. Defense.gov. https://www.defense.gov/News/News-Stories/Article/Article/1785308/dods-artificial-intelligence-initiatives-outlined-before-senate/. Accessed 30 Jan 2024.

DARPA. 2023. AI next campaign. Defense advanced research projects agency. https://www.darpa.mil/work-with-us/ai-next-campaign. Accessed 30 Jan 2024.

Department of Defense. 2012. Department of defense directive 3000.09: Autonomy in weapon systems. https://irp.fas.org/doddir/dod/d3000_09.pdf. Accessed 30 Jan 2024.

———. 2018a. Summary of the 2018 national defense strategy of The United States of America: Sharpening the American Military's Competitive edge. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf. Accessed 30 Jan 2024.

———. 2018b. Summary of the 2018 department of defense artificial intelligence strategy: Harnessing AI to advance our security and prosperity. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF. Accessed 30 Jan 2024.

———. 2020. DOD adopts ethical principles for artificial intelligence. https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/. Accessed 30 Jan 2024.

———. 2022a. DoD announces release of JADC2 implementation plan. https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/. Accessed 30 Jan 2024.

———. 2022b. National defense strategy of The United States of America. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF. Accessed 30 Jan 2024.

———. 2023. Deputy secretary of defense Kathleen hicks keynote address: 'The Urgency to Innovate' (As Delivered). https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/. Accessed 30 Jan 2024.

Department of Defense Office of Inspector General. 2022. Audit of the department of defense's implementation of predictive maintenance strategies to support weapon system sustainment (DODIG-2022-103). https://www.dodig.mil/reports.html/Article/3063635/audit-of-the-department-of-defenses-implementation-of-predictive-maintenance-st/#:~:text=Predictive%20maintenance%20is%20a%20technique,reduce%20or%20eliminate%20unscheduled%20maintenance. Accessed 30 Jan 2024.

Department of State. 2023. Political declaration on responsible military use of artificial intelligence and autonomy. https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/. Accessed 30 Jan 2024.

DIU. 2021. DIU Annual report FY 2021 In Review. https://assets.ctfassets.net/3nanhbfkr0pc/5JPfbtxBv4HLjn8eQKiUW9/cab09a726c2ad2ed197bdd2df343f385/Digital_Version_-_Final_-_DIU_-_2021_Annual_Report.pdf. Accessed 30 Jan 2024.

———. 2023a. Who we are/our mission: Defense Innovation Unit (DIU). https://www.diu.mil/about. Accessed 30 Jan 2024.

———. 2023b. Artificial intelligence portfolio: xView challenge series. Defense Innovation Unit. https://www.diu.mil/ai-xview-challenge. Accessed 30 Jan 2024.

DoD Responsible AI Working Council. 2022. U.S. Department of defense responsible artificial intelligence strategy and implementation pathway. https://www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf. Accessed 30 Jan 2024.

Esri. 2019. Esri chosen to support department of defense JAIC emergency response program. https://www.esri.com/about/newsroom/announcements/esri-chosen-to-support-department-of-defense-jaic-emergency-response-program/. Accessed 30 Jan 2024.

Feickert, Andrew. 2022. The army's project convergence. Congressional research service. https://crsreports.congress.gov/product/pdf/IF/IF11654. Accessed 30 Jan 2024.

GAO. 2015. Defense advanced research projects agency: Key factors drive transition of technologies, but better training and data dissemination can increase success. https://www.gao.gov/products/gao-16-5. Accessed 30 Jan 2024.

———. 2022. Artificial intelligence: DOD should improve strategies, inventory process, and collaboration guidance. https://www.gao.gov/products/gao-22-105834. Accessed 30 Jan 2024.

Gentile, Gian, Michael Shurkin, Alexandra T. Evans, Michelle Grisé, Mark Hvizda, and Rebecca Jensen. 2021. A history of the third offset, 2014–2018. Rand Corporation. https://www.rand.org/pubs/research_reports/RRA454-1.html. Accessed 30 Jan 2024.

Gould, Joe. 2020. AI's dogfight triumph a step toward human-machine teaming. Defense News. https://www.defensenews.com/congress/2020/09/10/ais-dogfight-triumph-a-step-toward-human-machine-teaming/. Accessed 30 Jan 2024.
Govini. 2022. The national security scorecard: Critical technologies edition. https://govini.com/research/the-national-security-scorecard-critical-technologies-edition/. Accessed 30 Jan 2024.
Greenwalt, William C., and Dan Patt. 2021. Competing in time: Ensuring capability advantage and mission success through adaptable resource allocation. Hudson Institute. https://www.aei.org/research-products/report/competing-in-time-ensuring-capability-advantage-and-mission-success-through-adaptable-resource-allocation/. Accessed 30 Jan 2024.
Halpern, Sue. 2022. The rise of A.I. fighter pilots. The New Yorker. https://www.newyorker.com/magazine/2022/01/24/the-rise-of-ai-fighter-pilots. Accessed 30 Jan 2024.
Hoehn, John R. 2022. Advanced Battle Management System (ABMS). Congressional research service. https://crsreports.congress.gov/product/pdf/IF/IF11866. Accessed 30 Jan 2024.
Horowitz, Michael C. 2018. Artificial intelligence, international competition, and the balance of power. *Texas National Security Review* 1 (3): 36–57.
———. 2021. War by timeframe: Responding to China's pacing challenge. War on the rocks. https://warontherocks.com/2021/11/war-by-timeframe-responding-to-chinas-pacing-challenge/. Accessed 30 Jan 2024.
Horowitz, Michael C., and Lauren Kahn. 2020. The AI literacy gap hobbling American Officialdom. War on the rocks. https://warontherocks.com/2020/01/the-ai-literacy-gap-hobbling-american-officialdom/. Accessed 30 Jan 2024.
———. 2021. Two cheers for the department of defense's new data and artificial intelligence leadership initiative. The Council on Foreign Relations. https://www.cfr.org/blog/two-cheers-department-defenses-new-data-and-artificial-intelligence-leadership-initiative. Accessed 30 Jan 2024.
———. 2022. Why DoD's new approach to data and artificial intelligence should enhance national defense. The Council on Foreign Relations. https://www.cfr.org/blog/why-dods-new-approach-data-and-artificial-intelligence-should-enhance-national-defense. Accessed 30 Jan 2024.
Horowitz, Michael C., Lauren Kahn, and Laura Resnick Samotin. 2022. A force for the future: A high-reward, low-risk approach to AI military innovation. *Foreign Affairs* 101 (3): 157–164.
Ignatius, David. 2022a. How the algorithm tipped the balance in Ukraine. The Washington Post. https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/. Accessed 30 Jan 2024.
———. 2022b. A 'good' war gave the algorithm its opening, but dangers lurk. The Washington Post. https://www.washingtonpost.com/opinions/2022/12/20/ukraine-war-russia-tech-battlefield/. Accessed 30 Jan 2024.
Insinna, Valerie. 2021. US Air Force completes tests of swarming munitions, but will they ever see battle? Defense News. https://www.defensenews.com/air/2021/06/07/us-air-force-successfully-completes-tests-of-swarming-munitions-but-their-future-is-unclear/. Accessed 30 Jan 2024.
———. 2022a. Meet 'Phoenix Ghost,' the US Air Force's new drone perfect for Ukraine's war with Russia. Breaking Defense. https://breakingdefense.com/2022/04/meet-phoenix-ghost-the-us-air-forces-new-drone-designed-for-ukraines-war-with-russia/. Accessed 30 Jan 2024.
———. 2022b. Air Force pilots to try out XQ-58A Valkyrie drones ahead of potential UAV wingman program. Breaking Defense. https://breakingdefense.com/2022/11/air-force-pilots-to-try-out-xq-58a-valkyrie-drones-ahead-of-potential-uav-wingman-program/. Accessed 30 Jan 2024.
JAIC. 2020a. About the JAIC: The JAIC Story. (Archived from the original). https://web.archive.org/web/20200807163038/https://www.ai.mil/about.html. Accessed 30 Jan 2024.
———. 2020b. 2020 Department of Defense Artificial Intelligence Education Strategy. https://www.ai.mil/docs/2020_DoD_AI_Training_and_Education_Strategy_and_Infographic_10_27_20.pdf
JAIC Public Affairs. 2022. DoD Joint AI Center holds fifth International Dialogue for AI in Defense. AI in Defense: DoD's Artificial Intelligence Blog. https://www.ai.mil/blog_03_04_22_dod_jaic_holds_fifth_international_dialogue_for_ai_in_defense.html. Accessed 30 Jan 2024.

Kahn, Lauren. 2022. How Ukraine is remaking war: Technological advancements are helping Kyiv succeed. Foreign Affairs. https://www.foreignaffairs.com/ukraine/how-ukraine-remaking-war. Accessed 30 Jan 2024.

———. 2023. Scaling the future: How replicator aims to fast-track U.S. defense capabilities. War on the rocks. https://warontherocks.com/2023/09/scaling-the-future-how-replicator-aims-to-fast-track-u-s-defense-capabilities/. Accessed 30 Jan 2024.

Kenyon, Tilly. 2022. US DoD selects Torch AI for cyber security capabilities. Technology Magazine. https://technologymagazine.com/ai-and-machine-learning/us-dod-selects-torch-ai-to-for-cyber-security-capabilities. Accessed 30 Jan 2024.

Lacdan, Joe. 2022. Project convergence 2022: Army to work closely with allies in the future fight. Aerotech News. https://www.aerotechnews.com/blog/2022/11/22/project-convergence-2022-army-to-work-closely-with-allies-in-the-future-fight/#:~:text=Project%20Convergence%20is%20an%20all,electronic%20warfare%20and%20signals%20intelligence. Accessed 30 Jan 2024.

Maslej, Nestor, et al. 2023. The AI Index 2023 Annual Report. AI Index Steering Committee, Institute for Human-Centered AI, Stanford University. https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf. Accessed 30 Jan 2024.

Mizokami, Kyle. 2022. By 2045, one-third of U.S. Navy Warships Will Be Robotic 'Ghost Ships'. Popular Mechanics. https://www.popularmechanics.com/military/navy-ships/a40732357/one-third-navy-warships-robotic-by-2045/. Accessed 30 Jan 2024.

NSCAI. 2021. National Security Commission on Artificial Intelligence Final Report. https://www.nscai.gov/2021-final-report/. Accessed 30 Jan 2024.

Office of the Deputy Secretary of Defense. 2017. Memorandum for: Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven). https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf. Accessed 30 Jan 2024.

Osborn, Kris. 2021. X-47B UCLASS Stealth Drone: The U.S. Navy's big mistake? The National Interest. https://nationalinterest.org/blog/buzz/x-47b-uclass-stealth-drone-us-navys-big-mistake-180595. Accessed 30 Jan 2024.

Pomerleau, Mark. 2022. DOD creates new JADC2 integration office, puts CDAO in charge of data integration. DefenseScoop. https://defensescoop.com/2022/10/26/dod-creates-new-jadc2-integration-office-puts-cdao-in-charge-of-data-integration/. Accessed 30 Jan 2024.

Roland, Alex, and Philip Shiman. 2014. *Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983–1993*. Cambridge, MA: The MIT Press. https://ondoc.logand.com/d/2721/pdf. Accessed 30 January 2024.

Sayler, Kelley M. 2020. Artificial Intelligence and National Security. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45178. Accessed 30 Jan 2024.

Scharre, Paul, and Megan Lamberth. 2022. Artificial Intelligence and Arms Control. Center for a New American Security. https://www.cnas.org/publications/reports/artificial-intelligence-and-arms-control. Accessed 30 Jan 2024.

Schuchmann, Sebastian. 2019a. History of the first AI Winter. Towards Data Science. https://towardsdatascience.com/history-of-the-first-ai-winter-6f8c2186f80b. Accessed 30 Jan 2024.

———. 2019b. History of the second AI winter. Towards data science. https://towardsdatascience.com/history-of-the-second-ai-winter-406f18789d45. Accessed 30 Jan 2024.

Segal, Adam, and Gordon M. Goldstein. 2022. Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet. The Council on Foreign Relations. https://www.cfr.org/report/confronting-reality-in-cyberspace. Accessed 30 Jan 2024.

Simonite, Tom. 2021. 3 years after the Project Maven Uproar, Google Cozies to the Pentagon. Wired. https://www.wired.com/story/3-years-maven-uproar-google-warms-pentagon/. Accessed 30 Jan 2024.

Spataro, Noah, Trevor Phillips-Levine, and Andrew Tenbusch. 2022. Winged Luddites: Aviators are the biggest threat to carrier aviation. War on the rocks. https://warontherocks.com/2022/01/winged-luddites-aviators-are-the-biggest-threat-to-carrier-aviation/. Accessed 30 Jan 2024.

Stone, Mike. 2022. U.S. Congress moves to boost Biden's record defense budget. Reuters. https://www.reuters.com/world/us/us-congress-moves-boost-bidens-record-defense-budget-2022-06-22/. Accessed 30 Jan 2024.

Strout, Nathan. 2020. Inside the Army's futuristic test of its battlefield artificial intelligence in the desert. C4ISRNET. https://www.c4isrnet.com/artificial-intelligence/2020/09/25/the-army-just-conducted-a-massive-test-of-its-battlefield-artificial-intelligence-in-the-desert/. Accessed 30 Jan 2024.

Tarapore, Arzan. 2021. AUKUS is deeper than just submarines. Stanford Freeman Spogli Institute for International Studies. https://fsi.stanford.edu/news/aukus-deeper-just-submarines. Accessed 30 Jan 2024.

The White House. 2022a. Indo-Pacific strategy of the United States. https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf. Accessed 30 Jan 2024.

———. 2022b. The Department of Defense Releases the President's Fiscal Year 2023 Defense Budget. https://www.defense.gov/News/Releases/Release/Article/2980014/the-department-of-defense-releases-the-presidents-fiscal-year-2023-defense-budg/. Accessed 30 Jan 2024.

———. 2022c. National Security Strategy. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf. Accessed 30 Jan 2024.

U.S. Air Force. 2021. NORAD, USNORTHCOM lead third Global Information Dominance Experiment. https://www.af.mil/News/Article-Display/Article/2703548/norad-usnorthcom-lead-3rd-global-information-dominance-experiment/. Accessed 30 Jan 2024.

U.S. Government Publishing Office. 2019. National Defense Authorization Act for Fiscal Year 2020. https://www.govinfo.gov/content/pkg/PLAW-116publ92/html/PLAW-116publ92.htm. Accessed 30 Jan 2024.

Vincent, James. 2017. Putin says the nation that leads in AI 'will be the ruler of the world'. The Verge. https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world. Accessed 30 Jan 2024.

Vincent, Brandi. 2022. Amid a high-stakes transition, questions linger about Project Maven's future management. DefenseScoop. https://defensescoop.com/2022/09/09/amid-a-high-stakes-transition-project-mavens-future-management-remains-unclear%ef%bf%bc/. Accessed 30 Jan 2024.

Wasserbly, Daniel. 2021. AUSA 2021: US Army's 'Scarlet Dragon' project aims to use AI, satellites for targeting. Janes. https://www.janes.com/defence-news/news-detail/ausa-2021-us-armys-scarlet-dragon-project-aims-to-use-ai-satellites-for-targeting. Accessed 30 Jan 2024.

Zhang, Daniel, et al. 2021. The AI Index 2021 Annual Report. AI Index Steering Committee, Human-Centered AI Institute, Stanford University. https://aiindex.stanford.edu/ai-index-report-2021/. Accessed 30 Jan 2024.

———. 2022. The AI Index 2022 Annual Report. AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University. https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf. Accessed 30 Jan 2024.

Zwetsloot, Remco, et al. 2021a. The immigration preferences of top AI researchers: New survey evidence. Centre for the Governance of AI. https://www.governance.ai/research-paper/the-immigration-preferences-of-top-ai-researchers-new-survey-evidence. Accessed 30 Jan 2024.

———. 2021b. Skilled and mobile: Survey evidence of AI researchers' immigration preferences. Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society: 1050–1059. https://arxiv.org/abs/2104.07237. Accessed 30 Jan 2024.

When the Teeth Eat the Tail: Defence AI in Canada

Robert C. Engen

Canada is in trouble when it comes to defence artificial intelligence (AI) and is positioned to become a cautionary tale of the early AI years. Although Canada is well-placed globally for AI research, development, funding, and implementation, the country's defense force is badly positioned to embrace digital transformation. This is a consequence of the organization's structure, history, and culture, rather than of technical shortcomings. Canada's positive advances in AI are minor, fleeting, and scattershot, not representing systematic effort, and enjoying little priority. These positive advances are hardly worth talking about in comparison to the problems, which are potentially insurmountable. This chapter deviates slightly from the other chapters in this volume by presenting the historical background of Canada's legacy problems for defense AI, before proceeding with assessments of the current state of defense AI in Canada.

The Department of National Defence (DND) is the arm of Canada's federal public service related to defense. The Canadian Armed Forces (CAF) are the country's uniformed military services. The "Defence Team" refers to both DND and the CAF, as well as other defense stakeholders.

1 Background: Canada's Legacy Problems for Defense AI

Three historical developments heavily influence how DND/CAF behaves as an organization. First, a cultural overemphasis on mission success and operations primacy has contributed to a dysfunctional organizational mentality. Second, the transformation from three services to one service (unification) in the 1960s had the long-term effect of creating an enduring organizational fragmentation. Third,

R. C. Engen (✉)
Deakin University and the Australian War College, Canberra, Australia
e-mail: rob.engen@deakin.edu.au

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_3

drastic budget and personnel cuts in the 1990s destroyed much of the organization's collective memory and left it without the ability to manage its own data and information. None of these problems is directly linked to AI, but they collectively have created a culture that possesses major limiting factors for the implementation of AI systems in Canada's defense establishment.

1.1 Cultural Problems

One of the basic assumptions of the Canadian Armed Forces is the idea of "operations primacy" or "mission first": that mission success receives priority over everything else (Hansen 2022). This assumption dates back to the Second World War, and recently operations primacy was reaffirmed as a professional expectation in the new CAF professional ethos (Department of National Defence 2022a: 33; Leslie 2011). This expectation promotes a "get-it-done" mentality privileging mission accomplishment over wellbeing, and even accepting a degree of wilful disobedience so long as results are achieved (Rozema-Seaton 2019: 15). There is very strong cultural pressure in Canada for every mission to be no-fail. Justice Louise Arbour's (2022) external review of the CAF noted that, "the long-established way of doing business in the CAF is anchored in operational imperatives that are often nothing more than assumptions" (Arbour 2022: 9).

The basic assumption of operations primacy has often been illustrated using the biological metaphor of "teeth and tail," imagining the CAF as an animal whose fighting components are the "teeth," while the supporting functions of the organization are the "tail." The metaphor lionizes deployable, operational fighting elements, while denigrating and even vilifying the supposedly non-essential "tail." The metaphor justifies cuts to "tail" areas (headquarters, administration, record keeping, data analysis, etc.) and assumes that it is always preferable to cut the "tail" of the CAF instead of its "teeth." "We are going to have to reduce the tail of today while investing in the teeth of tomorrow," wrote Canadian Army Commander Lieutenant-General Andrew Leslie in a 2011 capstone report on one of the CAF's failed transformation efforts (Leslie 2011).

This basic assumption persists for perfectly logical reasons. Unlike the United States, where the armed services wield significant political clout, the CAF has little independence and no meaningful ability to shape political decision-making or strategy (English 2004: 88–89). The ability to complete those missions assigned to it in superb fashion is a protective mechanism for the CAF: government and public indifference to the military is so great in Canada that mission failure could feasibly provoke fresh rounds of budget cuts. The "teeth" must always be kept sharp.

However, the metaphor of the teeth and the tail is a faulty one. No higher animal consists only of teeth and tail; biological organisms are complex systems of systems, the most important of which is the guiding intelligence in the central nervous system. As historian Allan English has asked, "Is it better for the animal to lose a tooth or two, or a significant part of its brain?" (English 2016: 202–203). However

understandable it may be, the primacy of operational requirements and the persistent privileging of "teeth" over "tail" has far-reaching consequences.

Operations primacy means that those elements of the CAF that are immediately deployable on operations, and specifically those that fulfil direct combat functions, are the most esteemed by the organization. The system rewards people and perpetuates structures that are operationally focused. The CAF suffers an organizational addiction to mobility, and expects key people (especially leaders) to move jobs every 2 to 3 years (Wakeham 2022). Promotions in the CAF hinge upon achieving short-term goals and then moving on, and privileges breadth and variety in postings—particularly on operations—over the development of expertise or depth. The CAF's culture has inadvertently rewarded dysfunctional behavior. The cultivation of technical expertise in the CAF is not part of a career path that leads to promotion, and those who stay "locked" in jobs or locations for extended periods forfeit all organizational advancement (Department of National Defence 2024: 22; English 2011: 11). The CAF demands a willingness from its members to move jobs constantly to meet short-term operational imperatives.

1.2 The Long Hangover of Unification

Unification was a cost-saving program of the 1960s that transformed Canada's traditional three military services (the Royal Canadian Air Force, the Royal Canadian Navy, and the Canadian Army) into one unified service containing different subordinate Commands. This restructuring was unprecedented among the military forces of the Western democracies, and was closely examined by policymakers in allied countries; notably, none of them followed the Canadian example (Irwin 2002: 41). Ironically, after dispensing with the three "strong services," unification eventually created dozens of semi-autonomous, highly siloed organizational entities—the "Level 1 s" (L1s). The head of each L1 reports directly to the two "Level Zeros" above them: either the uniformed Chief of the Defence Staff (CDS), the Deputy Minister (DM) of National Defence, or both. The L1 system can charitably be described as federated, and more accurately as balkanized. Each L1 typically pulls decision-making authority together at the top of its own silo, to ensure control and to minimize the influence of both subordinate elements and enterprise-wide initiatives (Author Correspondence with LGen R. Crabbe 2022).

The way that data and information are handled within DND today—that is to say, poorly—is a consequence of this history. The L1s all operate semi-autonomously and have separate IT systems, independent procurement processes, and differing data requirements (Department of National Defence 2019: 29). As of 2019, the civilian Assistant Deputy Minister (Information Management) (ADM(IM)) "provides IM direction, procedures, and enterprise tools, [but] each L1 is responsible for implementing IM plans and activities within their respective operational areas" (Chief Information Officer 2019: 8).

1.3 "Records-Keeping Bedlam"

The second highly relevant development on Canada's current path was the significant budget cuts and reductions in personnel following the end of the Cold War. The 1994 cut reduced the size of Canada's Regular Forces by 32%, cashing out the peace dividend by reducing active military personnel from 89,000 to 60,000 as part of the Forces Reduction Program (FRP). However, there was a concurrent sharp rise in operational tempo, and many new high-intensity deployments of troops to the former Yugoslavia. Because that operational tempo had to be sustained and the government needed infantry battalions in Croatia and Bosnia-Herzegovina, the cuts were not distributed evenly.

In order to keep the fighting power of the organization sharp, the cuts fell on the back end, reducing administration and headquarters functions by half (Chief Review Services 2001a: 1). As Canadian historians wrote two decades ago: "In the relentless paring of military personnel in the [CAF] and civilian staff in [DND], inevitably many of the first positions to go have been the information handlers such as clerks, secretaries, archivists, and librarians," whom the FRP deemed over-staffed and expendable in comparison to combat arms operators. These were the people who constituted the record-keeping and information management (IM) backbone of Canada's defense establishment. With them gone, the well-disciplined analog record-keeping systems inherited from the Cold War military disintegrated, just as digital technology became widespread. The CAF let these personnel go before the IM tools were in place to support a smaller staff (Chief Review Services 2001b). E-mail and instant messaging took root as the preferred communication media, allowing everyday business to bypass a crumbling centralized record-keeping system (Lizotte 2019: 7). By 2001, observers described DND/CAF as already being in a state of "records-keeping bedlam" (English et al. 2001: 479). It has never recovered.

Canada's DND/CAF is probably two decades behind where it needs to be on information management. The CAF's 2022 *Digital Campaign Plan* accurately described the organization as being at the lowest stage of digital maturity:

> Legacy analog systems and processes, stove-piped capability development, and generally low levels of digital literacy. Members of the CAF struggle to access data, analyse the data, and to generate decision-ready information supported by descriptive analytics. Data manipulation is predominantly done manually. Users adjust their behaviour and actions to existing systems and processes. (Canadian Armed Forces 2022: 6)

As of 2024, the CAF still has no centralized record-keeping system, and its inability to manage its own information has been the source of repeated scandals and professional malpractice for three decades (Desbarats 1997: 59–70; Sharpe 2000; Sabry 2015: 33; Berthiaume 2021; Arbour 2022: 54–55). Due to operational imperatives, key information managers within the L1 entities are typically double-hatted from their regular jobs, and are not dedicated specialists. Some powerful digital tools are available enterprise-wide within the CAF, but user training and instruction are not. Most areas of the CAF's information ecosystem are effectively ungoverned, with

networked shared drives, websites, SharePoint instances, mail servers, and document repositories holding huge volumes of ad hoc, disorganized content. "The result," one CAF information management officer has written, "is an information environment which is untrustworthy, inefficient, that frustrates users, and limits the value the DND/CAF can glean from its own information" (Lizotte 2019: 2).

These problems must be addressed with culture change, as there is at present no culture of "working horizontally" among L1s at DND/CAF. However, the current structure, processes, and incentives are working against the necessary changes. In its 2022 digital strategy, the Canadian Army correctly described the current era in DND/CAF as an ongoing "digital winter" (Canadian Army 2022: 12). And external reviewer Louise Arbour strongly condemned the CAF's information systems, writing that, "a more thoughtful approach would ensure that the sum of each organization's data represents the whole picture … [but] with the current silo model focused on achieving individual organizational mandates, this is simply not possible" (Arbour 2022: 52).

1.4 Consequences of these Legacy Problems

These historical developments have contributed to a Canadian military culture and organization with notably toxic characteristics, and this presents substantial barriers for the adoption of defense AI. To return to the "tooth-and-tail" metaphor: when confronted with the choice of what to cut, the DND/CAF animal has historically preferred lobotomy to dentistry, shedding brain matter rather than risk losing "teeth." This attitude, married to the cloistered, siloed structure of the organization and the dystopian state of its IM, is anathema to building a meaningful AI capability, especially at scale. By DND/CAF's own reckoning, the basic prerequisites for understanding, developing, and fielding AI systems include research and development (R&D), agile project management, software as an essential capability equal to hardware, massive investment in digital infrastructure and information management, and application development across the enterprise. While DND has some promising R&D capabilities, none of the other elements are close to being met.

These historical, cultural, and organizational problems shape everything about the potential for Canada to develop a meaningful AI capability for its armed forces.

2 Thinking About Defense AI

The real tragedy of the legacy problems discussed above is that informed elements within DND/CAF are fully cognizant of the transformations that are necessary to implement defense AI. A significant amount of intellectual heavy lifting has been done on incorporating AI into the future of the CAF. In all cases where they have adopted explicit stances on AI, DND/CAF entities have maintained a commitment

to keeping humans "in or on 'the loop'" when it comes to decision-making, and there is no thought at present to permitting fully autonomous offensive weapon systems that "complete the loop" and engage targets without human oversight. Attempting to ensure that combat remains an activity featuring meaningful human involvement is a cornerstone of Canadian AI thinking (Department of National Defence 2024: 7). The CAF's most-used leadership framework, the Pigeau-McCann Model, explicitly deals with how "cybernetic control" systems involving some degree of autonomy are feedback mechanisms, fundamentally lacking the properties of command (Pigeau and McCann 2002: 54).

Thinking about defense AI begins at the top, with Canada's 2017 defense policy, entitled *Strong, Secure, Engaged* (*SSE*), which enshrines many of its formal military aspirations for the future. According to *SSE*:

> Canada is committed to employing new technological capabilities in a manner that rigorously respects all applicable domestic and international law, and ensures full oversight and accountability. As a country that has led several efforts to advance human rights and establish new international norms, Canada is also well-placed to advocate among international partners for the highest standards. (Department of National Defence 2017: 55)

After *SSE*, the highest-level document concerning AI is the DND/CAF *Artificial Intelligence Strategy*, written in 2022 but only approved in early 2024, which is a comprehensive and soul-searching examination of the path towards defense AI for Canada's military. It envisions five lines of effort that will allow DND/CAF to become an "AI-enabled organization" by 2030, "with ethical, inclusive, and trusted AI for interoperability and advantage in the battle space and improved stewardship in the corporate space." These lines of effort are: (1) Key Capabilities; (2) Culture; (3) Ethics, Safety, and Trust; (4) Talent and Training; and (5) Partnerships (Department of National Defence 2024: 1). The *AI Strategy* is an outstanding effort to confront the many problems facing DND/CAF in this space. However, it has some problems of its own. The *AI Strategy*, like other organization-wide strategies before it, operates on the assumption of the siloed L1 structure of DND/CAF and hesitates to even broach the topic of overarching governance, preferring to devolve responsibility and authority to the L1s. No one entity is responsible; which in Canada often means that nobody is responsible. The authors completed the *AI Strategy* in final draft form in mid-2022, but it languished on the desks of distracted "Level Zeros" awaiting signatures for 18 months. This is a poor start for a strategy meant to modernize Canada by 2030; it is suggestive of what kind of priority AI can expect within a department filled with conflicting, competing demands between L1s.

The environmental L1s (land, air, maritime, special forces) have also put thought individually into their future integration of AI within their siloes. Since this is the level where implementation is most likely to occur, it is worth examining overviews of the thinking about AI on the part of the Canadian Army, Royal Canadian Air Force, Royal Canadian Navy, and Canadian Special Forces Command:

- *The Canadian Army*

The Canadian Army is the most forward-thinking of the environmental L1s concerning AI. In its 2020 *Modernization Strategy*, the Army stated that it is their responsibility "to examine the potential of AI and machine data [sic] to transform some aspects of land operations, including exploiting data and information to produce intelligence and predictive modelling to support decision-making" (Canadian Army 2020: 51). The Army's more recent addendum, the 2022 *Modernization Vital Ground: Digital Strategy*, reflects thinking on technological drivers, committing to the concept of "human-machine teaming" (integrating soldiers and autonomous systems) and the vital need to utilize "Big Data" in to process more information while decreasing the cognitive load on humans (Canadian Army 2022: 9). The Army's Land Warfare Centre has written thoughtfully on how the adoption of AI by the Army "must proceed with caution and be informed by a realistic set of limits … nonetheless, if pursued and applied carefully, much of what AI offers generally aligns well with [Army] requirements" (Priems and Gizewski 2021: 43).

- *The Royal Canadian Navy (RCN)*

The RCN issued its *Digital Navy* strategy in 2019, addressing a broad range of technologies, including AI, machine learning, automation, and data analytics. *Digital Navy* establishes the need to cultivate a "data-centric mindset" in the RCN, as "quality data will be a fundamental enabler" of success going forward. The RCN stresses three categories of defense AI applications: (1) Autonomous Things (advanced robots, autonomous vehicles, intelligent agents); (2) Augmented Analytics (using AI to enhance analysis of structured and unstructured data); and (3) AI-Driven Development (using AI in design process for naval equipment and systems). The *Digital Navy* strategy concludes with the promise to establish a Digital Navy Office "to facilitate the implementation and evolution of this initiative," with a mandate including program alignment, communications, performance measurement, look-ahead functions, process enhancement, training, and contract vehicles (Royal Canadian Navy 2020: 6–17). The plan apparently remains intact, though no updates have been provided by the RCN on its progress.

- *The Canadian Special Operations Forces Command (CANSOFCOM)*

The CANSOFCOM enjoys special privileges in terms of access, autonomy, and authorities that allow it to sidestep bureaucracy better than other L1s. In its 2020 strategic plan, *Beyond the Horizon*, CANSOFCOM provided broad details on Gradient Ascent, a digitalization and data analytics initiative designed to ensure the same competency in the digital space that its operators have achieved in the kinetic space (Canadian Special Operations Forces Command 2020: 31). Gradient Ascent saw CANSOFCOM investing in a complete modernization of its data architecture to permit data analytics at scale, supporting streams ranging from operations to intelligence to enterprise management, providing dynamic analytics products leveraging data from CANSOFCOM IT systems and sensors. Gradient Ascent reportedly "changed the game" in terms of how CANSOFCOM develops software and solves

data problems through insourcing (Gonthier 2022b: 3–4). Little information is publicly available.

- *Royal Canadian Air Force*

The last environmental command, the RCAF, has published the least on AI. The organization's *Future Air Operating Concept* is almost a decade old. Recent Aerospace Warfare Centre publications offer few comments on technology and nothing specifically about AI. (Goette 2020). The *RCAF Journal* has published a few articles relating to AI between 2019 and 2022, but has just entered a three-year hiatus due to funding shortfalls. Most of the RCAF's work on AI—if it is happening—is being done outside the public eye.

3 Developing Defense AI

Canada represents a potentially rich site for AI research and development, and for decades the country has been a locus of AI work. Some of the seminal work in the field came from academics at Canadian universities. The Government of Canada's *Pan-Canadian Artificial Intelligence Strategy* has invested hundreds of millions in AI research institutes, education, and student talent development. However, Canada's relative position in the world of AI research continues to drop, and Canadians only hold about 0.5% (and dropping) of the world's nearly 1 million AI-related patents (OECD AI 2021). Between 2018 and 2022, one-third of Canadian AI firms either permanently closed or were acquired by foreign firms (Araya 2022: 5).

The main L1 within the Canadian defense community that is working on AI technologies today is Defence Research and Development Canada (DRDC). DRDC's role within the Defence Team is to provide leadership and advice on issues of science and technology, to engage and collaborate with a network of domestic and international partners, and to exercise functional authority to "ensure coherent of defence and security science, technology and innovation investments" (Defence Research and Development Canada 2022). The organization serves as the bridge between Canada's AI potential and its defense applications. DRDC defense scientists carry out research internally on behalf of or in partnership with other L1s, and commission contract research from approved third-party vendors, sometimes working in partnership with them. DRDC has invested heavily in research related to AI and machine learning for decades, and a considerable corpus of relevant work associated with and funded by DRDC has accrued: 45 defense research projects and reports relevant to AI are on file as being completed between 2009 and 2022.

Presently, the main route for pursing defense AI within DND/CAF is through DRDC's Innovation for Defence Excellence and Security (IDEaS) program, announced in 2017. The intention behind IDEaS is to "bring together academics, industry, and other partners to form collaborative innovation networks." IDEaS is a competitive funding model intended, in part, to bypass the cumbersome and archaic

CAF procurement system (discussed later in this chapter) by streamlining academic and industry technical cooperation with the military. According to DRDC, seven in every ten proposals from academia and industry for IDEaS grants each year involve AI components (Directorate S&T Strategic Partnerships 2022).

Many of the IDEaS related to defense AI are through the program's Competitive Projects funding mechanism. "The Competitive Projects element funds projects fast," according to the program website. "It advances promising technology quickly through a phased approach." It begins with up to 6 months of funding, after which there is an option for a further 12 months of funding at a much higher rate. After this, DND also has the option of pursuing the project further using non-IDEaS funding through Science & Technology Solution Advancement. (National Defence Undated) IDEaS's "Spot the Hack" challenge, issued on behalf of the RCAF, studies cyber vulnerabilities in the Military Standard 1553 bus used by RCAF aircraft avionics networks; many of the bids which received first- and second-round funding, including those from CAE, Palitronica, and Queen's University, included AI learning agents for intrusion detection purposes (National Defence 2022).

Outside of DRDC, a potentially significant development avenue for AI is a relatively new DND program called "Mobilizing Insights in Defence and Security" (MINDS). MINDS is governed by DND's office of the Assistant Deputy Minister (Policy) responsible for the development and management of defense policymaking. The MINDS program is based on the idea that "policy and decision-making are strengthened when assumptions are challenged, and diverse viewpoints are considered." MINDS provides collaboration opportunities between DND/CAF and the academic defense and security community, allowing for bespoke briefing engagements, targeted engagement grants, support for emerging scholars, a "rapid response mechanism" for addressing evolving priorities, and the creation of Collaborative Networks. (Mobilizing Insights in Defence and Security (MINDS) 2022). One Collaborative Network, the Security-Policy Nexus of Emerging Technology (SPNET) based out of Concordia University in Montreal, specifically focused on AI as an emerging policy issue.

The lynchpin of Canada's defense AI ecosystem, however, are the private interests working as contractors for DND/CAF. Given the internal problems facing Canada's military, the importance of working with trusted AI vendors is magnified. The Treasury Board of Canada Secretariat maintains a list of interested AI suppliers. Federal departments can use these pre-qualified suppliers to launch streamlined procurement processes for technologies and services, for up to CAD9M before taxes. As of December 2023, there are 121 companies on the Treasury Board List, ranging from very small startups to large enterprises such as Palantir Technologies, Amazon Web Services, IBM Canada, and Microsoft Canada (Treasury Board of Canada 2022).

4 Organizing Defense AI

The most pressing question for organizing defense AI in Canada involves governance: who owns the AI problem, and to whom are they beholden and responsible? Canada's DND/CAF is reluctant to commit itself to governance standards for the use of AI and is equally reluctant to propose firm internal governance models. Given the department's "federated" L1 system, the lack of broad governance mechanisms to organize the use of AI will likely default to each L1 within DND/CAF doing as it pleases in developing AI, with little higher accountability.

4.1 External Governance for AI

Federal entities in Canada are bound by the government's 2019 Treasury Board Directive on Automated Decision Making, which ensures that AI systems are used responsibly by government institutions (Treasury Board of Canada 2019). This Directive is a supposedly mandatory policy instrument applied throughout federal government departments. The Directive applies to the use of all systems that make, or assist in making, recommendations or decisions. As part of the Directive, every department must complete an Algorithmic Impact Assessment (AIA) of any AI system prior to production, or whenever system functionality changes. The AIA assesses a systems' impact based upon factors such as the systems' affect on the rights, health, wellbeing, and interests of individuals and communities, as well as sustainability, reversibility, and duration (Riley et al. 2022). Based upon responses to risk and mitigation questions, the AIA assigns an impact rating and requires publication of the AIA on an open government portal. Having a person make the final decision in a system does not exempt departments from complying with the Directive; any system that provides advice to public servants who make the final decision is within its scope (Beshaies and Hall 2021).

The Directive on Automated Decision Making appears robust on paper but contains escape clauses that dilute its effectiveness. The Directive applies only to the "external" eservices of government—services offered to individuals or organizations *by* government—and does not apply internally within departments, a "glaring oversight" in the governance regime (Scassa 2022). The team carrying out a periodic review of the Directive recommended expanding the scope to include internal as well as external systems (Bitar et al. 2022).

DND/CAF does not believe the Directive applies to it, and thus far has ignored it. DND/CAF's *AI Strategy* notes that any new AI systems used by DND should be developed and implemented "in accordance with applicable laws, policies, and guidelines." However, it also warns that "because of their application to defence and national security, many DND/CAF use cases [of AI] will fall outside the guidance provided by the Treasury Board Secretariat, and the gap between the development of AI and other emerging technologies and legislative and policy coverage only

continues to widen." The *AI Strategy* carefully discusses how it will be "aligned with" the Directive in considering risks, without actually stating that it is subject to the Directive (Department of National Defence 2024: 19–21). Recent cases of DND using AI-driven hiring services to help fill executive positions within the department became a small scandal when Canada's Privacy Commissioner accused DND of skirting the rules surrounding the use of AI. DND did not submit an Algorithmic Impact Assessment to the Treasury Board: a DND spokesperson claimed that because "final decisions" were not being made by AI, the department did not feel obliged to complete the Treasury Board's algorithmic assessment (Cardoso and Curry 2021). This excuse was neither in the spirit nor the letter of the Directive on Automated Decision Making. In fact, as of 2023 DND/CAF have never made a submission to the Algorithmic Impact Statement, strongly suggesting that DND will resist having AI governance decisions imposed by other parts of the federal government.

4.2 Internal Governance for AI

The *AI Strategy* does not state how governance of AI will function internally to DND/CAF, though there are hints. Most likely the federated L1 entities will be left to govern their own uses of AI. The *AI Strategy* proposes the creation of a Defence AI Centre of Excellence for Canada to "accelerate AI experimentation and scaling across the Defence enterprise," creating a hub of AI expertise. However, centers of excellence are increasingly commonplace and establishing them falls under Mme Arbour's category of the "flurry of activities" that DND/CAF tends to do that do not necessarily accomplish anything. The AI Strategy does not propose to actually invest this center of excellence with governance responsibilities. Instead, it argues that DND/CAF must "Vest decision authorities for AI at the lowest appropriate level to encourage innovation." Given how Canada's military works, the "lowest appropriate level" will mean the L1s.

The office of the Assistant Deputy Minister (Data, Innovation, Analytics) (ADM (DIA)) is in one L1 silo of DND, reporting directly to the Deputy Minister of National Defence. The office of Assistant Deputy Minister (Information Management) (ADM(IM)) and Assistant Deputy Minister (Defence Research and Development Canada) are in different siloes. On 6 December 2022, DND announced the removal of the ADM(DIA) office as an L1, merging it with the Directorate of Knowledge and Information Management (DKIM) under the ADM(IM) to stand up the Digital Transformation Office (DTO). The ADM (IM) L1 is now called the Chief Information Office and is charged with managing both IM and data analytics enablement "in support of initiatives like machine learning and artificial intelligence" (Matthews 2023). CAF insiders suggest that the ADM(DIA) had not accomplished anything since it was stood up in 2017 and will be little missed, so this reorganization may correct some of the divisions over IT that have plagued the organization.

Perhaps with cross-cutting, general-purpose capabilities such as AI, there is nobody in Canada who can lead radical change except the "Level Zeros." The thinking within DND/CAF may well be that trying to govern AI is like trying to govern electricity, and this may prove to be the correct interpretation. However, it seems equally likely that the "balkanized" character of DND/CAF's organization means that devolving power and responsibilities to the L1s was likely to be the outcome no matter what, and it is not necessarily aligned with good practices. The question of internal governance and organization for AI within DND/CAF is therefore an extremely difficult one.

5 Funding Defense AI in Canada

The Government of Canada has spent lavishly to develop a thriving homegrown AI ecosystem. As mentioned earlier, DND's Defence Research and Development Canada (DRDC) is the primary delivery agent for defense science and technology investments, and their main vehicle has been the Innovation for Defence Excellence and Security (IDEaS) program. The government has committed to investing CAD85M per year for 20 years into IDEaS, significantly exceeding the funding for their civilian and commercial Pan-Canadian Artificial Intelligence Strategy. IDEaS allows for five funding mechanisms to assist Canadian "innovators" in addressing defense issues: competitive projects up to CAD1.2M; "Innovation Networks" of up to CAD$1.5M; contests on approved topics; sandboxes for field testing; and test drives for high-readiness ideas.

The key advantage of IDEaS initiatives is that they individually involve quite small expenditures. In Canada, the Treasury Board has a CAD10M threshold for its Organizational Project Management Capacity level, meaning that a project valued less than CAD10M "will be exempt from much of the oversight and rigour" of the standard procurement system and does not need to prepare a project complexity and risk assessment. This is an extremely important point. AI projects valued at less than CAD10M are quite easy; anything beyond that becomes an order of magnitude more difficult (Bedley 2021: 39). The IDEaS initiative is vital because of the procurement context that it has been designed to bypass.

5.1 Canada's Procurement Disaster

Canada's DND has, for over a decade, been effectively disabled from procuring major technological systems. This is part of the wider, slow-motion disaster that is Canadian defense procurement. Beginning in 2008, when significant new capital investments occurred, major capital projects became "jammed up" and have never become unstuck. 70% of procurement contracts for Canada are now overdue or seriously delayed. The procurement system requires the achievement of concord

between three different government departments. Making matters worse, Canada's Treasury Board (rightly) deems DND a fiscally risky institution and has forced the adoption of manufacturing industry best practices and standards on the military procurement process, meaning that all projects must follow the same Project Approval Directive (PAD). This process is also designed to prioritize investment in the Canadian defense industry over actually building the capabilities of the armed forces. A recent study showed that the average length of information technology-related procurement projects in DND was 9.6 years, with some IT projects open for over 16 years.

The PAD can bypass much of its own process when DND decides there is an Urgent Operational Requirement (UOR) that streamlines procurement to address short-term operational deficiencies. However, the UOR approval requirements "demand that the project directly affect combat operations and contribute to a life-saving capability." This makes the UOR ideal for CAF operational requirements but there is no chance that such a mechanism can be used to help with the broader digital transformation.

There are recent signs that DND/CAF is hoping to create new, more expansive relationships with industry partners to speed up procurement. This shows promise, but will require significant shifts in mindset and the ceding of some elements of control of process by DND/CAF (Fawcett 2023).

The *AI Strategy* cites the need to improve the procurement process to support the development and acquisition of AI as a critical element of its plan, but this appears to be a forlorn hope. Procurement in Canada will not be fixed soon. Even if it was, money in DND/CAF flows towards improving tactical capabilities that allow the CAF's commands to maximize their fitness for operations on the near horizon, not towards more general, longer-term, or enterprise-wide capabilities. And so many of DND/CAF's aspirations for defense AI are likely going to have to cost CAD10M or less each if they want to be realized this decade.

6 Fielding and Operating Defense AI

There are few instances available in the unclassified realm of defense AI systems being fielded and operated within DND/CAF. Most projects are still being researched, under development, being tested, or finding limited tactical or business applications.

A few defense AI initiatives are certainly underway, as detailed by Canada's Open Government transparency site for procurement. These included a noncompetitive contract for "artificial intelligence / inference systems (R&D)" awarded to IMRSV Data Labs in Ottawa in December 2021. No tender description is available, but products such as IMRSV's "Anvil Crucible" intelligence fusion platform use machine learning to automate data analysis tasks such as establishing relationships between entities and making predictions for key variables (IMRSV Data Labs 2022). This is almost certainly the software that has been used by the CAF's Joint

Targeting Intelligence Centre, and was employed in support of the evacuation of Afghan personnel after the fall of Kabul in 2021, discussed below (Department of National Defence 2024: 29).

Operations primacy continues to shape Canada's investment priorities. In its recent Modernization Strategy, for instance, the Canadian Army decided to prioritize the modernization of their tactical C4ISR (command, control, communications, computers, intelligence, surveillance, reconnaissance) capabilities, while putting off the investments needed to support a transformation into a "digital army" until a minimum 2025–2030 timeframe. Their stated assumption is that "modernization efforts must be undertaken concurrent to force employment on operations – there will be no pause" (Gonthier 2022a: 2–3; Canadian Army 2020: 26). This is a textbook application of the operations primacy assumption. The C4ISR capabilities are certainly important and are likely to involve AI components; several ISR-related projects are going through the IDEaS process at present. However, these will be narrow tactical applications of the technologies, embedded within existing organizational stovepipes and without any wider integration or governance.

There are a few other AI systems that are now in service, or will be shortly, with DND/CAF today. The RCN has a large contract with Kraken Robotic Systems Inc., out of Newfoundland, to provide remote mine hunting and mine disposal equipment, and an additional contract for underwater sound equipment (Department of National Defence 2022b). This acquisition includes autonomous underwater vehicles and the use of Kraken's AquaPix synthetic aperture sonar that allows for embedded automatic target recognition and data exfiltration (Kraken Robotics Inc. 2022). Since 2016, DND has awarded large contracts to IBM Canada to provide both the Canadian Forces Health Services Group and the Canadian Institute for Military and Veterans Health Research with the data infrastructure and cognitive computing capabilities to conduct advanced "big data" analytics related to healthcare research for service members (Bélanger and Cramm 2016). The Calian Group consulting firm has also been awarded large sums for data remediation and marking of serially managed material, a project to make more DND assets machine-readable that has been ongoing, with stops and starts, since 2016 (Department of National Defence 2020).

One use case publicized by DND/CAF as an effective application of AI, however, is in fact an indictment of the organization's current data ecosystem. The *AI Strategy* cites the example of an AI tool (probably Anvil Crucible) which maps networked relationships. It reads:

> In 2021, CAF was presented with an urgent request from Immigration, Refugees and Citizenship Canada (IRCC) for the names of Afghan personnel who had worked for Canada and now needed evacuation. This data existed, but as large quantities of paper files that would take dozens of people hundreds of hours to review manually. With permission from JITC and support from the vendor, the team spent a weekend scanning the documents and used the tool to extract thousands of names for IRCC. (Department of National Defence 2024: 29)

While the story suggests that applying an "agile AI-based solution" was a major accomplishment, the problem it solved was entirely manufactured by the failure of

basic digitization and stove-piped information within DND/CAF. Perhaps this points the way towards what might be the best possible use of defense AI for Canada: rescuing the organization from its own poor practices.

7 Training for Defense AI

The Canadian Armed Forces are presently facing an existential threat in the form of a human resources crisis among uniformed personnel. As of December 2022, the CAF was 10,000 uniformed members short of its authorized strength, with a catastrophic 10% annual attrition rate (Hansen 2022). The Chief of the Defence Staff issued a directive on reconstitution was issued on 6 October 2022 that scaled back non-essential operations and activities to "recover and rebuild (reconstitute) the organization," but noted that the personnel shortfalls had already "severely impacted the organization's ability to deliver professional and collective training." The directive reads that "we will need to make difficult choices about our readiness levels, capacity for sustained operations, as well as our level of commitment to all activities, while continuing to deliver strategic effects for the [Government of Canada]" (Eyre and Matthews 2022). A year later, things are no better. In late November 2023, the commander of the Royal Canadian Navy gave a brutally honest assessment that the RCN was in a "critical state" and would be unable to meet its readiness commitments for the next year and beyond. This is the result of a severe shortage of sailors and technicians, over 20% in many roles. The commander affirmed that the CAF recruitment wing has failed to meet its targets for more than 10 years, and that current attrition rates are unsustainable (Ritchie 2023).

What does reconstitution mean for defense AI? The DND/CAF *AI Strategy* highlights that "Talent and Training" requires its own line of effort: "We must identify and plan for our workforce needs, we must cultivate AI readiness amount our existing people, and we must find new ways to bring critical skills into the enterprise – and to retain and use them" (Department of National Defence 2024: 22). However, this will be an uphill struggle. Recent polling has found low and declining levels of enthusiasm among Canadians for joining the CAF, which is mirrored in disastrously low recruiting and high attrition rates. While this creates serious problems along the breadth of the organization, they pose special problems for nurturing an internal talent pool with fluency in the discipline of AI. If the values and principles of DND/CAF do not appeal to prospective servicemembers with skills in AI and digital technologies, then the "Talent and Training" conundrum is likely unsalvageable, because those skills will fetch an unmatchable premium on the open market in North America.

The *AI Strategy* says that it will meet the talent and training challenge first with a review of DND/CAF workforce needs for AI: "identify the skills, competencies, and personnel required to implement AI successfully. This must include not only subject matter experts in AI, but also staff whose roles support the AI lifecycle, including civilian and military leadership." The *AI Strategy* also urges DND/CAF to

identify priority AI workforce needs and either develop or procure training curricula to meet them: "This review should consider training needs at all levels, and the exploration of new options for both academic and professional training to ensure a talent pipeline for future needs." Finally, it flags the urgent need to "Explore and identify processes to recruit and retain AI talent, and to utilize it where it is needed." Some of the solutions the document offers are the creation of technical Reserves, short-term exchanges, and more flexible career pathways allowing for the attraction of tech-savvy talent above entry level in the CAF (Department of National Defence 2024: 22–23). These are all potentially viable paths, and the *AI Strategy* does a good job identifying problems and systemic barriers.

The barriers, however, are likely too many. The assumption of operations primacy has far-reaching consequences for the training and posting cycles. Promotion at the mid-level ranks is disproportionately determined by success in commanding operations (Hansen 2022). Personnel in non-operations career trajectories are unlikely to "have legs" in the CAF rewards system and are unofficially barred from holding the seniormost leadership positions within the organization (Kelley 2020). "While the CAF recognizes its own need for AI skills," the DND/CAF *AI Strategy* confirms, "it often struggles to make use of those it already has. Members have described their specialization in AI and related fields as career-limiting and speak of having to choose between remaining within their technical field and [choosing] a career path that would lead to promotion" (Department of National Defence 2024: 22). It is therefore difficult to see how CAF will be able to train a reliable AI talent pipeline internally, particularly with uniformed servicemembers.

DND/CAF is already embroiled in the wicked problems of training and talent retention, which creates an unpromising milieu for harnessing defense AI. The special problems of talent retention in a hot tech market are aggravated by the CAF's basic assumptions of operations primacy and unlimited job mobility discussed earlier. Neither hard-won technical expertise in a specific field, nor a focus on computer science occupations are rewarded within the CAF. Changing that will require an overhaul of the rewards and promotions system, and such an overhaul will meet fierce resistance from vested interests. At minimum, DND/CAF may have to place more reliance upon the civilian public servants on the DND side of the organization, which creates a different set of problems. DND/CAF may have no choice but to seek external partnerships and contracting for their AI needs, as the development of an internal talent pipeline poses, at present, a major problem without obvious solutions on the horizon.

8 Conclusion

Technologies classified as AI are in use in Canada's Department of National Defence and Canadian Armed Forces today, and their incorporation will continue at a modest pace in the years to come. However, the organization faces serious challenges to any kind of digital transformation or large-scale adoption of defense AI systems. These

problems are primarily historical, cultural, and organizational, rather than purely technical. As a country, Canada is well-positioned to engage with the transformative effects of AI. The country's armed forces, however, are not.

Historical and cultural trends within the Canadian military have left the institution heavily decentralized, and its L1 organizations (including the main force employers) are stovepiped from one another, strongly preferring to develop capabilities in isolation. DND/CAF's enterprise-wide information management has been a disaster for three decades and the organization's data stewardship is a constant source of scandal and embarrassment. Progress in AI is uneven across the organization. Governance appears to be an afterthought. While agile procurement is possible for minor projects, right now it is extraordinarily challenging for projects above a certain threshold. Closer partnerships and heavy reliance upon commercial interests and industry are likely the only meaningful way forward, and these partnerships have historically been harder to achieve and maintain in Canada than in the United States (Department of National Defence 2024: 26–28).

What will defense AI look like in Canada over the next 10 years? Barring major culture and organizational change, it will likely look something like this: small-scale AI projects, spread throughout the L1 siloes, with almost no cross-pollination between them. These AI systems will be focused on hyper-specific operational and tactical uses cases faced by the various commands. The amount of computing hardware used in training cutting-edge AI models has increased by a factor of 10 billion since 2010 and is doubling every 6 months. This growth wildly outstrips improvements in hardware, and so AI labs are making up the difference by buying more chips. Costs for training high-end AI models are already astronomical (Scharre 2023: 35–37). DND/CAF will not keep up, particularly with a cap of roughly CAD10M for timely technology purchases. If the organization wants cutting-edge AI models, the digital infrastructure, training data, and learning model architecture for them will need to be sourced from outside the organization as DND/CAF information management practices will need reform before they can be of use at scale. DND/CAF will probably also need outsourced engineers to run them, since the future of cultivating internal tech talent within the CAF looks very bleak. Barring major change, it is difficult to see how Canada can even nominally keep a hand in the defense AI game without extensive new public-private partnerships, the sort that generally run counter to how Canadian defense procurement traditionally works. In short, something fundamental must change before Canada makes any serious advance towards integrative defense AI across its military institutions. Realistically, many fundamental things must change, and it seems unlikely that they will change in a great hurry. The fact that it took the "Level Zeros" eighteen months to sign off on the excellent DND/CAF *Artificial Intelligence Strategy* is suggestive of what kind of priority AI can expect going forward in a department crippled by so many conflicting demands and crises.

This brings us back to the "teeth-and-tail" metaphor for operations primacy. Although AI technologies are broad and cross-cutting, enabling them as strategic assets will require transformational investment in what is derogatorily referred to as the "tail" of the organization. In a small defense force such as Canada's, this will

require uncomfortable trade-offs. The idea that new combat equipment should be (further) delayed or cancelled in favor of back-end computing capabilities or enterprise-wide information management will be anathema to the L1s. But the DND/CAF "animal" of the metaphor is in deep trouble, and its teeth are falling out on their own for lack of strength in the rest of the organization. If the global adoption of defense AI proceeds on its present course, Canada is going to be left well behind both adversaries and allies. The list of what must be done is daunting, and almost every point on it will be contested. But Canada will mostly likely continue to muddle through as it presently is, developing minor tactical AI-related capabilities while neglecting the more serious problems until it can do so no longer.

References

Araya, Daniel. 2022. *Artificial Intelligence for Defence and Security*. Waterloo: Centre for International Governance Innovation.

Arbour, Louise. 2022. Report of the Independent External Comprehensive Review of the Department of National Defence and the Canadian Armed Forces. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/report-of-the-independent-external-comprehensive-review.html. Accessed 30 Jan 2024

Bedley, Kenneth P. 2021. Closing the Tech Gap: A CAF Startup Model for Digital Transformation. Canadian Forces College. https://www.cfc.forces.gc.ca/259/290/23/286/Bedley.pdf. Accessed 30 Jan 2024

Bélanger, Stéphanie, and Heidi Cramm. 2016. Canadian Military Healthcare Consortium Taps Analytics for More Comprehensive Research. https://www.ibm.com/blogs/think/2016/11/canadian-military-healthcare-consortium-adopts-analytics-for-deeper-research/. Accessed 30 Jan 2024

Berthiaume, Lee. 2021. Head of Sexual Misconduct Response Centre Says Complaints Against Military Brass Are a Sign of Progress. The Globe and Mail. https://www.theglobeandmail.com/canada/article-female-officer-quits-canadian-forces-sickened-by-leaders-alleged/. Accessed 30 Jan 2024

Beshaies, Benoit, and Dawn Hall. 2021. Responsible Use of Automated Decision Systems in the Federal Government. Statistics Canada. https://www.statcan.gc.ca/en/data-science/network/automated-systems. Accessed 30 Jan 2024

Bitar, Omar, Benoit Deshaies, and Dawn Hall. 2022. *3rd Review of the Treasury Board Directive on Automated Decision-Making*. Treasury Board of Canada Secretariat.

Canadian Armed Forces. 2022. Canadian Armed Forces Digital Campaign Plan. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canadian-armed-forces-digital-campaign-plan.html. Accessed 30 Jan 2024

Canadian Army. 2020. *Advancing with Purpose: The Canadian Army Modernization Strategy*. Ottawa: HQ Canadian Army.

———. 2022. *Modernization Vital Ground: Digital Strategy*. Ottawa: HQ Canadian Army.

Canadian Special Operations Forces Command. 2020. Beyond the Horizon: A Strategy for Canada's Special Operations Forces in an Evolving Security Environment. CANSOFCOM

Cardoso, Tom, and Bill Curry. 2021. *National Defence Skirted Federal Rules in Using Artificial Intelligence, Privacy Commissioner Says*. The Globe and Mail. https://www.theglobeandmail.com/canada/article-national-defenceskirted-federal-rules-in-using-artificial/

Chief Information Officer. 2019. *Defence Information Management Plan*. Ottawa: Department of National Defence.

Chief Review Services. 2001a. NDHQ 99: Review of Restructuring and Re-Engineering: Volume 1. 7050-10 (CRS). https://publications.gc.ca/collections/collection_2015/mdn-dnd/D58-83-2001-eng.pdf. Accessed 30 Jan 2024
———. 2001b. NDHQ 99: Review of Restructuring and Re-Engineering: Volume 3. 7050-10 (CRS).
Defence Research and Development Canada. 2022. Mandate. https://www.canada.ca/en/defence-research-development/corporate/mandate.html. Accessed 30 Jan 2024
Department of National Defence. 2017. *Strong, Secure, Engaged: Canada's Defence Policy 2017. Defence Policy*. Ottawa: Department of National Defence. http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf. Accessed 30 Jan 2024.
———. 2019. *The Department of National Defence and Canadian Armed Forces Data Strategy*. Ottawa: Department of National Defence.
———. 2020. Informatics Professional Services, Contract #W6381-170008/001/XG, Awarded to Calian Ltd. CanadaBuys Award Notices. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/w6381-170008001xg. Accessed 30 Jan 2024
———. 2022a. *Canadian Armed Forces Ethos: Trusted to Serve*. Kingston: Canadian Defence Academy. https://www.canada.ca/content/dam/dnd-mdn/documents/reports/The_Canadian_Armed_Forces_Ethos_Trusted_to_Serve_FINAL.pdf. Accessed 30 January 2024.
———. 2022b. Remote Minehunting and Disposal Systems, Contract #W8472-105270/001/QF, Awarded to Kraken Robotic Systems Inc. CanadaBuys Award Notices. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/w8472-105270001qf. Accessed 30 Jan 2024
———. 2024. *Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy*. Ottawa: Department of National Defence.
Desbarats, Peter. 1997. *Somalia Cover-Up: A Commissioner's Journal*. Toronto: McClelland & Stewart.
Directorate S&T Strategic Partnerships. 2022. Artificial Intelligence. PowerPoint Brief, Ottawa, September
English, Allan D. 2004. *Understanding Military Culture: A Canadian Perspective*. Montreal & Kingston: McGill-Queen's University Press.
English, Allan. 2011. Enabling Innovation in Canada's Army: Cultural Transformations and Military Effectiveness. Conference Presentation. Canadian Army Historical Workshop. Kingston
———. 2016. Sex and the Soldier: The Effect of Competing Ethical Value Systems on the Mental Health and Well Being of Canadian Military Personnel and Veterans. In *Military Operations and the Mind: War Ethics and Soldiers' Well-Being*, ed. Stephanie A.H. Belanger and Daniel Lagace-Roy, 191–208. Montreal & Kingston: McGill-Queen's University Press.
English, Allan, Angus Brown, and Paul Johnston. 2001. Are We Losing Our Memory? Decision Making in DND. In Canadian Military *History Since the 17th Century: Proceedings of the Canadian Military History Conference, Ottawa, 5–9 May 2000*, edited by Yves Tremblay, 473–480. Ottawa: Directorate of History and Heritage
Eyre, Wayne, and Bill Matthews. 2022. CDS/DM Directive for CAF Reconstitution. Department of National Defence. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/dm-cds-directives/cds-dm-directive-caf-reconstitution.html. Accessed 30 Jan 2024
Fawcett, Rick. 2023. Industry Support to the Reconstruction and Modernization of the Canadian Armed Forces. Vanguard. https://vanguardcanada.com/a-new-day-for-caf-industry-partnerships/. Accessed 30 Jan 2024
Goette, Richard. 2020. *Preparing the RCAF for the Future: Defining Potential Niches for Expeditionary Operations*. Astra: RCAF Aerospace Warfare Centre.
Gonthier, Nicholas. 2022a. *Accelerating the Canadian Army's Digital Transformation*. Toronto: Canadian Forces College.
———. 2022b. Building the CAF Digital Factory: A Guide for the Executive Leadership. Canadian Forces College. https://www.cfc.forces.gc.ca/259/290/24/286/Gonthier.pdf. Accessed 30 Jan 2024

Hansen, Ken. 2022. The Canadian Armed Forces Are Heading for a Titanic Collapse. The Globe and Mail. https://www.theglobeandmail.com/opinion/article-canada-military-shortage-crisis/. Accessed 30 Jan 2024

IMRSV Data Labs. 2022. Our Products: Anvil Crucible Defence Suite. https://imrsv.ai/products. Accessed 30 Jan 2024

Irwin, Anne. 2002. *The Social Organization of Soldiering: A Canadian Infantry Company in the Field*. PhD Thesis. Manchester: University of Manchester.

Kelley, Travis. 2020. "Correlation of Military Trade with Selection of Generals and Flag Officers." Master of Defence Studies Paper, Canadian Forces College. https://www.cfc.forces.gc.ca/259/290/22/286/kelley.pdf Accessed 23 May 2024.

Kraken Robotics Inc. 2022. Kraken Awarded $50+ Million Navy Contract for Royal Canadian Navy Minehunting Program. https://krakenrobotics.com/kraken-awarded-50-million-navy-contract-for-royal-canadian-navy-minehunting-program/. Accessed 30 Jan 2024

Leslie, Andrew. 2011. Report on Transformation 2011. Department of National Defence. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/report-on-transformation-2011.html. Accessed 30 Jan 2024

Lizotte, Ryan. 2019. *Learning to Swim in a Sea of Information: Improving Information Management in the Department of National Defence*. Toronto: Canadian Forces College.

Matthews, Bill. 2023. "Message from the Deputy Minister Regarding the Digital Transformation Office." The Maple Leaf. https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2022/12/message-deputy-minister-digital-transformation-office.html Accessed 23 May 2024.

Mobilizing Insights in Defence and Security (MINDS). 2022. Ottawa: Department of National Defence. https://www.canada.ca/en/department-national-defence/programs/minds.html. Accessed 30 Jan 2024

National Defence. 2022. Spot the Hack: Intrusion Detection Systems for Avionics Networks and Bus Technologies. Innovation for Defence Excellence and Security (IDEaS) Competitive Projects. https://www.canada.ca/en/department-national-defence/programs/defence-ideas/element/competitive-projects/challenges/spot-hack-intrusion-detection-avionics-networks-technologies.htmlion-detection-avionics-networks-technologies.html. Accessed 30 Jan 2024

———. Undated. Competitive Projects. Innovation for Defence Excellence and Security (IDEaS). https://www.canada.ca/en/department-national-defence/programs/defence-ideas/element/competitive-projects.html. Accessed 30 Jan 2024

OECD AI. 2021. Visualisations Powered by JSI Using Data from MAG. https://oecd.ai/en/data?selectedArea=ai-research&selectedVisualization=ai-publications-by-country-over-time. Accessed 30 Jan 2024

Pigeau, Ross, and Carol McCann. 2002. Re-Conceptualizing Command and Control. *Canadian Military Journal* 3: 53–64.

Priems, Geoffrey, and Peter Gizewski. 2021. Leveraging Artificial Intelligence for Canada's Army: Current Possibilities and Future Challenges. *Canadian Army Journal* 19: 40–51.

Riley, Alycia, et al. 2022. Bill C-27: A Depper Dive into Canada's Proposed Artificial Intelligence and Data Act. Gowling WLG. https://gowlingwlg.com/en/insights-resources/articles/2022/canada-s-artificial-intelligence-and-data-act/. Accessed 30 Jan 2024

Ritchie, Sarah. 2023. Canadian Navy in Critical State, Could Fail to Meet Readiness Commitments: Commander. The Canadian Press. https://www.cbc.ca/news/politics/canadian-navy-critical-state-1.7044267. Accessed 30 Jan 2024

Royal Canadian Navy. 2020. *Digital Navy: A Strategy to Enable Canada's Naval Team for the Digital Age*. Ottawa: Royal Canadian Navy.

Rozema-Seaton, Erik. 2019. BOXTOP 22: The Cost of Focusing on an Operational Culture. *Royal Canadian Air Force Journal* 8: 6–23.

Sabry, Omar. 2015. Torture of Afghan Detainees: Canada's Alleged Complicity and the Need for a Public Inquiry. Canadian Centre for Policy Alternatives https://policyalternatives.ca/publications/reports/torture-afghan-detainees. Accessed 30 Jan 2024

Scassa, Teresa. 2022. Comments on the Third Review of Canada's Directive on Automated Decision-Making. https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=354:comments-on-the-third-review-of-canadas-directive-on-automated-decision-making&Itemid=80. Accessed 30 Jan 2024

Scharre, Paul. 2023. What AI Means for Global Power. *Foreign Policy*: 35–41.

Sharpe, G.E. 2000. Executive Summary - Board of Inquiry - Croatia. Fonds 31, Box 2, 04.37.05. PPCLI Archives

Treasury Board of Canada. 2019. Directive on Automated Decision Making. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592. Accessed 30 Jan 2024

———. 2022. List of Interested Artificial Intelligence (AI) Suppliers. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/list-interested-artificial-intelligence-ai-suppliers.html#wb-auto-5. Accessed 30 Jan 2024

Wakeham, Alexandre. 2022. Career Management: Modernization Is a Must. Canadian Forces College. https://www.cfc.forces.gc.ca/259/290/24/192/Wakeham.pdf. Accessed 30 Jan 2024

Bright Prospects, Big Challenges: Defence AI in the United Kingdom

Kenneth Payne

The UK is superbly placed to take advantage of developments in AI, including in the area of national security. In recent years it has begun to chart a way ahead, notably by developing an AI strategy for defence and national security. Much work is underway within defence and more broadly in government, industry, and academia. The military is experimenting with new autonomous platforms and with the doctrines and concepts that might allow their effective employment. Aerial drone swarms, pilotless "loyal wingmen," unmanned submersibles and tactical ground robots—all are part of the British military's ongoing work. New partnerships with industry and academia have been developing. Autonomous systems are already at work in data processing and intelligence analysis. And across defence and in wider society, lively debates are underway about the ethical implications of using AI in national security, including in decisions about the employment of lethal force. Today, the pace of change is accelerating. New organisational structures are coming into being; new dedicated career streams are mooted; military education increasingly incorporates the study of AI; and, of course, new military systems, including weapon systems, are coming online.

But there are several challenges ahead. There is considerable uncertainty about the future development of AI. Equally there are concerns about its application to defence—not only from an ethical standpoint, but also in terms of its performance. How robust will AI systems be to adversarial countermeasures, including electronic and cyber warfare? How susceptible might AI systems be to bias; how brittle might their performance be in novel situations of the sort they might encounter in battle?

Such concerns are not unique to the British national security sector. But what makes them particularly challenging are Britain's longstanding aspiration to retain full spectrum military and intelligence capabilities, to operate at global reach, and to do so whilst undertaking a significant technological transformation. The British

K. Payne (✉)
King's College, London, UK
e-mail: kenneth.payne@kcl.ac.uk

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_4

defence budget is large and growing, but so too are its aspirations, and commitments. It will be a formidable challenge to develop new technologies, including AI (but also others, like new hypersonic missiles, satellites, sixth generation fighter aircraft and a new generation of nuclear submarines) while still maintaining its broadly constituted armed forces.

More broadly there are wider concerns about the economic and political environment in which these changes will occur. The next few years will bring marked economic challenges from high inflation and slow growth, a combination not seen since the 1970s. Again, these are not unique difficulties, but in Britain they are exacerbated by uncertainties following Brexit, and by the UK's low productivity. These headwinds impact the economy and society beyond immediate defence budgeting. Eventually, however, those broader issues will feed into defence via their impact on the UK's research base, or its attractiveness to inward investment and high-skilled migration.

1 Thinking About Defence AI

The UK's recent Integrated Defence and Security review stressed the significance of AI for national security. The Review charged the government with establishing "a leading (global) edge in critical areas such as Artificial Intelligence" (HMG 2021a: 7). Responding to the Review's top-level direction in a "Command Paper" the Ministry of Defence (MoD) described AI as transformative and so "essential to Defence modernisation." The paper stressed the need to move quickly on AI and envisaged applications "from the battlespace to the back office" (MoD 2021: 42).

A year later, in 2022, the Department published a detailed AI Strategy, produced following engagement with industry and academia (MoD 2022a). The new strategy added much more detail to the vision for defence AI outlined in the MoD's 2019 Defence Technology Framework, where it was bracketed alongside materials science, electronics, robotics, power storage and other rapidly developing technologies (MoD 2019: 18–20). In the years since, AI expanded in importance such that the current head of the Army referred to it in a 2021 speech as the "one ring to rule them all" (Sanders 2021). The new, expansive strategy paper sets the Ministry of Defence's bold ambition to become, in terms of AI, "the world's most effective, efficient, trusted and influential Defence organization or our size" (MoD 2022a). These are all somewhat subjective benchmarks—but perhaps rather than taking them literally, or dismissing them as corporate boilerplate, they can best be seen as indicative of genuine ambition and organizational drive to reform.

Among the many salient points raised in the Strategy were significant organisational changes, intended to boost the scale and pace of AI adoption across defence. AI would be jointly managed by a strategic-level Defence AI and Autonomy Unit (DAU) and a Defence AI Centre (DAIC). While the former sets the overall direction and policy framework, the latter oversees research and development and technical issues. In addition, the Strategy called for upskilling of military and civil service

personnel and the creation of new AI-focussed career pathways. There was emphasis on the need to build a wider and deeper collaborative network with other actors, signalling the departments enthusiasm to invest in AI technologies. And there was an important distinction between what the MoD calls "AI Now"—technologies that are reaching maturity, and able to be instrumentalised as practical systems for Defence; and "AI Next," cutting-edge research that might perhaps deliver utility in years ahead. On AI now, the Ministry is eager to speed the process of experimentation, validation, and adoption of useful AI.

Lastly, of note is the Strategy's emphasis on the continued role of human decision-makers, amidst rapid technological change. It stresses the need to develop effective "human machine teams," and to assess and mitigate the risks of AI systems. There will, the authors note, always be human political control of the UK's nuclear weapons.

1.1 The UK's Definition of AI

Much discussion of AI in UK national security, as elsewhere, focusses on kit, especially weapon systems that can operate autonomously and demonstrate intelligent decision-making. That is understandable; equipment is visibly striking, as with swarming drones and crewless ships. More than that, attention often concentrates on weapon systems—the final part of the so-called "kill chain," which delivers lethal force. That is reflected in the reams of analysis on the ethics of "killer robots." There is, of course, some technology like that in service with the UK, and much more in the pipeline, some of which features below.

But AI in national security extends much further than this. AI is a general-purpose technology or becoming one. Some analysts compare its likely influence to electricity, or the internal combustion engine, but even these comparisons miss something of the quality of the technology involved. AI is better seen as a decision-making technology, or rather technologies. As such, it is applicable across a broad range of activities, many with national security implications. This makes less visible from the outside, and so it can be challenging to analyse the extent and quality of any AI transformation. That is especially so where the information is classified, as it often is, and when change is happening at pace. Any reflections on defence AI in the UK, as elsewhere, are liable to miss important details.

In its new AI strategy, the MoD describes AI as something that can "supplement or replace human intelligence." It borrows its overarching definition from the overall UK National AI Strategy, which in turn defined AI as "machines that perform tasks normally requiring human intelligence, especially when the machines learn from data how to do those tasks" (HMG 2021b: 4). It is a broad definition, and this breadth is a mixed blessing. On the one hand, its flexible enough to accommodate a range of underlying computer technologies, architectures, and systems, performing a wide range of tasks. On the other hand, this flexibility and wide range of possible

defence-related activities it encompasses could compromise the coherence and focus of reform efforts.

Moreover, the UK definition might be critiqued as overly focused on human intelligence as a yardstick. AI can perform tasks that are far beyond human intelligence in some domains, as with lightning-fast exploitation of vulnerabilities in adversary computer systems. AI allows qualitatively different decision-making to the human variety: It is not that AI replaces or supplements human decision-making but does something entirely different.

1.2 AI Demands New Concepts, British Thinking Is Nascent

While much attention is spent on physical platforms, the story of AI in defence is far broader. UK doctrine distinguishes between physical and conceptual components of "fighting power," and the conceptual is likely to be every bit as important as the physical, with new possibilities for combined arms warfare. Work here is nascent, with little formal doctrine yet. There is existing conceptual writing on human-machine teaming, which stresses the continued importance on human judgment in military activities; a theme that emerges frequently in military discussions of defence AI (MoD 2018a). AI features in passing in other conceptual work too, as with the Royal Air Force's (RAF) doctrine on "unmanned" aerial systems, dating from 2017, which states:

> The UK does not possess armed autonomous aircraft systems and it has no intention to develop them. The UK Government's policy is clear that the operation of UK weapons will always be under human control as an absolute guarantee of human oversight, authority, and accountability. Whilst weapon systems may operate in automatic modes there is always a person involved in setting appropriate parameters. (MoD 2017b: 14)

That remains the most explicit doctrinal statement on autonomous lethal weapons, but it is increasingly strained by technological advances over the last half decade, notably swarming. The MoD has, we will see, developed further views on AI ethics, but the essential problem of "meaningful" human control remains.

More broadly than ethics, the next generation of doctrine will need to wrestle with how best to employ AI—exploring the ways in which it might alter combined arms warfare. To inform this conceptual thinking, there is considerable experimental work underway in the armed services. Some of this is explored below. More broadly, the UK is home to a small number of specialists in industry, academia, and the wider armed forces, all engaged in thinking through the practical and conceptual dimensions of warfighting AI. Focal points include the UK's Defence Academy and the Royal United Services Institute. Doctrine and concepts typically originate and evolve in the context of the UK's close Alliance relationships, especially with the US. There is a long history of shared intellectual endeavour, and AI thinking in both countries is developing along broadly similar lines. As of yet, there is limited formal

evidence of common approaches to AI, although in several areas parallels are emerging.

1.3 AI Ethics, the UK Debate

Ethical debate in the UK over AI weapons has thus far been largely limited to small groups of concerned specialists and activists, rather than the wider public. There is some evidence that this is changing. In 2021, the BBC's high profile annual lecture series, the Reith Lectures, featured a prominent British computer scientist, Stuart Russell, discussing some of the ethical challenges of AI, including in warfare (Russell 2021). Algorithms were implicated in the controversial awarding of high school student grades when exams were impossible during the covid pandemic. There were concerns about personal health data collected by the National Health Service being accessed by technology companies. And stories about the surveillance capabilities of intelligence agencies periodically make the national press, as with the extensive coverage of the Snowden leaks from the US National Security Agency (NSA). At the moment though, there is little evidence of widespread, deeply held or sustained public engagement with AI issues. It does not yet, for example, feature explicitly in polling of public concerns.

Ethical debate happens inside Defence too, including in defence legal circles. The Defence AI Strategy makes frequent mention of ethics and the need to develop AI in line with the UK's democratic values. It notes that adversaries are likely to use AI in ways that the UK would consider unethical. And the Ministry published, in conjunction with its Strategy, a separate policy paper on the "ambitious, safe, responsible" use of AI. That paper insists:

> there must be context-appropriate human involvement in weapons which identify, select and attack targets. This could mean some form of real-time human supervision, or control exercised through the setting of a system's operational parameters. (MoD 2022b: 3)

Further, it outlines some key challenges, including AI bias and unpredictability, and it sets out some ethical principles, not least of which is "human-centricity." The MoD has also convened an AI ethics advisory committee to offer informal input on its approach, and to act as a forum for engaging wider views. It is a serious effort to grasp some tricky issues—though the MoD certainly would not claim to have solved them. What, for example, is meant by "context appropriate?"

As AI becomes more pervasive, perhaps it will become part of a larger public discourse in the UK. There will certainly be Parliamentary scrutiny, perhaps even a dedicated select committee. There may be scope for AI commissioner, along the lines of the UK's Information Commissioner. The challenge for the UK will be to maintain its current lead in AI, including in national security, while ensuring that the changes AI spurs are sympathetic to the broader norms of wider society. The MoD's paper grasps that much, at least.

2 Developing Defence AI

AI research is currently advancing more rapidly than its adoption by defence. Earlier AI systems allowed rudimentary autonomy and were well suited to some military applications—defensive weapons, for example, like the Royal Navy's shipboard Sea Viper anti-missile system. For the last decade, research progress has been remarkable in machine learning, where computers improve optimisation through repeated exposure to training data. It is this generation of AI, especially its "deep learning" subset, modelled loosely on biological brain cells, that is currently driving UK defence applications—whether of autonomous aircraft, sophisticated language translators, or intelligence analysts. All these applications are part of the UK approach to AI.

AI now enables offensive weapon systems that can proactively identify and attack targets, and some are already in service. The UK's Brimstone air-launched missile from MDBA is a good example of a weapon that can scour a search area as it flies, looking for a pre-set target-type. Newer weapon systems will be able to "loiter" over the battlefield before striking targets of opportunity selected from a pre-set list of target types. The UK has begun to experiment with such weapons, including the US manufactured Switchblade—but it has not yet acquired these in significant numbers. Nor does it possess an offensive weapon system that can integrate reconnaissance and strike functions fully autonomously, like the Israeli Harpy. That is increasingly a matter of choice rather than necessity though—the UK's Protector drone, armed with Brimstones, would theoretically be able to do so, flying autonomously and parsing target information using autonomous image analysis.

Still, the UK's autonomous combat capabilities remain, for now, somewhat rudimentary. Protector, for instance, is not designed to operate in highly contested environments. AI platforms capable of performing aerial attack and air superiority roles are still a little way off in the UK, as elsewhere. The UK is currently working on its sixth-generation fighter programme, the Tempest. There will be plenty of AI involved—in parsing incoming information, for example, or in autonomously deploying defensive countermeasures to protect the aircraft. Perhaps there will be something more fundamental still; no human on board. Unclassified concept designs still conceive of Tempest as a crewed fighter with a cockpit. The MoD's Combat Air Strategy calls for an aircraft "manned or unmanned (sic)," suggesting that Tempest may yet be crewless (MoD 2018b). In either case, the main platform may operate as part of a system alongside unmanned platforms—"loyal wingmen" of some variety yet to be determined. The UK did not have an entry in the Defense Advanced Research Projects Agency's (DARPA) recent AI dogfighting contest and has no publicly known equivalent process underway to competitively refine AI-fighter pilots.

Rather than air superiority or strike aircraft, AI systems are more immediately promising in the intelligence, surveillance, and reconnaissance (ISR) roles—whether through unmanned platforms and sensors operating in space, air, sea and on land; or through machine intelligence analysis of the data that they collect. Understandably, much of the detail about the autonomous capabilities of such

systems is classified. Nonetheless it is reasonable to suppose that similar technologies are being employed in the UK as in the United States, not least because some of the same suppliers, platforms and systems are involved—General Atomics supplies the RAF's Protector unmanned aerial vehicle (UAV), a variant of its Reaper platform; and Palantir, which is main contractor of the US Department of Defense's (DoD) "Project Maven" also offers its AI-powered analytics to the MoD. With technologies like these, autonomous flight, real time high-definition image capture, and AI labelling and processing of such imagery is eminently feasible, even if not yet operational.

Throughout British defence, a menagerie of robotic, unmanned systems is coming into being (Table 1). Some will be used for ISR, some for logistics activities, and some for strike, or for combat roles. Some will combine roles, like the strike-capable Protector. Increasingly systems will span the traditional domains of land, air, and sea, as with small unmanned helicopters like Anduril's Ghost, used in tactical airspace for short-range ground reconnaissance, and perhaps attack. That raises some interesting organisational dilemmas: are such drones the purview of the Royal Air Force, or the Army? In field experiments, they have been used by the Royal Marines.

Experimental kit is arriving so frequently that it is impossible to keep up. Newer models will undoubtedly be featuring in trials, even as you read this report. Nonetheless, some general observations can be made:

- All three armed services are following a similar model—acquiring small numbers of platforms from a range of traditional and non-traditional suppliers. This includes suppliers from the UK and overseas; large, established providers; suppliers of military hardware and—perhaps more importantly for AI—of the code and systems underpinning it.
- Alongside established defence corporations like BAE, MBDA and so on, are newer, software-focused arrivals like Adarga and Rebellion Defence who offer AI and data analytical services to the MoD.

Table 1 UK military services experiment with different types of unmanned systems

• The Royal Navy has been experimenting with crewless minesweepers (Atlas Elektronik's Sweep system), large submersibles (the Manta XLUUV), and carrier-borne UAVs able to perform a variety of roles, including ISR, airborne early warning and resupply. Recently it acquired a dedicated experimental surface vessel, the XV Patrick Blackett, which in time will itself be autonomous.
• The RAF has created an experimental drone swarming squadron and is working closely with the Defence Science and Technology Laboratory (Dstl) to build ever larger swarms. The last public information described a swarm of 20 aircraft, comprising five different drone types, operating collaboratively. It uses machine learning techniques in its existing, inhabited platforms too—notably the intelligence fusion module of its F-35 fighter.
• The Army, meanwhile, is also undertaking experimental work on autonomous systems—including tactical land and air platforms. Examples include Elbit System's swarming micro-drones and loitering munitions aloft, and unmanned ground vehicles, like the Rheinmetall Mission Master or Horiba Mira's Viking.

- There are giants, like Amazon, who furnish the UK MoD and intelligence agencies with the cloud computing services that securely house the data on which the AI works; mid-sized outfits, like Palantir who provide ways of parsing that information; and comparatively tiny outfits, like Callen Lenz, whose small UAVs have formed part of the RAF's experimental swarming work.

There is a lot of work going on, only some of it visible to outsiders. But there is still a palpable sense of being in the foothills of more profound changes to come, driven by the national AI strategy. And whilst established customer relationships and organisational habits will continue to exert influence, there is a feeling of the kaleidoscope having been shaken.

2.1 From 'AI Now' to 'AI Next'

The British AI capabilities being fielded now, even experimentally, are a long way behind the cutting edge of AI research. Some lag is inevitable—it takes time to develop and validate applications, and culture invariably intercedes to shape adoption. But the strength of the UK ecosystem is that it innovates basic research, rather than merely attempting to instrumentalise approaches developed elsewhere. In this it has few peers beyond the US, or perhaps France or Israel. In the foreword to the Integrated Review, the Prime Minister called for the UK to remain "at least third in relevant performance measures for scientific research and innovation" (HMG 2021a: 7). The top two were not listed, but likely included China alongside the US—a somewhat debatable proposition.

UK defence AI activity is embedded within a wider context, involving the defence industry, academic research and wider, civil research and development. The UK has long been a leading actor in the development of AI, reaching back decades to the emergence of the discipline of computer science. The UK possesses world leading AI researchers, and in DeepMind (owned by Alphabet/Google) it has perhaps the outstanding AI innovation hub of the last decade. It also has, we will see, a large in-house research base, an established defence industrial sector, and several newly prominent AI companies offering services to the MoD.

The innovation that will emerge from this ecosystem is, of course, uncertain. But it is already apparent that some areas will be important. Among these, advances in unsupervised machine learning and learning from limited data are already underway. There will likely also be dramatic developments in computer architecture—notably in quantum computing. The British MoD recently acquired its first quantum computer—a technology that promises computer processing orders of magnitude faster than conventional, binary supercomputers (McMahon 2022). As it matures, quantum computing may lead to radical developments in AI, and also in decryption—posing a threat to network security. In its AI Strategy, the MoD suggests that the next stage of AI might help with military tasks including automated cyber

defence and intelligence fusion. Further out, it identifies more challenging activities, like operational planning and "machine speed command and control" (MoD 2022a: 34–35). That will require further conceptual breakthroughs in AI, including perhaps the ability to reason conceptually, or to better model adversary intentions.

Whilst the UK is well placed to innovate new approaches and technologies, it has some notable weaknesses. Today, the UK has no global technology giant, along the lines of Baidu, Google, or Microsoft—all of whom are currently leading funders of AI research. Brexit has created an economic headwind, affecting the UK's attractiveness to inward investment and high-skill migration—especially from the EU—whilst sapping demand for UK output, both in services and manufacturing. The UK's university sector remains world-class but faces multiple challenges—whether competition from American high-technology research companies for talent, or access to EU research funding after Brexit. Another challenge is British productivity, which again lags peers, especially in the US and EU. The reasons are hotly debated and likely multifaceted but have unarguably proved resistant to change.

3 Organising Defence AI

New ideas are one thing—the arrival of AI has also spurred plenty of organisational change, and some degree of muddle. There is a palpable sense of being at the beginning of changes that may soon be more far reaching, especially as AI drives conceptual changes.

One challenge is that AI itself is often "domain agnostic"—capable of operating across all three traditional domains (land, maritime, air) as well as the two newer ones (space, cyber). This suggests the value of central organisation at Departmental level, where we already saw the creation of a new Defence AI Centre to champion AI, alongside the existing Defence Autonomy Unit. Plenty of other actors within UK Defence are involved in developing approaches to AI, and the following is certainly not exhaustive.

One key player is Strategic Command, one of the UK's four Front Line Commands, alongside Army, Navy, and Air Commands. Strategic Command is responsible for a range of joint capabilities and enablers. It already coordinates a range of AI-related activities and organisations, notable among which is its jHub unit, which promotes innovation by building relationships with technology suppliers, especially those with "dual use" civilian and military application. Also in Strategic Command is Defence Digital, charged with overseeing military IT. Defence Digital has an interest in AI, for example via its work on digital twins and synthetic environments that simulate the real world. Developing secure approaches to processing huge volumes of data is an important aspect of the MoD's aspirations for AI but extends more broadly than AI to encompass all aspects of military information processing. So, the organization is responsible for developing a digital

"backbone"—the physical capacity to share data, and its Foundry works to support organizations in accessing and exploiting the data.

Elsewhere, organisational partnerships on AI are increasingly common. For example, the MoD has established a defence BattleLab to facilitate technological experimentation. The lab is a collaboration between the Navy, Army and two other units, the Defence Innovation Unit and the Defence Science and Technology Laboratory (Dstl), the government's main in-house science and technology research agency.

Dstl is perhaps the key government player in defence AI research. Although much of its output is not publicly accessible, it publishes open access guides, called "biscuit books," on aspects of AI for wider audiences in Defence (DSTL 2021). The organisation partners with a range of other actors—some in government, as with the two Front Line commands in the BattleLab, some outside. One important and deepening Dstl relationship is with the Defence and National Security theme at the UK's Alan Turing Institute, with which it has recently created a Defence Centre for AI Research (DCAR) (DSTL 2022). The Turing Institute, established in 2015 by a partnership of leading universities, is the UK's national institute for AI and data science, and engages in a wide range of basic and applied research. Clearly the goal of the DCAR is to foster connections between academic researchers who are part of the Turing's network, and those within Dstl. Another Turing-Dstl project is its work with the UK National Cyber Security Centre, an offshoot of the UK's Government Communications Headquarters (GCHQ) electronic intelligence agency, to explore the employment of AI in automated cyber defence. Elsewhere in the UK's defence apparatus, likely at the recently established interagency National Cyber Force, similar work is almost certainly underway exploring offensive autonomous cyber techniques.

Meanwhile, co-located with Dstl, but organisationally separate from it, is the MoD's Defence and Security Accelerator (DASA). Founded in 2016, DASA works with private enterprises of all sizes in a bid to promote innovation—as with its funding of Flare Bright's hand launched Snapshot tactical reconnaissance nanodrone, or with Marlin Submarine's work in rapidly prototyping the Manta large submersible project (DASA 2021; Navy Lookout 2020).

4 Funding Defence AI

Broadly, there is substantial investment in British research, and it has clearly produced excellent outputs, including some cutting-edge defence equipment. The business sector accounts for a majority of overall R&D spending in the UK, much of which, of course, is not for defence. Private business funded some £20.7bn of R&D in 2019, some 54% of the total, comfortably outstripping the 27% spent by the public sector (Hutton 2021: 14–15). Defence R&D spending is also substantial, with government spending alone amounting to some £1.1bn in 2020.

Yet the UK is surprisingly weak when measuring R&D comparatively. While expenditure has been rising steadily in the UK, in nominal terms, over an extended period of several decades, as a percentage of GDP expenditure has been broadly flat for many years. It is currently around 1.7% of GDP, a figure that compares unfavourably with peer countries in Europe (Germany 3.2%, France 2.2% in 2019) and north America (USA 3.1% in 2019). The incumbent government has plans to increase R&D spending to 2.4% of GDP by 2027, but even that would only be broadly in line with the OECD average.

There are also plans to increase defence R&D. In its Command Paper responding to the Integrated Security and Defence Review, the MoD announced its intention to rapidly expand its R&D budget over coming years. The headline figure of £6.6bn spent over four years would represent a significant increase over the £1bn or so currently spent annually. The fine-grained details of what gets spent where are currently lacking—but the Review's emphasis on AI makes it clear what the Department's priorities are. Again, this all sounds striking—and it is far from small potatoes. But a comparison with the United States is sobering. The current defence budget in the US projects a 9.5% annual increase in R&D spending, to some USD130bn each year. That's more than 100 times the UK figure.

While Dstl is an obvious focus of research on AI for UK defence, there are plenty of others engaged in AI R&D as part of the national security ecosystem. One major government-funded actor is UK Research and Innovation (UKRI), a conglomeration of the UK's funding councils that direct funding into academic research. In 2020, UKRI accounted for £6.1bn of investment, and while much of this would have little direct impact on defence, plenty would—either directly in the innovation of new technologies and applications, or indirectly in advances in basic research.

One final government initiative is noteworthy—the establishment in 2022 of a new funding body, ARIA—the Advanced Research and Invention Agency, explicitly, if loosely, modelled on DARPA, the US Defense Department's research powerhouse. ARIA is supposed to inject UK funding with a dash of risk tolerance, with the obvious inference that other funders, notably UKRI, have been too conservative. Its explicit mission is to invest in projects with the potential for paradigm shifting, transformative effects. This is certain to include considerable funds for AI research, though perhaps on basic research with applications some way downstream. With a projected £800M budget, ARIA will be a significant part of the innovation ecosystem—but critically, unlike DARPA, it lacks a formal link to defence.

5 Fielding and Operating Defence AI

The individual Front Line Commands clearly have an interest in developing approaches to AI. By "pulling through" emerging technologies, these commands, perhaps at least as much as the centralised allocation of R&D budgets, will shape the eventual employment of AI systems. There is plenty of salient scholarship on cultural approaches to understanding defence, including some that reflects on the

British military's long relationship with technological innovation. A key takeout is that ostensibly similar militaries, even allies, can employ similar technologies in rather different ways, with dramatic effects on fighting power.

5.1 The Army

Accordingly, the Army's Futures Directorate is considering the implications of AI and unmanned systems for land warfare. The Directorate's short paper on the Army's Approach to Robotics and Autonomous Systems sketches some ideas for concept development, arguing that autonomous and remotely commanded systems will allow it to increase mass and dispersal, "whilst detecting and engaging the enemy in the most dangerous parts of the close and deep battle" (British Army 2021). There is not a huge amount of detail in the paper, and it is the land domain where adoption of AI will perhaps prove most challenging, owing to the complex terrain, both human and physical. The army is experimenting with small tactical robots, but AI's immediate utility for the Army is likely to come in other areas, like the integration of command, control and ISR activities, the domain-agnostic cyber-contest for digital advantage, in tactical airpower, and perhaps in the longer-range coordination of indirect fires.

There is considerable debate in professional forums about the future structure of the Army, the sorts of equipment it should acquire, and how many personnel it needs. Of the services the Army seems the most unsettled in terms of its vision for future warfare—a reflection not just of the arrival of more sophisticated AI, but of the muddled and unsatisfactory conclusion of longstanding deployments in Iraq and Afghanistan, of the rapidly evolving high-intensity conflict in Ukraine, and of the Army's longstanding procurement difficulties with major combat systems, like the Ajax Armoured Personnel Carrier (APC), Watchkeeper UAV and Warrior Infantry Fighting Vehicle (IFV). The Futures Directorate is responsible for shaping the intellectual way ahead, via its Project Wavell, which seeks a "theory of victory" fit for an era of increased autonomy and AI. And the Directorate has an ambitious goal for the Army of fielding a light brigade enhanced with robotic systems by 2025—only one year hence.

5.2 The Royal Marines

The Royal Marines (RM), meanwhile, have undertaken frequent small scale field experimentation with advanced technology, including autonomous weapons, often as part of their Future Force Commando programme.

The RM have a clear vision of small, technologically sophisticated units operating in the maritime domain and littoral, and in so-called "grey zone" conflicts, at the threshold of major combat operations. This concept has sharpened the focus of their field exercises. In one attention grabbing exercise, a combined RM-US Special Operations Forces (SOF) unit with experimental technologies reportedly outperformed a larger United States Marine Corps (USMC) adversary force (Brown 2021). There is plenty of autonomous-capable equipment under test here—including Anduril's small reconnaissance helicopters and loitering munitions. But it is the conceptual work as much as the kit that stands out—as when the Marines experiment with platforms operating across multiple domains simultaneously.

The other notable feature is how much of this work is being communicated publicly—including on YouTube (Royal Marines 2021). The RM is clearly keen to be seen to be at the cutting edge, perhaps because in common with its American counterparts, also known for their conceptual agility, the small force faces continued threats to its independence and funding, and so seeks a distinctive identity.

5.3 The Royal Navy

Unsurprisingly given its maritime focus, the Royal Navy (RN) has been working with the Royal Marines on its Future Force concept. But the implications of AI systems for the Navy are likely to be broader and more profound than that. The RN's forays into AI equipment are as yet relatively small scale—small (relative to crewed) non-nuclear-powered submersibles; and similarly small drones and surface vessels, notably autonomous minesweepers. Of course, it already employs autonomous systems in its missile defences and torpedoes. And the F-35 aircraft that fly from its two large aircraft carriers utilise AI in their information management systems.

Larger changes are inevitable. One example: DASA and Dstl are working with business and academic teams on an Intelligent Ship competition, which will explore the utility of human-machine teams across a range of maritime tasks, including engineering decisions and mission analysis (Lye 2021). The Navy itself has established several teams to work on technological innovation. In addition to its Chief Technology Officer, there is NavyX, described as an "autonomy accelerator" and Project Nelson, which focuses on digital technologies (Royal Navy 2022). In common with the other services, there is a palpable sense of energy and enterprise, but work remains relatively small scale. In time AI may challenge some more fundamental tenets of Britain's approach to naval warfare—whether that is the focus on the carrier strike group, with crewed aviation; the role of Navy nuclear submarines as sole leg of the UK nuclear deterrent; or the way in which amphibious force is projected ashore. While there will inevitably be conceptual work underway on all these aspects and more, much remains outside the public sphere.

5.4 The Royal Air Force

The Royal Air Force might be expected to be at the forefront of efforts to innovate and instrumentalize AI. Certainly, many peoples' visions of AI in national security are of an unmanned lethal drone. In reality, however, AI will make more of an immediate contribution to other aspects of air power, invariably as part of data-processing and decision-making systems that involve humans—not least because of ethical unease about full-autonomy, but also because the technology to do so remains immature.

Conceptually too, the RAF approach remains in its early stages. Extant air and space power doctrine dates to 2017 and includes no mention of AI, but there is plenty of discussion of the topic in professional air power forums and journals (MoD 2017a). The RAF's Rapid Capabilities Office (RCO) is one in-house area of expertise—and is leading on the Tempest future combat fighter project. One of its other projects, Bablefish 7, neatly illustrates an area where AI can, and increasingly is, playing an important role; in integrating, filtering, and sharing all-source information—whether that is initially acquired from a space satellite, an aircraft of platforms on land or sea (RAF 2021). It was the RCO's decision to abort work on the Mosquito, the RAF's initial stab at creating a viable "loyal wingman" drone to fly alongside its fifth and sixth generation fighters (Jennings 2022). Successor wingman projects are inevitable.

Another important RAF project is its work on experimental swarming, for which it stood up a new dedicated squadron, No. 216 Test and Evaluation Squadron (Allison 2021). As with the Navy, the work on drones remains small scale and low-key, with the squadron, RCO and Dstl running a score of experimental exercises in the last few years. The two projects neatly encapsulate an unresolved tension for the RAF—which is the appropriate vision given the prospect of AI increasingly capable of flying aircraft in complex, contested environments? The current emphasis is on crewed aviation in exquisitely capable, incredibly expensive aircraft. An alternative is large numbers of less capable, perhaps disposable, swarming platforms that exploit mass and saturation to overwhelm air defences. Still another vision is of a missile-centric future, with long range, hypersonic missiles exploiting pure speed. That last vision seems the least prominent aspect of the RAF's work and that raises a further dilemma—of balancing limited resources against costly technologies that are relatively unproven.

5.5 The Intelligence Agencies

Less publicly visible than the Commands, but certainly part of the UK's national security ecosystem, the UK's intelligence agencies, notably GCHQ, have a long-standing interest in using AI techniques to identify useful information within the torrent of data it acquires. There is crossover with the work of the services,

particularly the RAF, which has taken the lead in space power. There is overlap too with the work of Defence Intelligence, which leads on intelligence analysis. For his part, the Chief of the Secret Intelligence Service (colloquially, MI6) recently pointed to greater use of AI in his organisation. Beyond generalities, however, it is not possible to say much. Occasional insights can be gleaned from investigative journalism like that of Barton Gellman following the Snowdon leaks, which confirmed a good deal of UK-US cooperation on the collection (sometimes in bulk) and analysis of electronic information, and the use of sophisticated machine learning techniques to parse it (Gellman 2021). But the technologies it details, while strikingly advanced, are already some years old. As with other areas of AI use in national security, there are important issues here of oversight, and a need to balance the priorities of the state with the rights of citizens.

5.6 Future Trends

This snapshot of Defence AI activity doubtless misses out many salient governmental organisations involved in developing AI technologies and concepts, whether in-house or in partnership with industry and academia. Still, it attests to both the range and dynamism of work underway. Many of these organisations are relatively new on the scene. More will likely follow in time, whether in response to developments in technology, or perhaps the desire of ambitious organisations and leaders to gain a foothold in what is increasingly perceived as a critical general-purpose technology. There is certainly a sense of organisational muddle and overlap in some areas. Skills bottlenecks and shortfalls, competition for resources, bureaucratic politics, and organisational culture—all these will shape the AI ecosystem as it evolves.

UK national security is currently likely only at the beginning of changes that will be more profound than the creation of bolt-on organisations, or of collaborations between different national security agencies. In common with other countries, there is clear potential for AI to drive fundamental change in armed forces, and in wider society too. Such changes will inevitably be refracted via prevailing cultures of national security, both within and across states. The UK's Strategy for AI, as with other MoD publications, hints at the changes—whether that is talk of new platforms, concepts, or personnel requirements—but does little to spell out the details.

Can we say more about what those changes might be? In part this depends on the capabilities of the technology itself, and this is fast changing, almost on a weekly basis. But some large conceptual ideas are emerging in the UK context that bear further reflection. Among these:

- *Human Decision-Maker*

The enduring importance of the human decision-maker, even in an era with pervasive and increasingly sophisticated machine cognition. That reflects an ethical, and also cultural, desire to preserve "meaningful" human control. Fleshing out the tactical details will be more difficult than expressing the desire.

- *Skillsets*

Related is the need to "upskill" the workforce involved in defence, and more broadly to promote AI literacy in wider society. The AI Strategy highlighted the need for a skilled cadre of AI specialists in defence, and hints at the emergence of a career stream or structure that might foster that specialism within the uniformed services (MoD 2022a: 18). There are discussions about the possibility to bring experienced mid-career professionals with relevant skills into defence—along those lines, the AI strategy mentions the use of specialist reservists and flexible entry paths (MoD 2022a: 19). AI though is likely to be ubiquitous, and the government will need to strike a sensible balance between promoting AI knowledge as a generalist military competence and a specialism.

- *Mass and Scale*

AI affords potential advantages in terms of mass, distribution and decision-speed. The head of the British army, perhaps optimistically, called for an army of 30,000 robots. And the head of the RAF argued that with AI, "We can have mass and technology and technological sophistication" (Mehta 2021). As in other wealthy democracies, defence inflation, driven by exquisite technology and cutting-edge designs, has shrunk the armed forces. Britain's armed forces are smaller, both in personnel terms and in numbers of main platforms—tanks, surface combatants and multi-role fighter jets than at any time in the modern era. The emerging British vision is clear—AI will enable scale, while maintaining qualitative advantage. Whether that vision is feasible is another question. The practical implications will be profound—whether that is the tactical question of how to organise (and lead) a platoon of mixed humans and autonomous machines, or whether it still makes sense to organise armed forces along three traditional domain/service lines.

- *Vulnerabilities*

AI systems are potentially vulnerable, for example, to Electronic Warfare countermeasures like jamming, or spoofing and susceptible to offensive cyber warfare. If the British vision is of a clone army of 30,000 machines—the clones had better not all feature the same Achilles heel. Then there are difficulties of assurance and trust, as when AI is susceptible to bias in training data. As will other states, the UK needs military AI that is reliable and trustworthy. Part of that demands AI that is sufficiently transparent that users can understand its decision-making.

6 Training for Defence AI

The defence AI strategy outlines in broad terms the need to develop the right skills for the autonomous era it envisages. So far, detailed work to flesh out that vision is lacking. There are some early indicators of more significant changes to come. For example, the military offers short courses in coding, including some sponsored by

its jHub innovation team. The same unit has recently launched "innovation fellowships" for serving military officers, with the aim of fostering links across government and the private sector.

Elsewhere, AI is becoming increasingly prominent in professional military education syllabuses, whether distance learning, or residential courses. The three services have established programmes to allow competitively selected officers time in UK higher education pursuing advanced degrees or visiting fellowships—increasingly these are in AI or AI-adjacent subjects. Short professional development courses in AI-related subjects are also becoming increasingly available, as with one on data led decision-support and AI at Cranfield University's Defence Academy campus.

7 Conclusion: An AI Transformation Debate

The UK's defence budget is large and projected to grow further. The current government has pledged further increases over the decade, although it now faces stiff competition from other fiscal priorities. Unlike many NATO allies, the UK meets its 2% of GDP commitment, albeit with a suspicion of some deft accounting. But spending is stretched between competing priorities. The UK's armed forces have long aspired to a full range of military capabilities, and an ability to deploy and sustain significant military power globally. This strategic culture is reflected in the Integrated Review, with its recognition of a tilt in geopolitical power towards the Indo-Pacific region, and an attendant desire to gear British military capabilities for national security challenges there. That includes a reinvigorated focus on blue water naval capabilities, the retention of long-range strategic airlift capabilities, and some forward basing. This thinking was already reflected to some degree ion the acquisition of two large conventional aircraft carriers and the F-35B jets to operate from them.

The Indo-Pacific turn in the UK's outlook also reflects the current government's pronounced EU-scepticism and its post-Brexit difficulties of forging a new relationship with the EU. But the war in Ukraine has challenged that worldview; refocusing attention on continental defence and creating an urgent need to restock munitions expended in Ukraine. Balancing its budget against its Pacific ambitions, its support for Ukraine, and its military modernisation programme, including its AI efforts, will be difficult.

The Ukraine conflict has also prompted further reflections in Britain on the future of warfare, not least because the UK has been one of Kyiv's most prominent allies. Events in Ukraine are keenly studied by those charged with modernisation of the UK's own forces. Part of this debate is visible in professional forums and on social media. On one hand, modernisers observe, combat in Ukraine relies on high technology, including AI technologies used in intelligence gathering and analysis, or as offensive and defensive tools in the cyber domain. The fighting itself presages an era of advanced, digitised warfare—a battlefield saturated with sensors, and the extensive use of unmanned platforms, especially commercially available drones.

Distributed light forces, especially using man-portable air-defence systems (MANPADs) and guided anti-tank missiles (ATGMs) were much evident in the conflict's early phases, where they proved effective against crewed aviation and Russian armour. AI's tactical strength is likewise purported by enthusiasts to lie in distribution and scale.

But on the other hand, the Ukraine war demonstrates the continued utility of some vintage equipment and longstanding concepts. Artillery has been dominant in much of the fighting, especially long-range rocket systems which have been in service with Western militaries, including the British, for decades, just as have those MANPADs and ATGMs.

The upshot is that all sides in the British modernisation debate can take some support from events in Ukraine. Advocates for extensive AI-related reforms can argue plausibly that the combatants have not made full use of technologies that are only now beginning to emerge as viable military systems. Sceptics can point to the continued utility of existing systems and the need to hedge against the risk of trading in too much useful equipment for unproven technology. Gauging where the debate in the UK currently stands is a subjective exercise, but certainly the war has tempered the degree of enthusiasm for AI in many public national security debates, if only by drawing the focus away from what was until 2022 a prominent feature of defence-modernisation discussions.

To some degree, these tensions are not new. The UK has a long history of defence reviews in which rising defence inflation is set against the constraints of the economy, the emergence of new technologies and an uncertain geopolitical environment. Should the armed forces be more focused on global challenges, or the pressing concern of a continental threat? How far should the government of the day seek to promote domestic industry, even if the result is higher cost, lower quality equipment? Often the result has been belt-tightening and salami-slicing. Capabilities and personnel are thinned out, in-service dates for equipment are extended. To remain at the cutting edge, successive defence reviews have cut personnel numbers, rationalised formations, extended equipment in-service dates and gapped some roles, like carrier aviation and long-range anti-submarine aviation.

Too much despondency, however, would be wrong. Set against these challenges are a large and growing defence budget, strong, longstanding alliances with technologically capable partners including those in NATO, and the "Five Eyes" intelligence community. The UK has a track record of fielding highly capable, modern armed forces with global reach; of developing advanced military technologies and cooperating with allies. The UK's armed forces are small in terms of numbers—both of personnel and major equipment. But they are high-quality, experienced, adept at operating in alliances and at adapting to new technologies.

Also weighing in the balance for the UK are the capabilities of likely adversaries, most notably China and Russia. Both states are mentioned explicitly as potential challenges in the Integrated Review, with China described as an increasingly assertive "systemic competitor" and Russia as "the most acute threat to our security." Both challengers frame the need for the rapid and transformative adoption of AI in defence.

Yet conflict in Ukraine has amply demonstrated that Russia's conventional threat was greatly exaggerated by Western analysts. Many were impressed by Russia's modernisation efforts, by its ability to operate at reach, and to exploit opportunities in the unconventional, "grey zone" of modern warfare—notably, for example, through its propaganda efforts in social media. Despite longstanding efforts to modernise its armed forces and to develop cutting-edge military technologies, Russia's combat performance has been poor, and advanced computer technology not much evident.

China spends much more, has larger, more modernised armed forces, and has a considerable research base. But China too faces substantial challenges to developing effective AI for national security, including significant corruption, skills and equipment bottlenecks, and a centrally planned ethos in government, business, and its armed forces. Long term demographic challenges and a markedly weakening economic outlook are additional impediments to progress.

The threats to national security and wider British interests from these two countries were a significant motivation for Britain's own efforts to modernise defence. That modernisation will almost certainly continue, regardless of the authoritarian states' evident difficulties. Analysts seem predisposed to emphasise the worst-case scenario when it comes to adversaries.

Compared to both these potential adversaries, however, the UK's AI-defence prospects look bright. British scientists are at the forefront of AI research and have a long history of innovation. And parts of the British state have a longstanding track record of using machine learning techniques for national security. The two largest challenges for the UK will be developing AI that reflects British values (as the MoD acknowledges); and keeping pace with its vastly better resourced ally, the United States.

References

Allison, George. 2021. UK to introduce additional drone swarming squadron. UK Defence Journal. https://ukdefencejournal.org.uk/raf-to-introduce-additional-swarming-drone-squadron/. Accessed 30 Jan 2024

British Army. 2021. The British Army approach to robotics and autonomous systems: Generating human-machine teams. British Army. https://www.army.mod.uk/media/15790/20220126_army-approach-to-ras_final.pdf. Accessed 30 Jan 2024

Brown, Larisa. 2021. US Marines routed by Royal Marines in war games. The Times. https://www.thetimes.co.uk/article/us-troops-routed-by-royal-marines-in-war-games-scrx888m8. Accessed 30 Jan 2024

DASA. 2021. Case study: Autonomous nanodrone captures aerial intelligence in a snap. DASA. https://www.gov.uk/government/case-studies/autonomous-nanodrone-captures-aerial-intelligence-in-a-snap. Accessed 30 Jan 2024

DSTL. 2021. Assurance of AI and autonomous systems: A Dstl biscuit book. Defence science and technology Laboratory https://www.gov.uk/government/publications/assurance-of-ai-and-autonomous-systems-a-dstl-biscuit-book. Accessed 30 Jan 2024

———. 2022. Launching the Defence Centre for AI research. Defence Science and Technology Laboratory. https://www.gov.uk/government/news/launching-the-defence-centre-for-ai-research Accessed 30 Jan 2024

Gellman, Barton. 2021. *Dark mirror: Edward snowden and the American surveillance State*. London: Penguin.

HMG. 2021a. Global Britain in a competitive age: The integrated review of security, Defence development and foreign policy. HM Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf. Accessed 30 Jan 2024

———. 2021b. National AI strategy. HM Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020402/National_AI_Strategy_-_PDF_version.pdf. Accessed 30 Jan 2024

Hutton, Georgina. 2021. Research and development spending. House of commons library briefing paper, no. SNO4223. House of commons. https://researchbriefings.files.parliament.uk/documents/SN04223/SN04223.pdf. Accessed 30 Jan 2024

Jennings, Gareth. 2022. UK cancels Mosquito 'Loyal Wingman'. Janes. https://www.janes.com/defence-news/news-detail/uk-cancels-mosquito-loyal-wingman. Accessed 30 Jan 2024

Lye, Harry. 2021. DASA Awards £3m Funding for Intelligent Ship Competition. Naval Technology. https://www.naval-technology.com/news/dasa-awards-3m-funding-for-intelligent-ship-competition/. Accessed 30 Jan 2024

McMahon, Liv. 2022. MOD acquires government's first quantum computer. BBC News. https://www.bbc.co.uk/news/technology-61647134. Accessed 30 Jan 2024

Mehta, Aaron. 2021. Britain's royal air force chief talks F-35 tally and divesting equipment. Defense News. https://www.defensenews.com/interviews/2021/05/09/britains-royal-air-force-chief-talks-f-35-tally-and-divesting-equipment/ Accessed 30 Jan 2024

MoD. 2017a. Air and space power. Joint Doctrine Publication 0-30. UK Ministry of Defence/Development, Concepts and Doctrine Centre. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668710/doctrine_uk_air_space_power_jdp_0_30.pdf. Accessed 30 Jan 2024

———. 2017b. Unmanned aircraft systems. Joint Doctrine Publication 030-2. UK Ministry of Defence/Development, Concepts and Doctrine Centre. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/673940/doctrine_uk_uas_jdp_0_30_2.pdf. Accessed 30 Jan 2024

———. 2018a. Human-machine teaming. Joint Doctrine Note 1/18. UK Ministry of Defence/Development, Concepts and Doctrine Centre. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/709359/20180517-concepts_uk_human_machine_teaming_jcn_1_18.pdf. Accessed 30 Jan 2024

———. 2018b. Combat air strategy: An ambitious vision for the future. UK Ministry of Defence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/725600/CombatAirStrategy_Lowres.pdf. Accessed 30 Jan 2024

———. 2019. Defence technology framework. Ministry of Defence. https://www.gov.uk/government/publications/defence-technology-framework. Accessed 30 Jan 2024

———. 2021. Defence in a competitive age. Ministry of Defence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-Defence_Command_Plan.pdf. Accessed 30 Jan 2024

———. 2022a. Defence artificial intelligence strategy. Ministry of Defence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082416/Defence_Artificial_Intelligence_Strategy.pdf. Accessed 30 Jan 2024

———. 2022b. Ambitious, safe, responsible: Our approach to the delivery of AI-enabled capability in Defence. UK Ministry of Defence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082991/20220614-Ambitious_Safe_and_Responsible.pdf Accessed 30 Jan 2024

Navy Lookout. 2020. Manta: The Royal Navy gets its first extra-large autonomous submarine. https://www.navylookout.com/manta-the-royal-navy-gets-its-first-extra-large-autonomous-submarine/. Accessed 30 Jan 2024

Royal Air Force. 2021. RAF rapid capabilities office demonstrates new technologies developed with industry partners. RAF News. https://www.raf.mod.uk/news/articles/raf-rapid-capabilities-office-demonstrates-new-technologies-developed-with-industry-partners/. Accessed 30 Jan 2024

Royal Marines. 2021. Drone swarms. YouTube. https://www.youtube.com/watch?v=7R0LcFfVxpQ. Accessed 30 Jan 2024

Royal Navy. 2022. Technology and innovation. https://www.royalnavy.mod.uk/news-and-latest-activity/features/innovation. Accessed 30 Jan 2024

Russell, Stuart. 2021. AI in warfare. BBC Reith lecture. https://www.bbc.co.uk/programmes/m00127t9. Accessed 30 Jan 2024

Sanders, Patrick. 2021. Sharpening the UK's defence in the 2020s. Speech at the RUSI Strategic Command Conference. https://www.gov.uk/government/speeches/commander-of-strategic-command-rusi-conference-speech. Accessed 30 Jan 2024

A Fertile Soil for AI? Defense AI in Sweden

Alastair Finlan

Sweden is very well positioned today regarding the development of AI for both civil and military applications. Most of the essential conditions are in place to make this high-technology Nordic nation an ideal environment for AI to grow, develop, and flourish at a rapid pace. This is in part due to bold and relatively recent strategic initiatives from the government and private foundations to invest in Sweden's AI future.

Nevertheless, the long-term fertility of Sweden's AI soil depends heavily on what is nurtured now, and though conditions are as good as they can be, it still requires active planning and preparatory work to ensure that the optimum benefits of this technology for defense AI purposes can be reaped in the future.

The current stage of AI's development in Sweden also comes at a rare moment in history when the country has decided to massively invest in its armed forces in the light of increasing instability in Europe and the War in Ukraine as well as abandon its longstanding policy on neutrality by applying to join the North Atlantic Treaty Organization (NATO) in 2022.

Together, these elements combine to create an extraordinarily beneficial climate for AI to flourish in what is already one of the most advanced and digitally networked societies in Europe.

Research on AI in the defense sector has long roots in Sweden. The country is also home to one of the leading-edge defense industries in the world in the form of Saab, which is already incorporating AI into deployable military systems. Much of the initial concept work about AI has already been started, and thanks to the massive investment in AI research in Swedish universities, this should develop rapidly.

The old and now resurrected total defense concept in Sweden also promises to ensure the flow of ideas and technologies between civil society and the armed forces to help defend the country if needed. AI has many significant benefits for the unique

A. Finlan (✉)
Swedish Defence University, Stockholm, Sweden
e-mail: Alastair.Finlan@fhs.se

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_5

strategic circumstances of Sweden, with a vast but sparsely populated territory to defend, which has been identified by earlier research in this area as something that could be offset by these new technologies.

The only major risk for the development and exploitation of AI for defense purposes is the question of prioritization in view of the massive scale required to revitalize and rebuild the Swedish conventional forces. There are so many areas that need attention after over two decades of decline and contraction of resources in the form of units, major equipment and bases. The question is whether investing in present-day military needs will push back investment in future capabilities (to the detriment of AI research) or whether a balance can be found.

1 Thinking About Defense AI

Sweden has a remarkable track record of success with regard to the production of engineering and technical innovations in the civilian and military spheres that has generated a global impact for a Nordic state with a relatively small population.

The spirit of rigorous scientific inquiry continues to reverberate strongly within and across educational, health, military, political, and social realms within Swedish society to the point that Sweden today is one of the most advanced digitalized nation-states in the world. From seamless money transfers from mobile phones (Swish) to effortlessly networked health systems, from health professionals to pharmacies, Sweden offers a rich and fertile environment for the so-called "Fourth Industrial Revolution" (AI, biotechnologies, and the Internet of Things (IoT)) to develop.

The connection between civil society and military organizations is an intimate one, and as Sweden embraces AI into the warp and weft of civil life, it will inevitably feed into and affect the military community that civilians consciously maintain for the security of the state.

Until the end of the Cold War, Sweden regularly recruited around 50,000 conscripts (about 18 years of age) every year and they constituted between 68–77% of the Swedish armed forces at any one time (Sørensen 2000: 321). In times of national emergency, Sweden had an impressive 850,000 military personnel available in the mid-1980s for operations with mobilization (Åselius 2005: 35).

Historically, the footprint of the armed forces in Swedish society has been surprisingly large, with nearly 10% of the nation serving in the armed forces during the latter part of the Cold War. That means that the senior leadership of the workforce in Sweden today will have, in all likelihood, military experience of some form or another.

Equally, the rapid reduction of the Swedish armed forces at the end of the Cold War shut down entire units but, conversely, opened up space for personnel to move around the services. Consequently, it is not unusual to meet a fighter pilot in the Air Force who started their military career in the army. This means that there is a degree of porousness in Swedish military culture that is not evident in other countries.

Naturally, the successful adoption of AI will necessarily be infused within a culturally influenced context to characterize a particular Swedish interpretation of this innovative and multi-dimensional technology from a "smaller military" perspective.

Unsurprisingly, Sweden has a long interest in AI given the seamless cosmopolitan connections and networks between scientific communities across continents in the time before the internet. While the concept of AI was first articulated by the American computer scientist John McCarthy in the 1950s, Swedish defense researchers were examining the idea as early as the 1980s (Schubert 2017: 22).

The critical turning point for Sweden with regard to AI and, as a corollary for its armed forces, occurred a little over 5 years ago when a scoping study from Vinnova, the Swedish innovation agency, looked at the state of AI in Sweden. Its conclusions were concerning. It assessed that:

> Swedish AI research has, overall, limited international competitiveness. It is a generally accepted view that development within AI, both in research and commercially, is dominated by the USA, with China being the main contender, while Europe has tended to lose ground, relatively speaking. (Vinnova 2018: 14)

This was a surprising statement in view that Sweden possessed considerable advantages over other nations in terms of digitalization and infrastructure. It clearly needed some form of government intervention to set Sweden on a better trajectory for the development of AI in both civil and military areas.

1.1 Sweden Embraces the AI Pathway

Sweden's government in 2018 published its AI strategy called "National Approach to Artificial Intelligence" and set out a bold vision of the future in the first paragraph of the document:

> Sweden aims to be the world leader in harnessing the opportunities offered by digital transformation. By international standards, Sweden is in the vanguard. Many countries have high ambitions for their digital development and Sweden must work hard to advance and strengthen its efforts. If Sweden succeeds, there will be considerable scope to develop Swedish competitiveness and welfare. One rapidly evolving field of digital technology is artificial intelligence (AI). (National Approach to Artificial Intelligence 2018: 4)

"National Approach to Artificial Intelligence" is primarily focused on stimulating and encouraging growth in AI in Sweden through the development of what it describes as four conditions: 'education and training, research, innovation and use, framework and infrastructure' (National Approach to Artificial Intelligence 2018: 5). By strengthening engagement in these conditions, Sweden should be well placed in terms of AI in society.

Much of the focus in the document is on growing AI within civil society, but there is a focus within the 'research' condition for benefitting from "the synergies between civil research and defense research from a total defense perspective"

(National Approach to Artificial Intelligence 2018: 7). More specifically, it suggests that:

> AI is also a growing field in defense research. There are potential opportunities for coordination between civil research and defense research, including cybersecurity and autonomous systems, that should be seized. (National Approach to Artificial Intelligence 2018: 7)

For a society that is very advanced and highly reliant on digital systems, there is an acute awareness of the vulnerability of all these technologies to malicious attack from outside of Sweden. Equally, though not an area of large development yet by the Swedish armed forces, there is also a recognition that autonomous platforms will be an important technological pathway in the defense sector in the future.

"National Approach to Artificial Intelligence" defines AI quite broadly as "intelligence demonstrated by machines" that is taken from the Vinnova report, but it recognizes that there are many definitions of it (National Approach to Artificial Intelligence 2018: 4).

1.2 Total Defense and AI

The total defense concept has significant potential to be an indirect driver of the adoption of defense AI as it is designed to meld and harness the power of civil and military spaces in times of national need. Sweden has promoted the concept of total defense for a very long time, and it has become culturally embedded in society and among political and military elites on how to think about war and defense in the modern age.

The Swedish armed forces have famously not fought a war in the name of the state for over 200 years, but its thinking about war and warfare has continued with limited experience of actual combat through international missions with the United Nations and with coalition forces in Afghanistan in the twenty-first century.

According to Sebastian Larsson, the conceptual and historical foundations of total defense emerged in the dark days of the Second World War when Sweden trod a delicate and dangerous diplomatic path between Nazi Germany, the Soviet Union, and the Allies. An official report argued that the lines between civil and military "have to a large extent been erased" (Larsson 2021: 47).

This thinking of an entwinned space between the civilian and military world dedicated together to defend Sweden was further developed throughout the Cold War in which Sweden could assemble and equip a 300,000-man field army (Finlan 2021: 475), if necessary, by drawing upon its small cadre of military professionals combined with trained conscripts from civil society.

The end of the Cold War witnessed Sweden, along with many nations in Europe, drawdown their military capabilities to exploit the benefits of the peace dividend, but Russia's invasion of Crimea in 2014 provoked a resuscitation of the total defense concept. As James Wither explains, the updated contemporary idea of total defense:

> is defined in Swedish law as 'all activities preparing the society for war' and consists of both military and civil defence. (Sweden, Government Offices 2018) In contrast to Finland, Sweden abandoned its traditional whole of government and society preparations for defence after the Cold War. Policy changed in 2015, when the government tasked the Ministry of Defence and the Civil Contingencies Agency of the Ministry of Justice jointly to develop a total defence proposal. (Wither 2020: 65)

In many other societies in Europe, the armed services are often perceived as a separate dimension of society that are given significant autonomy to conduct operations without much involvement of civilians, except in specialist roles. In contrast, Sweden's armed forces have a much larger societal imprint, through residual memory of the original total defense concept in the Cold War and an expectation or norm that the active participation of civil society in defense is critical to military success. This is very different to other countries, such as the United Kingdom, for instance.

AI can potentially handle the vast information loads concerning the mobilization of key sectors of civil society such as healthcare to cater for the anticipated needs of the armed forces if combat occurs. Mobilizing a society, even for a so-called small state like Sweden, with a population of 10 million inhabitants, still requires massive data lakes to be accessed and actioned at appropriate times, using cutting edge mobile phone technology. AI can greatly assist in these critical preparatory measures.

1.3 The Impact of AI on the Future of Warfare

Swedish thinking about AI and its potential applications for the armed forces and for Sweden's security is very much at an early stage. This is reflected in the sparsity of debates about the potential ethical aspects of defense AI, though initial work is beginning to emerge in Sweden (Malmio 2023).

Consequently, inceptive thinking has been naturally quite conceptual in scope and initial studies suggest that it may have broad benefits across the spectrum of warfare and for the concept of total defense. An early investigation by the Swedish Defense Research Agency or FOI in 2019 made the case that AI could offer "advantages" (Andersson et al. 2019) in specific areas.

FOI's research pointed toward various dimensions of warfare that could be augmented by the incorporation of AI data such as sensor analysis (Andersson et al. 2019). Monitoring of sensors ostensibly seems to be an innocuous and tangential aspect of warfare when compared to the kinetic dimension such as active fighting, but it has even greater significance in the light of the recent introduction of hypersonic weapons by Russia. Hypersonic weapons are a game-changer in modern warfare (Finlan 2021: 481). The reason is simple: speed.

The extraordinary velocity of hypersonic weapons places enormous pressure on humancentric command and control systems to respond in a timely manner. Hypersonic speed exceeds the natural abilities of people to react and, consequently, a military advantage gap develops between those who possess this technology (Russia) and everyone else. Swedish researchers argue that AI offers, through

sensor analysis, an ability to improve decision-making cycles (Andersson et al. 2019) by increasing the speed of assessment of the raw data being thrown up by different inputs such as "radar signals and sonar data" (Andersson et al. 2019). To a degree, the pace of technology is also acting as another indirect driver of defense AI is this respect.

The benefits of integrating AI into the military system architecture would potentially greatly enhance situational awareness and act as a "force multiplier" (Finlan 2021: 477). Situational awareness should be elevated to a principle of war (a guideline for planning/action) in the twenty-first century because of the power of innovative and new technologies, such as drones, that overlap and influence traditional boundaries in warfare.

Principles of war vary from country to country and generally range between nine and twelve. Many are derived from twentieth century warfare. That said, warfare as witnessed in Ukraine now has clearly undergone some significant alterations in terms of the absorption of new technologies such as drones of all varieties with traditional arms in the form of artillery and infantry.

Together, they have greatly augmented the power of traditional formations that has necessitated the return of old tactics such as the construction of trenches to offset the improved firepower element and exploit the protective qualities of earth and wood. A future refresh of the principles of war in the light of modern technology and praxis needs to embrace the significance of situational awareness with an eye on future AI applications in this area.

Another aspect highlighted by the Swedish researchers was the utility of AI when combined with intelligence work. The problem with intelligence in the twenty-first century is the excessive volume of data that often overwhelms the ability of human analysts to see the bigger picture or draw a line between significant dots that point to another "9/11" or "Pearl Harbor" (Andersson et al. 2019). FOI argues that "AI offers an opportunity to identify the unexpected – the so called 'black swan' – by analyzing large volumes of traditional intelligence data in combination with open web data" (Andersson et al. 2019). The use of web-based data also facilitated the employment of so-called algorithmic warfare that enables the monitoring of internet traffic and chatter to specifically identity targets of opportunity that can be actioned against by military forces. This was recently demonstrated in Ukraine when a concentration of Russian soldiers being moved up to the front line was precisely targeted with a missile based on this method of identifying clusters of soldiers from their internet/digital footprint (Candlin 2023).

2 Developing Defense AI

Sweden finds itself in an unexpected place in terms of its defense posture. For years after the end of the Cold War, successive governments in Sweden assumed that defense was a low priority to the point that they drew down their forces and capabilities on a massive scale, from shutting bases, closing entire military units and

selling off heavy equipment such as artillery. The future Sweden imagined was of a small, largely professional military that would contribute to expeditionary international missions without much concern for homeland defense in view of the peaceful and stable European environment.

Russia's seizure of Crimea in 2014 provoked a shift in government and public attitudes towards the issue of defense that has gained significant momentum today. The Russian invasion of Ukraine in 2022 and the ongoing war have solidified defense policy around national defense, and the Swedish armed forces find themselves in the challenging position of receiving vast amounts of increased funding while trying to resurrect, reconstruct and revive former capabilities while at the same time looking ahead to the future to see what it should invest in now.

This context dominates the future R&D priorities. An inkling of the future direction is provided by a very new publication by the Swedish armed forces called 'A Stronger Defense for a Challenging Future' in which it states that "the future operating environment will be greatly affected by technological developments" (Försvarsmakten 2022: 26). A great emphasis is placed on digitalization and the connections between different systems that will facilitate better situational awareness. The research is acutely conscious of the links between the five domains of air, land, sea, cyber and space in future warfare and technologies must have an ability to synchronize within this multidomain environment (Försvarsmakten 2022: 29).

What is interesting between the FOI and Swedish armed forces studies is how the research agency sees many applications for AI whereas the military focuses really on just a few explicit pathways for development. A focus on digitalization and the connections between different systems would be an ideal developmental area for AI.

It needs to be recognized that FOI is a research support agency for the armed forces. It can make suggestions and drive research in specific areas, but these are directed by the Swedish military.

The report specifically mentions AI regarding its future applications with autonomous platforms (Försvarsmakten 2022: 27) and intelligence support. This is highly interesting in view that this is an area of limited development within the armed forces, but clearly it sees applications here. Presently, the armed forces have just eight very small UAVs (Finlan 2021: 475) and a research stake in Dassault's nEUROn drone (Finlan 2021: 480) and have recently become involved "on the margins" with the British Tempest sixth generation fighter aircraft development that may well be unmanned or offering an unmanned option. The focus is clearly on more kinetic options for the future, rather than the more attainable information management dimension of warfare.

2.1 The Swedish AI Ecosystem

There is a fair degree of uneven development in the Swedish AI ecosystem that has been formally recognized by state research agencies and the government. Typically, for Sweden, the solution is a mixture of state intervention and private financing to

improve key competencies in the ecosystem linking primarily civilian applications; though increasingly through the total defense posture, it will flow into the military world.

2.1.1 Civil Initiatives

The largest private investment in autonomous systems research was offered in 2015 by the Knut and Alice Wallenberg Foundation (WASP Undated), which is part of the extraordinary family of industrialists and bankers in Sweden who own many famous companies, including Saab. Its chairman is Marcus Wallenberg, who is also vice chair of the Knut and Alice Wallenberg Foundation.

It is called WASP (Wallenberg AI, Autonomous Systems and Software Program) and involves five partner universities including "Chalmers University of Technology, Linköping University, Lund University, KTH Royal Institute of Technology and Umeå University." It is claimed to be "the largest individual research program in Sweden" (WASP Undated). This perhaps indicates how important the development of AI and autonomous systems and associated software is to Sweden.

Linköping University is home to the National Supercomputing Centre and has greatly benefitted from WASP's funding. In 2021, it inaugurated one of Europe's fastest supercomputers for AI called Berzelius. This has pushed Sweden to the forefront of these technologies in Europe. Berzelius has "94 AI systems, which together consist of 752 GPUs. With more interconnected systems, which also have higher clock rates, the new computing power equates to as much as 470 petaflops for AI calculations" (Linköping University 2023). The important aspect to note about Berzelius is that it is seen as a "national resource" (Linköping University 2023) for all researchers across Sweden. Thus, this technology is not parochial to Linköping University and can act as a core engine for innovation and development in the Swedish AI ecosystem.

2.1.2 Military Initiatives

The Swedish armed forces own university, the Swedish Defense University, has also developed expertise in AI systems over the years through encouraging doctoral research in this area that spans technical and warfare dimensions. The massive research funding that the armed forces use to encourage research in areas of national defense interest through programs such as Forskning och Teknikutveckling (Research and Technology Development or FoT) also stimulates critical research across numerous universities and research institutes in Sweden. For 2023 alone, the FoT budget is planned to be almost SEK952M (nearly USD100M) rising to over a billion Swedish kronor by 2025 (Budgetpropositionen 2023: 56).

Along with all aspects of defense, FoT and Forskning och Utveckling (Research and Development or FoU) funding pathways are enjoying a significant uplift to

fulfill the burgeoning research needs of the armed forces as it orientates itself towards potential future warfare.

The Swedish Air Force is the only service that pointedly mentions AI in its list of future capabilities. Admittedly, not at the top of the list, but nevertheless included in its line-up of new strengths.

The Air Force wants to create "a unit for intelligence analysis with support from AI" (Försvarsmakten 2022: 61). It does not go into specific details of what this unit will do, but it can be speculated that such a unit could naturally be employed to develop an overview of enemy forces, movements, strengths, and weaknesses in order to support the Swedish Air Force's decision-making processes at the strategic and tactical levels.

It is quite natural for AI to have just a minor support role at this early stage of development, but with time and confidence this very new capability will undoubtedly encourage further applications if it works well.

It is highly likely that military AI research will be an important aspect of the Swedish AI ecosystem as the shift to greater digitalization and integration of systems will demand much more computer (supercomputer) power in the armed services. This is very much at a nascent stage as other more pressing priorities such as manpower, units, bases, and major equipment programs take precedence; but—inevitably—the armed forces will have to makes some big decisions regarding AI and the supporting AI infrastructure soon, if it wants to fulfil its digital and multidomain ambitions.

2.1.3 AI Partners in Sweden and Abroad

The Swedish AI ecosystem is fortunate to possess some of the most high-technology and globally renowned defense industries in the world. Saab, for example, is universally known for the quality of its military products and their reliability in modern combat. Most recently, one of its lesser-known technologies, the Next Generation Light Anti-Tank Weapon (NLAW) has proven to be one of the most effective weapon systems of the ongoing Russo-Ukraine War. It is unsurprising given the history of the company that they are very much at the leading edge of AI for military purposes with a very practical view on what is possible at this evolutionary stage of AI. Two main areas stand out at the moment. These are:

- *Predictive Maintenance*

Modern military vehicles such as aircraft and ships generate a great deal of data and AI can predict when a problem is likely to arise "before it breaks down" (Saab 2021). This not only potentially saves an enormous amount of cost, but also makes military technologies "smarter" (Saab 2021) and more effective. Maintenance of vehicles seems an unglamorous part of warfare, but some areas of fighting are wholly dependent on them. For example, armored warfare involving modern main battle tanks has gained great prominence in Ukraine. For every one tank in the field, two will be in the process of being repaired or completely broken down. This is a

standard condition of mechanized warfare that has been the case since tanks arrived on the battlefield in World War I.

AI can potentially affect this dynamic through predictive maintenance and enable military commanders to maximize the utility of their armored forces and air forces in a way not seen in warfare to date. For smaller armies with less resources, it enables them to punch above their weight when fighting against more powerful opposition because they are getting the best possible performance out of their equipment.

- *Massive Data Fusion*

This is a relatively simple idea that has extraordinary potential across civil and military applications. In essence, according to Saab, it is "a cloud-based data lake where we take data and put it into the context of time and space" (Saab 2021). This is a very powerful tool because it offers a means to make "real-time predictions about the physical behaviors of where people, ships or planes are going, and also predict the contextual behaviors of what these people, ships or planes are actually doing" (Saab 2021).

A cloud-based data lake offers many advantages for military services. First, it builds in redundancy into the system because it is not dependent on just one physical platform site. If a key base, facility, or platform is destroyed as a result of combat or hostile electromagnetic fire, the system continues and survives. Second, it lays the connective groundwork for the next step in modern warfare, beyond combined and joint operations towards integrated operations. In theory, the integration of all these sensors through a common data lake offers a powerful machine-based sensitivity to unfolding actions on the battlefield that greatly outstrips people-based capabilities.

Sweden has longstanding relationships and engagements with many of the leading IT companies in the world, such as IBM, who are at the forefront of AI research. That said, however, its 2022 application to join NATO promises even greater benefits in terms of AI cooperation for military purposes.

2.1.4 NATO

The decision by the Swedish government to jointly apply together with Finland for NATO membership in 2022 is historic in every sense of the word. Abandoning 200 years of neutrality was no easy step for a country that has tried to stay away from entangling agreements that could potentially drag the country into a major war.

From an AI perspective, the relationship with NATO offers huge benefits and it is likely to be an indirect driver for defense AI in Sweden. Despite not being a member of NATO as of January 2024, the Swedish armed forces have closely followed doctrinal and planning developments in the North Atlantic Alliance. For example, it has been teaching NATO's planning tool or the Comprehensive Operations Planning Directive (COPD) to senior officers undertaking higher education courses for many

years. Consequently, what NATO decides with AI will be mirrored to some extent in Sweden and it merits attention.

NATO recognizes the military significance of AI and is striving to adopt it in a responsible way that both incorporates its advantages for NATO operations and also protects it from counter-AI use from potential enemies. In a very typical way for a long-established organization, NATO has put in place certain drivers to push forward with AI research. The first of these is DIANA (Defense Innovation Accelerator for the North Atlantic) "to bring nations and their industries into closer partnership to fund, develop, and field dual-use EDTs, with AI being one of the primary technologies" (Fata 2022). EDT means emerging and disruptive technologies and DIANA is designed to act as a catalyst for cutting-edge research to develop in partnership with NATO.

Alongside of DIANA, NATO has also established the NATO Innovation Fund (NIF) (Fata 2022) that offers a funding pathway for promising research in this area. These drivers indicate how seriously the North Atlantic Alliance takes AI and how it aims to be at the leading edge of this research in terms of practical applications.

Sweden's membership of NATO would thus not only have benefits for the Alliance regarding AI research, but also open up new avenues for research cooperation and funding in this area.

3 Organizing Defense AI

In Sweden, the lead organization regarding the use of AI for defense purposes is FOI. It has by far produced the most reports and conducted research in this area for quite a long time. FOI has a very central remit when compared to defense research in other countries that are often just part of a wide constellation of competing research agencies vying for government funding. In many ways, the centrality of FOI fits the innate drive for respect of science-based knowledge and the Swedish armed forces are steeped in it. According to FOI, its purpose is:

> to support the shaping, build-up, and utilisation of Sweden's defence resources through its research-based knowledge and experience. In concert with the Swedish Armed Forces and the Swedish Defense Materiel Administration, FOI's task is to develop its knowledge and expertise for the benefit of Sweden's operational defense forces, both in the short and in the longer term, as well as helping to apply this knowledge in the full range of defense processes from perspective studies to evaluation. (FOI Undated)

FOI researchers are usually civilians that are commissioned by the armed forces and other state agencies to do work/tasks in specified areas.

Essentially, what starts off as innocuous research in FOI can well lead to profound impact in terms of affecting how a technology or concept is adopted and employed at the operational level by the Swedish armed forces. Consequently, what FOI is looking at the paper level regarding AI has great significance several years down the line given this intimate relationship between researcher and warrior. The relatively small size of the Swedish armed forces and their joint outlook that starts

right from initial officer training (Finlan et al. 2021: 357) ensures that ideas percolate relatively quickly in the overall organization.

The Swedish Armed Forces can be broken down into (Hackett 2023: 137–139:

- The Army (6850 soldiers) with 120 Leopard 2 tanks, 411 infantry fighting vehicles, 1064 armored personnel carriers, 35 Archer 155 mm guns and 6 Patriot PAC-3 systems.
- The Navy (1250 sailors and 1100 amphibious forces) with 5 conventionally powered submarines, 5 Visby Class corvettes, 4 coastal combatants, 133 small combat boats (troop transport), 7 mine warfare vessels and 11 landing craft.
- The Air Force (2700 in total) with 98 Gripen multi-role combat aircraft, 3 Airborne early warning and control aircraft, 8 transport aircraft, 8 RQ-7 Shadow UAV and 53 helicopters.
- Special Forces (2950 with supporting staff)
- In total, 14,600 with 10,000 reservists

Providing a detailed breakdown of the Swedish armed forces in this way shows how AI can augment and bind the different aspects of the services to maximize their potential utility. It also reveals the challenges that the armed forces face in quickly expanding the size of the individual services in view of how much they contracted from the time of the Cold War. The reintroduction of voluntary conscription is one pathway to increasing the size of the forces alongside building up the size of the total officer corps. Again, with both measures, it will take years to substantially boost the number of combat personnel. Nonetheless, the small size and porousness of the Swedish armed forces provide an environment conducive to advancing defense AI as parochial, service-specific interests that can hamper the diffusion of defense AI are less pronounced in Sweden than in other countries.

There has been much speculation in various research papers from FOI as to how AI can best serve the armed forces given the state of its development. Much of the work from FOI focuses on the benefits of AI in terms of Command and Control (C2) applications using AI for planning, analysis, and execution (Schubert et al. 2018), but other work stresses the benefits of training purposes.

The most recent defense perspective study, "A Stronger Defense for a Challenging Future" stresses a future in which multi-domain operations and coordination between these domains will be vital. This points naturally towards AI, but it is not explicitly stated as such.

A large part of the problem with AI is that it is quite an opaque technology for people who do not have more than a layman's understanding of it. Explainable AI is one pathway to improve general knowledge about possible applications, and this is an area that FOI is exploring. Nevertheless, military organizations are inherently conservative, and that perhaps has some explanatory value as to why only the Swedish Air Force has explicitly embraced AI so far. Air forces tend to be on the cutting edge of technology so that explains to a degree why the Swedish Air Force has taken this quite radical step forward with this new and promising technological pathway.

The inherently joint nature of the Swedish armed forces will ensure that should AI work well for the Air Force, then these lessons will be quickly absorbed by the other two services, and increasingly, through training with the technology, it should seem a more natural fit. The Swedish armed forces have invested significantly in game and simulation technology for training purposes and AI will fit very well with these applications.

4 Funding Defense AI

4.1 The Armed Forces

The funding landscape for Defense AI is unusually beneficial due to the massive increase in defense funding in general, which includes research into specific future technologies and capabilities, but also from civilian sources as well. In 2022, Sweden announced that its defense funding would reach 2% of Gross Domestic Product (GDP) by 2026 and that funding alone would enjoy an increase of USD800M in 2023 (O'Dwyer 2022). In total, the Swedish defense budget will grow from USD7.3bn in 2022 to USD12bn by 2028 (O'Dwyer 2022).

Admittedly, while much of the funding will go to major equipment projects and expanding the size of the Swedish armed forces; nevertheless, there are also signs of a willing to fund leading edge technologies such as AI. A great focus of the 2023 increase is towards boosting cyber-defenses through a dedicated cyber defense unit that will protect both military and civilian vital IT assets (O'Dwyer 2022).

4.2 Wallenberg AI, Autonomous Systems and Software Program (WASP)

From purely the civil sphere of research funding, the Knut and Alice Wallenberg Foundation, through WASP will provide funding over a 15-year period, from 2015–2031 of SEK4.9bn (nearly USD500M) that will be supplemented by more funding from other partners taking the total to SEK6.2bn or almost USD600M (WASP Undated).

This is one of the largest specific funding programs for AI in Europe and indicates how seriously Sweden intends to build up core competencies for the benefit of Swedish society.

Specifically, it has the ambition to produce 600 PhD students and an intention to create 80 research groups. They have already recruited 53 international senior faculty and have 80 companies and organizations involved in WASP.

These budget and program trends in Sweden suggest that within 5 years (the typical duration of a PhD in Sweden) a significant increase of human capital

expertise will be available for both civil, military, and total defense purposes. This represents a significant R&D investment in this area that has manifold societal benefits.

Thanks already to WASP, Sweden now possesses one of the most advanced supercomputers in Europe devoted specifically to AI applications that promises to help push and develop the boundaries of research in numerous related fields that have security benefits for society.

4.3 Vinnova and AI Sweden

Vinnova, Sweden's innovation agency, also directly stimulates and funds research into artificial intelligence through an entity called AI Sweden that has resulted from a public/private finance initiative.

AI Sweden is "the national center for applied artificial intelligence" (AI Sweden Undated) and encourages a wide range of activities related to AI across society in Sweden. According to AI Sweden (AI Sweden Undated), it manages:

> projects of national interest together with our partners in areas such as information-driven healthcare, decentralized AI, edge learning in space, and language models for the Swedish language. Moreover, we are building talent programs and provide courses and resources for driving organizational change.

The founding partners of AI Sweden include many of the largest state and private actors in Swedish society, from the National Tax Office (Skatteverket) to Volvo and a host of universities and private companies such as AstraZeneca. It is an extraordinarily influential group of partnerships that demonstrates how much AI research is being encouraged within Swedish society by the state authorities in close collaboration with private industry.

Many of these organizations and companies have close relationships with members of the armed forces and through the total defense approach, the flow of ideas and technologies from civil sector to defense will be intimate. The Swedish armed forces finance a great deal of applied research in defense-related technologies through the FoT and FoU pathways in many of the world-leading universities in Sweden.

5 Fielding and Operating Defense AI

The application of Defense AI industries is very much at an early stage of development in Sweden with much work ongoing in the civil sphere with a few dedicated companies developing it specifically for defense purposes. Sweden has a long history of thorough testing of military technologies before releasing them for general use and AI is no exception in this respect. Necessarily, it means that initiatives with

AI will take time to become operational but nevertheless there are green shoots of activity right now in specific companies such as Saab with real world applications. As Saab publicly admits:

> In recent years we've seen Artificial Intelligence (AI) become a key element in much of Saab's security and defense product portfolio, be it for the likes of surveillance sensors, smart cockpit technology or autonomous sea rescue systems. (Saab 2021)

The benefits of AI for military sensor information processing are numerous. It can handle significant quantities of data from different sensors and provide a form of fusion capability to render the results as quickly as possible for decisionmakers in a tactical environment. One of Saab's products, the Information Fusion System, "collects data and information from a large variety of sources, such as Communication Intelligence (COMINT), Electronic Intelligence (ELINT), Acoustic Intelligence (ACINT) and Geographic information systems (GIS)" (Saab Undated).

The AI algorithms "can be integrated and trained" with this data to enhance the already powerful processes within the system that focus on classic AI applications such as "speech-to-text, entity detection, topic detection, speaker identification and language identification" (Saab Undated). Together, a fusion ability here provides a powerful augmentation to existing capabilities.

This technological augmentation pathway for improving sensor data was clearly highlighted by FOI's influential study and dovetails with a national priority: to be able to defend Sweden from external attack. Sweden is a vast country (twice the size of the United Kingdom), but it has a relatively small population of around 10 million. This means as the FOI report indicates:

> AI could have a significant impact on what has long been one of the major challenges facing the Swedish Armed Forces; namely surveillance of a vast and, in parts, very sparsely populated territory. (Andersson et al. 2019)

This perhaps explains why the first concrete planned use of AI for the Air Force is to provide "intelligence support" and the ability to handle sensor data in vast quantities offers significant benefits for monitoring the very large Swedish battlespace.

The complexity of AI necessitates a very large support infrastructure that relies heavily on industry-supplied expertise. Back in 2018, the Vinnova report into AI recognized that Sweden lacked sufficient human resources regarding AI. Its SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis highlighted (Vinnova 2018: 13):

- AI competence hard to recruit;
- Lack of competence for digital business models;
- Universities and university colleges have weak drivers for flexible professional training;
- Many SME have limited resources and competence.

The report specifically looked at civil society, but the situation in the military sphere naturally reflects the state of the nation that supplies and sustains its force structure. It is likely, given the huge investment in AI education and training, that the AI competence gap is being gradually filled, but the armed forces will have to rely heavily

on defense industries such as Saab to lead the way in developing and sustaining these innovative technologies.

This places a great emphasis on nationally based digital hubs/networks to provide support conduits for the vital AI sustenance that the armed forces require in operations. Inevitably, it reduces the space between civil and military spheres, but within the total defense concept, this state of affairs would be seen as a desirable working framework rather than something unusual.

The advanced state of digitalization and networking in Sweden offers enormous benefits regarding the successful operationalization of AI capabilities within the national military battlespace; but equally it highlights how important the protection and security of these technologies are for Sweden's future defense.

6 Training for Defense AI

The potential applications of artificial intelligence for military purposes in the defense realm are manifold and potentially game-changing regarding autonomous platforms in the form of aerial, land, and sea-based armed and unarmed drones.

Nevertheless, this remarkable technology is not immediately human compatible in relation to warfighting utility because it requires training and understanding to grasp how AI sees and interprets the digital and physical worlds.

This element was identified in a 2019 FOI report called "Explainable Artificial Intelligence". It stressed that:

> in the military domain the ability to understand and explain the behaviors of AI systems is critical. In this context, the decisions and recommendations provided by the AI systems may have a deep impact on human lives. This is valid at the tactical level where autonomous weapons and drones are used, as well as at the operational and the strategic level where long-term decisions are made by military leaders and political decision makers. (Luotsinen et al. 2019: 45)

Put simply, AI is not a "plug and play" technology. Military personnel must be trained alongside its gradual introduction to understand and develop trust in the AI. For most people, AI is a nebulous term and consequently, researchers have realized the importance of developing 'explainable artificial intelligence' so that operators of these systems grasp what the AI can and cannot do.

This is of great significance for any profession in which the risk to life is high, whether it be for military organizations or health agencies of the state.

For the Swedish armed forces, adequate training of key personnel who both operate and command AI systems will be critical to the successful employment of this technology in the field. While in early stage, it is an area that needs to be prioritized in the future in the same way that Sweden's national strategy document places an emphasis on education and training as one of its essential four pillars for AI development.

The likely initial use of AI for training purposes will be in the areas of games and simulations that Sweden has considerable experience with, not least at the Swedish Defence University that has a game unit for assisting with officer training.

One avenue of exploration is how AI can be used to improve enemy representations and behavior in simulations to make them "more realistic" (Kamrani et al. 2019: 4) and have more value to the Swedish armed forces when training. This can be considered one of the easiest aspects of AI to develop that does not require all personnel to understand how the technology works, but rather small teams of experts who create the scenarios and run the technology.

In view that much warfare is platform-based (aircraft, ships, tanks, and armored personnel carriers), it has great potential for leadership training before applying these skills physically in the field. It also enables young officers and more senior officers to grasp the bigger picture of the battlespace that is often unseen in actual combat because it is so compartmentalized in terms of geography and place in the order of battle. For example, a soldier of a campaign only sees what is in front of them in terms of platoon-based warfare rather than the bigger picture that senior commanders have. It offers a better or holistic understanding of command networks and functions within a battlespace.

This also explores an element that is focused on in explainable artificial intelligence: to show visually (in terms that humans can quickly grasp) how AI reaches its conclusions and translate that facet into a training regime. If the training appears unrealistic, then people will not take it seriously and that affects training outcomes.

7 Conclusion

The conditions for the successful development of artificial intelligence for defense purposes are clearly visible today in Sweden, but much depends on how much of a priority it is given. The winds of war from Ukraine are palpably felt in this Nordic country, more so than other European partners such as the UK or Spain, and its historical and cultural links to the region have added great impetus to the revitalization of its defense forces.

Nevertheless, the opportunities afforded by the massive reinvestment in its military forces also carries a risk: Will investing in the future (capabilities) have a lower prioritization than investing in the present-day ones?

The scale of Swedish defense reconstruction is massive, from its army to the navy and the air force, but difficult choices need to be made about new technologies that are already affecting modern warfare such as drones, hypersonic missiles, and AI. It requires not just a technological reinvestment, but also an educational one to grasp the significance of the new warfighting environment currently unfolding in Ukraine.

The latter is perhaps harder than the former to achieve because it requires new thinking, a shaking up of educational, doctrinal, and training curricula that only the strongest military leadership and/or a significant external shock usually achieve.

Regardless of which, AI is going to develop at a rapid pace in Swedish civil society thanks to a forward-looking national strategy from 2018 backed up by massive amounts of private and public investment. The Swedish government has set the course for Sweden to be at the forefront of the AI revolution within the next two decades and the establishment of one of the most power supercomputers for AI in Europe at Linköping University shows that the country is putting words into practice.

This enlightened approach to AI policy could well lay the foundations for Sweden's high-technology society to embrace the benefits of the fourth industrial revolution far sooner than many other countries in Europe.

What links this potential dynamic pathway to AI maturation to its armed forces and the security of Sweden is the total defense concept that will ensure a smooth flow of ideas and technologies concerning AI between the civil and military spaces.

Through total defense, the Swedish armed forces will be able to benefit from the surge in competence in AI that is already coming to fruition as each cohort of PhD students is produced. The natural partnership between the cyber realm and autonomous platforms means that demand for AI expertise in the armed forces is likely to grow.

An additional benefit for the Swedish armed forces is the close partnership with one of the globally leading defense companies in the form of Saab, who is not only pushing forward with the development and deployment of AI at the sensor level, but also developing exciting and cutting-edge applications for the near future.

The possession of such a national defense industry with a dynamic research environment will offset any organizational resistance internally from within the armed forces for its adoption.

Externally, the Swedish Defense Research Agency has already laid down much of the initial conceptual work for thinking about AI for defense purposes and it is likely to provide further intellectual support for the armed forces for a way ahead.

In sum, given the weight of investment in AI by Sweden's government, state research agencies and private foundations, this technology has solid foundations for development in the near term that has great benefits for a military in transition and supported by one of the best defense industries in the world.

The AI future is potentially very bright in Sweden.

References

AI Sweden. Undated. Accelerating applied AI in Sweden. https://www.ai.se/en. Accessed 30 Jan 2024

Andersson, Christer, Tove Gustavi, and Maja Karasalo. 2019. Artificial intelligence – opportunities and challenges for Sweden's National Security. FOI Memo 6869. https://foi.se/en/foi/reports/report-summary.html?reportNo=FOI%20Memo%206869. Accessed 30 Jan 2024

Åselius, Gunnar. 2005. Swedish strategic culture after 1945. *Cooperation and Conflict* 40 (1): 25–44. https://doi.org/10.1177/0010836705049732.

Budgetpropositionen. 2023. *Regeringen.se*. https://www.regeringen.se/rattsliga-dokument/proposition/2022/11/prop.-2022231. Accessed 30 Jan 2024

Candlin, Alex. 2023. Role of algorithmic warfare is a 'game-changer' on the battlefield. Forces Net. https://www.forces.net/technology/role-artificial-intelligence-game-changer-battlefield. Accessed 30 Jan 2024

Fata, Daniel. 2022. NATO's evolving role in developing AI policy. Center for Strategic and International Studies, https://www.csis.org/analysis/natos-evolving-role-developing-ai-policy. Accessed 30 Jan 2024

Finlan, Alastair. 2021. The shape of warfare to come: A Swedish perspective 2020–2045. *Defense and Security Analysis* 37 (4): 472–491. https://www.tandfonline.com/doi/full/10.1080/14751798.2021.1995976.

Finlan, Alastair, Anna Danielsson, and Stefan Lundqvist. 2021. Critically engaging the concept of joint operations: Origins, reflexivity and the case of Sweden. *Defence Studies* 21 (3): 356–374. https://www.tandfonline.com/doi/full/10.1080/14702436.2021.1932476.

FOI. Undated. Swedish defence. https://www.foi.se/en/foi/about-foi/swedish-defence.html. Accessed 30 Jan 2024

Försvarsmakten. 2022. Ett Starkare Försvar för en Utmanande Framtid. Slutredovisning av Försvarsmaktens Perspektivstudie FM 2022-1997 9:15

Hackett, James, ed. 2023. *The military balance 2023*. London: Routledge.

Kamrani, Farzad, Mika Cohen, Frederik Bissmarck, and Peter Hammar 2019. Beteendemodellering med imitationsinlärning. FOI. https://foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R%2D%2D4890%2D%2DSE. Accessed 30 Jan 2024

Larsson, Sebastian. 2021. Swedish total defence and the emergence of societal security in idem and. In *Nordic societal security: Convergence and divergence*, ed. Mark Rhinard, 45–67. London: Routledge.

Linköping University. 2023. Swedish AI research gets more muscle. https://liu.se/en/news-item/svensk-ai-forskning-far-mer-muskler. Accessed 30 Jan 2024

Luotsinen, Linus J., Daniel Oskarsson, Peter Svenmarck, and Ulrika Wickenberg Bolin. 2019. Explainable artificial intelligence: Exploring XAI techniques in military deep learning applications. FOI. https://foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R%2D%2D4849%2D%2DSE. Accessed 30 Jan 2024

Malmio, Irja. 2023. Ethics as an enabler and a constraint—Narratives on technology development and artificial intelligence in military affairs through the case of project maven. *Technology in Society* 72: 1–10. https://www.sciencedirect.com/science/article/pii/S0160791X22003347. Accessed 30 Jan 2024.

National Approach to Artificial Intelligence. 2018. Stockholm: Government Offices of Sweden. https://wp.oecd.ai/app/uploads/2021/12/Sweden_National_Approach_to_Artificial_Intelligence_2018.pdf. Accessed 30 Jan 2024

O'Dwyer, Gerard. 2022. Sweden boosts defense spending, NATO goal in mind. Defense News. https://www.defensenews.com/global/europe/2022/11/22/sweden-boosts-defense-spending-nato-goal-in-mind/. Accessed 30 Jan 2024

Saab. 2021. AI at Saab: Artificial eye. https://www.saab.com/newsroom/stories/2021/september/artificial-eye. Accessed 30 Jan 2024

———. Undated. Data fusion for common processing and reporting. https://www.saab.com/products/information-and-intelligence-fusion. Accessed 30 Jan 2024

Schubert, Johan. 2017. Artificiell Intelligens för Militärt beslutsstöd. FOI. https://foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R%2D%2D4552%2D%2DSE. Accessed 30 Jan 2024

Schubert, Johan, Joel Brynielsson, Matthias Nilsson, and Peter Svenmarck. 2018. Artificial intelligence for decision support in command and control systems. *Proceedings of the 23rd international command and control research & technology symposium*, paper 30. http://internationalc2institute.org/s/23rd_ICCRTS_Revised_paper_30.pdf. Accessed 30 Jan 2024

Sørensen, Henning. 2000. Conscription in Scandinavia during the last quarter century: Developments and arguments. *Armed Forces & Society* 26 (2): 313–334. https://doi.org/10.1177/0095327X0002600207.

Vinnova. 2018. Artificial intelligence in Swedish business and society: Analysis of development and potential. Vinnova Report, VR 2018:09. https://www.vinnova.se/contentassets/72ddc02d541141258d10d60a752677df/vr-18_12.pdf. Accessed 30 Jan 2024

WASP. Undated. Wallenberg AI, autonomous systems and software program. https://wasp-sweden.org/. Accessed 30 Jan 2024

Wither, James Kenneth. 2020. Back to the future? Nordic total defense concepts. *Defence Studies* 20 (1): 61–81. https://www.tandfonline.com/doi/full/10.1080/14702436.2020.1718498.

Cautious Data-Driven Evolution: Defence AI in Finland

Sami O. Järvinen

Finland has recognized artificial intelligence (AI) as a top priority for technological and economic development, setting ambitious policy goals in the civilian sector. For defence AI, policy objectives seem less ambitious, focusing on general guidelines. Defence AI has been piloted in administrative and support functions, permeating military capabilities only gradually.

The Finnish Defence Forces (FDF) tackles AI in the broader context of digitalisation. Its cross-cutting Digitalisation Programme envisions AI applications within the FDF's internal development programs. A key element of the programme is educating staff in AI to identify use cases and fostering expertise for developing and procuring AI. National Defence University (NDU) incorporates AI in its curriculum at all levels.

AI is a priority research area for the FDF. Potential use cases have been identified in virtually all areas of defence, and various R&D projects are underway. Robotics and Autonomous Systems are one area where disruption is being fuelled by AI developments. Another potentially disruptive area of AI application is in dynamic management of the electromagnetic spectrum.

The FDF acknowledges the crucial importance of data for defence AI, in particular machine learning. The availability of training data for developing AI applications needs to be ensured by tackling legal and organizational barriers, improving data storage systems, and enabling data sharing without compromising integrity and appropriate protection of data.

Ethical and legal issues pertain to both autonomous systems and the gathering and use of data for machine learning. Vis-à-vis Lethal Autonomous Weapon Systems, Finland's proposals have been pragmatic: rather than an outright ban, case-by-case scrutiny is proposed as a potential basis for regulation, backed by a conceptual framework.

S. O. Järvinen (✉)
Defence Command Finland, Helsinki, Finland
e-mail: Sami.o.Jarvinen@mil.fi

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_6

International cooperation provides a force multiplier for R&D, with the EU and NATO being the main multilateral forums of cooperation and the U.S. and Sweden ranking among key bilateral partners. The ratification of Finland's NATO membership in April 2023 is boosting possibilities for R&D cooperation.

Fielding of defence AI applications seems to be taking baby steps. Publicly available information paints a picture of AI being procured in military-off-the-shelf systems, even if the FDF's R&D portfolio hints at the possibility of original applications. Finland's acquisition of 64 F-35 fighters and the corresponding industrial cooperation with the U.S. will propel the FDF's use of AI to a new era within the next decade.

Finland's AI ecosystem builds upon a solid foundation of AI research and education, estimated to be the best in the Nordic countries. Paradoxically, shortage of talent is the bottleneck for Finnish companies in their effort to scale AI (Seehus et al. 2022). The defence sector and the civilian sector share a challenge of data management, partly exacerbated by legislative hurdles. One key challenge for the FDF is to make its organizational culture and procurement process more conducive to innovation and experimentation.

1 Thinking About Defence AI

At the highest policy level, guidelines on defence AI stem from the Government's Defence Report of 2021. It recognizes digitalisation and AI as prerequisites for developing national defence and key drivers shaping the operational environment. The report underscores the link of AI with autonomous military systems but expects AI to have a major impact on all domains of defence, e.g. information processing, situational awareness, management of weapon systems and logistics (Finnish Government 2021).

The Defence Report outlines a broad objective for digitalisation.

> to manage risks associated with emerging technologies, take advantage of opportunities, optimize activities, create new services, activities and knowledge, develop new abilities, and be involved in national decisions. A key objective is to develop abilities related to utilising information and knowledge and leading with knowledge, which can be reinforced with different artificial intelligence applications. Applications can be used to improve the basis for decision making, since information will be available faster and it will be more accurate. (Finnish Government 2021)

The Ministry of Defence (MoD) published Strategic Guidelines for Developing AI Solutions in 2020. Outlining a policy framework on the development and use of AI in the context of defence, the document sets five strategic guidelines:

- Defence policies and programs on AI should be coherent, compatible and updated regularly;
- Acquisition of AI research, development and maintenance of AI should be agile;
- AI know-how should be continuously improved via staff training and recruitment;

- Data should be made available and used with flexible techniques with up-to-date infrastructure;
- Defence administration must ensure the legality and solid ethical foundation of its AI applications (MoD 2020).

1.1 Definitions of AI

No single definition of defence AI has been consolidated across the defence administration. Moreover, most policy documents do not recognize a "military AI" per se but provide a general definition of AI and then proceed to elaborate potential military applications. For instance, the influential MoD Strategic Guidelines for Developing AI Solutions (Ministry of Defence 2020) starts from a very broad definition: "AI enables machines to perform tasks for which human intelligence has previously been required." The document notes that AI is best used for tasks where human intelligence falls short, for instance, when the amount of data or required processing speed is too high or if there is a "need for analysis independent of human factors."

Even if an all-encompassing definition of defence AI is lacking, one important piece of conceptual thinking has informed most policy documents on defence AI since its publication: the conceptual framework for defence AI commissioned by the Prime Minister's Office (Ailisto 2018). Situating AI in the broader context of digitalisation, it defined AI as software or technology that "enables machines, programs, systems, and services to function in a reasonable way as required by a given situation. A reasonable level of functioning requires the AI to be able to recognize different situations and environments and operate in accordance with how the situation evolves" (Ailisto 2018).

The conceptual framework recognized AI to be not one single technology, but a diverse group of methods, applications, and research areas. Consequently, the framework presents ten dimensions underlying defence AI (Ailisto et al. 2019):

1. Data analytics
2. Perception and situational awareness
3. Natural language and cognition
4. Human-machine interaction
5. Digital know-how in working life, problem-solving and computational creativity
6. Machine learning
7. System level and system effects
8. Computational environments, platforms, services, and ecosystems for AI
9. Robotics and machine automation: the physical dimension of AI
10. Ethics, morality, regulation, and legislation

1.2 Ethics and Regulation of AI

The Government's Defence Report 2021 states that while "taking advantage of the opportunities provided by new technology, it is necessary to consider the related ethical challenges and legal limitations" (Finnish Government 2021). The MoD stresses the importance of complying with international legal and ethical obligations "in the construction and use of artificial intelligence," highlighting the role of legality and ethics as one of the five Strategic Guidelines for developing AI (Ministry of Defence 2020).

The Strategic Guidelines feature a categorization of defence AI application areas helping to clarify certain ethical and legal issues. Figure 1 shows that most applications of defence AI are unproblematic from a legal and ethical viewpoint; that is, they are subject to the same stringent ethical and legal considerations as non-AI

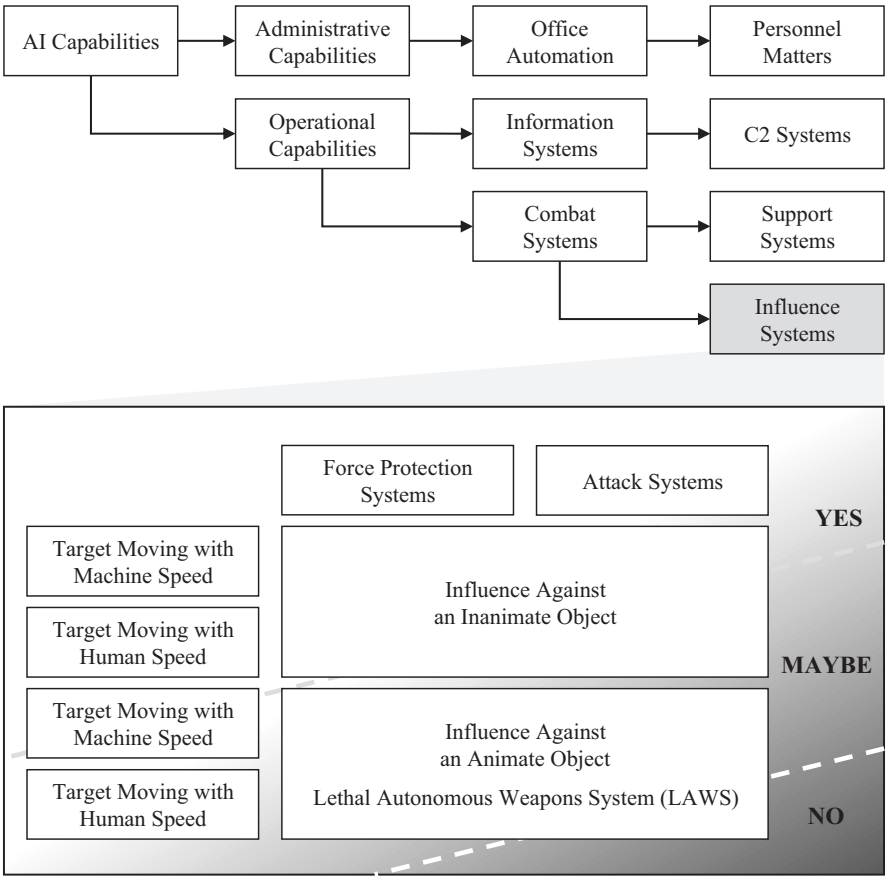


Fig. 1 Finnish categorization of AI application areas in defence. Source: Ministry of Defence 2020

applications. AI-specific legal or ethical scruples mainly arise towards the bottom right corner of the image.

Finland is fully committed to International Humanitarian Law (IHL) and an active proponent of its application to all aspects of warfare, including defence AI. Finnish defence experts note that the same rules of IHL must in principle apply to autonomous weapon systems as to conventional forms of warfare. Special care must be taken to ensure that new weapon systems and military AI really comply with IHL in all circumstances (Finland 2020). However, the Finnish defence administration "does not self-regulate more stringently than what is required by law" (Ministry of Defence 2020). The MoD stresses that national or international regulation must not prevent the development of ethically justified, necessary and appropriate AI based solutions (Ministry of Defence 2020). A specific challenge is posed by hostile actors that do not comply with international regulation. Hence, FDF develops know-how "preparing against a threat that does not adhere to international, commonly agreed restrictions on the use of autonomous weapons in the future battlefield" (Nieminen et al. 2022).

While cautious of the potential threats, the Finnish defence administration also recognizes the potential benefits of military AI and autonomous systems for improving IHL compliance of warfare. "Artificial intelligence can also be used to reduce human suffering" the MoD notes (Ministry of Defence 2020). And Finnish experts (Finland 2020) argue, if "AI enabled machine autonomy is applied to weapon systems with appropriate human involvement and by using ambitious ethical standards, it can also support humanitarian objectives, by allowing higher precision and distinction for military purposes." An AI-enabled unmanned asset can get closer to its target than a manned unit would, therefore enabling far more precise situational awareness and targeting data. This may reduce collateral damage to civilians. The unmanned weapon can also abort its mission, if on-board AI infers that civilian collateral damage is imminent.

Finland participates in the United Nations Convention on Certain Conventional Weapons and its Group of Governmental Experts (CCW GGE) on Lethal Autonomous Weapon Systems (LAWS). Food for Thought papers contributed by Finland to the GGE and the EU feature potential principles for the regulation of defence AI. Grosso modo, Finland does not advocate an outright ban on all weapon systems possessing a degree of autonomy, nor is it in favour of complete non-regulation. Even if no consensus is reached on the definition of LAWS, regulation can still advance based on an agreed categorization or characterization of AI.

In Finland's 2020 Food for Thought paper to the GGE a framework for the appropriate level of human involvement in LAWS was proposed. The five-phase framework outlines the required level of human involvement to ensure IHL compliance in operational use. The first phase is a rigorous and comprehensive weapons review in line with Article 36 of the first Additional Protocol to the Geneva Conventions. A second phase constitutes reviewing military doctrines and their operational and tactical implementation. The third phase reviews mission planning, and sets pre-defined boundaries for the operation of LAWS. The fourth phase deals with launch—to be decided by a human—and operation beyond the

point-of-no-return, where human control is no longer present, but where advanced AI could still enable LAWS to analyse information and adapt its conduct. For instance, observing it has surpassed the boundaries preset for its operation, the LAWS could adapt or abort the mission. The fifth and final phase of the review regards monitoring and ending of the mission.

A contribution to GGE in 2021 by Finland further elaborates a practical approach by identifying clear boundaries for the application of IHL vis-à-vis LAWS. The idea is that by stating the obvious, one can better delineate the non-obvious. Obvious cases violating IHL would include, e.g., a system (currently existing only in science fiction) that would be completely autonomous, operating beyond any human involvement (Finland 2021). Conversely, many applications of military AI are clearly as unproblematic as traditional non-AI systems, for instance most dual-use technologies, solutions making use of AI as supporting elements of a weapon system controlled by humans etc. (Ministry of Defence 2020). The grey area, then, situated between the obvious cases, is where contextual assessment case by case is always needed, as no universal rules apply.

1.3 FDF Strategies and Programs

The FDF AI Roadmap of 2018 was an early attempt at an internal guiding document for applying AI in defence, informing FDF decision-making. The document did not set precise long-term objectives in an uncertain field, but rather proposed an iterative, evolutive and agile approach: technical design should not be too refined or robust at too early a stage since that could lead to unwanted path-dependency. Existing AI technologies and products were to be applied more extensively, without fixed long-term commitment to suppliers, technologies, or products.

While the Roadmap is a classified document, some of its key areas have been publicly highlighted (Heiskanen 2018): situational awareness and support for decision making; improved foresight; accelerating operational tempo; real-time sensor data fusion and analysis in service of situational awareness; establishing and communicating situational awareness for cross-sectoral cooperation between authorities; and applying AI for training and real-time simulation.

The FDF Research and Development Strategy[1] (2019) emphasizes AI as one of its priority R&D areas along with cognition and autonomous military systems. The Strategy underlines the need to assess the potential of AI across a wide spectrum of areas, ranging from logistics to ISTAR, from decision-making and C2 to management of big data. Consequently, also the NDU's Department of Military Technology ranks autonomy, robotics, AI, and machine learning as one of their five main research areas for 2022–2026 (Nieminen et al. 2022). Moreover, the FDF identifies

[1] The strategy is referenced here via the author's own unpublished presentations which have been cleared for publication by FDF.

a few critical technologies intertwined with the development of AI: human and machine cognition, man-machine teaming, remote and autonomous systems, cognitive spectrum management, C2 and ISTAR, as well as positioning, navigation, and timing (Kosola 2022). Moreover, sensor and data fusion is a crucial area of application for AI. The basis for leadership and situational awareness is a networked data system, which combines information produced via sensor fusion with an AI that analyses it and provides solution proposals. FDF researchers point out that "(t)he impact of modern ground troops is based on data analysed by AI from a wide selection of sensor sources" (Tiilikka et al. 2021).

The FDF Digitalisation Programme (2021, 2022) is the overarching internal document for setting the pace and principles for AI development and deployment across the defence system. Digitalisation is defined as a cross-cutting functionality to be implemented via all the FDF sectoral development programs. The document encompasses plans for educating and training personnel on AI, creating and nourishing a digitalisation ecosystem, focusing on data, piloting a prototyping workshop activity, and establishing a process for gathering ideas as well as managing risks. Moreover, development processes need to be rendered more agile while promoting an organizational culture that encourages sharing and innovation (Karsikas 2022).

The Digitalisation Programme identifies processes and measures for harnessing digitalisation as a driver of change, enhancing the understanding of FDF staff on the possibilities of digitalisation for developing military capabilities. Concrete development projects will be based on selected use cases, with process owners in each service or branch leading their respective projects. The Digitalisation Programme highlights the central role of data as a prerequisite for making use of AI.

1.4 Data: Key Enabler, Key Challenge

Data is pivotal for digitalisation and AI. The MoD notes that "the amount of data has increased exponentially, which means that more efficient methods are needed to deal with it" (Ministry of Defence 2020). Finland's EU Presidency Food for Thought paper (Finland et al. 2019) recognized obstacles for exchanging data even within the armed forces of one country, not to mention for the international sharing of data. Data needs to be stored and classified in such a way that will enable flexible and appropriate use in applications and pave the way for increased cooperation between EU Member States and NATO Allies. Indeed, one of the strengths of the EU should be the striving for joint procurement of materiel, pooling and sharing of equipment—and exchange of experiences and data.

The FDF Digitalisation Programme highlights the central role of data for improving current capabilities as well as enabling new capabilities (Karsikas 2022). This requires, on the one hand, that relevant data be made available e.g., for training AI applications, and on the other hand, that infrastructure and computational models be capable of handling the increasingly voluminous data masses.

The availability of teaching data is a key challenge for machine learning. Supplier selection for data gathering, management and storage solutions may inadvertently grant the supplier an advantage that may be unfair or even unproductive. The procurer must be alert, protecting the data used for training AI, so that the procurer retains full authority for future development of the solutions, also ensuring integrity against cyber threats. Turnkey procurement of AI systems is a potential pitfall for the uneducated client (Hemminki et al. 2021). A potential remedy for this may be found using synthetic data.

Various obstacles may hinder the efficient use of data, for instance if data is protected in such a way that relevant stakeholders cannot access it, or if data is stuck in silos due to organizational barriers, incompatible formats, or sloppy structuring. A special hurdle is posed by Finnish data protection legislation, which prevents the authorities, among other things, from using data in a database for any other reason than the one it was collected for. Rigorous data anonymization may provide a partial workaround.

One unpublished FDF study highlighted the need for quality inputs: in the context of predictive maintenance of armoured vehicles, it was found that when the original data was too ambiguous, neither a human expert nor the AI managed to make use of it. The AI can refine and use unstructured and uncategorized data but can't deal with fuzziness any better than humans do. Therefore, maintenance data systems should provide preset, unambiguous structures for inputting data. Moreover, for wider application of AI, the maintenance system should enable reliable search functions for data allowing for workflow automatization, as well as develop a systematic, iterative function able to complete missing terms or correct errors. On the other hand, based on recent milestones in the development of civilian AI, some predict that AI can even be trained on unstructured data in the very near future.

The FDF is preparing a new Data Concept aimed at supporting the planning and use of the defence system by fostering better and more cross-cutting availability of data. A broad objective is to enable multi-domain operations jointly with allies. The guiding principle is to use data to support military and political decision making, based on an improved situational awareness. Ideally, situational awareness data will be compiled jointly among all NATO members in all domains. This will enable effective joint operations, including enhanced joint fires with an "any sensor to any shooter" approach (Solante, Interview 2023).

Achieving such objectives requires that data not be confined in silos but be made accessible between services and subsystems. This implies a paradigm shift in data security thinking—from "need to know" towards "need to share." The approach is Data-Centric Security (DCS): security controls are aimed at the data itself rather than at the information systems. The objective is to combine data protection and sharing in an unhindered manner (Solante, Interview 2023). The FDF strives to implement DCS efficiently also in order to harmonize with NATO's data architecture, of which DCS is an integral component.

A shift of organizational culture may be needed also to resolve the challenge of data ownership. In developing AI solutions, the FDF should take care to retain usage rights for the data machine learning algorithms are trained on—otherwise the

supplier may get an unfair advantage over competitors, or an unhealthy client-supplier relation may emerge. When the use of synthetic data is possible, problems with data ownership should not arise.

Traditional acquisition processes pose a challenge to AI procurement due to the evolutionary character of machine learning. If the AI application is based on continuous improvement, it may not make sense to acquire it at full capacity. Moreover, machine learning solutions are rarely final but constantly evolve throughout their life cycle. Traditional procurement may therefore made obsolete by a more agile, incremental, and iterative acquisition model. This would require the FDF to significantly increase its tolerance of experimentation (Hemminki et al. 2021).

1.5 Ideal Roles for Man & Machine

Finnish defence policy documents reflect a way of thinking whereby AI and automatization complement but don't replace human abilities. Autonomous systems are classically seen as well suited for dull, dirty, or dangerous (3D) tasks (Hemminki et al. 2021). Automation can improve cost-effectiveness of military systems as well as reduce the cognitive burden of humans. In cases where the amount of data exceeds human processing capacity or where the situation requires superhuman reaction speeds, automated or AI systems can bring capabilities to a new level. Moreover, one area that has so far been fairly uncharted is how soldiers' social and ethical performance is impacted by the implications of human-machine teaming (Aalto 2022).

In discussions related to manned-unmanned teaming, the notion begins to emerge that a "wingman" approach may not be the optimal way to use unmanned assets. If the unmanned platforms are focusing on supporting the manned aircraft, the mobility of the faster aircraft is limited to that of the slower ones. Stealth capabilities would be only as good as those of the least stealthy member of the swarm. Therefore, it might be more useful to grant the unmanned assets more independence. Drones could be sent in advance to the area of operation, loitering in search of potential targets or commanded to advance to trigger the enemy's air defence, followed by other drones tasked with a jamming or target acquisition mission; the role of the manned aircraft would then be to launch a missile from stand-off distance. An analogy is a hunter and a pack of hounds. As long as the hounds are on a leash, the team is inefficient. With the hounds unleashed, they can locate the prey and chase it into the range of a rifle. The decision to use lethal force is made by the human.

2 Developing Defence AI

2.1 AI in FDF Research

The Finnish Defence Forces conduct research and development (R&D) to generate knowledge that supports decision-making and to create the technological basis and knowhow for building and maintaining military capabilities. As Finland is a small country with a specialized but limited defence industry, much of the defence materiel is procured off the shelf. Consequently, much of FDF R&D focuses on experimentation, testing and integration.

However, a new Defence Materiel Policy Strategy states that "it is essential for national security that Finnish companies have an adequate technological level of know-how of critical technologies. Especially in digitalisation, AI, analytics, and autonomy, the security of supply for national know-how is an area of growing importance" (Ministry of Defence 2023). Certain capabilities need to be developed nationally to ensure technological sovereignty.

A rough outline of the FDF's R&D modus operandi is as follows. Research topics are always based on defence capability needs. Low-TRL defence research is funded via public calls, such as the annual MATINE funding that links the defence sector with academia and research institutes. The most successful projects can be upscaled through FDF funding for higher TRL projects. International cooperation is used as a force multiplier when applicable. Once development projects mature, fieldable defence materiel is procured through the FDF Development Programs.

MATINE, or the Scientific Advisory Board for Defence, is a special structure established to ensure an active link between the worlds of academic and civilian research and the defence community. It promotes research on national defence and security while also functioning as a network of over 300 scientists. MATINE gives university professors a window into defence matters while functioning as an unofficial multidisciplinary think tank for the FDF. MATINE's research funding focuses on risky or low TRL projects, the best of which can be subsequently upscaled with FDF funding.

The Finnish Defence Forces' Research Program is a spearhead of FDF R&D. The current program (2021–2025) features several projects exploiting the potential of AI. It benefits from a particular feature of Finnish society, the long tradition of general conscription: since most men have completed military training, R&D procured from Finnish companies is inherently carried out by people with a hands-on military understanding. Detailed research objectives are not public, but project titles give a hint to the extent AI permeates FDF's current R&D: the Situational Awareness portfolio of the program includes such projects as AI for Detection and Classification of Radar Signals; AI as Situational Awareness Operator and Analytical Support; Producing Situational Awareness with a Drone; AI in Processing Big Data Masses; and Target Situational Awareness and Sensor Fusion. Another portfolio is entitled Human-Machine Teaming, featuring projects like Autonomous Systems for

Surveillance and Engagement; and Technology and AI-Powered Development of Operations.

International cooperation is a force multiplier for R&D. Much of the FDF's multilateral R&D cooperation makes use of the technical expertise of the European Defence Agency (EDA) and the funding leverage of the European Defence Fund (EDF) and its predecessors. NATO is becoming increasingly important: Finland is already active in NATO's Science and Technology Organization, participating in more than 70 activities, many of which focus on AI. Finland joined NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) in April 2023 and the NATO Innovation Fund (NIF) in May. DIANA helps identify and develop dual-use technologies with defence potential, while NIF provides funding for bringing innovation into the market. Spearhead Finnish accelerators and test centres for DIANA specialise in quantum technologies and 6G connectivity.

2.2 Potential Uses of AI

The FDF has identified numerous use cases for AI across all levels of the defence system, ranging from support functions to lethal force. The following is an attempt to summarize, based on publicly available sources, what types of use cases the FDF has identified as potential building blocks for AI-enabled capabilities.[2]

AI could assist in forming troops by optimizing the assignment of tasks and missions, by providing a personal assistant to conscripts or monitoring the performance of soldiers or groups. Moreover, conscription could even be revolutionized by the introduction of virtual elements whereby a select portion of the training could be tailor-made and executed remotely. AI can support leadership and decision-making by compiling and analysing situational awareness data (Kallinen 2022), by formulating proposals and assessing the potential implications of decisions, by drafting orders and instructions as well as by synchronizing and monitoring execution. Moreover, AI could be used to simulate alternative decisions across a few scenarios far exceeding human processing capacity:

- *Intelligence*

The constantly growing computational capacity of sensor systems, along with predictive analysis, enable a more and more complete and up-to-date situational awareness. Image recognition software is constantly improving and has, in certain cases, already surpassed human capability. Best results can often be achieved by applying AI in combination with human judgement, making use of the virtues of each.

[2] It is particularly noteworthy that doctrine and concepts of operation as well as related planning documents are classified; therefore, this listing does not cover the actual extent of application.

- *Electromagnetic and Cyber Domain*

Ubiquitous digitalisation opens up new pathways for intelligence data gathering from the electromagnetic spectrum as well as from the internet. As demonstrated by the war in Ukraine, and discussed in Vitalyi Goncharuk's chapter, even data from social media can quickly transform into target acquisition. The cyber domain is a well-established area for AI for both defensive and offensive applications. Information warfare may be heavily exacerbated by AI which enables the automatic monitoring and targeting of people with low resources—a threat scenario to prepare against (Kosola 2021c).

- *Logistics*

Logistics is already being optimised via such AI-powered processes as predictive maintenance and the automatization of stock and transport management. Military medicine is improving via preventive precision medication, and new ways of continuous measuring and enhancing of human performance are also made possible by AI systems. Searching for wounded soldiers can be improved by drones, and their evacuation can be carried out by Unmanned Ground Vehicles (UGV) with increasingly autonomous capabilities.

- *Force Protection and Engagement*

More military-specific applications of AI include force protection and engagement. Protection can be enhanced by AI application via improved detection and identification of threats and automation of countermeasures on the one hand, and via improved techniques of concealment, decoys or misleading the enemy on the other. Engagement can be enhanced if the planning of kinetic force is improved via AI techniques; collateral damage could be reduced with AI-powered risk assessments; and AI can also enable advanced cyber or electronic warfare functionalities. Notably, AI applications can be used to enhance joint fires by exploiting targeting data from any sensor to any shooter (Solante, Interview 2023).

- *Acceleration of Decision-Making*

AI can enhance every phase of the observe, orient, decide, act (OODA) loop. Decentralized AI applications, either in the physical domain in the form of robot swarms or as software agents operating in networks, can help to achieve a superior tempo of operations (Kosola 2020c).

All of the aforementioned themes are recognized by the FDF as potential areas applying AI. One broad theme is already emerging on the battlefield, partly enabled by the development of AI: unmanned systems with autonomous capabilities.

2.3 The Next Disruption: Robotics and Autonomous Systems

FDF Research Director Jyri Kosola estimates that the next disruption in warfare will be propelled mainly by unmanned systems and the combination of AI, digitalisation and data (Kosola 2020a, 2020b, 2020c). Analysing the possible ways in which robotic and autonomous systems could disrupt the battlefield, Kosola notes that unmanned sensor and weapon platforms can either act as a force multiplier for existing concepts or enable completely new doctrines of fighting. For instance, a traditional minefield based on guessing where the enemy might move and then deploying masses of stationary mines might be rendered obsolete by smart mines (Kosola 2021b). Areas and pathways to be denied could be decided only hours before the event and moving mines with targeting capacity free engineers from predicting enemy moves and making time-consuming installations. Moreover, fewer mines would suffice—and the blue force can pass through.

As the development of AI and sensor technologies enables machines to become increasingly aware of their own state and their environment, they become increasingly autonomous, requiring less external control. This evolution is expected to result in combat teams consisting of humans and machines in the 2030s. An appropriate division of labour retains humans in control of decision-making and monitoring, based on human capacity for situational awareness and contextual judgment. Correspondingly, the machine would play the implementing role, especially for 3D missions as well as situations requiring superhuman execution speed (Kosola 2020d).

How to use this disruption to gain operational advantage? Kosola reasons that this requires defining the man-machine division of labour already at the planning stage of operational concepts, thereby optimising the machine for its mission and conditions. For instance, an unmanned platform can be much smaller, since it doesn't have to have space, life support or protection for a human. This enables improved mobility and resilience. The unmanned platform can also be more difficult to detect, enabling it to operate closer to its target.

A potential concept starts to emerge, one based on multiple small, inexpensive, and expendable platforms operating in a swarm-like fashion. Each unit may be much less capable than a large and expensive platform, but their large quantity more than compensates for the inferior quality. Expendability enables completely new concepts of operation. Kosola refers to mosaic warfare as opposed to monolithic capabilities. The swarm, enabled by AI-powered autonomous features, is stronger and more resilient than a corresponding monolithic capability (Kosola 2021a).

While these reflections do not necessarily reflect existing or even emerging FDF doctrine, they provide some insight into possible pathways into future capabilities. Many FDF research projects aim at creating a knowledge base and developing technological enablers that could be used as elements for various systems involving remote and autonomous platforms. A few such projects are introduced below.

2.3.1 Project iMUGS

Finland participated in the EU-funded R&D project Integrated Modular Unmanned Ground Systems (iMUGS) aimed at enhancing the autonomous features of unmanned systems and facilitating joint operation of machines and humans. The FDF's main objective was developing knowhow and technologies as enablers for various autonomous solutions irrespective of supplier. Enablers include communications and navigation solutions capable of operating in Global Navigation Satellite System (GNSS) denied environments and sensors and algorithms enabling the platforms to cooperate. These also need to be resilient to cyber and electronic attacks as well as arctic conditions.

iMUGS achieved progress in autonomy, with UGVs capable of manoeuvring autonomously to pre-planned battle positions, choosing their trajectory, detecting obstacles, and navigating accordingly, also beyond line of sight. However, these feats were achieved only in a simplified environment; reliable and consistent autonomous navigation across a complex terrain such as thick forest remains a challenge. Swarming capabilities were demonstrated both with and without a link to a central controller, but the latter only in simulation. AI applications by Finnish companies included the development of swarming algorithms by Insta (machine learning for path planning and optimising swarm behaviour) and communications optimisation by Bittium (analysis of node data, smart routing, dynamic spectrum management).

2.3.2 Project Laykka

Several AI-related Finnish R&D projects are currently underway revolving around an experimental micro UGV platform named Laykka (Andersson 2022). It can be used for stealthy anti-tank missions, removing the human from the extremely dangerous task of destroying enemy battle tanks. It can also be used for intelligence missions, automatised patrolling and logistics tasks, medical evacuation, transport of ammunition, mobile communications relay station, as a UAV charging base or a loitering weapon (Hemminki et al. 2021). One particularly promising AI-based application is smart minefields: instead of mines being permanently placed at fixed locations, the mines can loiter for long times but also move around as necessary while the situation unfolds.

Numerous research projects led by the NDU are underway, each focusing on a particular field of narrow AI. In one project, AI functionalities are integrated into Laykka for field testing to verify simulation results from concept models run in a virtual environment (Nieminen et al. 2022). Another project develops military medicine solutions, especially casualty evacuation. A third project developed visual identification and classification of military vehicles using neural net algorithms with promising results (Hemminki et al. 2021).

2.3.3 Manned-Unmanned Teaming

The FDF collaborates with the German Bundeswehr and Airbus to develop capabilities of manned-unmanned teaming. A major milestone was achieved in 2022 with Europe's first large-scale multi-domain flight demo held in Finland: two fighter jets, one helicopter and five unmanned drones teamed up to execute a mission under near operational conditions.

The fighter jets, helicopter and unmanned drones were connected via a meshed networking data link provided by Patria, allowing them to seamlessly interact, negotiate division of labour and switch control of unmanned platforms between several manned units. The remote carriers were commanded by humans aboard a fighter jet but executed much of their given mission autonomously. Drones with electromagnetic sensors detected enemy air defence positions. With visual confirmation provided by other drones, the fighter jet proceeded to eliminate the air defence.

2.3.4 New Concepts: Dynamic Electromagnetic Spectrum Management and AIMA

One area where AI may propel a breakthrough is dynamic electromagnetic spectrum management (EMSM). Equipping communications, radar and electronic warfare systems with cognitive capacities would allow the use of the electromagnetic spectrum in a dynamic way: A software-based transceiver could use AI to analyse the available spectrum, making optimal use of the spatially and temporally available bands and generating new waveforms depending on the frequencies available. With machine learning, the system could also extrapolate from previous experiences while adapting to new situations. The AI should learn to avoid interfering with civilian and blue force communications by dynamic use of frequency bands and could even execute simultaneous jamming or spoofing of enemy signals while providing blue force C2. The latter capabilities could be based, e.g., on signal modulation or polarization, combined with dynamic adjustment of output power. Moreover, machine learning may enable electronic warfare and intelligence systems to autonomously provide situational awareness of the spectrum and to identify anomalous signals and equipment.

While dynamic EMSM is an emerging area for R&D, the main hurdle for fully exploiting such systems might not be technological but regulatory. Current regulation of the use of the electromagnetic spectrum is fairly inflexible: the law simply divides the spectrum into frequency bands, which are then granted for or prohibited from use by defined operators. This does not provide for much spatial or temporal flexibility for dynamic AI applications.

Finland has launched international initiatives seeking to develop new capabilities applying AI-based autonomy combined with dynamic EMSM. The Permanent Structured Cooperation (PESCO) project "Arctic Command & Control Effector & Sensor System" (ACCESS) builds on the idea of developing an AI-based

Multifunctional Aperture (AIMA) and transceiver capable of simultaneously providing mobile ad hoc network data link, localization and classification of enemy radio signals, blue force tracking, identification friend-or-foe, passive electronic surveillance, and even electronic warfare functions. AIMA should be both modular and scalable: bigger units in vehicles would be more powerful, while smaller units could be mounted on small UAVs working in swarms. AI-based swarming would make the system effective even if a single unit is not powerful. Smart emission control can help units get closer to the enemy, requiring less signal power (Kosola 2023). Combining AI, miniaturization and technological convergence, these projects may lead to novel capability concepts.

3 Organising Defence AI

On the national level, an ecosystem approach is applied both to the development of civilian AI and to the digitalisation of defence. Finland's civilian AI ecosystem consists of over 400 startups (FAIA 2020), as well as more established software developers such as Reaktor and Futurice. The ecosystem is boosted by specialised initiatives, such as the Finnish Centre for Artificial Intelligence (FCAI) and Finland's AI Accelerator (FAIA). FCAI is a community of experts promoting research, fostering linkages between the private and public sectors, while FAIA works to connect AI suppliers with organizations looking for solutions.

Defence specific AI development is fostered by the launch of Digital Defence Ecosystem (DDE) in 2022. With the aim of reinforcing competitiveness, cross-pollinating know-how and ideas, finding synergies and leveraging funding for key technology development, DDE strives to interconnect major defence industries, small and medium-sized companies and start-ups, academia, and end-users. DDE is industry-led with close connections to the FDF, whose role is to ensure the military relevance of project proposals, provide ideas and guidance for products that correspond to defence capability needs, and potentially contribute expertise and testing sites for projects.

Although briefly discussed as an organizational option, the FDF does not have a specialized AI agency but a matrix organization promoting digitalisation and AI. The FDF's matrix organization is tasked with implementing FDF's Digitalisation Program, whereby AI is to be mainstreamed into defence capability development programs. The main objectives of FDF digitalisation are capacity building for digitalisation and exploiting the value-added of digitalisation in the development, maintenance, and use of military capabilities. With top-down guidelines and interoperability requirements drawn from the programme, each service and each development programme come up with their own AI applications (Karsikas 2022).

4 Funding Defence AI

Funding volumes in the civilian sector are of interest, since that's where most of AI development takes place currently, potentially spawning defence capability development via dual-use technologies. The Finnish Government launched a €200M investment package in 2018, financing AI innovations, development of know-how for AI technologies as well as enhancing public sector efficiency through AI applications. FCAI runs on a budget estimated at €250M for its flagship period 2019–2026. Its core budget is also frequently augmented by project-based funding from e.g. the Academy of Finland.

For defence specific AI funding, we need to turn to defence industries and the FDF. The FDF hasn't published exact figures for AI, but its annual R&D budget is about €50M. AI being highlighted as a strategic priority area, this gives us some idea of the order of magnitude. Leveraging of national R&D investment is also being sought through international cooperation, increasingly via the EDF. An additional source of AI funding is embedded in FDF Development Programs other than research, which should contain mainstreamed AI applications along the principles of the Digitalisation Program.

5 Fielding and Operating Defence AI

Specific AI capabilities of the FDF have scarcely been publicly discussed: information on currently operational equipment is publicly available, but technical details on battle management systems, sensor systems etc. are mostly limited to information published by manufacturers.

The Finnish Army notes that AI is featured in dozens of applications within their operational systems. AI is most prominently used in areas such as support of planning, processing of geodata, data fusion, virtual assistants and other support functions, expert systems, simulations and wargaming. Other areas of application include machine vision and image recognition, predictive analytics, resource allocation, reporting, and various elements pertaining to unmanned and autonomous systems. The Army engages in specialized research to ensure that internationally developed concepts and equipment can be adjusted to conform to the Finnish conditions and particular requirements (Lampinen and Tahkokallio 2022). Predictive maintenance is one known area of AI application, with very high accuracy achieved in AI-based fault data analysis of armoured vehicles.

In the Navy, battle management systems feature some degree of AI in processing sensor information. For instance, Hamina class fast attack ships and Hämeenmaa class mine vessels are equipped with Atlas Elektronik's ANCS combat system. Fire-and-forget missiles and torpedoes have a degree of AI for navigation and friend-foe identification (IFF). Rauma and Hamina missile boats are equipped with a tailored version of Saab's RBS15 with inertia and GPS navigation. Hamina and Hämeenmaa

class vessels also have the ITO 2004 air defence system equipped with Umkhonto missiles, processing sensor data for target acquisition and applying missiles with on-board inertial navigation and infrared seekers after launch. The Navy's coastal mine hunter vessels of the Katanpää class are equipped with Kongsberg HUGIN and REMUS unmanned underwater vehicles (UUV).

The Finnish Navy is about to enter a new era with the ongoing *Squadron 2020* project. The project involves the acquisition of four modern corvettes that will eventually replace seven current vessels to be decommissioned. Construction of the corvettes should be finished by 2026, with half of the €1.2bn budget spent on sensors, weapon systems and integrated C2.

The Finnish Air Force does not disclose details of how it applies AI in its systems, with the exception of certain projects related to logistics and predictive maintenance of Hornet F/A-18 s. Two of these projects are a failure prediction system based on machine learning and a Fatigue Life Analysis neural network model.

The failure prediction project was based on machine learning analysed data from the fighter jet's equipment. An adequate level of accuracy proved to require extensive amounts of data, and therefore such systems are applicable only for equipment used frequently and yielding ample data. The HN F/A-18 s fulfil these criteria, with a single flight yielding millions of data points. Since the project results have been promising, such analysis tools will potentially be a significant aid to maintenance decision-making for future platforms.

In another project a neural network model was created by Patria simulating the structural stresses of the F/A-18 s using recorded flight data. The model was taught against direct physical strain gauge measurements from two aircraft, with the aim of reaching an adequate level of accuracy in predicting fatigue life for the rest of the fleet. First, a computational model of the HN F/A-18 was created, superimposed with an aerodynamic model, enabling the simulation of specific in-flight stresses. The model predicted the most critical points aircraft structure. Based on these predictions, onboard equipment measured physical stresses. The neural network AI was then taught to produce stresses from the physical measurements, flight data and engineering parameters. Similar systems may be applied in the next generation fighter aircrafts since the results were found to be both useful and cost-efficient.

The Finnish Air Forces are currently undergoing a generational shift with the replacement of Hornet fighters by 64 Lockheed Martin F-35A multi-role fighters. The largest public acquisition in Finnish history at €10bn, the F-35 s will be operational in Finland from 2025 onwards. The weaponry with which the F-35 s will be equipped involves AMRAAM, Sidewinder, SDB I/II, JDAM-family weaponry, JSM and JASSM-ER. Optimized during the procurement, the weapons package will be adapted to Finland's operating environment and latest system upgrades (Ministry of Defence 2021). Moreover, the acquisition includes a voluminous industrial cooperation package—a potential force multiplier for FDF R&D including defence AI.

6 Training for Defence AI

Though a small country, Finland punches above its weight in AI: it produced the second most AI patents in Europe per capita in 2003–2017 (Ailisto et al. 2019). One strength of the ecosystem is cross-fertilization with neighbouring technology areas such as signal processing, electronics, edge computing and 6G, which have been successfully combined with AI. A prominent example is the cognitive sensor fusion development at Tampere University.

Finnish universities offer a broad array of AI related education. Master-level education and corresponding research is featured covering all the major subfields of AI: data analytics, perception and situational awareness, human-machine interaction, machine learning, problem solving and computational creativity, platforms, and robotics. Applied research in private companies focuses on data analytics, robotics, and perception (Ailisto et al. 2019).

The FDF recognizes the need for boosting education to apply AI across all areas of defence. This pertains to the whole spectrum of AI elements, ranging from perception and situational awareness to data analytics, cognition, computational creativity, and machine learning, from system effects and ecosystems to machine automation, human-machine teaming, ethics and regulation. Training and education for AI are also at the core of the FDF Digitalisation Programme. In-house expertise is being reinforced by supplementary education as well as new recruitments, coupled with procurement of external expertise provided by academia and industries.

The NDU is strengthening the role of AI in its curricula with elements of AI already present at all levels. AI also often features in theses in such topics as operational analysis and planning, battle management, internet of things, Big Data and machine learning and AI applications for specific weapon systems. Conversely, the use of AI and digitalisation to enhance FDF training processes on various level are being explored, with applications ranging from improved selection processes of defence staff, digitalising conscript training and enhancing simulators used for weapon systems training. In particular, the KESI simulator used for leader training applies AI for troop behaviour simulation and decision-making support functions (Rautio 2022).

7 Conclusion

Finland has ambitious national goals for AI, and there are ample policies guiding the development of military AI. Digitalisation of defence is underway with emphasis on support processes aiming and cost-effectiveness. Baby steps are now being taken in the direction of digitalising core military capabilities, but most public projects remain at the level of R&D.

The FDF acknowledges the central role of data for digitalisation in general and AI applications in particular. A new Data Concept seeks to enhance gathering and

storing data, improve availability and enable more flexible utilization. Silos between data systems and organisational branches should be surpassed. Achieving such holistic data use would imply a real paradigm change. Finland's NATO membership provides impetus for this development, with the Data Concept streamlined to fully harmonise with standards and procedures of the Alliance.

The defence administration has put effort into addressing ethics and regulation of AI. Their analytical framework indicates that most military AI is applied other systems than kinetic engagement and is therefore unproblematic. Scruples arise in the area of lethal autonomous weapon systems, and for this Finland proposes a conceptual framework outlining a pragmatic level of human involvement. IHL always applies both for man and machine, with the human commanding the troops bearing ultimate responsibility. In certain cases, IHL compliance can be improved by AI, for instance by enhancing situational awareness and the precision of targeting, or by enabling better decision-making through reducing the cognitive workload of the human.

AI will play a key role in enabling potential disruptions on the battlefield. One such disruption is already looming in robotics and autonomous systems, a key R&D topic in Finland. Autonomous systems could enable completely new ways of fighting, provided that an optimal division of labour between man and machine is inherently embedded in the concepts of operation.

Dynamic management of the electromagnetic spectrum is seen as an area that could potentially be revolutionized by AI. Communications or electronic warfare transceivers may soon feature spectrum situational awareness, autonomously choosing frequency bands and generating tailored waveforms. AI and machine learning could spot spatial and temporal margin of manoeuvre in the spectrum inoffensively to civilian frequencies, achieving blue force C2 without enemy interference, all the while intercepting or jamming enemy communications.

Indeed, Finland is advancing a project combining the disruptive elements of autonomous swarming and dynamic EMSM. Finland's AI Multifunctional Aperture (AIMA) initiative and the corresponding PESCO project ACCESS strive to develop a system capable of simultaneously providing ad hoc mobile networking, electromagnetic spectrum situational awareness and electronic attack capabilities with a swarm of inexpensive, multifunctional units. A modular, scalable, and multifunctional swarm system could allow for previously unseen tactical concepts.

Despite a few innovative projects, Finland's defence AI seems to be somewhat lagging behind the ambitious national AI policies, with the defence administration taking a cautious and very gradual approach. AI development is initially focusing on administrative and support capabilities as well as low to mid TRL research. However, Finland's NATO membership, its F-35 acquisition and corresponding industrial R&D cooperation with the U.S. provide a boost to AI development. Cumulative developments may eventually bring about a real transformation of defence.

References

Aalto, Janne. 2022. Autonomiset aseet ja etiikka. In *Puolustustutkimuksen vuosikirja*, 46–48. Tampere: Finnish Defence Forces.

Ailisto, Heikki. 2018. Tekoälyn käsitekartta. https://tietokayttoon.fi/documents/1927382/2158283/Teko%C3%A4lyn+k%C3%A4sitekartta/a5c4b469-d8ae-4ce1-a5fc-f12981bae796. Accessed 30 Jan 2024.

Ailisto, Heikki et al. (ed.). 2019. Tekoälyn kokonaiskuva ja osaamiskartoitus—loppuraportti. https://julkaisut.valtioneuvosto.fi/handle/10024/161282. Accessed 30 Jan 2024.

Andersson, Christian. 2022. Laykka-AMPGV:n inkrementaalinen kehitysprosessi runkoversio X.2:sta X.3:een sekä kehityksen seuranta kenttätesteillä ja -kokeella. Master's Thesis. Maanpuolustuskorkeakoulu. https://www.doria.fi/handle/10024/185591. Accessed 30 Jan 2024.

FAIA. 2020. State of AI in Finland. http://www.faia.fi. Accessed 30 Jan 2024.

Finland. 2020. *Considerations on the appropriate level of human involvement in LAWS. Food-for-thought paper by Finland for UNCCW GGE*. Unpublished.

———. 2021. *Elements for possible consensus recommendations. Contribution to UNCCW GGE*. Unpublished.

Finland et al. 2019. *Digitalisation and Artificial Intelligence in Defence. Food for Thought Paper for EU Member States*. Unpublished.

Finnish Government. 2021. *Government's Defence Report*. Helsinki: Finnish Government. http://urn.fi/URN:ISBN:978-952-383-852-9. Accessed 30 Jan 2024.

Heiskanen, Mikko. 2018. Puolustusvoimien näkökulmia tekoälyyn. Presentation at a MATINE seminar 21 December. https://www.defmin.fi/files/4463/AI_Roadmap_MATINE_JULK.pdf. Accessed 30 Jan 2024.

Hemminki, Petteri, Kai Virtanen, and Kimmo Halunen. 2021. Tekoälyn kehityksellä autonomiaa asejärjestelmiin—mihin pitäisi varautua? In *Sotataloustietoutta XI*, ed. Kaarlakoski, 210–235.

Kallinen, Kari. 2022. Kognitiivinen sodankäynti. In *Puolustustutkimuksen vuosikirja*, 50–52. Tampere: Finnish Defence Forces.

Karsikas, Jarkko. 2022. Puolustusvoimien digitalisaatio valmistaa huomisen haasteisiin. https://puolustusvoimat.fi/blogi/-/blogs/puolustusvoimien-digitalisaatio-valmistaa-huomisen-haasteisiin. Accessed 30 Jan 2024.

Kosola, Jyri. 2020a. Robottiaseet herättävät keskustelua. *Sotilasaikakauslehti* 1: 72–78.

———. 2020b. Maasodankäyntiä vuonna 2020. *Sotilasaikakauslehti* 2: 80–86.

———. 2020c. Naton teknologianäkymiä vuoteen 2040. *Sotilasaikakauslehti* 4: 74–78.

———. 2020d. Sodankäyntiä muuttavat teknologiset ilmiöt. *Sotilasaikakauslehti* 6: 70–74.

———. 2021a. Palapelin rakentelua vai peliä mosaiikilla. *Sotilasaikakauslehti* 2: 74–78.

———. 2021b. Paradigman muutos. *Sotilasaikakauslehti* 4: 60–66.

———. 2021c. Hyvä—paha digitalisaatio. *Sotilasaikakauslehti* 7: 64–70.

———. 2022. Presentation 22 November at ASDA seminar. Unpublished.

———. 2023. Convergence Multipurpose Apertures Will Cause Disruption. Nordic Defence Review. https://nordicdefencereview.com/convergence-multipurpose-apertures-will-cause-disruption/. Accessed 30 Jan 2024.

Lampinen, Timo, and Tatu Tahkokallio. 2022. Autonomian rooli tulevaisuuden maataistelussa. In *Puolustustutkimuksen vuosikirja*, 68–69. Tampere: Finnish Defence Forces.

Ministry of Defence. 2020. *Strategic Guidelines for Developing AI Solutions*. Helsinki: Ministry of Defence. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162372/Strategic_guidelines_for_developing_ai_solutions.pdf. Accessed 30 Jan 2024.

———. 2021. Lockheed Martin F-35A Lightining II on Suomen seuraava monitoimihävittäjä. https://www.defmin.fi/ajankohtaista/tiedotteet_ja_uutiset/tiedotearkisto/tiedotteet_2021/lockheed_martin_f-35a_lightning_ii_on_suomen_seuraava_monitoimihavittaja.12334.news. Accessed 30 Jan 2024.

———. 2023. *Puolustushallinnon materiaalipoliittinen strategia*. Helsinki: Ministry of Defence. http://urn.fi/URN:ISBN:978-951-663-269-1. Accessed 30 Jan 2024.
Nieminen, Mika, et al. 2022. Autonomia taistelukentällä—tulevaisuusorientoitunut tutkimus. In *Puolustustutkimuksen vuosikirja*, 119–121. Tampere: Finnish Defence Forces.
Rautio, Samu. 2022. Komentaja- ja esikuntasimulaattorin käyttöönotto—monivaiheinen prosessi. In *Puolustustutkimuksen vuosikirja*, 116–118. Tampere: Finnish Defence Forces.
Seehus, Ronny, et al. 2022. *The Nordic AI and Data Ecosystem*. Oslo: The Nordic Council of Ministers. https://www.nordicinnovation.org/2022/nordic-ai-and-data-ecosystem. Accessed 30 Jan 2024.
Tiilikka, Jari, et al. 2021. Taistelija-hanke. In *Sotataloustietoutta XI*, ed. Kaarlakoski, 123–131.

Caught Between Today and Tomorrow: Defence AI in Estonia

Tomas Jermalavičius

The Estonian defence leadership recognises Artificial Intelligence (AI) as an increasingly important suite of technologies that will transform society, the economy, and the defence sector. There is a clear understanding that Estonia must remain part of this technology's wave, not least because its defence forces will have to interact and remain interoperable with the allies racing to embrace AI-enabled capabilities.

Concurrently, Estonia's national defence development faces a major challenge of addressing significant capability gaps within the compressed timeframes, given the assessments that the reconstituted Russia's capabilities will pose a direct and existential threat to Estonia by the end of the decade, if not earlier. Combined with resource constraints and inherent scepticism within the military about emerging technologies that so far hold more promise than they deliver, this rapid capability build-up is pushing investments into defence AI development down the list of priorities.

On the other hand, war in Ukraine is increasingly supplying insights into what effects the use of AI can have in a battlespace when combined with old technologies and pique interest in how small states such as Estonia could employ this technology to offset imbalances vis-à-vis a numerically superior enemy force. Some in-house development projects aimed at digitalising "kill webs;" enabling better information sharing and enhancing common battlespace awareness are also emerging as important vehicles for introducing AI.

At the same time, the Estonian security, defence, and space industry, dominated by agile start-ups and small or medium enterprises, is emerging as a significant driver of defence AI development. Enterprises in Estonia are quickly becoming important sources of concepts of AI applications in defence and security, even

T. Jermalavičius (✉)
International Center for Defense and Security, Tallinn, Estonia
e-mail: tomas.jermalavicius@icds.ee

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_7

though their products and services based on those concepts are often likely to reach foreign customers sooner than the Estonian ones.

Most importantly, a wave of procurement of state-of-the-art weapon systems and equipment is bringing the Estonian military into close contact with advanced technologies that will include, as part of the package, elements of AI, further necessitating increasing knowledge and competence in AI technology. In this regard, Estonia will have to strengthen its military training and education system and find ways to leverage conscription and reserve training more effectively to enhance AI competence.

1 Thinking About Defence AI

As for many nations, Estonia's journey into defence applications of AI started in the civilian sector, where its main strengths lie in information technology, digitalisation of public services, cybersecurity and, increasingly, semi-autonomous robotics. AI, defined as "a system based on an autonomous software algorithm capable of learning, allowing it to perform tasks that typically require human intelligence" (Government of Estonia 2019), is making its way into civilian applications through these key areas, with the national strategy providing the overall direction for public and private stakeholders. The second iteration of this strategy is being drafted and will give a better conceptual basis, context, and coherence to the overall effort (ERR 2023b). It is important to note, however, that the level of digitalisation—fairly high in various international indices (e.g. EU's Digital Economy and Society Index or UN's E-Government Development Index)—may not necessarily be a reliable indicator of the level of digitalisation and AI adoption across the defence sector.

1.1 Estonia's Strategic Culture of Pragmatism

Estonia's strategic culture shapes its defence AI approach in important ways (Salu and Männik 2013; Atmante et al. 2019). First and foremost, Estonia relies on NATO and the EU to ensure national security, particularly in managing a persistent, multifaceted, and overwhelming threat Russia poses. This key tenet rests on clear-eyed understanding how large the power asymmetry with Russia is that Estonia needs to offset to survive as a sovereign nation. Reliance, however, is not seen as a one-way street. Rather, it requires both maximising Estonia's contribution to the collective enterprise wherever possible and being an active and involved member of these organisations. This also entails continuously investing into credible national defence capabilities and allocating the necessary financial resources. Since re-establishing its independence after 1990, Estonia had to rebuild its defence forces from scratch.

Second, Estonia's security culture reflects the understanding that developing national military defence and further focusing it on homeland (territorial) defence is

confined neither to national boundaries nor solely to the defence sector. It requires close interaction (and thus interoperability) with allies and the ability to draw upon inputs from broader society, including the corporate sector and science. Third, its strategic culture is focused on practical solutions that deliver concrete results, preferably within a relatively short time. In general, Estonia shies away from slow-motion conceptualisations and over-strategizing, even though in such sectors as cybersecurity the value of multi-stakeholder strategy-making to bring together all relevant experts and sustain understanding is well appreciated (Kaska et al. 2021).

This pragmatic and practical mindset is important as it shapes how defence AI is approached—with a high degree of uncertainty-induced caution in the military mixed with sufficient space for entrepreneurial attitude on the industry and policy side "to get things done." It also reflects the military's general approach to technology adoption, underpinned by a clear understanding of Estonia's narrow margin of error in initiating (or not initiating) major change and limited resources to pursue any new high-flying ambitions (see Suurkask 2023). Such pragmatism means it cannot and will not be a trailblazer of defence innovation until and unless the evolving nature of military threat from Russia makes a rapid introduction of some unique solution—that no one else in the Alliance has yet adopted at scale—a clear and urgent imperative.

1.2 The Current Defence AI Strategy Void

Estonia still needs to have a dedicated defence AI policy, but the MoD is gradually rising to the challenge of drafting it. The current approach tantamount to informal policy on AI-related issues is shaped through its existing R&D and defence industrial policies, but also by the developments in the framework of NATO, the EU and minilateral initiatives that the MoD is keen to participate in. As a member of NATO, Estonia subscribes to the Alliance's AI Strategy of 2021, and as a member of the EU, it participates in defence cooperation frameworks that have elements of AI technology and AI-enabled capabilities (e.g. Permanent Structured Cooperation, European Defence Fund, European Defence Agency, etc.). Furthermore, it joined the US-led AI Partnership for Defence initiative—a "coalition of the willing" that reinforces, amplifies, and benefits from the US leadership in the field (Chief Digital and Artificial Intelligence Office 2022). This is seen as recognition of Estonia's strengths in cybersecurity—a field where synergies with AI are significant.

The MoD's key strategic message is that AI is pivotal to future military capabilities and that Estonia must keep abreast of the developments in this field and contribute to them in the areas of its technological excellence and expertise. Although the understanding of what capabilities will be transformed or created by AI's use is still lagging in the wider Estonian defence establishment, the basic principles that the MoD follows in relation to AI projects for defence are (Roundtable, 2 September 2022):

1. They must add value.
2. They must simplify rather than complicate employment of military capabilities.
3. They should be of dual-use purpose.

There is also strong determination at the policymaking level to get Estonia involved in a web of multinational collaborative initiatives that will allow tapping into the results, ensuring interoperability and avoiding early (and often costly) mistakes made by "first movers" in the field. Such involvement also compensates for the lack of critical mass that hampers small nations such as Estonia in their technological and capability development ambitions.

In this regard, two key role models emerge as pivotal for Estonia. First, the United States is a global leader in AI technology and a strategic partner of immense importance for transatlanticist Estonia. In addition, the UK is as another long-standing and trusted strategic partner in military affairs (Jermalavičius and Billon-Galland 2023). The UK is a framework nation for both the Joint Expeditionary Force (JEF) in which Estonia participates alongside other ten nations and NATO's enhanced Forward Presence (eFP) battlegroup deployed in Estonia. It has recently committed a high-readiness brigade for Estonia's defence (Estonian MoD 2023b), thus making interoperability with the British forces a key consideration for Estonia. The UK also is among the leading technological powers in the Alliance, further boosting its relevance to Tallinn's defence AI thinking.

The pivotal role of these two nations does not imply that other partners do not matter. Estonia participates in the French-led European Intervention Initiative and hosts French troops as part of NATO's eFP, so the evolution of the French defence AI strategy and technology leadership will certainly be of interest to Tallinn. Collaboration with Germany—a source of military technology and equipment of growing importance to Estonia and a nation that resolved to enact far-reaching transformation of its defence as part of the *Zeitenwende*—will shape Estonia's defence AI agenda and thinking. Last but not least, some of the like-minded small allies with similar strategic outlooks—such as Finland, Norway, Latvia and Lithuania—are likely to be among partners of choice in keeping up with the defence AI trends in the Alliance.

1.3 Defence AI Ethics: Yes, but…

In terms of general thinking about defence AI, Estonia seeks to subscribe and adhere to the overall principles of its responsible and ethical use, although remaining sceptical of the normative regulation (e.g. arms control treaties in relation to lethal autonomous weapon systems) and advocating instead norms-building approach—something that also defined its approach to international legal norms in cyber domain (Crandall and Allan 2015; Osula 2021).

The government's thinking—including how it defines autonomous weapon systems and their governance framework—is best reflected in the joint

Estonian-Finnish paper presented to the UN expert group's working session (GGE CCW 2018). In particular, the paper articulates that "autonomy should be understood as a capability to perform the given task(s) in a self-sufficient and self-governing manner" and argues that "humans must retain ultimate control over decisions of life and death." Crucially, it sets a baseline for the human operator competence in the armed forces. According to the paper, human operators must possess, "at a minimum, an understanding of the performance characteristics of the system and of the operational environment" and, consequently, "if the operator lacks such an understanding, or based on that understanding has no confidence as to compliance with the law, he/she must not permit the weapon to deliver force."

At the same time, however, some members of Estonia's government and the business community are concerned that multinational and the EU efforts (e.g. the EU's AI Act) will stifle development of innovative AI-based solutions in defence and will stall the emerging vibrant ecosystem of AI industry enterprises that are potential suppliers of such solutions (Riigikogu 2023b). Given the focus of Estonia on promoting these ecosystems, restrictive international and EU regulation seems to pose a risk to its future ability to contribute to collective defence AI endeavours. Policy-wise the MoD and other relevant government organisations are bound to continuously balance between nurturing the Estonian AI start-ups ecosystem and responding to the pressures from various directions to constrain the development of technology seen as posing unacceptable level of risk.

1.4 Industrial Push and Military Caution

Estonia's defence, security, and space industry has indeed been one of the key drivers of defence applications of AI in Estonia—not only through adoption of AI in cyber defence, but also in developing unmanned systems, counter-UAV capabilities, and digital battlefield management solutions. It has also been, thanks to the industry-funded studies and concept development and experimentation (CCD&E) efforts, at the forefront of thinking about the future of warfare where AI-enabled autonomous military systems are dominant in the battlespace (Interview, 20 December 2022). Some of the enterprises working with AI-enabled solutions are in direct contact with the armed forces and industrial partners in Ukraine, seeking to harness their insights and experience from the ongoing war and leverage them towards new concepts and product development.

The military's visionary thinking has been limited by the realities of defence development, whereby the Estonian Defence Forces (EDF) has had to address most basic capability gaps and needs first, before turning their eyes to more advanced capabilities and emerging disruptive technologies. This pivot is at its infancy but already underway, with parts of the military establishment already considering future scenarios—building upon NATO's work such as NATO Warfighting Capstone Concept (NWCC). They are also alarmed by the developments in the technology sector of the main adversary, Russia, and inspired by certain elements of war in

Ukraine. For these military thinkers, AI will be a major part of capabilities in most of the military functions—from ISTAR (Intelligence, Surveillance, Target Acquisition, and Reconnaissance) to indirect fire support and armoured manoeuvre to combat service support and military administration—in the coming decades (Interview, 14 July 2023).

In line with most of the thinking among Western militaries, AI is viewed as an enabler of dense "kill webs" characterised by compressed OODA (Observe, Orient, Decide, and Act) loops and associated with greater effects on the battlefield (Interview, 21 December 2022). In some of the most forward-leaning thinking, compartmentalised parts of the future battlespace (e.g., absorbing and delaying first waves/echelons of assault by the enemy along particular axes of advance) would be fully unmanned, even though always with human operators "on the loop" (Allik et al. 2021). Most relevant for small nations like Estonia, AI-aided capabilities such as unmanned systems are regarded as a means to limiting manpower losses that even a reserve-based wartime organisation such as the EDF would struggle with, and, furthermore, as a compensator for the lack of human resources that various military functions (e.g., staff work) require (Interview, 14 July 2023).

The military, however, remains cautious and reserved about AI-enabled capabilities and does not have an overarching vision for it. They readily admit that AI is already creating havoc and opening new opportunities in the information warfare domain. However, this is regarded as affecting the political layer of defence more than the military directly and therefore the understanding and management of the associated risks should be a matter for the political and policy-level attention in the first place. In general, they remark that AI will first transform societies before it transforms defence and that the latter transformation will not be in full swing in the coming decade or so anyway (Interview, 6 July 2023). Such remarks justify the focus of acting on the challenges of the more immediate future such as building greater mass, firepower, and reserves. Some military planners contend that, due to technological developments, some form or degree of AI-enabled man-machine teaming might become possible by the end of this decade (Interview, 14 July 2023). However, the overall sentiment is that the entire field of emerging disruptive technology is too unpredictable beyond a time horizon of 5–10 years.

Still, at the most senior levels of defence command, there is already an understanding that something profound is afoot. In some regards, the Allied presence in Estonia is a catalyst of a gradual change in perceptions of the military. The protracted period of experimenting with various iterations of indigenous Estonian platforms unaccompanied by any serious conceptual work on the military side about its potential seems to have created a blind spot in the perspective of the Estonian military. However, the British forces bringing unmanned ground vehicles (UGV) to the exercises in Estonia served as an "eye-opener" about the pace and potential impact of such systems on the capabilities of Estonia's key allies (Interview, 9 May 2023). Given the importance of maintaining interoperability with these allies, this is a major consideration for envisioning Estonia's future capabilities and the role of AI in them.

Likewise, Russia's war against Ukraine is serving as a source of insights about elements of warfare based on the adoption of various new technologies (including commercial-of-the-shelf) that is prompting some progressive thinking—even though data from primary sources on the use of these technologies by Ukraine remains very limited and, according to one senior Estonian officer, does not even provide enough material for lessons identified, let alone learned (Interview, 6 July 2023). Nonetheless, the war in Ukraine is accelerating ongoing efforts to prioritise defence capabilities like ISTAR, that requires greater reliance on ubiquitous and interconnected sensors, or digitised command and control (C2) processes to accelerate information sharing and decision-making. Long-range stand-off fires integrated with comprehensive sensor webs also receive greater attention in the Estonian military thinking, as does the role of loitering munitions (Jäärats 2022).

At the same time this view will be tempered by the observation made at the highest command level that there is no single "silver bullet" in the war in Ukraine, despite some advanced weapon systems being "elevated to the podium" at various points in time. Rather it is the combined, coordinated and sustained use of different systems on a large scale that is seen as most impactful in delivering the desired effects (Jäärats 2022). As a consequence, it is argued that Estonia should invest in more armour, mass and firepower (including long-range stand-off munitions), while adopting mature technologies (including, presumably, AI-enabled) that make their application more efficient and effective.

Future efforts to develop AI-enabled military capabilities will also have to contend with a high degree of caution in Estonian society. A public opinion survey conducted in late 2021 revealed that 62% of respondents agreed that AI can become more dangerous than nuclear weapons, while 85% did not trust the application of autonomy in military capabilities and 89% were against delegating "life or death" decisions to autonomous military systems (Idarand 2023). Partly reflecting this sentiment, but also to meet high standards sought at the EU level for the EU-funded projects, some companies have been instituting clear and robust ethical AI governance policies (Milrem Robotics Undated). They reflect the current state of thinking in Estonia about corporate responsibility and accountability in developing and fielding defence AI applications.

2 Developing Defence AI

Developing AI-enabled solutions is not consciously prioritised by the Estonian MoD when selecting and supporting R&D projects. For instance, in the framework of the defence industrial policy, the MoD provides annual grants to enterprises for developing solutions that are highly innovative, contribute to enhancing capabilities, and have export potential. Some of those successful projects may indeed contain elements of AI and, with time, are more likely to do so given the overall trajectory of technological development in the commercial sector. However, there is currently no deliberate demand pull from the defence organisation to do so. There is

some expectation though that the number of such projects will grow and, at some point, will organically reach critical mass (Roundtable, 2 September 2022).

This "bottom up" approach at the policy level is echoed by military practice. The EDF is quite open to testing new solutions such as robotic platforms with various units in the field and providing feedback to the developers. However, it does not place any special emphasis on those solutions being AI-aided or -enabled. The focus is firmly set on whether they resolve any specific technical, tactical, or operational problem and address an existing capability gap rather than on laying ground for introducing new paradigms and concepts of future warfare. The capacity of the EDF to define generic requirements for future capabilities and develop concepts for their employment remains very limited, further constraining the demand pull for AI-based solutions.

This is not to say that the ground is not being laid for such solutions. As an example, the efforts to stand up the Estonian Division (ESTDIV)—a formation that will serve, among other things, as a "plug and play" environment for NATO Allies deploying to Estonia—require addressing various shortcomings in the C4I (Command, Control, Computers, Communications, and Intelligence) systems. The ongoing integration and further digitisation of command and the resource management processes are a prerequisite for future AI-based applications, including those of the allies whose units will become part of the ESTDIV. This will have to overcome the proclivity of national contingents contributed by various Allies to limit information sharing across national lines—a procedural and policy rather than a technical problem requiring the constant use of staff liaison officers (Briefing, 28 September 2023).

In addition, the EDF has been making steady progress with two in-house development projects that form the basis and core of its digitalised battlespace management:

- *KOLT (Kaitseväe olukorra ja lahinguteadlikkuse süsteem)*

KOLT is a Defence Forces Situational and Combat Awareness System that was initiated in 2014–2015 by conscripts and reservists with IT background and has since become an EDF-wide solution used by various units and tested during major exercises such as *Kevadtorm* (Spring Storm) (EDF 2019). Some small development projects to use AI to facilitate its various functions (e.g. mapping, handwriting recognition, etc.) are being pursued by the EDF, showing how a major technological step forward opens opportunities for more AI-related "bottom up" ideas and add-ons.

- *TOORU*

TOORU is a fire support system that seeks to combine fire managers, fire control centres, calculation points, weapon systems, fire support officers, logistical components, and aerial fire control elements into a single digitalised "kill web." Conceived as one of the modules of KOLT, it already generates datasets from various fire systems and is envisaged as an excellent platform for introducing AI solutions aiming to reduce the workload of human operators in preparing fire missions (e.g.

performing calculations) (Dieves 2021). Thus, it has already been designed from the start as a system that will both generate data for training AI algorithms and integrate new capabilities based on AI.

Overall, however, there is a sense that the defence organisation needs take a step back and assess the potential and requirements for AI across a range of capabilities. An MoD-funded study project by the National Defence Academy (NDA), together with Germany's Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), aims to examine the potential requirements and narrow down the broad spectrum of AI applications to more specific priority areas (Interview, 9 May 2023). This should lay the ground for stronger demand pull and the defence AI strategy with a degree of top-down guidance as well as facilitate greater coherence in selecting, encouraging, and supporting development projects in the future.

Estonian enterprises take a lead not only in thinking about, but also developing AI-enabled solutions, often in close collaboration with the University of Tartu and Tallinn University of Technology (TalTech), the country's two leading universities, and the NDA. A vibrant innovation ecosystem has helped set up several companies that also develop defence products with AI applications (some of them are R&D-intensive in their business model as well) such as Milrem Robotics (UGV development), Threod Systems (UAVs), DefSecIntel Solutions (sensors and surveillance systems), SensusQ (data sharing and intelligence management platforms), Marduk Technologies (counter-UAV solutions), Rantelon (electronic warfare and communication systems), Wayren (digital communication platforms), or Krakul (internet of things for defence).

The Estonia cybersecurity sector also has enterprises that work on AI-enabled solutions. Chief among them are Cybernetica (encryption technologies), CybExer Technologies (cyber range technology and services), Guardtime (data security and blockchain technology applications) and others. Many of them are collaborative partners of the Foundation CR14 as well as Estonia-based NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE)—important players in the defence AI development ecosystem.

In addition, two well-established Estonian companies are coordinating major pan-European consortia financed within the framework of the European Defence Fund:

- *iMUGS*

Launched in 2020 and led by Milrem Robotics, iMUGS (Integrated Modular Unmanned Ground System) strives to develop "a modular and scalable architecture for hybrid manned-unmanned systems in order to address a large range of missions and to enable easy update or modification of assets and functionalities within the system (aerial and ground platforms, command, control and communication equipment, sensors, payloads and algorithms)" (European Commission 2020). It heavily builds on the TheMIS UGV platform and works on the premise that such platforms are supposed to be part of a broader system of systems where AI in C2 as well as AI-enabled autonomy will be major pillars of the new capabilities.

- *EUROGARD*

Launched in 2022 and led by Baltic Workboats, this project is less ambitious in its scope than iMUGS and has set out to "build a vessel capable of a range of different autonomous operations in coastal areas" (European Commission 2022). In this case, Estonian leadership of the consortium draws heavily on the expertise in developing autonomous maritime surface platforms for civilian applications that has already seen through deployment of a research vessel capable of autonomous operations at sea in collecting various data (ERR 2023a).

Cybersecurity is viewed as a pivotal element of future secure, safe, and trustworthy AI systems, allowing Estonian companies to leverage their competitive advantages in larger projects led by their allies. As an example, Estonia's Cybernetica signed a contract with the US Office of Naval Research to develop cryptographically secure AI. According to the company, "the PAI-MACHINE project will optimise algorithms for collaborative AI applications so that allies can share work together for the common good without having to share their confidential data in full" (Cybernetica 2023).

The opportunities related to the European Defence Fund are also pursued in this field. In the 2023 cycle of proposals, Foundation CR14 is leading AIDA (Artificial Intelligence Deployable Agent), a consortium of 28 organisations from 15 nations. The consortium aims to develop a set of Technology Readiness Level 7 software agent prototypes that rely on AI algorithms for their operation in the cyber incident management cycle. The project is expected to improve protection of the EU's critical infrastructure (e.g. satellite communications), alleviate human resource availability problems in cybersecurity, and enhance military mobility through securing operations of autonomous vehicles and aircraft. The decision of the European Defence Fund is anticipated in 2024 (E-mail communication, 1 December 2023).

3 Organising Defence AI

Estonia's approach to organising defence AI reflects its overall organisation for defence innovation. The system rests on the "bottom up" initiatives from within the defence organisation as well as stimulating and facilitating the innovation ecosystem outside the government structures—in the civilian universities and enterprises. It also focuses on enhancing relations with foreign partners. This ensures that ideas for development and experimentation are relevant to national and international end-users, while also staying connected to wider trends in the transatlantic and European arenas. At the same time, however, this approach lacks overall strategic coherence, continuity in projects, and momentum in harnessing such disruptive technologies as AI.

3.1 A Broad Alliance for Defence AI…

Estonia's defence policy has always placed strong emphasis on the so-called "broad-based national defence," whereby all national stakeholders—public and private—ought to have a role in ensuring the nation's defence and provide capabilities for the common efforts (Estonian MoD 2010, 2011). When it comes to defence technology and innovation, this whole-of-society and whole-of-government approach in practice often means that the MoD spends portions of the defence budget for the projects of civilian research establishments or companies that have potential or clearly identified military applications.

The AI-related efforts at the national level—just as digitalisation of governance and cybersecurity—are coordinated by the Ministry of Economic Affairs and Communication. The MoD, in turn, has consolidated numerous activities within a single department of defence innovation, even though other departments such as those overseeing NATO and the EU affairs or national defence information systems, contribute to its mission from their respective roles. The department is responsible for formulating R&D and defence industrial policies. It has recently established a position for coordinating all AI-related matters and, eventually, developing the Estonian defence AI policy.

On a working level, however, the MoD must draw upon the expertise and contribution of state agencies and other entities outside its formal structure but within its area of governance. One such agency is the Estonian Centre for Defence Investment, where management of most procurement programmes was centralised in 2015. The centre prepares technical requirements of equipment acquisition and has specialised managers for various categories of equipment. AI will inevitably become part of these requirements across a range of capability projects, thus necessitating a certain level of competence and the capacity to incorporate impartial external advice from the national and allied S&T base.

Moreover, the MoD area of governance includes organisations that have great flexibility in combining various sources of funding, incorporating national and foreign public and private sector partners into common projects, and providing hubs for testing various practical solutions. Foundation CR14 is key to the Estonian efforts to advance cybersecurity and cyber defence solutions, with AI rapidly becoming an important part of this effort. CR14 operates cyber ranges that are used by various stakeholders (including NATO CCDCOE) to conduct exercises and test new solutions (Foundation CR14 Undated). These cyber ranges also help to generate datasets that can be used by the data owners (e.g., nations that provide "blue teams" at Exercise Locked Shields (NATO CCDCOE Undated) to train AI algorithms in cyber defence. The foundation's CEO has also been appointed to represent Estonia in NATO's Data and Artificial Intelligence Review Board (DARB).

The MoD also provides support for non-governmental entities and programmes initiated by other stakeholders. One such programme is Cyber North, a cybersecurity AI accelerator, launched by Start-up Wise Guys, a major Estonian technology start-up accelerator, in cooperation with the Estonian Defence and Aerospace

Industry Association in 2019 (Enterprise Estonia 2018). Since then, it has become an accelerator within NATO's DIANA network (ERR 2022). This not only brings the Estonian entrepreneurial expertise in start-up creation and growth to bear on developing AI-powered solutions for defence, but also enhances Estonia's profile as a multi-spoke hub and integrator of such innovation benefiting the entire Alliance.

3.2 …Meets Defence Forces Not Yet AI Ready

While the MoD appears reasonably well organised and prepared to pursue defence AI-related ambitions, the EDF has a poorer organisational preparedness. For a start, there is no centralised innovation management function at the top-level EDF headquarters, and the office of the Chief of Defence no longer has a position of chief scientific or innovation adviser to provide advice on what should be included in the top-level defence planning and capability development guidance to the services and commands.

If any substantive consideration is given to the EDTs, and AI in particular, it should be included through the long-term planning processes managed by the defence planning department of the HQ (J5). However, as demonstrated by the failure to stand up an autonomy programme initiated to provide centralised coordination from the EDF HQ for this particular area of technology, it is all too easy to abandon organisational measures if they are not regarded as a strategic priority and do not have a powerful high-level advocate in the organisational hierarchy (Interview, 20 December 2022). Interest in and initiatives to advance innovative solutions that might include AI thus basically reside at the level of individual units and communities of practice (e.g. military intelligence, signals and communications, or electronic warfare).

The EDF, however, sought to centralise its interaction with the civilian S&T community and defence industry via the Applied Research Centre of the NDA. This has proven useful in providing a central hinge between external innovators and end-users within the EDF (Jermalavičius and Hurt 2021). However, it has not been able to build the capacity that is quite central for the military's ability to define the need for innovative solutions—operational analysis/operational research (OA/OR). It is also pushed into too many directions, such as securing funding from the EU sources through consortia, supporting the educational mission of the academy, and addressing the requirements for research in social sciences, thus diluting its ability to focus on the application of the EDTs, including AI, in defence (Interview, 9 May 2023). It is also too far removed from the centralised planning processes at the EDF headquarters, making it less impactful than it should be in future-proofing long-term defence development plans (Interview, 21 December 2022).

Existing challenges notwithstanding, long-term defence planning may undergo some important changes soon. The ongoing project to redesign planning methodology will open some important opportunities to consider EDTs in the future capability mix. For example, it will identify points in time when various external (e.g.

defence industry) or internal (e.g. the NDA) stakeholders will have a possibility to engage defence planners in a discussion on technological aspects of the capabilities. Services would be provided some funding to experiment with the technologies that may become part of their capability mix in the future, in the expectation that their analysis and lessons will shape their inputs into the defence plans (Interview, 14 July 2023).

Additionally, some of the more recent new force structure elements need to pursue new technological solutions within a very dynamic threat environment due to their core mission. Estonia's Cyber Command, established in 2018, is one example. Its mission is to conduct operations in cyberspace, including information operations, making it one of the domain-specific combatant commands alongside land, air, and naval forces. It also provides support to other EDF services and commands as well as agencies in the MoD's responsibility when it comes to information technology, infrastructure, and services, thus also making it akin to a C3I agency or combat service support organisation (EDF Undated). Uniquely among the EDF services and somewhat contrary to efforts to centralise EDF's R&D coordination at the NDA, it is also tasked with R&D work in its domain, thus linking it with external partners in the wider defence innovation ecosystem.

By virtue of this triple role, but particularly due to its exposure to the domain where AI applications are emerging very fast, it thus potentially becomes a major gateway for AI diffusion into the military organisation, especially given the synergies and overlaps between cyber operations, ISTAR, electronic warfare, information operations, and C3I management. This, however, will be contingent on greater acceptance of its role and mission across the EDF, which is not always there. Furthermore, its success will also rest on how well it will be able to combine its various tasks, as currently its cyber and information operations, for example, are quite poorly integrated (Interview, 30 November 2023).

This structural arrangement is, to some extent, mirrored by the Estonian Defence League (EDL)—a paramilitary organisation for territorial defence manned by volunteers. Its Cyber Defence Unit was stood up in 2010 and provides a platform for the volunteer members of the EDL from all walks of life to exchange their knowledge, train together and act when required (Estonian MoD 2010). The unit extends its remit into information operations as well, and it would be natural to expect that, with the proliferation of AI tools in the civilian cyber and strategic communication sectors, members of this unit will bring ideas and solutions from these sectors to the military environment.

The discipline of long-term defence planning seems, however, to have been put on the back burner recently. This will most likely also affect its interplay with defence innovation. Currently, Estonian defence development is driven by the fundamental assumption that Russia—a primary and existential threat to Estonia—will reconstitute most of its lost capabilities by the end of this decade if not sooner, necessitating a steep and rapid increase in Estonia's national defence capabilities. The country is now basically trying to compress a 10-year cycle into 4 years or even less to arm and prepare itself as much as possible ahead of what it regards as a

quickly approaching point of a direct military confrontation with Russia (Toom Kooli Strategic Talks, 15 November 2023).

In this mindset, there is little space left for considering long-term implications of various EDTs—including in terms of interoperability with allies. Only innovative solutions that are mature enough, readily available and in use by key allies—and therefore can be quickly introduced into the capability mix or adapted to military uses from their civilian origins without negative impact on interoperability—draw attention of the planners and military leadership.

4 Funding Defence AI

For years, Estonia has been one of the few NATO Allies spending more than 2% of its Gross Domestic Product (GDP) on defence. Russia's full-scale war against Europe has shifted the terms of the spending debate in the Alliance, whereby Tallinn is advocating this level as a floor rather than a ceiling. While Estonia's defence budget of 2021 was €749M (2.2% of GDP), it grew to €1.1bn (2.73% of GDP) in 2023 and is expected to reach €1.3bn (3.2% of GDP) in 2024 (Riigikogu 2023a).

Such growth, however, does not deliver a very large pool of funding in absolute terms or create too much additional space for funding R&D/R&T. The needs for capability development and stockpile build-up are considerable and, along with the need to compensate for the impact of inflation on personnel pay, crowd out more long-term requirements. According to senior military officials, the overriding principle in budget allocation currently is whether a programme or project is likely to deliver tangible results (i.e. fielded capabilities) within the next four to 5 years (Briefing, 28 September 2023).

As the defence organisation essentially resides in the emergency mode, spending on long-term technology and innovation pursuits might sound, to a large degree, as a luxury item. As of 2021 (i.e., before the war in Ukraine), Estonia was spending just €5.1M on R&D and only €1.1M on R&T (using EDA's definitions) (EDA 2022). However, it seems that the wave of fresh funding for defence is spilling over into the R&D investments, despite the long-standing scepticism and the pressure of current events. According to the MoD figures, its R&D investments were €5.6M in 2022 and €7.8M in 2023. They are projected to more than double in 2024 and reach €12.1M (E-mail communication, 20 November 2023), which can be explained by the need to co-finance involvement in the EU-funded projects. Still, this is only about half of the EDA's benchmark of 2% of the defence budget to be spent on R&D/R&T.

Given current budgeting methods, no data is available to identify specific spending priorities such as defence AI, for example. This makes it very difficult to gauge the MoD's funding levels for it. Nonetheless, some defence industry support grants of the MoD go to the projects the title of which explicitly or implicitly suggest the inclusion of at least some elements of defence AI (Estonian MoD 2023c):

- In 2021, a project "Prototype of Unit of an automated mini-drone-station with 'search & find' AI detection model software."
- In 2022, development of an Intelligent Decision Support System (IDSS) and Mixed Reality Situational Awareness System.
- In 2023, a project "Tactical Data Exchange Platform with Armoured Troops Awareness System Integration."

These are usually small grants, ranging between €72,000 and €200,000, but they are an important element of stimulating the industry's interest in defence markets, especially among young enterprises and start-ups. In contrast, Estonia's civilian AI sector receives far larger sums from the private financial sector or external sources. The OECD AI Policy Observatory estimated that Estonia's overall AI start-up ecosystem received a cumulative investment inflow worth USD437M as of 2023, which has almost tripled in size since 2021 (OECD Undated). Although this dwarfs anything that the MoD can offer to finance defence AI development, the benefits of such investments in the broader AI sector are bound to seep into defence-related projects at some point.

Multinational sources of funding like the European Defence Fund (and one of its precursors, EDIDP) as well as Horizons Europe (Horizons 2020 in the previous cycle) have emerged as pivotal in advancing AI-related developments in Estonia. The latter is still something that defence research and innovation projects are not eligible for (those are addressed via the European Defence Agency's instruments) but given the dual-use nature of AI and the reliance of the Estonian defence innovation on the civilian S&T base, this restriction eventually becomes trivial.

The European Defence Fund, on the other hand, has direct relevance and significance to the Estonian enterprises involved in the defence sector. Estonian enterprises have been particularly successful in tapping into this source, with 16 international projects that involve companies from Estonia receiving an overall total of almost half a billion euros of funding. Six of those projects also receive Estonian MoD co-funding (Estonian MoD 2023a). Again, it is hard to isolate, without additional research, what share is devoted to AI-related technologies. Some of the MoD co-funded projects (e.g. Cyber and Information Warfare Toolbox (EUCINF), Collaborative Combat for Land Forces (LATACC), Naval Collaborate Surveillance (E-NASCOS)), however, are bound to include AI one way or another and may even source this technology from Estonia, judging from the participating companies such as Milrem Robotics, Cybernetica, Cafa Tech or Criffin that seek to incorporate AI into their products and services.

If and how these projects will deliver tangible capability gains for the EDF, however, is an open question. For now, the military is fully satisfied with the arrangement that minimally taxes the defence budget and shifts the financial and technological risks to industry and the EU, while drawing upon the military end-user's knowledge and feedback. It is possible, though, that EU or NATO-funded development projects will eventually become a stimulant of interest and demand from the EDF when formulating their capability requirements, thus accelerating the adoption of technology that those projects seek to advance.

5 Deploying and Operating Defence AI

In a country without a formal defence procurement policy in place, it is difficult to assess whether AI-enabled capabilities are prioritised in any way—this would require analysis of technical requirements of each procurement on a case-by-case basis. However, as an informal matter, the Estonian MoD and its procurement agency adhere to the principle that past support for development projects does not warrant procurement of the outcomes. Rather tenders evaluate all offers and select the best match with the requirements while remaining agnostic about the source of technology (as long as it is not China, Russia, or other similar originators) or whether it has domestic roots and has drawn upon investments by the Estonian taxpayers (Jermalavičius and Hurt 2021).

Despite this, officials insist that most projects supported with MoD grants within the defence industrial policy successfully secure sales with the domestic customer (Roundtable, 2 September 2022). This is partly the result of the military's familiarity with technology built in a close consultation process between end-users and project teams, thus ensuring alignment of the results with military customer needs. For example, the defence forces gained useful experience in operating robotic systems as part of field tests and on missions. The THeMIS UGV was operated by the Estonian contingent in French-led Operation Barkhane in Mali, where three EDF platoons used the platform for patrols and transportation of supplies. This deployment provided the producer with valuable insights into the performance of the platform under harsh conditions (e.g., desert terrain, hot temperature) and enabled the military to better understand the added value of such platforms and the challenges in operating them (Milrem Robotics 2020).

Assessing the actual deployment of AI-enabled capabilities, however, remains complicated as they often constitute the most sensitive part of the package, especially in such domains as ISR or cyber, thus making them subject to high levels of classification. It can only be inferred that procuring ISR UAVs from Estonian producer Threod Systems for tactical and operational level combat service support functions could potentially feature in-built AI elements—if not yet currently then definitely in the future. Likewise, with the ongoing implementation of the in-house projects, KOLT and TOORU, are opening possibilities for deploying new AI tools to assist the processes in these systems.

However, the major ongoing shift in defence procurements will be a game changer for future AI-enabled capabilities. During the first two decades or so since restoring the independence, the EDF had to rely mostly on donated equipment or purchases of second-hand systems, with some notable exceptions such as long-range air surveillance radars or short-range air defence and guided anti-tank missile systems. But over the last few years, we are witnessing a surge in acquiring brand-new equipment and weapon systems with cutting-edge technology (Gosselin-Malo 2023). Many of these systems like

- Blue Spear (5G SSM) land-to-sea cruise missile system
- Blocker PM16 naval mines

- M142 HIMARS multiple rocket launchers
- K9 Thunder 155 mm self-propelled howitzers
- Iris-T SLM medium range air/missile defence system
- Long-range loitering munitions (LMs)

will already include AI or provide possibilities for incorporating it through upgrades or connectivity with AI-assisted battle management systems. Participation of the Estonian national representatives in the multinational end-user clubs and their interaction with the suppliers will play a crucial role in avoiding costly problems of integrating AI add-ons in the future. At the same time, the fact that some of these procurements are already undertaken jointly with foreign partners—such as Blue Spear and K9 Thunder with Finland and Iris-T with Latvia—opens opportunities for collaborative technology adoption pathways as envisaged by the emergent defence AI policy principle articulated by the MoD.

Herein lies a risk that the Estonian end-users will just not make sufficient effort to fully and comprehensively understand the AI technology packaged in the acquired cutting-edge systems, as in some cases it will primarily be examined, understood, and vouched for by the lead partners in joint procurement projects. This may not lead to the outright adoption of a black-box solution that would contravene Estonia's position which holds that operators need to understand built-in AI. Rather it might create a grey-box situation, whereby EDF operators will probably have some necessary understanding, but will depend upon the explanations of irregular AI behaviour from their foreign military or industrial partners.

6 Training for Defence AI

Doctrinally, the EDF is not well prepared to advance force-wide learning outside the whole-of-alliance framework, as there is no formal national military doctrine in place and the entire system often directly relies on Allied Joint Publications (AJP) and Allied Tactical Publications (ATP) (Interview, 21 December 2022; Interview, 14 July 2023). Without the national process to think through and develop conceptual ideas as well as to establish them as part of the Estonian doctrine, the EDF becomes highly dependent on the progress of NATO in incorporating AI into its AJP/ATP family of documents. This, on the other hand, may serve as an opportunity, given that a small country alone can hardly address the challenge of drawing an overarching doctrine for joint multidomain operations, for example.

Many of the preconditions for effective learning about AI, however, could be laid in the professional military education (PME) system, with the NDA and the Baltic Defence College playing a pivotal role. For the time being, however, AI is addressed as a fairly minor subject within larger technology and innovation modules and courses, even though air and naval officer training provides some more extensive exposure to this particular technology. Likewise, the training of non-commissioned officers (NCO) for the land component—by far the most dominant service in the

EDF—does not provide any significant skillset in managing AI as part of the military capabilities and tactics, techniques, and procedures (TTPs) (Interview, 21 December 2022).

As the Estonian defence system relies heavily on the mobilisation reserve, conscript and reserve (re-fresher) training programmes naturally constitute the core of the training activities undertaken by the EDF. These programmes undergo continuous modifications and adaptation, depending on, among other factors, when the defence acquisition programmes and projects deliver new weapons systems and equipment or their upgrades. In most cases, conscripts—and the units manned by conscripts—must demonstrate their ability and be certified to use these systems before being transferred to active reserve after 8–11 months of service, while the EDF's professional core needs to gain deep understanding of those systems well ahead of their actual fielding. This gives a few years head-start before any major influx of AI technology takes place—including potentially together with the joint procurement partners (e.g. Finland and Latvia), given that pooled training and logistics are often touted as key benefits of collaborative procurement projects.

As discussed, the policy thinking suggests that AI-enabled systems should not be used if the operators do not possess sufficient understanding of how the AI behaves in the respective systems. Therefore, readiness of individual and collective training system to deliver upon this principle becomes critical. Military leaders acknowledge that, to be a competent end-user of sophisticated weapon systems, many of which will be drawing upon AI, the EDF will require ever growing number of soldiers-technicians—with the backgrounds and skill sets related to STEM (Science, Technology, Engineering, Mathematics) disciplines—in addition to the usual soldiers-tacticians (Interview, 21 December 2022). This, in turn, shifts the onus onto the national higher education and vocational training system, whose graduates then go through the basic and advanced military training programmes. With STEM disciplines lacking popularity, the MoD and EDF are now working on co-operative arrangements with various civilian schools to give them a boost through scholarships and other incentives, in the expectation that future demand for technical skills—including those relevant to AI—will be met by sufficient supply from the national education system (Defence Resources Agency 2023).

The EDF is not arriving at the threshold of the AI era being deprived of talents. Using the ProgeTiiger programme framework and tools aimed to enhance technology literacy starting as early as kindergarten (Education Estonia 2021), the world-class Estonian education system (Schleicher 2019) is already dedicating attention to such subjects as coding and robotics from an early age. The EDF can tap into this trend through conscription—which also serves as one of the recruitment tools for full-time military employment—and, as the roots of KOLT demonstrate, is even capable of encouraging, capturing, and scaling up the innovations that arise from this talent pool. However, it is a different subject, whether it is capable of motivating and retaining the best and brightest in the fierce competition for talents in a small labour market where private enterprises in the high-tech sector offer much higher salaries and benefits.

The conscription and reserve training system is not a perfect solution, as military service is mandatory only for men and voluntary for women, thus depriving the EDF of easier access to a significant part of a demographically aging and shrinking talent pool. Notwithstanding the fact that younger generations might have natural instincts for handling high-tech systems, the current approach also fits relatively poorly with the world of complex technology as the effective mastering of new technologies requires longer periods than the current duration of conscript service or the amount of reserve refresher training. It also locks many of the full-time professionals into repetitive training cycles, giving them fewer opportunities to experiment, innovate, and develop new skills or tactics, techniques, and procedures (TTPs). Nonetheless, the current approach synchronises the EDF with the broader societal trends among which AI proliferation will inevitably be a major one.

7 Conclusions

Estonia's gradual embrace of defence AI illustrates the challenges and opportunities of broader defence innovation in a country where strong entrepreneurial drive and the government's willingness to facilitate and leverage technological progress meet the conservative and cautious military focused on quick build-up of capabilities required to counter an existential threat to the nation. The lack of a strong, sustained, and systematic demand pull for AI-enabled solutions from the military side is compensated, to some degree, by the enthusiastic, dynamic, and conceptually well-versed AI innovation ecosystem that has taken root in Estonia because of its strengths in cyber and robotic technologies. Russia's war against Ukraine and emerging AI-enhanced capabilities in key allies such as the UK, the US, and France serve as additional motivating factors for the Estonian military to increasingly pay attention on how to apply AI to shape future warfare.

Despite its relative novelty, AI is not finding Estonia's defence organisation writ-large just passively watching the incoming wave. Thanks to efforts by the MoD and industry, it is well integrated into NATO and EU fora where defence AI is a central theme. This also provides opportunities for Estonia to join leading countries in large EU-funded defence projects focusing on defence AI. The military has been open to experiments and provides feedback to developers, using the NDA as the main interlocutor. The Cyber Command and the communities of practice (intelligence, electronic warfare) are places where AI will be making major strides. The development of in-house projects is laying further ground for the future exploitation of AI. If successful, the reform of the long-term defence planning process will provide incentives for the military services, branches, and units to pay more attention to what longer-term future challenges might be and how to prepare for them.

Some preconditions for the effective adoption of defence AI, however, are clearly lacking. There is no vision in place for the EDF to become a data-centric organisation or how far-reaching its digitalisation will be. Without an overarching AI policy and a national military doctrine, a lot of AI-related (as well as generally

technology-driven) innovation might come to lack the scale, coherence with the national defence objectives, and eventual impact. The overwhelming focus on short and medium-term capability requirements leaves long-term foresight side-lined and marginalised. Almost entirely absent OA/OR capacity and concept development and experimentation structures in the EDF make it difficult to systematically estimate the impact of emerging disruptive technologies on warfighting and cast the existing organisational practices in a critical light. This is further reinforced by superficial coverage of AI and related technologies at all levels of the PME system.

The above shortcomings will, sooner or later, be addressed. It is clear though that Estonia is not setting itself an ambition to be first adopter of AI in defence, but rather seeks to tread carefully and avoid costly mistakes, while remaining integrated with the efforts and networks of its allies. Estonia will likely continue leading in some niche areas, where national strengths and civilian inputs are evident, such as cybersecurity and cyber operations or software for autonomous platforms and sensors. However, for a small nation, being a solid, competent, and active team player will be more important in defence AI adoption than pursuing its own high-flying visions or revolutionary transformations.

References

Allik, Sten, Sean Fahey, Tomas Jermalavičius, Roger McDermott, and Konrad Muzyka. 2021. *The rise of Russia's military robots: Theory, practice and implications*. Tallinn: International Centre for Defence and Security.

Atmante, Kristine, Riina Kaljurand, and Tomas Jermalavičius. 2019. Strategic cultures in the Baltic states: The impact of Russia's new wars. In *Strategic cultures in Russia's neighbourhood: Change and continuity in an in-between space*, ed. Katalin Miklóssy and Hanna Smith, 53–82. London: Lexington Books.

Chief Digital and Artificial Intelligence Office. 2022. AI partnership for defense (AI PfD) (Joint Statement). https://www.ai.mil/docs/AI_PfD_Joint_Statement_09_16_20.pdf. Accessed 30 Jan 2023

Crandall, Matthew, and Collin Allan. 2015. Small states and big ideas: Estonia's battle for cybersecurity norms. *Contemporary Security Policy* 36 (2): 346–368. https://doi.org/10.1080/13523260.2015.1061765. Accessed 30 Jan 2024.

Cybernetica. 2023. Cybernetica signs contract to develop cryptographically secure artificial intelligence with US Office of Naval Research. https://cyber.ee/resources/news/ONR-2024/. Accessed 30 Jan 2023

Defence Resources Agency. 2023. Kaitseressursside Amet soovib stipendiumikonkursiga suunata noori rohkem tehnikavaldkondasid valima [The defense resources agency wants to direct young people to choose more technical fields with a scholarship competition]. https://kra.ee/kaitseressursside-amet-soovib-stipendiumikonkursiga-suunata-noori-rohkem-tehnikavaldkondasid-valima/. Accessed 30 Jan 2024

Dieves, Veiko. 2021. Kiirema tulelöögi nimel—TOORU projekt [for the sake of faster fire support—TOORU project]. *Academia Militaris* 2: 12–16.

Education Estonia. 2021. ProgeTiger—Estonian way to create interest in technology. https://www.educationestonia.org/progetiger/. Accessed 30 Jan 2024

Enterprise Estonia. 2018. Estonia invites new cyber security startups—a unique cyber security and AI accelerator to be opened. https://investinestonia.com/estonia-invites-new-cyber-security-startups-a-unique-cyber-security-and-ai-accelerator-to-be-opened/. Accessed 30 Jan 2024

ERR. 2022. Tallinn, Tartu science parks to operate NATO innovation accelerator DIANA. https://news.err.ee/1608697294/tallinn-tartu-science-parks-to-operate-nato-innovation-accelerator-diana. Accessed 30 Jan 2024

———. 2023a. Scientists launch Estonia's first autonomous maritime research vessel. https://news.err.ee/1609117841/scientists-launch-estonia-s-first-autonomous-maritime-research-vessel. Accessed 30 Jan 2024

———. 2023b. State to make ready AI strategy by year-end. https://news.err.ee/1609054811/state-to-make-ready-ai-strategy-by-year-end. Accessed 30 Jan 2024

Estonian Defence Forces (EDF). 2019. Kevadtormil arendavad küberväejuhatuse ajateenijad IT-lahendusi [Cyber command's conscripts develop IT solutions during the Spring Storm]. https://mil.ee/uudised/kevadtormil-arendavad-kubervaejuhatuse-ajateenijad-it-lahendusi/. Accessed 30 Jan 2024

———. Undated. Küberväejuhatus [Cyber Command]. https://mil.ee/uksused/kubervaejuhatus/. Accessed 30 Jan 2024

Estonian Ministry of Defence (MoD). 2010. Kaitseliidu koosseisus luuakse küberkaitseüksus [Cyber defence unit is being created within the Defence League]. https://kaitseministeerium.ee/et/uudised/kaitseliidu-koosseisus-luuakse-kuberkaitseuksus. Accessed 30 Jan 2024

———. 2011. *National Defence Strategy*. Tallinn: Estonian Ministry of Defence of Estonia.

———. 2023a. Estonia achieves unprecedented success with European Defence Fund projects. https://www.kaitseministeerium.ee/en/news/estonia-achieves-unprecedented-success-european-defence-fund-projects. Accessed 30 Jan 2024

———. 2023b. Eesti ja Ühendkuningriik allkirjastasid pikaajalise kaitsekoostööleppe [Estonia and the United Kingdom signed long-term defence cooperation agreement]. https://kaitseministeerium.ee/et/uudised/eesti-ja-uhendkuningriik-allkirjastasid-pikaajalise-kaitsekoostooleppe. Accessed 30 Jan 2024

———. 2023c. Kaitsetööstuse arendusprojektide konkurss 2023 [Defence industry development projects competition 2023]. https://kaitseministeerium.ee/et/eesmargid-tegevused/teadus-ja-arendustegevus/kaitsetoostuse-arendusprojektide-konkurss-2023. Accessed 30 Jan 2024

European Commission. 2020. iMUGS—Integrated modular unmanned ground system. https://ec.europa.eu/commission/presscorner/api/files/attachment/865736/EDIDP%20-%20iMUGS.pdf. Accessed 30 Jan 2024

———. 2022. EUROGUARD—EUROpean Goal based multi mission Autonomous naval Reference platform Development. https://defence-industry-space.ec.europa.eu/system/files/2023-06/EUROGUARD%20-%20Factsheet_EDF22.pdf. Accessed 30 Jan 2024

European Defence Agency (EDA). 2022. *Defence data 2020–2021: Key findings and analysis*. Brussels: European Defence Agency.

Foundation CR14. Undated. Cyber ranges. https://www.cr14.ee/ranges/. Accessed 30 Jan 2024

Gosselin-Malo, Elisabeth. 2023. Estonia's global arms buying spree seeks drastic combat gains. Defense News. https://www.defensenews.com/global/europe/2023/06/13/estonias-global-arms-buying-spree-seeks-drastic-combat-gains/. Accessed 30 Jan 2023

Government of Estonia. 2019. *Estonia's national artificial intelligence strategy 2019–2021*. Tallinn: Government of Estonia.

Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. 2018. Categorizing lethal autonomous weapons systems - A technical and legal perspective to understanding LAWS (Submitted by Finland and Estonia). https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/257/85/PDF/G1825785.pdf?OpenElement. Accessed 30 Jan 2024

Idarand, Tõnis. 2023. *Reining in autonomous weapons: Impact on military innovation—An Estonian perspective*. Tallinn: International Centre for Defence and Security.

Jäärats, Raiko. 2022. Kaitseväe juhataja: kõik algab tahtest oma riigi kaitsta [Chief of defence: Everything starts with the will to defend one's country]. *Sõdur* 128 (6): 6–13.

Jermalavičius, Tomas, and Alice Billon-Galland. 2023. *British power in Baltic weather: The UK's role in Nordic-Baltic security and UK-Estonia defence cooperation*. Tallinn: International Centre for Defence and Security and Chatham House.

Jermalavičius, Tomas, and Martin Hurt. 2021. *Defence innovation: New models and procurement implications—The Estonian case*. Paris: ARES Group.

Kaska, Kadri, Liis Rebane, and Toomas Vask. 2021. Lessons from Estonia's national cybersecurity strategy: How to succeed or fail in delivering value. In *So far, yet so close: Japanese and Estonian cybersecurity policy perspectives and cooperation*, ed. Henry Rõigas and Tomas Jermalavičius, 12–21. Tallinn: International Centre for Defence and Security.

Milrem Robotics. 2020. Milrem Robotics' THeMIS UGV completes first deployment in Mali proving its effectiveness and reliability. https://milremrobotics.com/milrem-robotics-themis-ugv-completes-first-deployment-in-mali-proving-its-effectiveness-and-reliability/. Accessed 30 Jan 2024

———. Undated. Policy of ethical development of systems with intelligent functions. https://milremrobotics.com/policy-of-ethical-development-of-systems-with-intelligent-functions/. Accessed 30 Jan 2024

NATO CCDCOE. Undated. Locked shields. https://ccdcoe.org/exercises/locked-shields/. Accessed 30 Jan 2024

OECD. Undated. AI in Estonia. https://oecd.ai/en/dashboards/countries/Estonia. Accessed 30 Jan 2023

Osula, Anna-Maria. 2021. Aligning Estonian and Japanese efforts in building norms in cyberspace. In *So far, yet so close: Japanese and Estonian cybersecurity policy perspectives and cooperation*, ed. Henry Rõigas and Tomas Jermalavičius, 22–29. Tallinn: International Centre for Defence and Security.

Riigikogu. 2023a. 2024. aasta riigieelarve eelnõu [Draft budget of 2024]. https://www.riigikogu.ee/fookusteemad/2024-aasta-riigieelarve-eelnou/. Accessed 30 Jan 2024

———. 2023b. Tehisintellekti võimalustest ja mõjudest [On the opportunities and impact of Artificial Intelligence] (on YouTube). https://www.youtube.com/watch?v=eRrFcFPXnEk. Accessed 30 Jan 2024

Salu, Kadi, and Erik Männik. 2013. Estonia. In *Strategic cultures in Europe: Security and defense policies across the continent*, ed. Heiko Biehl, Bastian Giegerich, and Alexandra Jonas, 99–112. Potsdam: Springer VS.

Schleicher, Andreas. 2019. *PISA 2018: Insights and interpretations*. Paris: OECD.

Suurkask, Heiki. 2023. Mereväe ülem: Laevastike ühendamine on olnud edukas [Navy chief: Merger of the fleets was successful]. *Sõdur* 123 (2): 7–17.

Servers Before Tanks? Defence AI in Denmark

Andreas Immanuel Graae

Denmark is one of the most digitized societies in the world. The Danish defence and security sector is known for its technological advancements and commitment to innovation. Denmark is currently on the verge of pursuing defence AI through a range of emergent projects and initiatives. Moreover, the Danish armed forces are packed with advanced military technology that has the potential to collect large amounts of raw data with the help of radars and sensors.

The problem is, however, that data is not always used properly because it rarely leaves the frontline. Danish Defence therefore needs to adopt AI as a part of the development of a much stronger digital backbone to process the increasing amounts of information and share it across platforms, units, and domains. This is a prerequisite for integrating forces into synchronous, multi-domain operations; a goal Denmark is currently pursuing as a member of the NATO alliance.

Commenting on this strategic thinking, Danish Chief of Defence, Flemming Lentfer, has stated how he sees "a need for servers before fighter jets, ships and tanks," (Krog 2021) a viewpoint which is supported by several voices in the Danish defence and security environment. For instance, in the report Danish Security and Defence Towards 2035, the government's security policy analysis group notes how the "rapid technological development will require a significant technological boost to the Danish Armed Forces if it is to remain a relevant partner for our strongest allies" (The security policy analysis group 2022: 5). However, the question of how exactly this technological boost should be accomplished and implemented into the organisation remains uncertain and uncoordinated.

The path to adopt defence AI in Denmark is challenged by fragmentation and lack of governance and strategic vision. Whilst testing and evaluation of AI is starting to sprout from various branches of the organisation, these initial efforts are mostly isolated and uncoordinated. The potential benefits in this bottom-up

A. I. Graae (✉)
Institute for Military Technology, Royal Danish Defence College, Copenhagen, Denmark
e-mail: agra@fak.dk

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_8

approach—such as explorative and experimental initiatives and a higher willingness to take risks—does not compensate for the lack of strategic direction.

An imperative task therefore remains in formulating a Danish strategy for defence AI with specific focus on where in the organisation and how AI should contribute to the "technological boost" of the Danish Defence. This includes a more precise definition of AI and what it should do for the military organisation, operationally as well as in the support functions. Second, the recent paradigm shift, changed approach and establishment of public-private partnerships within the Danish defence industry and academia should be utilized to strengthen development of AI and AI-enabled software solutions in Denmark.

Finally, the need for testing, training, and evaluation, as well as education of future defence AI specialists should be included and considered within the framework of existing and new military education programmes in Denmark. This is crucial to recruit and retain the right digital skills and competences needed for future Danish AI-enabled multi-domain operations and to build and sustain a modern data-driven defence organisation.

1 Thinking About Defence AI

As a small nation, Denmark is in the early stage of adopting defence artificial intelligence (AI). Recognizing the increasingly central role AI plays in the global technology competition and on current battlefields, it has nevertheless become clear that Danish Defence needs a major technological boost to remain relevant for its allies (The security policy analysis group 2022: 5).

The intensified technological competition not only reshapes security policies for smaller states like Denmark but also influences the international framework for Danish defence and security policy. Denmark has a unique opportunity to contribute to and benefit from the evolving landscape. However, without a clear technological reform agenda, the Danish Defense risks disconnection from close allies (Breitenbauch and Liebetrau 2021: 9).

Accordingly, the Danish Ministry of Defence is about to launch a range of strategic initiatives on AI, data, and digitalization. These include setting a direction for a digital transformation of the organisation and establishing strong and robust connections between operational and supporting processes, AI and data analysis, IT support, and digital competence development among management and employees.

Supposedly, the upcoming strategic initiatives, including a strategy for digital transformation and a data strategy, will address a major challenge in relation to AI in Danish Defence: a growing gap between military and digital knowledge due to a general lack of AI literacy and understanding of how data can generate value for the organisation. These challenges remain significant barriers for adopting defence AI, which makes conscription and recruitment of IT-specialists, technical translators, and experts in data science a still more demanding task. Thus, the challenge of

cultivating a digital mindset for exploiting the possibilities of AI is becoming a top priority for Danish Defence (Bollmann and Jacobsen 2023).

In short, the people in the organisation should learn to see data as a strategic asset that can provide tactical advantages and strategic autonomy for a small state like Denmark. It is thus key to prioritize education and enhance the understanding of technology, digital literacy and trust in data, AI, and autonomous systems. But above all, it remains pertinent to consider the broader imagination about defence AI among employees and managers as well as the public debate among civil actors in academia and industry.

1.1 Imagining AI in Denmark

In Denmark, the common perception, discourses and imaginaries surrounding defence AI have been formed by popular culture and science fiction scenarios envisioning a future world of killer robots and super computers (like Skynet in Terminator or HAL in The Space Odyssey) turning against their human creators. Although arguably far from reality, such dystopic visions are still recurring themes in Danish media and public debate about future military AI in Denmark. For instance, the fictional video Slaughterbots created by the Campaign to Stop Killer Robots in 2018 is frequently featured in the Danish public debate and in campaigns warning against autonomous weapons. Another example: in a critical campaign called Autonome Våben, Slaughterbots features together with the armed drone called Lanius, developed by Israeli Elbit Systems. According to the featured promotion video for Lanius, the drone uses artificial intelligence and camera sensors to track down and kill enemies (Autonome Våben 2023).

The Danish debate on defence AI is further accelerated by the wave of critical opinions about AI in relation to ChatGPT such as the critique stated by the Future of Life Institute in March 2023 (Future of Life 2023). In an open letter, prominent voices such as Elon Musk called on all AI labs to immediately pause the training of AI systems more powerful than GPT-4 for at least 6 months. Inspired by this critique, Danish scientists and researchers made a similar statement in June 2023. In an open letter to the Danish Minister for Foreign Affairs, Lars Løkke Rasmussen, the 20 researchers called for the Danish government to support an international ban on autonomous weapons systems. According to the researchers behind the letter, the Danish government should therefore develop a national policy for defence AI with the goal of a legally binding international agreement that "prohibits the use of autonomous weapons which is not under meaningful human control or has humans as targets" (Nedergaard et al. 2023).

The response from the Danish Foreign Minister was a rejection of any specific Danish policy, ban or legislation against autonomous weapons. However, the minister stated how he sees a "need for an international framework" and that Denmark together with other European countries supports a "two-step approach" to

autonomous weapons where regulations according to international humanitarian law is central (Pilgaard 2023: 5).

The open letter from the Danish researchers addresses a sensitive issue in the official Danish approach to defence AI: a general lack of governance and political guidelines. The vague response from the Minister for Foreign Affairs is therefore symptomatic of the official Danish view offensive aspects of defence AI: to outsource such matters to international fora such as the United Nations. Moreover, the AI debate in Denmark discloses a lack of conceptual clarity in the Danish political and public discourse about defence AI (and AI in general). This lack is mainly due a gap between the national level of ambition and the fact that no political or strategic guidelines have so far been formulated on defence AI in Denmark.

1.2 Denmark as AI "Front-Runner"

In 2019, the Danish National Strategy for Artificial Intelligence was launched with the ambition that Denmark should "be a front-runner in responsible development and use of AI," (National Strategy for Artificial Intelligence 2019: 5). The strategy defines AI in highly generic terms based on principles from the OECD and the European Commission, as:

> systems based on algorithms (mathematical formulae) that, by analyzing and identifying patterns in data, can identify the most appropriate solution. Most of these systems perform specific tasks in limited areas, e.g., control, prediction, and guidance. The technology can be designed to adapt its behavior by observing how the environment is influenced by previous actions (National Strategy for Artificial Intelligence 2019: 6).

Defence and security are entirely absent. Thus, the text is not at all specific about how the military should implement and use AI while being exposed to the battlefield's many dilemmas. Instead, the strategy partly builds on ethical principles framed in the Declaration on AI in the Nordic-Baltic Region signed by the Ministers responsible for digital development from Denmark, Estonia, Finland, the Faroe Islands, Iceland, Latvia, Lithuania, Norway, Sweden, and the Åland Islands. In this declaration the countries agreed to collaborate to "develop and promote the use of artificial intelligence to serve humans" (Nordic Council of Ministers 2018: 1). Moreover, the Danish AI strategy supports the declaration objectives for making the Nordic-Baltic region a digital leader and embraces the European Commission Communication on "Artificial Intelligence for Europe" and the declaration of 24 EU Member States and Norway on "Cooperation on Artificial Intelligence."

The strategy focuses mostly on the possibilities for AI to contribute to better public-sector services and growth in the business community. It highlights how a safe and responsible use of AI should follow six ethical principles which are to be incorporated in the development and use of artificial intelligence to "secure respect for individuals and their rights, and for democracy" (National Strategy for Artificial Intelligence 2019: 8). The six ethical principles are:

1. Self-determination
2. Dignity
3. Responsibility
4. Explainability
5. Equality and justice
6. Development

Some of the goals pertaining to the principle Dignity include that "AI should not cause injury, it should support due process and it should not unjustifiably place people in a worse position." Moreover, "AI should not be used to infringe fundamental human rights" (National Strategy for Artificial Intelligence 2019: 28).

If these goals are understood literally, it seems unlikely that AI will be used in relation to power projection by the Danish military anytime soon—as long as AI-enabled warfighting power requires a legal and ethical mandate to actively and effectively cause harm, or threaten to cause harm, to humans.

Although not taking any stance on this issue, the Danish ambitions for a responsible and explainable development and use of defence AI are aligned with international norms and standards such as the principles for safe and responsible use of defence AI in the NATO AI strategy (NATO Artificial Intelligence Strategy 2021). Denmark adheres to the common notion that humans must remain in full and constant control and that AI must be hierarchically subordinated to humans. But unlike other countries, Denmark has not yet formulated any specific (ethical, juridical, or political) guidelines for the development and use of defence AI.

This absence of political or strategic guidelines has been critiqued by military commentators and legal experts. For instance, it has been questioned how the Danish Airforce will make proper use of the sophisticated AI technology built into newly procured platforms, such as the F-35 fighter jets, if it is to comply with the ethical principles formulated in the AI Strategy (Jarlner 2021). This critique exposes the paradox inherent in the Danish defence AI imaginary and the double ambition to be an AI frontrunner while simultaneously restricting these ambitions to ethics and security policies of defence AI.

Despite the absence of specific political guidelines for military use of AI, digitalization and datafication are rising priorities for the Danish Armed Forces. Danish Chief of Defence, Flemming Lentfer, in an interview noted that he sees "a need for servers before fighter jets, ships and tanks," (Krog 2021), thereby advising the politicians to invest accordingly. The statement provoked critical reactions among military analysts and commentators, arguing that data centres and AI do not compensate for the need for conventional military capacities and hardware (Nielsen 2021). The message from critics appears to question investing heavily in headquarters with splendid overviews and situational awareness if the military on the field lacks the necessary equipment to act.

1.3 A Shift in Strategic Culture

It seems as if the statement from the Chief of Defence marks a shift in strategic culture and procurement practice for the Danish Defence. The statement not only comes from the highest ranking military officer of the Danish Armed Forces, but also seems to be aligned political initiatives coming from the Ministry of Defence and the implementation of new and more agile procurement processes and practices in the Danish Defence Acquisition and Logistics Organisation (DALO).

Traditionally, Denmark has invested its military capabilities in weapons systems such as artillery and tanks, especially from US, with which Denmark shares a strong bond. Historically, the strategic culture and thinking in Denmark has been tied to the military principles and priorities of NATO and the foreign policy of the USA. When Denmark decided in 2001 to participate in the war in Afghanistan just three months after the terrorist attacks on 11 September 2001, it was an act of solidarity with the United States (Rasmussen 2005: 67). Already in the 1990s, the Danish military engagement in Kosovo marked a new form of military activism that broke with the more "defencist" passivity that marked the Danish security politics and discourse in the late 1970s and 1980s. This also included a new focus on European integration and globalization, giving a new interpretation to military power in Denmark.

The transformation of the Danish strategic thinking towards a culture of activism and cosmopolitism has naturally reached a new peak with the Russian invasion of Ukraine and the following Danish donation politics of military equipment. This not only includes tanks and F-16 fighter jets, but also capacities for intelligence, surveillance and reconnaissance. This includes drones equipped with AI-enabled sensor and software systems produced and delivered by Danish companies such as Nordic Wing and Skywatch in 2022 and 2023 (Dall and Lindegaard 2023). The latter's promotion efforts for their RQ-35 Heidrun drones were assisted by former Star Wars actor Mark Hamill (Luke Skywalker) as part of a project crowd-funding drones for Ukraine (Skywatch 2023). This emphasizes the role of media, public perception and the broader cultural drone and AI imaginaries in promoting new military technologies for the battlefield.

The threat from Russia has changed the geopolitical situation and increased the salience of the Baltic and Arctic regions for Denmark's security. This situation helps foster a renaissance of Denmark's maritime tradition through a reorientation towards maritime security and the protection of Danish territory (including Denmark, Greenland, and the Faroe Islands) and its immediate surroundings. Moreover, the renewed Danish focus on the Arctic is motivated by both NATO and the US, who have steadily pushed Denmark to improve the surveillance and defence of its own territory, as there is a growing concern over the so-called GIUK-gap that forms a naval choke point: the two stretches of ocean between Greenland, Iceland, and the United Kingdom. In 2021, this increased international pressure resulted in a political Agreement on Arctic Capacities (Danish Ministry of Defence 2021), that included acquisitions for DKK1.5bn (€201M) in surveillance and communication capabilities. This included air surveillance radars, coastal radars, space-based

surveillance and satellite communication, drones, etc. The purpose of all these investments in new Arctic surveillance capabilities is to gather and process huge amounts of data necessary for intelligence, surveillance, and reconnaissance (ISR).

Spending on Intelligence Processing and Analysis only makes up a small part in the agreement, however, which indicates another challenge in the Danish military and strategic force generation culture: that is, hardware capacities are often prioritized above software and data processing solutions. This reveals a need for more efficient data management processes and software, allowing for better utilization of the gathered data through AI-enabled Image Intelligence (IMINT), e.g., for maritime surveillance, search and rescue, dark target detection etc. It is therefore important to discuss whether AI solutions should be developed by Danish industry and partners or whether Denmark should look elsewhere and use already developed solutions for data management.

Several players in the Danish defence industry are ready to contribute to developing such solutions and have explored these through workshops and exercises. One example is the ArcticX exercise (IRSA Development Group 2023) that was held in 2021 and repeated in 2022 at the H.C Andersen Airport outside of the Danish city Odense. The consortium IRSA (Integrated Remote Sensing in the Arctic) Development Group demonstrated how various sources of intelligence (based on sensor data from drones, satellite imagery, etc.) could be fused and integrated into a joint common operating picture (JCOP). Through use-cases and live demonstrations, the exercise showed how AI (Machine Learning and Deep Learning algorithms) could be used for dark target detection, fishing control, identification and tracking of icebergs, oil slippage, etc. However, there is also here a tendency to valorise platforms and capacities (such as sensors, satellites, and remotely piloted aircrafts) over software and the "invisible" systems that are supposed to integrate the gathered data.

The discussion of the Danish tendency to prioritize traditional hardware becomes more pertinent with recent procurements of advanced and costly capabilities for the Danish Airforce—such as several Seahawk helicopters and F-35 fighter jets. This is why the forthcoming strategic initiatives for a future digitalized Danish Defence allegedly aim to ensure coherence between operational and supporting areas, including the management of data. This is crucial if Denmark is to get to optimal output from new digital technologies and improve situational awareness on the battlefield as well as increase the speed of decisions, information sharing and communications. In short, the Danish Defence's operational and administrative data as well as digital networks are critical to defence operations.

2 Developing Defence AI

In the pursuit of digital transformation, Danish defence has engaged in several research and development projects and activities related to AI. These involve partnerships with research institutions, collaboration with industry partners, focusing

on developing AI algorithms, data analysis techniques, autonomous systems, and other AI-enabled technologies that can enhance military capabilities.

However, gaining insight into new military technology through research and development in the organisation has long been downgraded by broader political agreements and alternative military focus areas. In contrasts to both Norway and Sweden's extensive military R&D capabilities, the Danish Defence R&D serves primarily to support the acquisition of new capabilities.

Consequently, the internal R&D of Danish Defence has been cut several times over the past 20 years while having been relocated from the services and centralized into the Defence Command under the Plan and Capabilities Division. Currently, Denmark spends less than 0.5% of its defence budget on research and development, compared to other EU countries at 1.7% (IDA 2023).

Independent R&D is therefore very limited and Danish Defence Research serves primarily as a node in a broader research network. This helps Denmark access allied cooperation partners and create new ventures with the defence industry (Breitenbauch and Mathiesen 2021).

2.1 Defence AI in Public-Private Partnerships

In the latest defence agreement for the period 2018–2023, research and development received renewed political attention. The agreement states: "The defence cooperation with industry on R&D is strengthened, among other things with a view to maintaining the Danish defence industry as an attractive partner for other countries' defence industries" (Danish Government 2018: 11).

This trend is further strengthened with the political agreement for the coming period (2024–2033). The Government and a broad majority of the Danish Parliament have agreed that Denmark shall reach 2% of the Gross Domestic Product (GDP) on defence no later than 2030. The agreement entails investments in Danish security and defence amounting to approx. DKK143bn (more than €19bn) during the period 2024–2033. The government also plans to strengthen research and development in new defence and security technologies, including drone and quantum technology (Danish Ministry of Defence 2023: 10).

In 2021 the Danish Government released its National Defence Industrial Strategy as a capstone document on the subject. A central element in the strategy is the realization that "the Danish defence industry is essential for Denmark's national security and our joint efforts with allies and partners" (Danish Government 2021: 5).

In short, Denmark finds itself in a changed and more complex threat landscape in which an increased great power competition is particularly pronounced in a long-term race for the development of new civil and military technology—such as the AI arms race between USA and China (Breitenbauch and Mathiesen 2021: 20).

The Danish AI R&D takes place in the private sector where technologies with commercial aims are merged into the military world. The strategy therefore articulates the need for stronger collaboration between the public sector, Danish research

institutes, and the defence industry. It also calls for better utilization of the potential that exists in small and medium-sized companies and in innovation and start-ups sprouting from the research environment at universities.

With the intent of strengthening the cooperation for Danish security, the strategy invites both industry and academia to collaborate closely regarding defence AI research and development through new civil-military partnerships and a bolstered AI ecosystem.

2.2 The Danish AI Ecosystem

The Danish AI ecosystem consists of various organisations, initiatives, and stakeholders involved in the development, promotion, and application of defence AI. Denmark has been actively fostering its AI ecosystem to drive innovation, economic growth, and societal progress, which has been further strengthened by the National Defence Industrial Strategy.

The strategy specifically mentions AI as an area of focus: "The Government prioritizes providing scope for collaboration with companies regarding disruptive technologies, including artificial intelligence" (Danish Government 2021: 9).

Central to the AI ecosystem and the Government's strategy are public-private partnerships and civil-military enterprises. This collaboration is based on the triple helix innovation theory, which emphasizes the importance of interaction between the public sector, industry, and universities. For instance, the strategy states how "innovation and new partnerships are necessary to ensure that defence authorities and Denmark's defence industry are ready to meet the future" (Danish Government 2021: 20). It is crucial for the realization of the strategy that Defence is brought closer to collaboration partners from industry and Danish research institutes.

2.2.1 Defence

In the Danish defence organisation, research and development of defence AI is formed roughly through the so-called "Bermuda Triangle" between the Danish Ministry of Defence (MoD), the Defence Acquisition and Logistics Organisation (DALO) and the Defence Command. The annual briefing for the Defence Command describes, for instance, how the Chief of Defence Development Forum is used as an arena for discussions of new trends and opportunities across types of weapons and defence. The declared goal is to strengthen the Armed Forces by challenging conventional solution models by applying new insights and flows (such as IT as a "force multiplier," including AI).

In addition, DALO is responsible for procurement, supply, maintenance, development and decommission of material capabilities, IT and services for the Danish armed forces and Emergency Agency. With the slogan "Open for Business", DALO (and the Danish MoD, which launched it as a strategy in 2013) wish to signal

openness and to support Danish industry and export, not least in the growing field of AI research and development (Danish Ministry of Defence Acquisition and Logistics Organisation 2012).

The Danish Defence Research Centre (Værnsfælles Videnscenter) supports DALO in research and development, trend analysis and technology scouting for current and future investments in military acquisitions, in particular on AI technology and other emerging and disruptive technologies (EDT). Moreover, the Danish Defence Research Centre co-finances research and development projects carried out in collaboration with Danish companies and research institutions.

In other words, the Danish defence uses co-financing projects to expand research capacity in several areas where it does not have the necessary resources at hand (due to the cuts on research and development). The purpose of the projects is partly to support the defence industry and partly to provide DALO with important technological knowledge for the benefit of the Armed Forces' operations. These co-financing opportunities have become increasingly popular, especially after a stronger connection to the European Defence Fund (EDF) had been established.

A core element in the National Defence Industrial Strategy is to accelerate "speed, flexibility, transparency and enhanced triple-helix collaboration" as important parameters for this modernized acquisition practice (Danish Government 2021: 13). The strengthened civil-military cooperation and partnerships can be regarded as a significant paradigm shift in Danish military strategic culture. While several of Denmark's allies, e.g., the Netherlands, France, and Norway, traditionally feature close ties between defence authorities and defence industries, the Danish Ministry of Defence and its agencies have historically been more reluctant to enter collaborations with the Danish defence industry. One reason is the historic Danish "defencist" way of thinking about military power in which private defence industry actors traditionally have not been invited into the governmental decision circles. It is therefore largely uncharted waters when the Armed Forces now enter various partnerships about AI with industry and research institutes.

2.2.2 Academia

Danish universities and research institutions play a crucial role in advancing AI knowledge and expertise. Institutions like the Technical University of Denmark (DTU), Aalborg University, University of Southern Denmark and the University of Copenhagen have research groups and programs dedicated to AI and machine learning. These institutions collaborate with industry partners and contribute to cutting-edge research. In particular, areas such as AI, big data, and quantum technology are targeted. Simultaneously, Danish research institutions are world-leading in select areas of space and military technology. This research can support Denmark's national security by converting new knowledge into innovation in Danish companies and into solutions for Denmark's operational entities.

For instance, DTU has extensive research in applications of AI for security purposes. And in 2022, NATO located a quantum research centre at the University of

Copenhagen's Niels Bohr Institute as part of the Defence Innovation Accelerator for the North Atlantic (DIANA) (The security policy analysis group 2022: 18). Another quantum technology test centre is located at DTU for the development and manufacture of quantum technological solutions. The centre develops quantum sensors and ultra-fast quantum encryption devices that can prevent hacking.

In 2023, the University of Copenhagen collaborated with the IT University of Copenhagen and other Danish universities to establish a Pioneer Centre for AI (P1). Also in 2023, the eight Danish universities and five government-approved technical service institutions (GTS) formed a joint National Defence Technology Centre (Nationalt Forsvarsteknologisk Center, NFC) to increase collaboration with industry and the Danish Armed Forces. Among the approved technical service institutions participating in the National Defence Technology Centre is the Alexandra Institute whose AI and Analytics Lab and Visual Computing Lab is one of the biggest commercially available providers of AI research and development in Denmark. The purpose of the National Defence Technology Centre is to contribute to a critical technological boost of the Danish Armed Forces and the Danish defence industry through interdisciplinary partnerships. It utilizes Denmark's strengths in AI and similar areas such as space, quantum, cyber security, green fuels, autonomous systems etc.

2.2.3 Industry

In recent years, Danish private commercial entities—including companies such as TERMA, Systematic and Weibel—have actively explored the potential of AI in military applications to address various defence challenges and build partnerships with the Danish armed forces and academia. These companies focus on leveraging AI to enhance the capabilities of armed forces, improve efficiency, and contribute to national security.

The Danish private industry's engagement in AI for the military is overall enthusiastic and encompasses a wide range of areas. One notable aspect is the development of autonomous systems, including unmanned aerial vehicles (UAVs) and ground vehicles. These autonomous platforms equipped with AI offer advanced reconnaissance, surveillance, and logistics capabilities.

Moreover, Danish companies specializing in defence AI have been at the forefront of developing intelligent data analysis tools and predictive analytics models for battle-management and command and control purposes. These technologies aid in processing vast amounts of data, extracting actionable insights, and supporting informed decision-making in real-time operational scenarios.

A significant, although paradoxical, example is the development of the F-35 fighter jet. For years, Danish defence companies such as TERMA have played a key role in the development and production of highly specialized AI-based software and sensor solutions for this fifth-generation fighter aircraft (Danish Government 2021: 13). Yet, the lack of an overarching Danish IT and data infrastructure has

made critics doubt how the Danish defence organisation is geared to make proper use of the gathered data and sophisticated technologies built into the F-35 jets.

Another crucial aspect of Denmark's private industry's involvement in AI for the military is cyber security. As the digitization and interconnectivity of military systems increase, the need for robust cyber defence measures becomes paramount. Here Danish companies specializing in AI develop advanced cybersecurity solutions that employ machine learning algorithms to detect and mitigate cyber threats effectively.

2.3 Current R&D Projects on Defence AI

In 2023, TERMA, the country's biggest defence company, set new standards for military R&D in Denmark by signing a 30-year contract with Danish Defence for delivering an air defence system to the Danish Army's 1st Brigade and thereby meeting NATO's capability goals for Denmark in Very Short-Range Air Defence (VSHORAD) (TERMA 2023).

With the agreement, TERMA becomes the responsible systems integrator for Danish air defence. This means that the company must integrate all the systems' sub-elements and ensure that future air defence capabilities can form an integral part of the brigade's operations in the overall air defence. This includes being able to communicate and exchange data with other air defence systems. The system will be based on TERMA's AI-assisted command and control system (C2), which can connect several units via integration with various sensors and communication systems (TERMA 2023).

Another significant example of a current AI project and international partnership is the AI for Defence (AI4DEF). AI4DEF is a consortium consisting of 22 partners (companies and research institutions) from 10 countries, including Leonardo, Airbus, and the Danish Aalborg University and TERMA as the consortium lead. The AI4DEF's intent is to develop defence AI in relation to specific use-cases, developed in collaboration with, among others, Danish Defence. According to the consortium, the aim is therefore to "pave the way for accelerated development and application of AI in defence in order to maintain European sovereignty and excellence in this area". The consortium is backed and funded by the European Commission as a part of the European Defence Industrial Development Programme (EDIDP).

Situational awareness and decision-making as well as planning optimization are studied, designed and tested through the AI4DEF partnership. For instance, AI4DEF demonstrates how AI can help human operators exploit the increasing amounts of data/intelligence from various sources, including creating better situational awareness and situational understanding (e.g. supporting operational planning through modelling and simulation). This has been tested in one of several demonstrations, showing how AI can improve unmanned aerial vehicles for ISR missions through automatization and optimization of route planning and processing of unequalised

data from a range of sensors and sources, e.g. satellite imagery, weather data, open-source intelligence, etc.

Several other R&D projects on defence AI have been co-financed by DALO. One example is a project that has prototyped and tested AI-based technologies for automated terrain analysis. Also, the Defence Command has run an experimental project on defence AI in collaboration with DALO. The project focused on testing and development of software using AI/Machine Learning to classify aircrafts based on radar data (Danish Defence Command 2022: 8–9).

3 Organising Defence AI

In Denmark, the lack of an overall organisational approach to defence AI is countered by upcoming strategic initiatives and a joint dialogue among different branches of the Danish Armed Forces, the Ministry of Defence, the Cyber Division (part of DALO), the Defence Command, and other relevant stakeholders. The primary objective is to leverage AI technologies to enhance the efficiency, effectiveness, and safety of defence operations. Only recently, Denmark has started to reorganize and adjust the organisational structure for a better adoption of defence AI. The formation of the above-mentioned Cyber Division in 2023 remains central to the development of the organisation's overall IT architecture and communication infrastructure.

At the organisational level, it is crucial for the overall readiness and maturity of the organisation to develop a so-called "digital backbone" for the defence collaboration and information sharing among the different services and stakeholders. While it has not yet been specified what this "digital backbone" should include, it has become clear that it is not primarily a technical solution or system but rather a concept, including not only technology or data, but also people and processes.

3.1 Joint Approaches

At the ministerial level, a forthcoming capstone document on digitalization will allegedly be decisive in setting a direction for the digital transformation of the organisation. The actual organisational changes that result from the digitalization strategy are expected to take place gradually and iteratively during the period from 2024 to 2029. In this regard, it is important to develop an open and agile mindset that allows for testing of AI-driven initiatives (or within other EDTs), which can be shut down ("fail fast") if they do not provide the desired value. Moreover, the forthcoming strategic initiatives and capstone documents will supposedly have a strong focus on data exploitation including the future users of digital technologies and AI systems as well as the design of user-friendly and intuitive AI-driven solutions. In

short, the users must be involved through user development and implementation and by using agile methods.

Preparing the organisation, including its people and culture, for the successful adaptation of defence AI, the Danish Ministry of Defence also participated in international fora and working groups, including the British-American initiative AI Partnership for Defence (AIPfD). Besides partaking in seminars and meetings in the partnership, Denmark also contributed to a sub-working group with the aim of developing an AI Readiness Model. In particular, Denmark contributed to the readiness framework with one out of the eight building blocks, which can be used to measure the AI readiness in the defence organisations: namely that of Culture and Organisation.

3.2 Single Service Approaches

The Danish Armed Forces aim to integrate AI into various aspects of their operations. The individual services within the Danish Armed Forces, such as the Army, Navy, and Air Force, have their own specific initiatives and applications for AI.

While the Army focuses on using AI for autonomous systems such as drones and other unmanned aerial or ground vehicles (UXVs) or intelligent logistics systems, the Navy explores AI-driven systems for maritime surveillance and autonomous underwater vehicles (DALO 2021b). Also, the air defence systems integrated on the Danish frigates such as CIWS (close-in-weapons-systems) and the newly procured SM2 air defence missiles are examples of AI-based systems incorporated into military technologies (Naval News 2021).

The Air Force leverages AI for tasks such as aircraft maintenance (e.g., predictive maintenance), mission planning, air traffic management and command and control—all of which are necessary for organising and operating the newly procured F-35 fighter jets.

In addition, the Danish Emergency Management Agency (DEMA) under the Ministry of Defence is already using AI-enabled systems for pattern analysis based on drone imagery in emergency operations and for search and rescue (SAR). Moreover, DEMA has strengthened its digital support and integration with international and national partners, such as the municipal emergency services and the police.

3.3 Building an AI-Driven, Data-Centric Organisation

For several years, the Danish defence has worked on a common data and information infrastructure, now called “the Danish Common Operational Information Environment” (DACOIE). The concept is supposed to provide the basis for an operative and data-based overview that strengthens the ability to make faster and better decisions and communicate them across defence organisational units.

While there has been some initial dispute concerning whether DACOIE should be regarded as a technical system or more of an idea or concept, the latter approach now seems to dominate. Thus, DACOIE represents a general direction for how to build a digital backbone for the organisation that enables the Danish armed forces to operate digitally and integrated across all five domains (land, sea, air, cyber and space), and allows live data to be exchanged between domains and units.

The incentive behind DACOIE is also based on needs and demands from Denmark's allies and partners, most importantly NATO, the US, and the UK. For a while, the conceptual discussions in the Alliance have focused on digital transformation to secure its position in the future. This includes converting its data usage to cloud-based solutions, where AI-enabled data analysis remains central as a basis for decision-making that outperforms that of our adversaries. The construction of a digital platform (Defence Information Cloud, DEFIC) is thus a prerequisite for this collaboration. And this is probably why DACOIE has become a prestige project for Danish defence—which gives the words from the Danish Chief of Defence about "servers before tanks" another dimension.

4 Funding Defence AI

With the Danish defence agreement for 2024–2033, the Government and a broad majority of the Danish Parliament agreed that Denmark shall reach 2% of GDP for defence no later than 2030. The agreement entails increased investments in Danish security and defence amounting to approx. DKK143bn (more than €19bn) during the period 2024–2033.

The government also plans to strengthen research and development in new defence and security technologies, including not only drone and quantum technology but also development of defence AI. As previously mentioned, this is a continuation of the latest defence agreement for the period 2018–2023, in which research and development received renewed political attention. As a rough assessment of the spending on digitalization and defence AI, the defence budget for 2018–2023 contained a range of new initiatives, including spendings on cyber and IT security for DKK567M (€76M).

The Danish government supports research and innovation projects related to AI and defence technologies, e.g. Innovation Fund Denmark and The Danish Council for Research and Innovation Policy. Moreover, Denmark has a growing technology sector and an active venture capital ecosystem that supports various industries, including defence and AI. The Danish Government has launched a range of initiatives to strengthen the national AI ecosystem, which could also benefit the development of defence AI. Prominent venture capital firms and investors in Denmark that have shown interest in AI and defence-related sectors include Denmark's Export and Investment Fund (EIFO) (previously Vækstfonden, AI Denmark, and Nordic Eye Venture Capital).

5 Fielding and Operating Defence AI

Defence AI will be central to future Danish operations as part of an information environment where the right information is available to the right people, in the right format, at the right time. The newly established DACOIE concept aims to improve the organisation's communication infrastructure and ability to process data and information to use AI to achieve battlespace advantage and connect sensors to decision-makers and effectors (supporting the understand-decide-act functions).

Danish defence is already working with AI-enabled command and control (C2) solutions. This includes the SitaWare Suite developed by the Danish company Systematic, which is used by the Danish Army as the preferred battle management system to create situational awareness and to support military leaders in decision-making on the battlefield. While the use of AI in SitaWare has so far been limited, the latest add-on to the suite, SitaWare Insight, further increases the use of AI for detection of anomalies with algorithms trained for detecting and assessing deviations from the common operating picture. However, the add-on has not yet been purchased by the Danish Defence, which means that the armed forces are still missing the AI-driven software to make proper use of the increasing amounts of data and information made available on the battlefield.

As discussed above, the discourses, narratives and imaginaries surrounding defence AI in Denmark—whether it is ethical principles in the National AI strategy or simply a lack of AI literacy and digital skills among the people in the organisation—can make it hard to imagine how AI is used in Danish defence. Yet, automation and AI-assisted solutions are already enrolled to some degree in the organisation for several different purposes, as discussed below.

5.1 Administration and Logistics

Administrative robots, or RPAs (Robotic Process Automation), have been used by the Danish defence since 2019 where they were created by the Robotics Operational Centre, part of DALO. The software was developed to automate administrative tasks, allowing military employees to focus on core tasks. Feedback from employees has indicated that using AI for the automation of workflow can make a big difference. Not least on one of the busiest administration days of the year in the Danish defence, namely the conscription day for the Army. Here, the robots handle large amounts of data and ensure that the conscripts are quickly registered in the Defence systems. The enrolment of administrative RPA robots for handling conscription data is expected to inspire several other administration and logistics functions in the organisation (DALO 2021a).

5.2 C4ISR

Various AI-based types of decision support in Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems are currently used by Danish defence. Systems such as the SitaWare suite by Systematic and the JIMAPS from TERMA incorporate various AI techniques and technologies to enhance the situational awareness of military decision-makers. For instance, AI is used to integrate and fuse data from multiple sources such as sensors, surveillance systems, satellites, and intelligence databases. The use of AI for such purposes will assumable be more broadly implemented if or when system add-ons (like SitaWare Insight) or a common data and information infrastructure is rolled out. This will also enable other AI techniques like data mining, pattern recognition, and machine learning to identify relevant information, filter out noise, and provide a comprehensive view of the operational environment.

5.3 Unmanned and Autonomous Systems

In recent years, the Danish military has started testing and using unmanned systems in a tactical capacity for tasks like reconnaissance and surveillance, target recognition, route planning, autonomous navigation, and mission execution. AI is increasingly incorporated into these unmanned or autonomous systems that enable effective coordination and collaboration between human operators and autonomous systems, enhancing overall ISR capabilities. For example, the Danish Army plan to integrate surveillance and reconnaissance drones into their units on all tactical levels expected to rely on AI in mapping terrain or threats and in processing data through on-board computing.

In the maritime domain, AI is about to be fielded on underwater drones and sonars to monitor and protect critical infrastructure on the seabed. Systems such as the Katfish highspeed towed sonar produced by Kraken Robotics are examples of how AI or Synthetic Aperture Sonar (SAS) enabled systems can help monitoring the seabed. Also, six new underwater drones (Light Autonomous Underwater Vehicle (LAUV)) from the Portuguese company OCEANSCAN have been procured and is to be used by the Danish Naval Command's Mine Counter Measure unit (MCM) on Mine Sweeping Drone ships (MSD). The new LAUVs are used when the MCM unit must search for and detonate mines on the seabed. In their search for mines, the units can be deployed simultaneously and use AI to calculate how to search the seabed within a given area as well as communicate with each other so that if one finds something, it autonomously calls another unit to take a photo of the object.

5.4 Cyber Security

As mentioned, Denmark is one of the most digitized societies in the world. Many critical sectors in Denmark are digitized and essential for ensuring the functioning of society. This explains why cyberattacks are particularly threatening to Denmark. In the National AI Strategy, the Danish Government states that it is a priority that Denmark preserves and develops national cyber expertise capable of protecting Danish society and the Danish defence industry against external attacks. This is done by using intelligent cyber security solutions such as the QRadar program developed by IBM. Using AI, QRadar can examine billions of pieces of information in a short period of time and look for signs that a network or system has been compromised by malicious players. The program can therefore help IT specialists find breaches of security that would be hard for a human to detect (Danish Government 2021: 21).

6 Training for Defence AI

Another way to "fill the gap" would be to prioritize and increase the teaching and training in AI and technology management in both current and future military education such as at the military academies and in the Master's in Military Studies program offered by the Royal Danish Defence College.

Currently, Danish Defence is not exploring all the possibilities that AI can offer for military education and training. As an example, the Command Course at the Royal Danish Defence College uses simulated exercises as an element in the training of the Danish Army's future staff officers at the battalion and brigade level. Using different types of simulation tools during the command exercises, the students get acquainted with the different roles and routines of staff work while both planning and decision-making are practiced.

In the digital part of the exercise, all input is generated through the more than 20-year-old simulation program Steel Beasts. The digital simulation in Steel Beasts is created based on the students' own staff work and results in a plan that is supplemented during the simulation. Through this combination of analogue and digital input, the students are exposed to a simulation that is unknown to them, and where the possibility of unforeseen actions on the part of the opponent is greatest. Yet, the element of surprise and unexpected Red Team manoeuvres are relatively limited due to the outdated AI software in Steel Beasts. But if combined with a more up-to-date AI computer simulation that cannot be controlled in the same way as the input during the existing computer game, then the mutual actions and decisions made by the students could have a much greater influence on the situation at all levels.

The Steel Beasts example serves as a symptom of how technologically immature the Danish military education system is in incorporating cutting-edge AI technology into existing courses, training, and exercises. However, some early-stage

initiatives are starting to sprout at the Royal Danish Defence College: there are ideas of creating an AI lab for experimenting and introducing military officers to the possibilities enabled by AI and Machine Learning. Such initiatives should serve as prototypes for teaching programs in AI technology at all levels of the military education system.

First, Danish defence personnel should receive specialized training and education in AI concepts, principles, and applications. This includes understanding the fundamentals of machine learning, data analysis, algorithm development, and AI ethics. Training programs may involve courses, workshops, and certifications to equip military personnel with the knowledge and skills required to work with AI technologies.

Secondly, Danish defence should establish stronger partnerships with academia and industry, including dedicated AI centres or labs where experts and users can conduct research, experimentation, and development of AI. These centres could serve as hubs for innovation, fostering collaboration, and providing resources for training personnel in AI. And they should facilitate hands-on learning, prototyping, and testing of AI algorithms and user-friendly systems specific to defence applications.

This should also involve simulation and training exercises, which are crucial for familiarizing defence personnel with AI-enabled systems and their operational implications. These exercises should create realistic scenarios where personnel can practice using AI tools, analyse AI-generated data, and make decisions based on AI recommendations. Training exercises also help identify any limitations, challenges, or vulnerabilities associated with AI implementation in defence contexts. But most importantly, training is necessary to build trust in AI systems and make military personnel feel comfortable with the transition from a human-centric organisation into human-machine teaming and "centaur"-warfighting (Warren and Hillas 2020).

Finally, the future training for defence AI in Denmark should emphasize ethical and legal considerations surrounding AI usage. This includes understanding the potential biases (including gender and race), risks, and consequences associated with AI, ensuring compliance with national and international laws, and adhering to ethical principles for responsible AI development and deployment. Training programs should address the ethical use of AI in military operations, data privacy, and the protection of civilian rights.

7 Conclusion

Denmark is still at an early stage of adopting defence AI. Despite the government's vision for Denmark to be an AI frontrunner. The National Strategy for Artificial Intelligence does not provide specific guidance for the military's implementation and use of AI, focusing more on public-sector services and growth in the business community.

Despite this, AI is being tested and used in the Danish defence for some purposes, including "low-hanging fruits" such as administrative tasks and logistics as well as in training and education. The problem is, however, that the exploration and initial testing of AI systems is highly fragmented and isolated within silos of the organisation. This results in redundancy and problems with sustaining the systems, challenging a near-future integration of AI into C4ISR systems that can enhance decision making and situational awareness.

Danish defence collaborates with the defence industry and academia regarding new partnerships and research of defence AI. Unmanned and autonomous systems with AI capabilities are being tested and evaluated for tasks such as intelligence, reconnaissance, and surveillance operations where AI is used for automation purposes such as creating waypoints and calculating routes.

However, there is a growing knowledge gap and lack of AI literacy in the Danish Defence, which makes the recruitment of IT specialists and data science experts an increasingly demanding task. Although the Danish Chief of Defence has emphasized the importance of investing in AI and data processing software, the real challenge will be to recruit or educate the right people with the right skills and competences to make proper use of these AI-enabled data and software systems. And in this endeavour, it remains pertinent to create a culture of thinking about technology, including defence AI and data, not as barriers but as something that the organisation can profit from.

The need for efficient data management and software systems has become evident with the procurement of advanced military capabilities. Danish Defence recognizes the criticality of data and digital networks for operational success, and future operations are integrated across multiple domains. Yet, the increasing amount of data gathered from advanced sensor platforms is not always used properly because it rarely reaches further than the crew in a fighter plane or frigate. Therefore, Danish Defence needs to adopt AI as a part of the development of a much stronger digital backbone to process the increasing amount of information and share it across platforms, units, and domains. Especially the latter is important if Denmark is to remain relevant for its allies in NATO and abroad.

While Denmark acknowledges the importance of defence AI and digitalization, there are huge challenges to overcome. Above all, the growing knowledge gap and lack of digital literacy is considered a major risk and should be met with investments in education and training. The Danish Defence aims to leverage AI to improve operational capabilities and decision-making processes, but careful consideration is required to ensure responsible and explainable use of AI in alignment with international norms and standards.

References

Autonome Våben. 2023. www.autonomevaaben.dk. Accessed 30 January 2024.

Bollmann, Anders Theis, and Katja Lindskov Jacobsen. 2023. *Militær dataoversættelse og digital transformation – Erfaringer fra Ukraine og fokusområder for det danske forsvar*. DJØF forlag and Center for Militære Studier. https://cms.polsci.ku.dk/publikationer/2023/CMS-Rapport_

Milit_r_dataovers_ttelse_og_digital_transformation_ebog.pdf/CMS-Rapport_Milit_r_dataovers_ttelse_og_digital_transformation_ebog.pdf. Accessed 30 January 2024.

Breitenbauch, Henrik, and Tobias Liebetrau. 2021. *Technology competition: Strategic implications for the West and Denmark*. DJØF forlag and Center for Militære Studier. https://cms.polsci.ku.dk/english/publications/technology-competition-strategic-implications-for-the-west-and-denmark/download-cms-report/CMS_Report_2021__6_-_Technology_Competition__Strategic_Implications_for_the_West_and_DK.pdf. Accessed 30 January 2024.

Breitenbauch, Henrik, and Jens Mathiesen. 2021. *Militærteknologisk situationsforståelse. En ny strategisk udfordring i dansk forsvarspolitik*. DJØF forlag and Center for Militære Studier. https://cms.polsci.ku.dk/publikationer/militaerteknologisk-situationsforstaaelse/. Accessed 30 January 2024.

Dall, Anders, and Lasse Lindegaard. 2023. *Efterspørgsel på droner til Ukraine giver vokseværk til dansk selskab*. DR Nyheder. https://www.dr.dk/nyheder/indland/efterspoergsel-paa-droner-til-ukraine-giver-voksevaerk-til-dansk-selskab. Accessed 30 January 2024.

DALO, Danish Ministry of Defence Acquisition and Logistics Organisation. 2012. Open for Business – Forsvarsministeriets strategi til støtte for fremme af dansk erhverv. https://www.fmi.dk/globalassets/fmn/dokumenter/strategi/-forsvarsministeriet-open-for-business-strategi-.pdf. Accessed 30 January 2024.

———. 2021a. FMI støtter hæren med ny robot. DALO News. https://www.fmi.dk/da/artikler/fmi-stotter-haren-med-ny-robot/. Accessed 30 January 2024.

———. 2021b. Nye autonome undervandsdroner. DALO News. https://www.fmi.dk/da/nyheder/2021/nye-autonome-undervandsdroner/. Accessed 30 January 2024.

Danish Defence Command. 2022. Årsberetning for Forsvarskommandoen 2022. https://www.fmn.dk/globalassets/fmn/dokumenter/aarsrapporter/2023/-2022-forsvarskommandoens-aarsberetning-.pdf. Accessed 30 January 2024.

Danish Government. 2018. Danish Defence Agreement 2018-2023. https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-danish-defence-agreement-2018-2023-pdfa-2018.pdf. Accessed 30 January 2024.

———. 2019. National Strategy for Artificial Intelligence. https://eng.em.dk/media/13081/305755-gb-version_4k.pdf. Accessed 30 January 2024.

———. 2021. National Defence Industrial Strategy. https://www.fmn.dk/globalassets/fmn/dokumenter/nyheder/engelske/-national-defence-industrial-strategy-of-the-danish-government-.pdf. Accessed 30 January 2024.

———. 2021. Agreement on Arctic Capacities. https://www.fmn.dk/globalassets/fmn/dokumenter/nyheder/2021/-factsheet-agreement-on-arctic-capabilities-.pdf. Accessed 30 January 2024.

———. 2023. Aftale om dansk forsvar og sikkerhed 2024-2033. https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-aftale-om-dansk-forsvar-og-sikkerhed-2024-2033-aftaletekst-28-06-2023-.pdf. Accessed 30 January 2024.

IDA, The Danish Society of Engineers. 2023. Forsvarsudspil sikrer forskning i nye teknologier. https://via.ritzau.dk/pressemeddelelse/forsvarsudspil-sikrer-forskning-i-nye-teknologier?publisherId=3427042&releaseId=13690275. Accessed 30 January 2024.

IRSA Development Group. 2023. ArcticX. https://www.idg.network/arcticx. Accessed 30 January 2024.

Jarlner, Michael. 2021. Militæret mangler klare rammer for brug af kunstig intelligens. Politiken. https://politiken.dk/udland/art8299138/Milit%C3%A6ret-mangler-klare-rammer-for-brug-af-kunstig-intelligens. Accessed 30 January 2024.

Krog, Andreas. 2021. Forsvarschef: Behov for servere før flere kampfly, skibe og kampvogne, *Altinget*, https://www.altinget.dk/digital/artikel/forsvarschef-behov-for-servere-foer-flere-kampfly-skibe-og-kampvogne

Naval News Staff. 2021. SM-2 Missiles Fitted Aboard Danish Frigate for the 1st Time (Danish Armed Forces press release translated by Naval News), Naval News. https://www.navalnews.com/naval-news/2022/05/danish-navy-installs-sm-2-missiles-niels-juel/. Accessed 30 January 2024.

Nedergaard, Alexander, et al. 2023. Letter to Danish Minister for Foreign Affairs, Lars Løkke Rasmussen: Autonome Våben. https://drive.google.com/file/d/1rm0R5YcSxU8Dj-d9meEjRzcgdcDXserO/view?pli=1. Accessed 30 January 2024.

Nielsen, Anders Puck. 2021. Militærforsker til forsvarschef: Datacentre opvejer ikke behovet for mere militært isenkram. Altinget. https://www.altinget.dk/forsvar/artikel/militaerforsker-til-fe-chef-datacentre-opvejer-ikke-behovet-for-mere-militaert-isenkram. Accessed 30 January 2024.

Nordic Council of Ministers. 2018. AI in the Nordic-Baltic region. https://www.stjornarradid.is/library/04-Raduneytin/ForsAetisraduneytid/Framtidarnefnd/AI%20in%20the%20Nordic-Baltic%20region.pdf. Accessed 30 January 2024.

Pilgaard, Ronja. 2023. Løkke afviser krav om dansk lovgivning mod dræberrobotter. Berlingske, June 18, 5.

Rasmussen, Mikkel Vedby. 2005. 'What's the Use of It?': Danish Strategic Culture and the Utility of Armed Force. *Cooperation and Conflict* 40 (1): 67–89.

Skywatch. 2023. The RQ-35 Heidrun Drone has been funded via the Air Alert App. Skywatch News. https://sky-watch.com/news/the-rq-35-heidrun-drone-has-been-funded-via-the-air-alert-app/. Accessed 30 January 2024.

TERMA. 2023. TERMA signs framework agreement with Danish Defence on system integration and maintenance for integrated air and missile defence system. TERMA News. https://www.terma.com/news-events/news/news-archive/2023/terma-signs-framework-agreement-with-danish-defence/. Accessed 30 January 2024.

The security policy analysis group. 2022. *Danish Security and Defence Towards 2035*. Copenhagen: Ministry of Foreign Affairs of Denmark. https://www.fmn.dk/globalassets/fmn/dokumenter/strategi/rsa/-regeringens_security-policy-report_uk_web-.pdf. Accessed 30 January 2024.

Warren, Aiden, and Alek Hillas. 2020. Friend or Frenemy? The Role of Trust in Human Machine Teaming and Lethal Autonomous Weapons Systems. *Small Wars and Insurgencies* 31 (4): 822–850.

Master and Servant: Defense AI in Germany

Heiko Borchert, Torben Schütz, and Joseph Verbovszky

The German Ministry of Defense (MoD), the Bundeswehr, and the defense technological and industrial base understand the importance of artificial intelligence (AI) in shaping the future strategic environment and the use of military power. Numerous projects have been launched, structures and processes are being reorganized, money has been earmarked, and training is underway or being readjusted.

Overall, however, Germany's AI path remains murky as it is caught in a "master and servant" logic that will be painful to overcome. The metaphor describes the struggle to readjust Germany's input-driven strategic culture, which puts greater emphasis on the socio-political acceptance and legitimization of military power than on the effects it can achieve. As a consequence, defense trumps offense with most of the current defense AI initiatives aiming at augmenting the survivability rather than the lethality of the Bundeswehr. Additionally, three decades of political neglect have pinned the Bundeswehr's socio-technological imaginaries to what matters here and now. Force planners could (and would) not request, what they did not know. This triggered a kind of technology blindness that has—unintentionally—been reinforced by a technology agnostic approach to capability development that describes capability requirements in generic terms. Today, the Bundeswehr operates in a bifurcated world: the armed forces need to envision the future defense environment while procrastinating future concepts and projects into today's procedures and processes—the master—to induce incremental change.

Against this background, Germany considers defense AI as a tool—the humble servant—subordinate to humans, who must always remain in the loop. Incrementalism dominates, which makes it difficult to assess what defense AI is expected to achieve and whether it delivers on this expectation. Although US ideas play a prominent role in the defense AI discourse, Germany's strategic culture acts as a filter that tames the US emphasis on performance and lethality to make it more

H. Borchert (✉) · T. Schütz · J. Verbovszky
Defense AI Observatory, Helmut Schmidt University, Hamburg, Germany
e-mail: hb@defenseai.eu; schuetzt@hsu-hh.de; joseph.verbovszky@hsu-hh.de

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_9

palatable for risk averse German decision-makers. As a result, most German defense AI projects focus on decision-making support and gradual improvements of other technologies in the fields of Command, Control, Computers, and Communications (C4) and Intelligence, Surveillance, Reconnaissance (ISR). In parallel, organizational adaptation is underway, but the MoD and the military services seem to operate at different levels of ambition and diverging speeds. It remains to be seen if the yet to be published defense AI implementation strategy will be able to remedy this shortfall.

Germany has stepped up investments in its digital infrastructure but slashed spending on defense research and technology (R&T). Based on a review of non-public budgets Germany currently spends around €50M per year on AI-related software development. As opaque as its spending is the Bundeswehr's current fielding and operating of defense AI. An open-source intelligence system for crisis early warning, AI-based warning receivers for helicopters, and intelligent image processing for missiles feature among the more prominent, publicly known examples. Finally, defense AI affects military education and training. The Bundeswehr's Command and Staff College is about to review its curriculum with the goal to incorporate AI elements as of 2024. In addition, the University of the Bundeswehr/Hamburg is setting up a new AI bachelor's and master's degree course. Individual services also explore opportunities for AI-enhanced simulation-based training. Moreover, different initiatives have been launched to train defense AI algorithms.

In sum, Germany has embarked on a defense AI journey, but substantial homework remains to be done. To this purpose the German MoD needs to be more precise about the future capability growth AI is expected to enable, the role of defense AI in Germany's (non-existent) defense industrial policy, its international defense AI ambition, and the framework needed to certify, qualify, and admit future defense AI solutions.

1 Thinking About Defense AI

The German government's 2018 AI strategy and its 2020 update (Federal Government 2018, 2020) describe Germany's ambition and line of efforts to use AI to advance national and European competitiveness. But both documents remain silent on the use of AI for defense and security. The same is true for the 2018 Concept of the Bundeswehr, the 2021 strategic guidance of then Minister of Defense Kramp-Karrenbauer, and the 2021 coalition treaty. Only the 2019 concept paper on "AI for use in the area of responsibility of the Ministry of Defense" (BMVg 2019a) fills the void.

This is disenchanting, but it is not surprising, as Germany's strategic culture tames the Bundeswehr's technology appetite, creating tensions. The Bundeswehr recognizes that technology is changing the future battlefield. It also embraces allied

concept ideas to signal its willingness to cooperate with partners. However, culture, the current organizational set up, and the lack of robust technology leadership pin the Bundeswehr down to the status quo. Defense AI thus has a hard time blossoming—in part also because its use is most often tied to large procurement projects that apply defense AI as part of broader functionalities. This makes it difficult to understand Germany's overall defense AI ambition and the added value AI is expected to deliver.

1.1 Structural Pacifism Shapes Defense Technological Imaginaries

Germany's security policy is characterized by a structural pacifism (Verbovszky 2024) in which the need to reconcile competing elements of Germany's post-war security identity with a byzantine policy process leads to the prioritization of security policy conformity over effectiveness (performance).

Resulting from the trauma of WWII, the nascent Federal Republic of West Germany "reinvented itself" in opposition to its authoritarian past (Stengel 2020: 102). The formation of Germany's post-war identity relied heavily on fantasy (Eberle 2019: 46)—a narrative scenario that promises the impossible fulfillment of a complete identity—and, more importantly, on negative contingency—the projection of catastrophe into the future, which is meant to be avoided. As Frank Biess (Biess 2019: 31) argues, negative contingency in the form of German Angst served to stabilize German democracy by emphasizing its fragility.

While conducive to internal stability, negative contingency retards German security policy. Reconciling the "Lessons of History" presents itself as the "right way" to do security policy, i.e., most conform with Germany's post-war identity (Verbovszky 2024: 36). But reconciling competing interpretations of German post-war identity is made more difficult by the byzantine logic of German security policy decision-making. Myriad actors all come with their own political interests. Resolving them in a way that conforms with Germany's post-war non-belligerent identity leads to a security policy dominated by inputs. Security policy decisions are done via "reverse consensus," i.e., even before going into respective committees for deliberation they are designed to be consensus-capable in the final vote (Verbovszky 2024: 48).

Similar forces underpin Germany's skepticism toward technological change. One tool for measuring the impact of cultural and political factors is the use of socio-technological imaginaries, i.e., "collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology" (Jasanoff 2015: 4). They "play an important role in the development, assessment and regulation of cutting-edge

technologies" (Burri 2015: 233). Comparative assessments across diverse technology areas like nanotechnology, space, and AI show, that these technologies are considered relevant for national competitiveness and to advance environmental assessments, whereas military applications receive scant attention. In addition, risk emanating from these technologies is used to express ever-present warnings justifying preemptive regulation as a preeminent political task, thus further embedding the political discourse in technology critical imaginaries (Federal Government 2018: 8; SPD/Bündnis90/Die Grünen/FDP 2021: 145; Burri 2015: 237–239; Kober and Schütz 2024).

1.2 Future Conflict Picture

Germany's strategic culture shapes how the Bundeswehr thinks about the future. Its capstone document Future Operating Environment 2035 (BMVg 2019c) describes fast-paced adversarial action and the amalgamation of different forms of conflicts that evolve in complex and chaotic environments. Advances in technology, international power shifts, new forms of decentralized organization, and the long-term consequences of climate change are key drivers shaping the future battlefield. Therefore, future military action needs to put more emphasis on accelerating data gathering, analysis, and application, requires a comprehensive recognized operational picture, depends on shorter sensor to shooter cycles, and demands more flexible and partially automated measures of response. Strategic depth and delivering effects at greater distance become more important and should go hand in hand with developing counter-Anti Access/Area Denial (A2/AD) capabilities.

The Chief of Defense's (CHOD) 2022 operational guidance (Generalinspekteur 2022) underpins these reflections. It calls for new innovative solutions to be "battle ready" and highlights the pressing need to assess sensor data "on the edge" to counter adversarial jamming. Emphasizing the need to transmit, store and make data available and usable, this document further argues that AI will become increasingly important to "support data correlation and data processing on behalf of the Commander and his command aides" (Generalinspekteur 2022: para 295, 297–98).

The CHOD's guidance also embraces the idea of Multi-Domain Operations (MDO). Although not new as a core idea, the document argues, today's focus provides opportunities to link capabilities across domains, advance operational tempo, and impose dilemmas on the adversary by precise direct and indirect effects (Generalinspekteur 2022: 286, 290). Therefore, the MoD's Directorate-General for Planning has tasked the Planning Office of the Bundeswehr at the end of 2022 to start the national MDO implementation and submit the respective concept document to the CHOD by mid-2024 (Interview, 28 February 2023).

1.3 Digitalization and Software-Defined Defense

Today's emphasis on digitizing armed forces originates from Network-Centric Warfare or Network-Enabled Operations, the state-of-the art military concept in the early 2000s. To realize the Bundeswehr's unique selling proposition—preparing and using armed force—Network-Enabled Operations and the ability to contribute to MDO are key. That's why a seamless and powerful ICT federation is indispensable (BMVg 2017) to make the armed force more assertive, increases the Bundeswehr's operational capability as a whole and on the digitized battlefield, and support administrative action (Färber 2023: 225).

Currently, defense digitalization morphs into software-defined defense, a concept that detaches the hardware aspects of military capabilities from the software aspects with the goal to connect the latter in "data-centric, multi-modal, multi-domain, adaptative battle networks" (Soare et al. 2023: 2). Gen Michael Vetter, the MoD's Chief Information Officer, backs software-defined defense as a new way of ensuring future capability growth by "digitally upgrading" legacy systems (Welchering 2023).

This understanding also underpins the MoD's 2021 data strategy (BMVg 2021) and shapes its AI approach (Prenzel et al. 2023). As the contributions in this volume show, the Bundeswehr joins the chorus of many other armed forces in calling data "an asset of significant value" that enables information and effects superiority. Therefore, the data strategy is geared towards providing data of high quality and accessibility to strengthen the mission-readiness and resilience of IT and weapon systems, reduce life-cycle costs of these systems, boost the use of data across the Bundeswehr, increase the use of data, and enable data analytics.

This vision, however, is not yet in line with reality. Today, the Bundeswehr effectively operates in two worlds—old and new—requiring soldiers to envision the future while procrastinating future concepts and projects into legacy procedures and processes as the only means available to induce incremental change. This creates obvious tensions between "feel-good" digitalization, operated to convey the image of a techno-savvy and attractive employer, and defense digitalization meant to meet the Bundeswehr's operational performance requirements (Interviews, 25 March 2022 and 6 February 2023).

1.4 Defense AI

1.4.1 Joint Thinking

Defense digitalization provides the umbrella for defense AI. The 2019 defense AI concept paper (BMVg 2019a) is Germany's current capstone document, discussing in detail the general goals of using defense AI, the operationalization for the Bundeswehr, as well as the requirements (e.g., organization, human resources, legal

aspects, IT hard/software aspects). In doing so, the paper follows the data-centric approach outlined above and defines

> AI as a technology that uses machines with sophisticated algorithms taking on tasks that require – some sort of – intelligence to accomplish tasks that have previously required primarily or exclusively human decision-making or action (BMVg 2019a: 6).

The document envisages a holistic defense AI approach taking into account political, military, and industrial aspects (BMVg 2019a: 10–11). On industrial aspects, however, the MoD pushes itself to the backseat by arguing that "AI is not an explicit military capability, and the Bundeswehr is not the driver of AI-related innovation" (BMVg 2019a: 13). As this document puts civil and commercial developments ahead of defense AI, it is not surprising, that the document mainly refers to gains in efficiency, effectiveness, and process improvements as the key imaginaries describing the goals of using defense AI (BMVg 2019a: 17).

The document discusses potential areas of applications of defense AI but refrains from describing how exactly defense AI is expected to enhance the Bundeswehr's key capabilities. Rather it argues that AI should be introduced with the help of broadly defined pilot projects that can quickly expose the Bundeswehr to defense AI (BMVg 2019a: 15), without specifying which capability areas should be targeted to achieve what kind of capability gain. Therefore, the strategic rationale underpinning defense AI is fuzzy, and it is unclear how defense AI will augment capability growth over the next decades. Consequently, there is a gap between high-level guidance and ongoing projects. The Armed Forces Digitalization Center is meant to close this gap with a new defense AI implementation strategy (Interview, 6 February 2023), which has not yet been published at the time of writing in January 2024.

1.4.2 Service Thinking

In this context defense AI ambitions of Germany's military services diverge. In 2017, the Germany Army (Kommando Heer 2017a, b) published a series of concept notes outlining the future digital battlefield and the role of AI, followed by a fully-fledged defense AI position paper by the German Army Concepts and Capability Development Center (Amt für Heeresentwicklung 2019) two years later. It argued that that defense AI would help render basic services more efficient, improve combat-ready capabilities, and overcome existing capability gaps. In so doing the paper reflects US and NATO discourse on the digital and accelerated battlefield (hyperwar), talks about operating at machine speed, taking decisions on the edge, and using AI to coordinate and synchronize a growing number of sensors and effectors. Moreover, the paper also outlines how to further improve defense AI for human resources and material management and to enhance training and education (Amt für Heeresentwicklung 2019: 5–7, 12; Brendecke et al. 2020).

Without AI, today's means of command and control will be insufficient to operate air power within the next 15 years, the German Luftwaffe contends. The

Luftwaffe expects defense AI to synchronize information for Recognized Air Pictures, optimize flight routes, mission planning and mission management, coordinate target acquisition, and submit proposals on how to design and implement plans of attack. The service is taking baby steps in using defense AI, but its thinking is highly aligned with the US Air Force vision of using AI to set up Advanced Battle Management Systems to enable Joint All Domain Operations (Autorenteam Luftwaffe 2021).

So far, defense AI has played only a subordinate role for the German Navy. The service considers itself as technology driven as the Luftwaffe, but dire savings plans have limited the Navy's capability development priorities to what is absolutely needed to ensure its survival. In the past, this even led the Navy to divest leading technology applications from aboard its ships to save costs. The current Navy leadership aspires a conceptual turnaround that provides more leeway to innovation, e.g., by establishing a new innovation cell with the Navy leadership team. As more defense AI use cases become known, sailors seem to become more aware how defense AI could offer added value aboard their ships (Interviews, 23 February and 14 March 2023).

The Cyber and Information Domain Service has an instrumental understanding of defense AI that is directly related to its core tasks. As this service plays a key role in providing common operational pictures (COP) it emphasizes the role of AI in providing analytical support and rendering digital processes more efficient and effective. As such, AI is part of the so-called "Analytics and Simulation" cluster which combines different methods such as pattern recognition, decision support, machine learning, and simulation (Bundeswehr 2020a; Färber 2023).

1.5 Ethics and Defense AI

Germany's strategic culture implies that ethics plays a formative role for developing and using defense AI. This also explains the focus on arms control to shape the use of AI and other emerging technologies (SPD/Bündnis90/Die Grünen/FDP 2021: 146). In addition, the MoD's 2019 defense AI concept unmistakably posits that the MoD needs to engage in a multi-stakeholder process to shape the public discourse on AI as—on its own—it can "neither lead nor shape the societal debate on AI as well as its risks and benefits, because the military use of AI constitutes only a small portion of a much broader topic" (BMVg 2019a: 10).

In this regard, leading officers opine that defense AI should always play a subordinate role to human decision-makers, who need to remain in control "of decision making as AI cannot replace human innovation, surprise, human values, personal experience, trust and emotions, and camaraderie" (Bock and Schmarsow 2023: 154). Ultimate human control is also paramount to prevent the rise of lethal autonomous weapon systems that Bundeswehr leaders reject (Ehlke 2021: 18). Furthermore,

asked about the strategic purpose of using defense AI, one interview partner argued that it is all about "humanitarian precision," a rhetorical figure that combines the reality of a post-heroic and risk averse society with the need for speed on the battlefield (Interview, 22 February 2023). As Jensen et al. (2022: 35–36, 40–46) have argued, such statements show that the Bundeswehr leadership holds a collective vision, which stabilizes institutional thinking about defense AI and narrates the socio-technical imaginary that shapes Germany's dealing with defense AI. This also shapes the defense industry's thinking, as the 2023 position paper of Germany's leading, defense-relevant associations illustrates (BDSV et al. 2023).

But demanding respect for ethical principles and implementing them via technology development are two different things. On this very specific aspect the MoD's guidance has so far remained vague, while in practice different initiatives emerge. At the international level the new ISO/IEC/IEEE 24787-700:2022 standard defines a process for value-based engineering (Hofstetter and Verbovszky 2023), which also informs the work of the NATO Data and Artificial Intelligence Review Board (DARB, Interview, 7 February 2023) and the German defense AI project GhostPlay (see below). At the national level the German Association for Electrical, Electronic, and Information Technologies (VDE) has submitted a cross-industry standard to ensure AI trustworthiness that shall lead to an AI Trust Label (VDE 2022). At the corporate level companies work on project specific solutions. One example is the FCAS Ethical AI Demonstrator envisaged to provide a scenario-based simulation environment to illustrate ethical dilemmas and possible solution options (Koch 2022).

2 Developing Defense AI

The German MoD and the Bundeswehr have kicked off numerous projects, but it remains difficult to understand how individual projects will contribute to future capability growth. In addition, structural pacifism has led to a bifurcated national ecosystem favoring knowledge stovepipes rather than an integrated approach.

2.1 Development Priorities and Projects

At the time of writing, a national defense AI capability roadmap has not been publicly released. Consequently, this section provides our assessment of more than a dozen ongoing projects that have been selected to illustrate the diversity of current activities.[1] We structure these projects along the Bundeswehr's capability value

[1] We respect information classification levels and thus remain generic in describing the relevant projects. Whenever possible, we provide references to public sources for additional information.

chain—with some projects crossing several capability areas—and highlight the primary domain on which the respective projects focus:

- *Command, Control, Computers, Communications, and Cyber (C4/C5)*

COPs are considered central to acting swiftly and precisely (Generalinspekteur 2022: para 271). Therefore, using AI is important especially with regard to assessing mass data, advancing pattern recognition, and computing suggestions for courses of action (BMVg 2019a: 17–18). This focus is also considered inconspicuous and in line with the dominant socio-technical imaginary thus giving the Bundeswehr freedom to explore AI's strengths and shortfalls (Interview, 28 February 2023). Furthermore, the Bundeswehr's military services have specific COP needs. The Navy, for example, wants to create a subsea situational picture by fusing data from various military sensors with geoinformation and information about key offshore and subsurface infrastructure. AI is meant to be used for object recognition, modelling, and new modes of data visualization (Interview, 23 February 2023). Space Situational Awareness satisfies a similar need for a different domain with BWI and the Cyber Innovation Hub of the Bundeswehr exploring the use of defense AI to forecast space weather and project orbital movements of objects to avoid space collisions (BWI 2021).

On a separate but related track the Luftwaffe's AirC2 project evaluates the contribution of AI in increasing C2 efficiency and tempo and enhancing air C2 education and training. In addition, the Air Combat Management System project evaluates the use of AI to anticipate adversarial action, produce recognized air pictures, and recommend future courses of action (Interview, 25 March 2022). In view of future air power, defense AI is also a major issue for the Future Combat Air System (FCAS) and the Next Generation Weapon System (NGWS). FCAS has identified a total of eight use cases for defense AI. Situational awareness with AI shall "support orientation, decision making, and planning; either for a human operator using tactical displays or for automated functions directly assessing (…) digital data" (Azzano et al. 2020).

- *Intelligence, Surveillance, and Reconnaissance (ISR)*

Project MITA[2] focuses on wide area surveillance with the help of an AI-augmented sensor grid and automated data fusion. The goal is to produce a COP that illustrates adversarial troop movements in 3D and identifies adversarial intruders in real-time (BWI 2022). AI for ISR is also of interest for the German Navy, which is developing AI-augmented solutions to assess sensor data and classify hydroacoustic signatures in cooperation with the University of the Bundeswehr/Hamburg (Written communication, 22 July 2022). Furthermore, BWI and the Navy have launched KALMAR in cooperation with the startup marinom to use AI to advance the Navy's underwater situational awareness (Tedeski 2023).

[2] MITA: "Military Internet of Things für taktische Aufklärung" or military internet of things for tactical reconnaissance.

- *Precision Effects*

Based on GhostPlay (see below) Wild Hornets supports the German Army Concepts and Capability Development Center to develop tactics for air-launched effector swarms that target an adversarial high-value asset and test the feasibility of using air-launched effectors against next generation ground-based air defense solutions (Henckel 2023).

- *Support*

Several FCAS use cases address AI for supporting functions, for example, to enable complex guidance and flight control behavior to navigate unmanned platforms, improve anomaly detection, systems operator training, and improve production, maintenance, and logistics, thus reducing life cycle costs (Azzano et al. 2020). The University of the Bundeswehr/Hamburg uses AI simulation and numerical modelling to advance existing test and validation methods to improve the electromagnetic resistance of unmanned systems. The MissionLab at the University of the Bundeswehr/Munich tests mission planning/management systems, intelligent sensor systems or adaptive assistance systems with experimental simulation and flight trials thereby also using AI.

- *Cross-Functional Projects*

Advancing situational awareness and situational understanding by improving the C2-ISR link with defense AI is a key national R&T priority for NGWS with a focus on sensor data fusion, sensor resource management, and the integration of both elements. This project also explores options for a so-called AI Backbone that would provide a "single set of algorithms" to support different tasks and establish an open and unitary framework to facilitate the comprehensive use of defense AI (Interview, 2 March 2023). From 2019 to 2021 the program office for the German-Franco Main Ground Combat System (MGCS) ran a project with industry partners to use several unmanned aerial vehicles (UAV) as sensor carriers to produce a recognized operational picture integrated into the Army's C2 system via SitaWare Frontline (Wiegold 2019; ESUT 2021). A comparable project looks at the role of AI in automatically assessing and incorporating terrain specifics into operational planning with the aim of using terrain features for tactical advantages (Interview, 14 November 2022). In addition, URANOS KI, a follow-on project to MITA, combines defense AI for modular effector systems with a UAV-based surveillance system. Automating the handover of targeting data to different effectors is one of the capabilities to be developed (Interview, 14 November 2022; Prenzel et al. 2023: 43). Finally, project GhostPlay develops defense decision algorithms (Play) for defender and aggressor tactics thereby using a powerful simulation environment (Ghost). GhostPlay started with a Suppression of Enemy Air Defense (SEAD) scenario using UAV swarms to target a high value asset protected by ground-based air defense. Attacker and defender use AI developed tactics to outsmart each other. The "ability to learn tactical behavior in cooperation with other machines and/or humans" constitutes the project's AI research focus (Borchert et al. 2022a).

2.2 Germany's Defense AI Ecosystem

The German government (Bundesregierung 2019: 3) considers AI a defense-relevant national key technology, but it is unclear, what this categorization implies. This is relevant because Germany's bifurcated techno-industrial ecosystem mostly segregates defense-relevant actors from the rest (Borchert et al. 2022b; Hagebölling and Barker 2022: 6). Therefore, the German Bundeswehr has only access to a limited spectrum of the country's techno-economic power. Overall, the defense AI ecosystem rests on four building blocks:

- *Bundeswehr*

The Bundeswehr has established new entities to advance defense digitalization, such as the so-called Systems Centers (Systemzentren) for single services. Some service-specific institutions also have a cross-functional task, such as the Center for Digitalization of the Bundeswehr. This center is key to develop Germany's CIR capabilities, provides software development and IT integration capabilities for the Bundeswehr, and oversees developing the Bundeswehr's capabilities for military intelligence, electronic warfare, and geoinformation (Bundeswehr Undated). Other institutions help spinning-in digital solutions from outside the Bundeswehr (Cyber Innovation Hub) and supporting digitalization by maintaining key infrastructure and application development (BWI). Finally, the German Army also uses its test and experimentation unit as a testbed for rapid technology insertion and experimentation as well as synchronized concept and technology development (Bundeswehr 2020b).

- *Research and Technology Organizations (RTO)*

RTO constitute the second pillar of the defense AI ecosystem. Here bifurcation becomes most obvious. More than 70 universities and universities of applied sciences adhere the voluntary civil clause that prevents them "from engaging in defense research and cooperating with the defense industry" (Borchert et al. 2022b: 437). This also means that the Bundeswehr will not directly benefit from the German government's decision to set up six centers of competence on AI and fund "the establishment of 100 new professorships in AI at German universities" (Federal Government 2020: 10). Furthermore, the German Research Center for AI (DFKI), which has been pioneering AI research since the late 1980s, does not engage in defense either. To some extent the Bundeswehr can close the gap by relying on R&T conducted at its universities in Hamburg and Munich. Activities at these two locations have received a boost thanks to a €500M budget to set up the Digitalization and Technology Research Center (dtec.bw) that is meant to advance defense

digitalization.[3] Beyond dtec.bw, the lion's share of Germany's defense research falls on the Fraunhofer Society and the German Aerospace Center.

- *Old and New Defense Industrial Players*

The defense industry forms the third pillar of the defense AI ecosystem. Most of Germany's well-established defense companies like Airbus, Atlas Elektronik, Hensoldt, KNDS or Rheinmetall are involved in developing or adopting AI for defense purposes in one way or another. More recently, several new players and startups (BMWK 2022) with a dedicated focus on AI and defense AI have entered the market. Some of them originate from the commercial world and join forces with incumbent defense players:

– 21strategies specializes in developing large scale multi-agent reinforcement learning to compute optimal decision-making strategies under uncertainty in the context of national security, capital markets, and supply chains. 21strategies works on GhostPlay, Wild Hornets, FCAS, and NGWS. Hensoldt cooperates with 21strategies.
– Aleph Alpha is working on large language models and develops generative AI solutions to support public and private sector applications. Among others, Aleph Alpha is working on defense AI solutions for FCAS.
– Data Machine Intelligence Solutions develops data modeling and visualization solutions, inter alia, with a focus on solutions for mission planning and management as well as simulation technologies. Data Machine Intelligence Solutions also contributes to FCAS's defense AI work stream.
– HAT.tec focuses on developing technologies in support of human-autonomy teaming, with a focus on automated reasoning, planning and decision-making. HAT.tec also works on defense AI solutions for FCAS.
– Helsing develops AI for real-time information processing and turning unstructured sensor data into common operational pictures. The company is headquartered in Germany with subsidiaries in France and the United Kingdom. Helsing works on defense AI for FCAS, NGWS and MITA. Helsing cooperates with Rheinmetall Defense Electronics, Saab, and MBDA.
– Traversals uses AI for open-source intelligence to analyze and assess global events, identify potential threats, and assessing multilingual information. Traversals AI Dynamic Frontline Monitoring, for example, uses AI-enhanced technologies to provide a 24/7 near-real time operational picture of the Ukrainian-Russian front line.

- *IT and Consulting Companies*

IT and consulting companies such as Accenture, Atos or SAP form the final pillar of the German defense AI ecosystems. These companies are instrumental in supporting concept development, providing hardware infrastructure and computer

[3] https://dtecbw.de/home. Accessed 30 January 2024.

processing capacities as well as assisting the synchronization of digitalization and organizational change.

3 Organizing Defense AI

The Bundeswehr is in its early days to adjust its organizational fitness to future defense AI requirements. The 2019 capstone document acknowledges that a strong Bundeswehr-common approach with joint responsibility for capability development is needed to counter the risks of duplication, parallel structures, crowding-out effects, and fragmentation (BMVg 2019a: 20). So far, however, tensions exist between top down-driven and decentralized service-specific approaches.

3.1 Joint Approaches

Defense AI is part of the digitalization agenda set by the Directorate-General for Cyber/IT (CIT). In 2019 the German MoD has also established a Digital Council (Digitalrat), which advises the Minister of Defense and provides impulses to advance defense digitalization (BMVg 2019b: 16). Additionally, the Directorate-General for Planning implements the Bundeswehr's integrated planning. Since defense AI is part of the toolbox needed for the Bundeswehr's future development, this Directorate-General provides the leading desk officer for defense AI. He also chairs the Bundeswehr's defense AI community, a semi-formalized network for information sharing.

Tensions arise from the fact the Bundeswehr's military services follow different digital levels of ambition and enjoy great leeway in implementing their respective digital agendas while CIT shapes the broad guidelines and the idea of a Bundeswehr-common AI backbone. This creates a "wait and see" atmosphere as the services need to strike a balance between following through on their own agendas and supporting a joint agenda, which might come at the cost of sacrificing service-specific resources for joint tasks. A cluster approach respecting joint and service-specific interests could work but very much depends on the willingness of the actors involved and the availability of extra resources (Interviews, 25 March 2022 and 14 March 2023).

3.2 Single Service Approaches

Against this background, the Army is digitalizing land-based operations (D-LBO) to create a whole-of-service digital federation for future operations. Its 2019 AI concept paper envisions setting up an AI steering group with the Army Command to

oversee the work of the so-called Army AI Work Bench at the Army Concepts and Capabilities Development Center. This work bench would serve as the overall coordination mechanism for all Army AI activities and liaise with industry and academia. In addition, the Army would create a development center mainly focusing on training defense algorithms and developing key data models as well as an AI data center that would take care of Army data, provide data expertise and data scientists (Amt für Heeresentwicklung 2019: 14–15/19–20; Dani 2022). Elements of this vision will be realized with the Army's forthcoming Systems Center for Digitalization. It is likely to be the powerhouse for all things digital of the Army and play an important role by strengthening sovereign defense software development (Interview, 22 February 2023).

The German Luftwaffe is exploring the impact of defense AI on future air power. So far, the service has taken organizational baby steps with one desk officer in the Luftwaffe Command overseeing the subject matter. The Luftwaffe also considers defense AI as part of its broader digitalization agenda and as an important enabler to advance air power innovation. Tensions exist as the service has two responsible officers for digitalization (Deputy Air Chief) and innovation (desk officer, LTC level). Both have pledged to inform each other but given "split" responsibilities true leadership on defense AI remains yet to be developed (Interview, 25 March 2022).

The new Chief of the Navy puts great emphasis on naval innovation. He has created the position of a Commissioner for Innovation, Digitalization, Empowerment, and Agility (ID:EA, Marinekommando 2022) at the Naval Command. This new position is to bridge the digitalization/innovation divide and push both agendas. Defense AI is part of the ID:EA tasks and will benefit from a vast network of naval reservists that is to be expanded. Overall, the current focus is on breaking up existing structures by creating opportunities for new digital naval projects outside existing planning processes that are considered too cumbersome to deal with (Interviews, 23 February and 14 March 2023).

Finally, the Cyber and Information Domain Service operates and protects the Bundeswehr's IT infrastructure, is engaged in electronic warfare, provides satellite-based imagery reconnaissance data, and operates the Bundeswehr Geoinformation Center. Its Center for Bundeswehr Digitalization and Cyber and Information Service Capability Development pools software analysis and software development expertise. Regarding defense AI, the Electronic Warfare Battalion 912, for example, plays an important role as its own AI laboratory is exploring the use of AI to calculate flight paths or analyze radio communications (Fleischmann 2022).

4 Funding Defense AI

Whereas the German government has pledged to spend €5bn until 2025 to implement the national AI strategy, it is difficult to gauge how much the Bundeswehr spends on defense AI. Overall, investments in Germany's digital defense infrastructure were set to rise with roughly 20% of the €100bn Sondervermögen (special

fund) originally to be spent on this priority. Among other projects, this included around €8.5bn for the Army's landmark D-LBO or €2.6bn for the German Mission Network. However, changes in the plans for the special fund make it difficult to assess whether this is still true. The 2023 budget law cut defense R&T by €200M to €330M whereas spending on defense development and experimentation stood at around €515M. Fortunately, the 2024 draft budget significantly increases R&T spending again to €565M in the regular budget, with an additional €50M coming from the special fund (Deutscher Bundestag 2023: 2199/2226). However, development and experimentation spending decrease to €215M in 2024. Furthermore, the MoD can spend around €40M (2023) and €50M (2024) respectively on methods such as Concept Development & Experimentation, modeling and simulation and innovation competitions, and around €25M on disruptive innovation in cybersecurity and key technologies (Bundesgesetzblatt 2022a: 1034; Bundesgesetzblatt 2022b: 45/48–49/69–70; Deutscher Bundestag 2023: 2201).

No public figures are available for spending on defense AI. The law on the Sondervermögen originally earmarked a total of €422M for research, development, and AI, with AI focusing on surveying and safeguarding wide areas (Eastern Flank) (Bundesgesetzblatt 2022a). The 2023 Sondervermögen budget law breaks this focus area down to a €16M increment without further specifying the AI amount. This budget line significantly increased in 2024 to €667M, but no further breakdown is publicly available. This suggests that a large part of these funds will most likely be used to partially offset the decrease of the experimentation budget in the regular defense budget (Deutscher Bundestag 2023: 2227). In addition, several dtec.bw projects focus on developing defense AI. Taken together, the total four-year budget of three AI projects at the University of the Bundeswehr/Hamburg is about €20–30M, or €5–7.5M per year. The MissionLab at the University of the Bundeswehr/Munich operates on a total budget worth around €20M, or around €5M per year. In addition, we speculate that the German MoD spends a lower two-digit million amount per year on developing AI for NGWS. Considering these figures and adding a calculated reserve for projects unknown at the time of writing, we assume that the MoD currently spends around €50M per year on defense AI software development.

5 Fielding and Operating Defense AI

In-service defense systems use AI applications but a clear delineation between software-enabled analytics and automation and proper AI is difficult to draw. Consequently, the true status of the Bundeswehr's fielding and operating of defense AI remains opaque. Overall, the following overview of selected projects is in line with the development priorities discussed above:

- *Command, Control, Computers, Communications, and Cyber (C4/C5)*

The German MoD's Directorate-General for Strategy and Operations uses the so-called Preview system to analyze open-source intelligence (OSINT) for early

warning with AI for data analytics and predictive analysis. Users can zoom in on each of the more than 60 indicators' quantitative assessment and track assessment changes over time. The system also provides access to the sources that underpin assessment results. Preview is a multi-language solution that also offers back casts to validate the feasibility of current assessments with a database reaching back to 2015. As Preview is an OSINT solution, classified and open date are not yet fused. In addition, a link between crisis early warning and the Bundeswehr's activities on establishing COPs has yet to be established (Interviews, 18 and 21 March 2023).

- *Intelligence, Surveillance, and Reconnaissance (ISR)*

In early 2022, the Bundeswehr decided to equip all NH90 helicopters with Hensoldt's Kalaetron Radar Warning Receiver, which uses AI for big data analysis to quickly detect new threat patterns and with a very low false alarm rate (hartpunkt.de 2019; EDR Magazin 2022). Since 2018, BWI has been experimenting with the use of AI in combination with radar technology already in use on construction sites to see through walls to detect humans as individuals or groups and identify the current state of motion (Ilg 2022).

- *Precision Effects*

The Luftwaffe uses Diehl's IRIS-T air-to-air missiles equipped with intelligent image processing to detect and ignore adversarial infrared decoys when engaging a target (Penney 2000). Similar technologies likely underpin the image-scanning seeker of the Rolling Airframe Missile (RAM) that the German Navy is using to protect frigates and class K130 corvettes (ESUT 2022b; Naval Technology 2014). In addition, Saab's Arexis electronic warfare sensor suite including AI algorithms by Helsing has been selected to upgrade Eurofighter jets (Saab 2023).

- *Support*

The Bundeswehr's Joint Support Service has been experimenting with the use of AI for an early warning system to support national crisis management and to support warehouse functions (Bundeswehr 2021; ESUT 2022a). The Medical Command uses civilian AI applications for decision support of doctors in the fields of analytics, diagnostics, and individual therapies (BMVg 2019a: 11). In addition, BWI has been developing BundesWEAR, an app with AI features that offers individual measurements, suggests the best fitting clothing size, and offers online orders for home or barracks deliveries (ESUT 2022a).

6 Training for Defense AI

The Bundeswehr is in the very early stage of exploring the impact of defense AI on training. The MoD's 2019 defense AI capstone document argues that future members of the Bundeswehr will need broad and specialized AI expertise, software

development know-how, improved MINT[4] knowledge, and interdisciplinary know-how to develop solutions for human-machine interaction (BMVg 2019a: 21–22). At the joint level, the Bundeswehr Command and Staff College (Führungsakademie) is responding. In view of launching the new curriculum in autumn 2024, stocktaking is underway to define the future role defense AI is going to play—both as an instrument for training and education and as a subject that future officers need to understand. In April 2023, the College launched a digital open space learning environment. The modular set up could also be used to create interfaces for integrating wargaming, serious gaming, and AI-enhanced training solutions.

In parallel, the University of the Bundeswehr/Hamburg is working on a new AI bachelor's and master's degree course. The program aims at teaching technical basics in the fields of mathematics and informatics as well as adjacent technology areas such as sensors, acoustics, or information technology. The new program would also embed defense-relevant AI in the broader societal context with building blocks focusing on law, ethics, sociology, and political science (Interview, 25 February 2023).

Complementary service-level activities are under way. The Army is looking at the role of defense AI in live and constructive training simulations as well as AI-augmented learning analytics to adjust teaching to individual learning progress (Interview, 7 March 2023; Amt für Heeresentwicklung 2019: 12). The Luftwaffe is exploring AI for new tactics, techniques, and procedures related to air defense and dogfight scenarios and looks at using AI to train Luftwaffe operators in advancing and improving planning cycles as part of its AirC2 project (Interviews, 7 and 25 March 2022). Not yet using defense AI for training, the Navy is mulling the idea of using AI-based training for sea-based signals intelligence (Interviews, 22 February and 14 March 2023).

Additionally, different initiatives have been launched to train defense AI algorithms. The Luftwaffe has procured an off-the-shelf software product to teach air power gaming. While the primary purpose was to improve the respective planning and operating procedures, data generated by using the software is also used as a basis to train future defense AI algorithms (Interview, 25 March 2022). The Army is working on using simulation-based training with reinforcement learning to train neural networks with the goal of enhancing the autonomous behavior of unmanned systems in battlefield scenarios. It also looks at reinforcement learning to train neural networks to command battlefield units. Another focus area of the Army emerges from the need to generate training data for AI-enhanced image recognition (Interview, 7 March 2023).

[4] MINT: Mathematics, informatics, natural science, and technology.

7 Conclusion

Today, German defense AI is a grassroots movement. Motivated people push projects to bring defense AI into the Bundeswehr. Structural and procedural provisions are in place to enable change. Overall, however, change is first and foremost about closing fundamental capability gaps. The Bundeswehr may want to operate at the technological edge, but existing shortfalls inhibit Germany's armed forces from doing so. New concepts that leverage emerging technologies are bound back by the resistance of a Bundeswehr bureaucracy solidly grounded in the status quo.

This is no surprise. As we have argued, Germany's defense AI approach is locked in a "master and servant" logic deeply rooted in the country's strategic culture and organizational set up (structural pacifism). Consequently, Germany prioritizes security and technology policy options, which comply with its non-belligerent post-war identity. Domestic socio-political legitimization of the use of force is consistently more important than the impact that can be achieved by using it.

This preference will undoubtedly continue to determine political visions on future roles of defense AI and the panorama of technologies deemed acceptable for military use. This narrows future development options and limits the impact of defense AI to an evolutionary trajectory from the start. Since innovation in a tightly regulated defense market relies heavily on capability-pull by the Bundeswehr, its muted technology appetite does not bode well for the defense industry, too.

Consequently, broadening the footprint and strengthening the influence of the defense AI grassroot movement will require the MoD to do some heavy lifting along four lines of effort. First, the Bundeswehr needs to be more precise on how defense AI will boost its capabilities. This guidance should delineate Bundeswehr-common and service-specific defense AI capability goals and identify current defense AI shortfalls. Prioritizing mitigation measures can lead to creating a roadmap to address these shortfalls via national or multinational R&T projects and procurement programs.

Second, a defense industrial policy for AI is needed. By arguing that it does not drive technological development, the Bundeswehr effectively drops out as a demanding launch customer for cutting-edge defense AI solutions made in Germany. This creates distorted market signals for innovative companies that might consider entering the defense business. It is therefore high time for the MoD and industry to specify the "terms and conditions" on which the future defense data ecosystem will operate. This requires striking a balance between the Bundeswehr's interest in unrestricted data access, industrial preferences for data monetization, and the general need to incentivize a data sharing dynamic that also involves stakeholders that have not participated in generating original data (Datenethikkommission 2019: 145–148).

Third, Germany needs to define its international defense AI ambition, for example, by positioning itself as a defense AI framework nation. A hardware-focused framework nation could advance multinational defense AI by offering international partners access to its new digital battlefield infrastructure. Alternatively, a

software-focused framework nation could zoom in on specific applications, for example, by offering AI-enhanced red teaming to support multinational capability development and design evaluation for multinational projects like FCAS and MGCS. Moreover, the Bundeswehr could turn its strong focus on ethics into an asset by combining value-based engineering with simulation to offer partners a new digital test lab for the responsible use of defense AI.

Finally, the Bundeswehr needs to consider how to certify, qualify, and admit future defense AI solutions. This is a daunting task because today's system benefits the original equipment manufacturers (OEM) in their role as gatekeepers that can resist modifications of existing defense products (Interview, 14 March 2022). This is likely to undermine software-defined defense if software-induced modifications change the overall characteristics of a defense solution for which the OEM—not the software developer—bears ultimate responsibility. Although there is no easy way out of this dilemma, an AI-enhanced simulation environment could provide an option to test the characteristics and the performance of future defense AI solutions. The resulting digital twin could be augmented, for example, with mission-critical data gathered during international Bundeswehr operations as well as AI-enhanced red force elements.

References

Amt für Heeresentwicklung. 2019. *Künstliche Intelligenz in den Landstreitkräften. Ein Positionspapier des Amts für Heeresentwicklung*. Cologne: Amt für Heeresentwicklung.

Autorenteam Luftwaffe. 2021. Der Einfluss künstlicher Intelligenz bei er Führung von Luftoperationen der Zukunft. *Wehrtechnik* II: 65–68.

Azzano, Massimo, et al. 2020. *The Responsible Use of Artificial Intelligence in FCAS. An Initial Assessment*. FCAS Forum. https://www.fcas-forum.eu/articles/responsible-use-of-artificial-intelligence-in-fcas. Accessed 30 January 2024.

BDSV, et al. 2023. *Beitrag zu Grundlagen und Grenzen Künstlicher Intelligenz (KI) beim Einsatz in Verteidigungstechnologien. Impulspapier des Arbeitskreises KI und Verteidigung*. Berlin: BDSV. Accessed 30 January 2024.

Biess, Frank. 2019. *Republik der Angst. Eine andere Geschichte der Bundesrepublik*. Munich: Rowohlt.

BMVg. 2017. *Strategische Leitlinie Digitalisierung*. Berlin: Bundesministerium der Verteidigung.

———. 2019a. *Künstliche Intelligenz. Nutzung im Geschäftsbereich des Bundesministeriums der Verteidigung*. Berlin: Bundesministerium der Verteidigung.

———. 2019b. *Erster Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung*. Berlin: Bundesministerium der Verteidigung.

———. 2019c. *Future Operating Environment 2035*. Berlin: Bundesministerium der Verteidigung.

———. 2021. *Datenstrategie GB BMVg*. Berlin: Bundesministerium der Verteidigung.

BMWK. 2022. *KI-Startups in Deutschland. Eine Untersuchung zu Unternehmensgründungen im Bereich Künstliche Intelligenz*. Berlin: Bundesministerium für Wirtschaft und Klimaschutz.

Bock, Christian, and Matthias Schmarsow. 2023. Gedanken zum Einsatz von Künstlicher Intelligenz beim militärischen Frühen und Entscheiden. In *Bundeswehr der Zukunft. Verantwortung und Künstliche Intelligenz*, ed. Norbert Lammert and Wolfgang Koch, 138–158. Berlin: Konrad-Adenauer-Stiftung.

Borchert, Heiko, Torben Schütz, and Joseph Verbovszky. 2022b. Unchain My Heart. A Defense Industrial Policy Agenda for Germany's Zeitenwende. *Zeitschrift für Aussen- und Sicherheitspolitik* 2: 429–451. https://link.springer.com/article/10.1007/s12399-022-00926-4. Accessed 30 January 2024.

Borchert, Heiko, et al. 2022a. *Free Jazz on the Battlefield. How GhostPlay's AI Approach Enhances Air Defense*. Defense AI Observatory. https://defenseai.eu/daio_study2203. Accessed 30 January 2024.

Brendecke, Jan-Wilhelm, Thomas Doll, and Daniel Kallfass. 2020. Der Führungsprozess von morgen. Wie Künstliche Intelligenz den Führungsprozess beschleunigen kann. *Europäische Sicherheit und Technik* 10: 68–71.

Bundesgesetzblatt. 2022a. Gesetz zur Finanzierung der Bundeswehr und zur Errichtung eines "Sondervermögens Bundeswehr" und zur Änderung der Bundeshaushaltsordnung. *Bundesgesetzblatt* 23: 1030. https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%271034878%27%5D&skin=pdf&tlevel=-2&nohist=1&sinst=0E04B990. Accessed 30 January 2024.

———. 2022b. Gesetz über die Feststellung des Bundeshaushaltsplans für das Haushaltsjahr 2023. *Bundesgesetzblatt* 54: 2485. http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl122s2485.pdf. Accessed 30 January 2024.

Bundesregierung. 2019. *Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie*. Berlin: Bundesregierung.

Bundeswehr. 2020a. *Von Big Data bis KI. Zweite Ausbaustufe des Gemeinsamen Lagezentrums CIR*. Bundeswehr. https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/von-big-data-bis-ki-zweite-ausbaustufe-des-glz-cir-1826878. Accessed 30 January 2024.

———. 2020b. *Test- und Versuchskräfte in Munster aufgestellt*. Bundeswehr. https://www.bundeswehr.de/de/organisation/heer/aktuelles/test-und-versuchskraefte-in-munster-aufgestellt-4960224. Accessed 30 January 2024.

———. 2021. *Heimatschutz durch künstliche Intelligenz. Die Bundeswehr auf dem Weg in die Zukunft*. Bundeswehr. https://www.bundeswehr.de/de/aktuelles/meldungen/heimatschutz-durch-kuenstliche-intelligenz-bundeswehr-zukunft-5054820. Accessed 30 January 2024.

———. Undated. *Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum*. Bundeswehr. https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum/zentrum-digitalisierung-der-bundeswehr. Accessed 30 January 2024.

Burri, Regula Valérie. 2015. Imaginaries of Science and Society: Framing Nanotechnology Governance in Germany and the United States. In *Dreamscapes of Modernity – Sociotechnical Imaginaries and the Fabrication of Power*, ed. Sheila Jasanoff and Sang-Hyun Kim, 233–253. Chicago/London: The University of Chicago Press.

BWI. 2021. *Wie KI bei der Vorhersage des Weltraumwetters hilft*. Golem.de. https://www.golem.de/news/anzeige-wie-ki-bei-der-vorhersage-des-weltraumwetters-hilft-2112-161343.html. Accessed 30 January 2024.

———. 2022. *Generalinspekteur lässt sich KI-gestützte Aufklärung vorführen*. BWI. https://www.bwi.de/magazin/artikel/generalinspekteur-laesst-sich-ki-gestuetzte-aufklaerung-vorfuehren. Accessed 30 January 2024.

Dani, Enrico. 2022. Digitalisierung landbasierter Operationen. Sachstand und Weiterentwicklung. *Europäische Sicherheit und Technik* 2: 40–43.

Datenethikkommission. 2019. *Gutachten der Datenethikkommission der Bundesregierung*. Berlin: Datenethikkommission der Bundesregierung.

Deutscher Bundestag. 2023. *Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes über die Feststellung des Bundeshaushaltsplans für das Haushaltsjahr 2024. Deutscher Bundestag – Drucksache 20/7800*. Berlin: Deutscher Bundestag.

Eberle, Jakob. 2019. *Discourse and Affect in Foreign Policy: Germany and the Iraq War*. New York: Routledge.

EDR. 2022. *Hensoldt equips Bundeswehr NH90 Helicopter with State-of-the-Art Protection Systems*. European Defence Review. https://www.edrmagazine.eu/hensoldt-equips-bundeswehr-nh90-helicopter-with-state-of-the-art-protection-systems. Accessed 30 January 2024.

Ehlke, Tobias. 2021. Interview mit Generalleutnant Dr. Ansgar Rieks, Stellvertreter des Inspekteurs der Luftwaffe. *cpm Forum für Rüstung, Streitkräfte und Sicherheit* 3: 16–19.

ESUT. 2021. *Live-Demonstration Aufklärung im "Gläsernen Gefechtsfeld"*. Europäische Sicherheit und Technik. https://esut.de/2021/12/meldungen/31593/live-demonstration-aufklaerung-im-glaesernen-gefechtsfeld/. Accessed 30 January 2024.

———. 2022a. *BWI entwickelt Lösungen mit künstlicher Intelligenz für die Bundeswehr*. Europäische Sicherheit und Technik. https://esut.de/2022/01/meldungen/32112/bwi-entwickelt-loesungen-mit-kuenstlicher-intelligenz-fuer-die-bundeswehr/. Accessed 30 January 2024.

———. 2022b. *Deutsche Marine: Vertrag für 600 RAM Block 2B unterzeichnet*. Europäische Sicherheit und Technik. https://esut.de/2022/11/meldungen/37952/deutsche-marine-vertrag-fuer-600-ram-block-2b-unterzeichnet/. Accessed 30 January 2024.

Färber, Michael. 2023. Digitalisierung der Bundeswehr. In *Bundeswehr der Zukunft. Verantwortung und Künstliche Intelligenz*, ed. Norbert Lammert and Wolfgang Koch, 224–235. Berlin: Konrad Adenauer Stiftung.

Federal Government. 2018. *Artificial Intelligence Strategy*. Berlin: The Federal Government.

———. 2020. *Artificial Intelligence Strategy of the German Federal Government. 2020 Update*. Berlin: The Federal Government.

Fleischmann, Armin. 2022. Das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum: 'Unser Beitrag als Treiber der Digitalisierung der Bundeswehr'. In *CIR 2.0: Von der Idee zur Dimension*, 34–38. Bonn: cpm Communication PresseMarketing. https://www.bundeswehr.de/resource/blob/5519316/29945909e7ed8cc36f2c9ff4ecd53186/download-sonderheft-cir-2-0-data.pdf. Accessed 30 January 2024.

Generalinspekteur. 2022. *Operative Leitlinien für die Streitkräfte*. Berlin: Generalinspekteur.

Hagebölling, David, and Tyson Barker. 2022. *Ethisch und einsatzfähig. Aufkommende und disruptive Technologien, die Bundeswehr und die Zeitenwende*. Berlin: DGAP.

hartpunkt.de. 2019. *Hensoldt präsentiert Radarwarner auf KI-Basis*. hartpunkt.de. https://www.hartpunkt.de/hensoldt-praesentiert-radarwarner-auf-ki-basis/. Accessed 30 January 2024.

Henckel, Ole. 2023. KI-Gefechtssimulation für die Bundeswehr – GhostPlay. *Europäische Sicherheit und Technik* 7: 39–41.

Hofstetter, Yvonne, and Joseph Verbovszky. 2023. *How AI Learns the Bundeswehr's "Innere Führung." Value-Based Engineering with IEEE7000™-2021*. Hamburg: Defense AI Observatory.

Ilg, Peter. 2022. *Militär-Projekt: Mit künstlicher Intelligenz durch Wände schauen*. Heise online. https://www.heise.de/news/Militaer-Projekt-Mit-kuenstlicher-Intelligenz-durch-Waende-schauen-7182283.html. Accessed 30 January 2024.

Jasanoff, Sheila. 2015. Future Imperfect: Science, Technology, and the Imaginations of Modernity. In *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power*, ed. Sheila Jasanoff and Sang-Hyun Kim, 1–33. Chicago/London: The University of Chicago Press.

Jensen, Benjamin M., Christopher Whyte, and Scott Cuomo. 2022. *Information in War. Military Innovation, Battle Networks, and the Future of Artificial Intelligence*. Washington, DC: Georgetown University Press.

Kober, Klemens, and Torben Schütz. 2024. Den Weltraum ordnen. Zukunftsvorstellungen und (New) Space Governance. In *Strategischer Wettbewerb im Weltraum. Politik, Sicherheit und Wirtschaft im All*, ed. Moritz Brake et al, 633-652. Wiesbaden: Springer VS.

Koch, Wolfgang. 2022. Elements of an Ethical AI Demonstrator for Responsibly Designing Defence Systems. *25th International Conference on Information Fusion*. https://ieeexplore.ieee.org/document/9841387. Accessed 30 January 2024.

Kommando Heer. 2017a. *Wie kämpfen Landstreitkräfte künftig? Thesenpapier*. Strausberg: Kommando Heer.

———. 2017b. *Digitalisierung von Landoperationen*. Stausberg: Kommando Heer.

Marinekommando. 2022. *Inspekteur der Marine – Absicht 2022*. Rostock: Marinekommando.

Naval Technology. 2014. *SeaRAM Anti-Ship Missile Defence System*. Naval Technology. https://www.naval-technology.com/projects/searam-anti-ship-missile-defence-system/. Accessed 30 January 2024.

Penney, Stewart. 2000. *Short-range square-off*. Flight Global. https://www.flightglobal.com/short-range-square-off/32654.article. Accessed 30 January 2024.

Prenzel, Daniel, et al. 2023. Künstliche Intelligenz in der Bundeswehr. Enabler oder Nutzer von Softare Defined Defence? *Europäische Sicherheit und Technik* 12: 40–43.

Saab. 2023. *Saab's Arexis selected for German Eurofighter electronic warfare variant*. Saab. https://www.saab.com/newsroom/press-releases/2023/saabs-arexis-selected-for-german-eurofighter-electronic-warfare-variant. Accessed 30 January 2024.

Soare, Simona, Pavneet Singh, and Meia Nouwnes. 2023. *Software-Defined Defence: Algorithms at War*. London: IISS.

SPD/Bündnis90/Die Grünen/FDP. 2021. *Mehr Fortschritt wagen. Koalitionsvertrag 2021-2025*. Berlin: SPD/Bündnis90/Die Grünen/FDP.

Stengel, Frank A. 2020. *The Politics of Military Force: Antimilitarism, Ideational Change and Post-Cold War German Security Discourse*. Ann Arbor: University of Michigan Press.

Tedeski, René. 2023. *KALMAR – Mit KI zur schnelleren Unterwasseraufklärung*. Europäische Sicherheit und Technik. https://esut.de/2023/12/fachbeitraege/45777/it-news-kalmar-mit-ki-zur-schnelleren-unterwasser-aufklaerung/. Accessed 30 January 2024.

VDE. 2022. *Kann Künstliche Intelligenz wertekonform sein? VDE SPEC als Grundlage künftiger Entwicklungen*. https://www.vde.com/de/presse/pressemitteilungen/ai-trust-label. Accessed 30 January 2024.

Verbovszky, Joseph. 2024. *German Structural Pacifism. Cultural Trauma and German Security Policy since Unification*. Wiesbaden: Springer Verlag.

Welchering, Peter. 2023. *Von der Bundeswehr zur digitalen Verteidigungsarmee*. Deutschlandfunk. https://www.deutschlandfunk.de/it-soldaten-das-software-defined-defence-konzept-soll-die-bundeswehr-umkrempeln-dlf-68c615bf-100.html. Accessed 30 January 2024.

Wiegold, Thomas. 2019. *Studie fürs 'gläserne Gefechtsfeld': Drohnen und KI*. Augen geradeaus. https://augengeradeaus.net/2019/04/studie-fuers-glaeserne-gefechtsfeld-drohnen-ki/. Accessed 30 January 2024.

Leveraging Data Science for Defence in the Digital Age: Defence AI in the Netherlands

Marierose M. M. Heineken-van Dooren and Roy Lindelauf

This chapter provides an overview of the Dutch Ministry of Defence's approach to artificial intelligence (AI) and data science, its strategic vision for 2035, and its efforts in developing, organizing, fielding, and operating defence AI. The Dutch Ministry of Defence (MoD) views AI and data science as crucial for the protection of the Dutch Kingdom and has set three ambitions for the future. These include technological advancement, information-driven operations, and becoming a reliable partner. The government commits to spend at least 2% of GDP on defence. The strategic knowledge- and innovation agenda 2021–2025 focuses on innovation in short cycles and gives direction to knowledge building, technology development and innovation (Ministerie van Defensie 2020c).

The Data Science and AI Strategy 2023–2027 highlights the Dutch MoD strategy for the next five years with objectives related to high-quality information technologies, data governance, personnel policy, and data-driven decision-making (Ministerie van Defensie 2023a). Regarding ethics and defence AI, an ELSA Lab (Ethical, Legal, Societal Aspects) is established to ensure responsible AI use within defence, focusing on ethical, legal, and societal aspects. In addition, the Netherlands hosted the REAIM 2023 summit on Responsible AI in the Military Domain (Government of the Netherlands Undated) and is an active contributor to NATO's Data and AI Review Board (DARB) (NATO 2022), which aims to develop a user-friendly and responsible AI certification standard in the military domain.

M. M. M. Heineken-van Dooren
Netherlands Defence Academy, Breda, The Netherlands
e-mail: MMM.Heineken.v.Dooren@mindef.nl

R. Lindelauf (✉)
Netherlands Defence Academy, Faculty of Military Sciences, Breda, The Netherlands

Tilburg University, Tilburg, The Netherlands

Data Science Center of Excellence, Ministry of Defence, The Hague, The Netherlands
e-mail: RHA.Lindelauf.01@mindef.nl

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_10

AI is recognized as an essential component for the future of defence. Therefore, the Dutch MoD focuses on integrating these technologies into unmanned autonomous systems, military decision support, logistics, business operations, safety, and security. To develop these technologies, the facilitation of data-driven working, improving data management, investing in knowledge and expertise, and optimizing decision processes, have been identified as key issues that will be synchronized in an all-encompassing roadmap. Collaboration with international partners and maintaining meaningful human control over AI systems is emphasized and described as essential.

During fielding and operating defence AI, the Dutch MoD is prioritizing responsible use. Examples of fielded defence AI projects include robotic and autonomous systems within the Army, a DataLab, and utilizing advanced algorithms and machine learning (ML) techniques within the Royal Netherlands Marechaussee.

It is vital to train and educate personnel at all levels to understand AI's impact, including legal and ethical aspects. The Data Science Centre of Excellence is a major player within the MoD, that aims to strengthen the knowledge base of the Netherlands Defence Academy (Ministry of Defence Undated) and to develop data science courses for the different educational programs within Defence.

This chapter demonstrates the Dutch MoD's commitment to adopting AI responsibly while acknowledging its importance for national security and defence. It underscores the efforts in research, development, and collaboration with knowledge partners, universities, and the commercial sector to remain at the forefront of AI technology while upholding ethical and legal principles. All information in this chapter is based open-source data.

1 Thinking About Defence AI

The Dutch MoD considers AI and data science as two areas of development that will significantly impact the way the Dutch Kingdom is protected and defended. The Dutch MoD holds a human-centric view on AI as a capability multiplier. To gain new insights and support decision-making through AI and data science, the MoD invests in enhancing knowledge and collaboration with public-private partners, and in experimenting with AI and data science. Dutch thinking on defence AI is influenced and inspired by NATO in general and several partners in particular. The Netherlands echo the principles for responsible military use of AI, laid out in NATO's first AI strategy.

1.1 Strategic Vision 2035

To ensure that the MoD can gain new insights and support decision-making through AI and data science in the future, the MoD identified three main ambitions for the following years (Ministerie van Defensie 2020b). These ambitions will positively influence the effectiveness and efficiency of the MoD and are based on an analysis focusing on possible future threats, such as cyberattacks, and problems, such as the availability of too much information, making it difficult or even impossible to filter, analyse and act on information.

First, the MoD is a technologically advanced organization that uses AI, data science, big data and (semi-)autonomous systems under meaningful human control. Such an organization requires personnel that focuses on innovation and is educated in (information) technology. This provides the opportunity to work more labour-extensive where possible and remain labour-intensive where necessary and desirable. The weapon systems and units of the MoD need to be modular and easily upgradable, so they can be integrated and combined with other compatible systems and units. It is expected that AI algorithms can support such force mix optimization considerations. When innovating, special attention is given to implementation as well as ethical and legal aspects. The Netherlands government has approved the national plan on the NATO Defence investment pledge, which commits the MoD to increase defence spending to achieve the NATO goal of 2% GDP.

Second, the MoD aims to attain and hold a prominent information advantage within both NATO and the European Union (EU). A focus is placed on information-centric warfare. A key concept in this regard is Information Manoeuvre (Reynolds 2020). It holds a prominent position in Dutch military discourse, playing an increasingly pivotal role in discussions. It centres on leveraging military information capabilities to shape the behaviour of audiences by creating impactful effects in the operational environment. As outlined in Dutch policy documents, a well-executed Information Manoeuvre is deemed crucial for establishing a military that is prepared for future conflicts and resilient over the long term (Ministerie van Defensie 2020a). This relates to the concept of Multi-Domain Operations (MDO), which recognises the need to synchronise Information Manoeuvre with other military operations to create effects. Both Information Manoeuvre and MDO are relevant in the context of the complex and rapidly changing operational environment (Townsend 2018). In addition, using data science and AI to analyse large volumes of data gathered by an increasing number of sensors, the MoD can effectively manage complex scenarios and operations and broaden and facilitate its deployment capabilities in increasingly complex multi-domain and predominantly hybrid contexts. Think of algorithms to support scenario analysis, image recognition in video data or algorithms for optimal route allocation to support data collection.

Third, the MoD is a reliable partner and protector. The Dutch MoD is more visible and enhances the provision of information to the parliament and public. This will improve awareness about security, so the Netherlands will stay alert to (hybrid)

threats and build resilience against them. In addition, the national security architecture will become more robust.

1.2 Strategic Knowledge and Innovation Agenda 2021–2025

The strategic vision 2035 calls for strengthening the innovative capacity of Defence and collaboration within its knowledge and innovation partners. The strategic knowledge and innovation agenda (SKIA) pays special attention to the ability to innovate in short cycles and gives direction to knowledge building, technology development, and innovation. With SKIA, the Dutch MoD has a concrete plan for action regarding the development of key enabling technologies such as AI and robotics. It focusses on four areas (Ministerie van Defensie 2020b):

- Strengthening the foundation of defence-specific knowledge;
- Embedding innovation in the work environment, culture, and management;
- Enhancing collaboration among knowledge and innovation partners of the MoD;
- Strengthening collaboration within the Defence Knowledge and Innovation Chain.

To attain these goals, SKIA defines several AI specific research and technology domains. These constitute, among others, the use of data science with respect to detection and deception using signature management in the electronic warfare domain. Another domain considers sensor systems and their use in countering remotely piloted aircraft systems. In the command-and-control domain AI is being used for increasing the speed of data collection and analysis, among other uses.

1.3 Data Science and AI Strategy 2023–2027

Even though AI and data science are described in the strategic vision 2035 and SKIA 2021–2025, the MoD has developed a Data Science and AI strategy for 2023–2027, as an explicit foundation for the optimal use of AI and data science for the next five years (which will be updated every five years). In shaping its strategy, the MoD consulted both public and private partners, such as leaders in industry and transatlantic partners like the US. In addition, frameworks and guidelines are being developed to document the functioning of an algorithm, the choices made, and its use in the workplace. The MoD is closely involved in interdepartmental developments in this field, such as various research initiatives and policy instruments. There is also significant international attention on the responsible deployment of data science and AI in the military domain. The MoD aspires to take a leading role in international standards and certification developments. Optimizing ethical-legal frameworks and the responsible use of data science and AI in the military domain, in close collaboration with NATO and EU partners, research institutions like the

Netherlands Organisation for Applied Scientific Research (TNO) and the Royal Netherlands Aerospace Centre (NLR), and industry, is a key focus for the MoD.

The Data Science and AI strategy considers five areas of application of AI that guide the development of AI together with strategic partners as NATO and EU (Ministerie van Defensie 2020b):

- Unmanned autonomous systems;
- Military decision support and intelligence;
- Logistics and predictive maintenance;
- Business operations;
- Safety.

In its call to action the strategy identifies the need for further European cooperation on data science and AI. There are four common objectives that require an integrative approach regarding AI and data science:

- Develop high-quality information technologies, to quickly and safely connect or share data within the MoD and with partners.
- Uniformly organise data management and governance, so data can be securely and quickly shared within the MoD and with partners.
- Develop personnel policy to invest in needed knowledge and expertise.
- Work-processes and decision-making have a data-driven approach, by investing in high-quality information technologies that enable this.

1.4 Ethics and Defence AI

To focus on developing knowledge that is relevant for the responsible development and application of AI in the context of the entire lifecycle, ELSA-labs were created by the Netherlands AI Coalition (NL AIC) together with the Dutch Science Organization (NWO). The ELSA Lab Defence aims to develop an ecosystem for responsible AI use within defence and examines conditions under which AI applications are acceptable, emphasising ethical, legal, and societal aspects. It focuses on the use case of cognitive warfare and other non-traditional physical warfare. The ELSA Lab Defence is an ecosystem consisting of several knowledge institutes (universities) and (semi-)governmental defence partners. In addition, the ELSA Lab Defence coordinates with the other national ELSA Labs on findings and possible collaborations (such as the ELSA Lab Police) to establish a nation-wide narrative on AI ethics in the public-private sector.

The lab aims to develop an ecosystem for responsible AI use within defence. It proposes two main solution avenues: integrating ELSA factors into requirements, specifications, acquisition, and deployment processes (currently under active investigation), and educating military personnel, media, and policymakers about ELSA concepts. Existing approaches like “value-sensitive design,” “explainable” algorithms, and human-machine teaming are adapted for the defence context. Think for

instance of the choice between complex machine learning models or simpler models that might be less accurate but better explainable in case of military combat. Realistic case studies such as terrain analysis for tactical helicopter missions are employed. The lab also studies public and defence personnel perceptions of military AI deployment, and tracks global technological, military, and societal trends influencing AI system deployment perceptions.

Simultaneously within the MoD, ethics, safety, and security must be integral components in the design process of data science and AI applications (privacy and security by design) to prevent vulnerabilities in the systems. It is crucial to consider data security and categorization, especially when linking systems for specific applications, as this introduces new challenges (Alfrink et al. 2022).

The MoD will therefore align its activities with similar initiatives related to secure data sharing brought forward by EU and NATO and beyond. In addition, the MoD opts for "privacy and security by design" and develops dynamic categorization for data science and AI applications based on combined data sources. The MoD continues to invest in knowledge building and technology development for new applications of data science and AI and invests in a robust analysis platform. A federative infrastructure for data science and AI will be developed. Furthermore, the MoD incorporates data science and AI as a focus area of cyber defence and develops a verification, validation, and accreditation system. The MoD also invests in knowledge building related to "counter-data science and AI."

In 2023, the government of the Netherlands hosted the first global Summit on Responsible Artificial Intelligence in the Military Domain, REAIM 2023, together with South Korea. The REAIM 2023 summit was the world's first global summit on responsible AI in the military and brought together governments, corporations, academia, start-ups, and civil societies to raise awareness, discuss issues, and to agree on common principles in deploying and using AI in conflict and war. Government representatives recognised not only the opportunities and potential but also the risks involved in using AI in the military domain. Therefore, they have agreed on a joint call to action on the responsible development, deployment, and use of AI in the military domain. The call-to-action focusses on the responsible use of AI in the military domain that follow international legal obligations in such a way that does not undermine international security, stability, and accountability. In 2024, the REAM conference is hosted by and organised in South Korea. It provides a good international platform in sharing knowledge and best practices about developing responsible AI in the military domain. In addition, it sets the international agenda on dealing with these technologies in the military.

Through its involvement in the REAIM summit, the Netherlands reinforced its dedication to ensuring responsible and ethical AI practices within the military that align with international law and respect of human rights. By leveraging its expertise in international law, the Netherlands contributes to shaping the global AI governance framework by emphasizing the importance of legal principles and maintaining accountability and transparency (under research in the ELSA Lab Defence among others) in the development and deployment of AI systems.

In 2023, NATO's Data and Artificial Intelligence Review Board (DARB) has started the development of a user-friendly and responsible AI certification standard to help industries and institutions across the Alliance make sure that new AI and data projects are in line with international law, as well as NATO's norms and values. The standard, which also applies to data exploitation and will include quality controls, is due to be completed by the end of 2024. Its aim is to translate NATO's Principles of Responsible Use, approved in October 2021 as part of NATO's first ever AI strategy, into concrete checks and balances, notably in terms of governability, traceability, and reliability. This will help to build trust among the innovation community, operational end users, and the public.

2 Developing Defence AI

The Dutch MoD envisions working in a "data-driven" manner by 2035. Data science and AI are critical enablers to conduct information driven operations in this regard. Several roadmaps, one for each of the five application areas discussed above, are being developed for this goal. It is imperative for the Netherlands to establish and maintain a strong position in the development and application of AI, especially with a strong focus within the MoD. By proactive deployment of AI-enhanced solutions it becomes possible to address the social and economic challenges that come with this new technology.

2.1 The Dutch AI Ecosystem

To realise and stimulate Dutch AI activities, the Dutch AI coalition (NL AIC) was established in October 2019 (NL AIC Undated). The NL AIC is a public-private partnership comprising government, business, educational and research institutions, and societal organizations, aiming to accelerate AI developments in the Netherlands and connect AI initiatives within the country. The ambition is to position the Netherlands at the forefront of AI knowledge and application for prosperity and well-being, while upholding Dutch and European norms and values. This is done by connecting traditional defence companies like Thales, IBM, and Deloitte for instance, in innovative ecosystems together with newer start- and scale-ups and universities. The traditional companies provide a solid basis upon which spin-offs and others can build and scale. The Dutch Defence Technological and Industrial Base (NLDTIB) consists of nearly 1000 companies with an annual turnover of €4.7bn. These companies focus on topics such as radar technology (Thales), sensor technology and/or international supply chains.

For the MoD this encompasses being at the forefront of each of the five identified application areas identified in the data strategy. Priorities are synchronized via a roadmap for each application area. The NL AIC acts as a catalyst for AI

applications, with a key goal of achieving impactful AI innovations in at least ten economic and societal sectors within three years. AI is considered a systemic technology that requires an integrated approach involving intensive government involvement, urgency, proactive and comprehensive strategies, stakeholder engagement, and societal debate to determine how AI is deployed for prosperity and well-being.

On behalf of the Ministry of Education, Culture and Science, the Dutch Research Council funded research in the context of the Dutch Research Agenda (NWA) since 2018. This provides the Dutch MoD with the opportunity to invest in research focusing on data science with knowledge partners TNO, NLR and the Maritime Research Institute Netherlands (MARIN), and in knowledge building at universities such as both the technical universities (Delft, Twente, Eindhoven) and others with specific AI mission like Tilburg University's focus on human-centric AI in understanding society. This builds a bridge between fundamental scientific research and applied knowledge building.

The MoD collaborates closely with the industry on various fronts to develop and apply data science and AI. This collaboration extends beyond the broader security domain to include other civilian application areas such as logistics, healthcare, and finance. Since 2021, the Dutch AI Coalition, in conjunction with Netherlands Industries for Defence and Security (NIDV) and TNO, has been providing additional opportunities for collaboration within ecosystems. Many start-ups and scale-ups are involved in a variety of research consortia and technical projects, varying from drone manufacturers to open-source predictive intelligence.

In addition, the Data Science Centre of Excellence (DSCE) was established, based on the cooperation of the Netherlands Defence Academy (NLDA) and the office of the Chief Information Officer (CIO) of the MoD. The aim is to enhance the scientific knowledge of the Academy in the field of data science and AI, by conducting research on data science and AI within the defence domain and developing data science courses for different educational programs. The research agenda will be based on topics that are fundamental for the future Defence organisation on the strategic, tactic and operational level, taking on a multidisciplinary perspective combining insights from the different research clusters of the Netherlands Defence Academy Faculty of Military Sciences. The research agenda will be the foundation for a long-term research and educational agenda. The DSCE will be located within MINDlabs—a participatory ecosystem of Tilburg University, several research labs, and companies—and closely cooperate both with partners within the MoD as well as outside (academic) partners (Ministerie van Defensie 2023b). Defence partners provide cooperation on long term research questions and opportunities for valorisation. Academic partners provide research collaborations as well as opportunities for shared education on data science.

2.2 Defence AI Development

As developments within AI and data science are occurring exponentially fast, the MoD intends to collaborate with EU and NATO partners, knowledge institutions and industry to keep up (Bharadiya 2023). The strategy contributes to a cohesive data and information field by connecting various developments within the organization through an overarching vision. As previously mentioned, the priority lies in developing AI for unmanned autonomous systems (UAS), military decision support and intelligence, logistics and predictive maintenance, business operations, safety, and security. For instance, unmanned autonomous systems are developed from a naval perspective with respect to maritime drones for intelligence, surveillance, and reconnaissance (ISR) missions, at the Army Robotics and Autonomous Systems unit with unmanned small ground vehicles combined with drone swarms, and at the Air Force to support manned-unmanned teaming. Military decision support with data science and AI is developed at all warfare centres (varying from Army, Air Force to Navy) and several data scientific units within organizational support units. Predictive maintenance applications for instance are being developed in collaboration with the knowledge centre smart maintenance and the Royal Netherlands Navy.

The MoD is investing in the development of a federated resilient IT infrastructure in which several networks can be coupled via satellite, wide area, or local networks to ensure connectivity and interoperability, and to ensure data sharing and processing. Simultaneously, it is implementing an ethical framework of norms for algorithms into internal policy. In addition, the DSCE is responsible for education on data science and AI for officers in training, and for academic research in an ecosystem of knowledge institutions and industry.

3 Organising Defence AI

In 2020, the Dutch MoD appointed a dedicated CIO, responsible for all data, IT, and cyber initiatives within the MoD. It recognized that the evolving nature of war, now encompassing digital battlegrounds, demands a focus on data science and cybersecurity. This includes safeguarding the nation and its allies against cyber threats. Traditional defence has expanded to include protecting against cyberattacks and misinformation campaigns, recognising the significance of digital expertise in national security. As state actors exploit virtual means to further their foreign policy goals, adapting to this changing landscape is crucial, and the ability to gather and utilise accurate and timely information is deemed essential for success. The CIO partakes in the Executive Board of the MoD, highlighting the importance of technology expertise in strategic decision-making. The MoD is also prioritising education and training in cybersecurity and data science for its staff, recognising the role of data-centric warfare in shaping future conflicts.

To efficiently organise the goal of the MoD to become a data-driven organization in 2035, several foundational steps are being taken. First, data-driven working will be facilitated across all units of the MoD but implemented in a decentralised fashion. The MoD aims for a model in which units are supported with their data-driven work by use of Defence-wide facilities, provided amongst others by the IT command, in the following three areas: (1) technology and tools to support the process from data analysis to production; (2) specialised knowledge and expertise; and (3) ethical frameworks, guidelines, and clear process steps (governance). To remain innovative, it is important that data initiatives are carried out bottom-up within the respective Defence units and coordinated across the services by the decentralised CIOs of the respective service. Involving the workforce and utilising domain-specific knowledge ensures that initiatives align with requirements of the specific units and by doing this contributes to Defence-wide data knowledge.

The second organisational step is to have all data management appropriately organized. In addition to technological capabilities, well-defined data management is a crucial prerequisite for achieving the ambitions of the MoD. Improving data quality and ensuring "one single version of the truth" are crucial for optimal data utilisation and the implementation of reliable data products (Dragt 2020). This is achieved in a federated structure where the central CIO provides the foundation upon which the decentralised CIOs of the services build using one generic platform. Access to data sources with associated concepts and definitions must be uniformly regulated and provided by the central CIO and coordinated by the decentralised service level CIOs. There will be agreements on data and algorithm ownership and responsibilities, as well as rules and conditions for using (aggregated) data sources in a Defence-wide or decentralised analytical environment. These agreements are risk-based (complex datasets using complex algorithms being highest risk). The quality of data largely determines the quality of data products and is therefore an essential part of data management.

The third organisational step is to invest in knowledge and expertise. To keep advancing in the realm of new technology and data, it is important that Defence invests broadly in knowledge and expertise (Hartmann and Henkel 2020). This is done by utilising existing knowledge and experience optimally. For instance, researchers at the NLDA that conduct research in the domain of data science and AI are connected through the newly created DSCE tasked with research but also education to increase the awareness and knowledge on this topic within the MoD. Different Defence units are at different maturity levels with respect to data science and AI. The lessons learned and experiences of those that are more mature can be used as growth nuclei to professionalise and scale through knowledge sharing. The DSCE is set up to become the main hub on education and research on data science and AI for the MoD.

The final adjustment to the organisation of the MoD is to evaluate and optimise decision processes and protocols. To use modern data technology, work and decision-making processes must be scrutinised if a significant increase in relevant data for decision-making is expected. This involves the creation of hybrid

man-machine teams and integrating data-based decision-making into existing or new protocols.

It is necessary to look beyond the impact of adopting new data and technology. Business and military operations must become aligned with data-driven work. This requires the adaptation of existing doctrines which can only be done step by step, by continuously improving military training, and changing business operations and workflows based on lessons learned on specific cases. One approach in this regard is to involve researchers from the DSCE as advisors in the doctrine formulation process and associated projects. This is done by active collaboration between researchers from the DSCE and the specific warfare centre of the relevant operational commands.

4 Funding Defence AI

Unclassified details regarding budget and spending of the MoD show that since 2020, Defence has established a material budget fund of approximately €66bn for the next 15 years. This enables the MoD to better plan its expenses, including the management and maintenance of investments such as infrastructure. As a result, Defence is investing in a high-quality, future-proof military and defence organisation.

In the previous years, the Netherlands was one of the countries of NATO that had the lowest spending of its MoD in research and technology development. However, for 2023, the Dutch government has increased its defence budget by 40% relative to the 2022 budget and approved an additional €5bn in budget for the MoD on a structural basis (Ministry of Defence 2022). This will mean that the Netherlands will meet the NATO's 2% of GDP standard by 2024 and 2025. However, investments in data science and AI are still limited compared to those of the US and China (Roberts et al. 2021).

Various measures described in the Defence Industry Strategy (DIS) will be intensified in the following years by €252M. The DIS describes the base of what is needed in the interest of national security and is another initiative to improve the technological striking power of the MoD and help transforming the armed forces. With an increased budget, the MoD will, for example, further invest in Research & Technology and in so-called short-cycle innovation, thereby strengthening ecosystems relevant to the MoD. In addition, the Netherlands will invest €56M into the NATO Innovation Fund that is being created for technology development using start-ups and scale-ups.

Specifically focusing on AI, a long-term program called AiNed, set up by the Netherlands AI Coalition, aims to strengthen the AI-position of the Netherlands. The program focuses on large-scale projects that tackle bottlenecks to enable AI opportunities. The National Growth Fund of the Dutch government has allocated €204.5M to the AiNed program 2021–2027. The National Growth Fund aims to allocate a total of €20bn for the period 2021–2025 to projects that focus on

knowledge development and research, development, and innovation, since these two fields have the highest potential for economic growth (Rijksoverheid Undated).

5 Fielding and Operating Defence AI

The Dutch MoD has been actively prototyping, fielding, and operating defence applications of AI. AI technologies are very promising, but the MoD is cautious in fielding them. Awareness of the dangers is important, and AI should be used responsibly. The MoD wants to act in line with international humanitarian law, and closely follows international developments around AI legislation. In addition, data requirements and data processing aspects are explicitly considered in the procurement processes of future weapon platforms and systems to ensure access to data and compliance with standards. Certification is considered on a per technology basis, depending on procurement requirements or other guidelines adopted for internally developed technology.

There is a limited amount of Defence AI projects being fielded and used that can be shared. As the second international partner to receive the F-35, the MoD is increasing its knowledge on the use of AI in modern weapon systems by actively engaging with the supplier. Most defence AI projects are still being researched and/or under development. We describe three distinct examples of defence AI that are currently actively being fielded and operated by the MoD below.

5.1 DataLab

In June 2021, the Datalab was officially launched within the IT-support command of the MoD. The Data Lab is intrinsically motivated to contribute to the peace and security of the society daily. Everything DataLab is therefore aimed at, is making the Dutch MoD a global leader in the performance of its main tasks. Since DataLab sees a crucial role for data science and AI in a highly diverse range of problems, the lab plays a leading role across the MoD to unlock that potential. To achieve this, the work of DataLab consists of four main processes:

- With its innovation process, DataLab identifies the challenges of tomorrow and the solutions for them in a structured manner.
- DataLab operationalises promising innovations in such a way that their contribution to the main tasks of Defence is made tangible.
- Datalab enables the Defence-wide development and production of applications by making tooling, standards and a secure and managed LGI platform (Defence Wide Data Development and Analysis Platform, DBDAAP) available.

- As a network organiser, DataLab facilitates and encourages a knowledge sharing and connection process across the Defence organisation to accelerate the development of meaningful applications.

Against this background, DataLab works on enterprise defence AI and AI for military use as the following two projects illustrate:

- *MLOps (enterprise defence AI)*

The MoD experiences a surge in machine learning (ML) demand amidst limited resources. Addressing this challenge hinges on efficiency. One way to achieve this is by adopting the MLOps process, which ensures that Data Science operations are transparent, reproducible, and meet stringent quality standards. Proper governance of the respective Data Science environment is essential, and these factors are key in achieving it. Through the introduction of a dedicated MLOps tool, the DataLab provides both low-code and high-code environments to the Data Science community. This tool empowers a greater number of users to engage in Data Science and participate effectively in the MLOps process.

- *Submarine detection with multispectral satellite images (AI for the military use of defence)*

This project focuses on investigating the possibilities of developing an improved detection method for submarines (as well as other objects and troop build-ups) using multispectral satellite images. For this purpose, a multispectral dataset is combined with ML image recognition algorithms.

5.2 The Robotics and Autonomous Systems Unit

The Dutch MoD has a Concept Development and Experimentation program on Robotic and Autonomous Systems (RAS) with the purpose of identifying the best combination of organisation, concept of operations, and unmanned systems to increase the combat power of land units and increase the protection of soldiers. Its unit is a subunit of the Dutch Army, with the following key topics: combat unmanned ground systems, swarming unmanned aerial systems, and autonomy.

Autonomy in unmanned systems is defined in various ways, for instance as the ability to execute ordered tasks within the set constraints and conditions and with delegated levels of decision-making authority (Antsaklis 2020). Automating functions such as navigation decreases the cognitive and physical burden of the human operators. Autonomy in unmanned systems is necessary to ensure the continuation of task execution when the datalink between the operator and the unmanned system is jammed or unavailable. Autonomy also facilitates upscaling to many unmanned systems performing ordered tasks that are supervised by a few humans. Maintaining meaningful human control over unmanned systems with autonomy is an essential element of the Dutch Army policy.

The RAS program started with the first practical experiments with the Milrem THeMIS and Rheinmetall Mission Master Unmanned Ground Vehicles (UGVs) in 2019 and deployed an infantry platoon with military qualified combat unmanned ground vehicles to Lithuania as part of NATO's enhanced forward presence mission to conduct further experimentation, validate the concept of operations and identify the process for operationalisation of innovation. The RAS program combines applied research, conceptual thinking, and practical experimentation in close connection with the operational 13th Light Brigade. Their unmanned systems provide the opportunity to increase the combat power of military units. The development and integration of AI functions increases the capabilities of the unmanned systems.

The two main intelligent functions are autonomous movement and aided target recognition. The development of autonomous movement includes global and tactical route planning, local path planning, obstacle detection and avoidance, and dynamic route re-planning on the UGV. Aided target recognition includes object detection and classification by computer vision algorithms, target tracking and reporting, and target environment assessment. The development of autonomy also encompasses tactical planning by an automated intelligent planner, plan visualization and course of action comparison and monitoring and dynamic plan adjustment during execution.

5.3 Deep Vision

By utilising advanced algorithms and ML techniques, the Royal Netherlands Marechaussee (RNLM) can process information more rapidly and accurately, enabling proactive measures against criminal activities. These criminal activities range from cross-border human smuggling or attacks on V.I.P.'s, both in the Netherlands and abroad. This strengthens the capabilities to secure the Kingdom of the Netherlands.

The Deep Vision team of the RNLM experiments with new technology in the field of sensing, robotics, large language models and other types of AI, and 3D-printing. The aim is to gain knowledge, to explore how innovative technology can facilitate the daily operations of the RNLM, and to provide insight into long-term implications of emerging technologies for the RNLM.

Developing in-house AI capabilities guarantees an independent position of the RNLM (and the MoD in general) in relation to commercial tech-suppliers and other partners. This ensures flexible and interoperable AI-deployment within the RNLM. In addition, given the possible ethical complications around the deployment of AI, it is essential for the RNLM to thoroughly understand both the benefits and the pitfalls of new technology. Therefore, it is crucial for the RNLM to not solely concentrate on the advantages of emerging technologies but also proactively anticipate potential adverse consequences. Close collaboration with other (inter) national Defence components and partners within the security domain (such as the Dutch Police) is essential for the exchange of technical knowledge and skills to

further develop AI-capabilities within this domain. The RNLM also collaborates with several high-tech universities, research institutes and tech companies to experiment with the most advanced AI and data science technology of the present day.

6 Training for Defence AI

The digital transformation and increasing datafication have a great impact on the work of military personnel and civilians (Mattila 2022). Therefore, one of the main points of attention of the MoD is having high-quality AI knowledge and skills. (New) training courses focusing on technology, the effects for military deployment, and associated legal and ethical dilemmas increase knowledge and insights among employees at all levels of the MoD.

For example, one expert group affiliated with the MoD develops simulation-based training using AI as a player in the simulation is the Royal Netherlands Aerospace Centre (Royal NLR). Royal NLR develops training and simulation programs for military forces and other clients. Their goal is to make training more effective and efficient by using integration and interoperability of live, virtual, and constructive elements. One example of such a training are tactical simulators for fighter pilots in which AI is used to increase the intelligence of the behaviour of opposing forces (OPFOR).

TNO's Defence, Safety, and Security unit runs several labs across the country and is focusing on innovation for defence and national security with an emphasis on combating crime, catastrophes, and terrorism. The involvement of this unit covers a range of activities: military operations, military equipment, command & control, and operational decision making, threat protection, and instruction and training. Among other TNO Defence focuses on enhancing the effectiveness and efficiency of armed forces by studying human factors, optimizing training through simulations, and experimenting with new security concepts and equipment. They also specialize in improving human-machine collaboration.

The unit focusses on four areas (TNO Undated):

- Operations and human factors, by supporting the Dutch armed forces with innovative analysis and evaluation methods, models, and the latest simulation technologies. Involved in the ELSAlab defence.
- Information and security systems, by devising and developing technology for an effective management of the military organisation and the deployment of resources.
- National safety, by focusing on five main themes: Resilient professionals, Smart security & surveillance, Intelligence in action, Rule of law & investigation, and Critical digital infrastructure.
- Protection, munitions, and weapons, by offering innovations for civil and military forces, from effective strategy through material innovation to weapon and system testing.

In the pursuit of secure and dependable Data Science and AI applications, the MoD collaborates closely with the private sector as mentioned before. One such example is their partnership with the Dutch AI Coalition (NL AIC), a "public-private collaboration involving governmental bodies, businesses, educational and research institutions, as well as civil society organizations, aimed at expediting and fostering AI advancements and initiatives" (NL AIC Undated).

The MoD also develops knowledge and skills from within by working together with the Defence Academy (NLDA), thereby strengthening the link between scientific research and defence practice. The NLDA is unique in the Netherlands as it combines (maritime) military education, university-level education, and personal development. Knowledge and skills in the field of data science and AI are being integrated in military training courses of the NLDA and in continuing training both for civilian and military employees of the MoD. Some examples of training focusing on data and AI at the NLDA includes the masterclass Cyber & Data Science and the "Data" course, which educates participants on data & ethics, data & military decisions, and data & intelligence. In addition, there is a "Data" module at the Open Defence Academy. This online module is about data and its importance for defence, where concepts such as algorithms, data science, and AI are discussed.

Furthermore, different research, education and training initiatives aim at increasing knowledge and skills regarding data science and AI within the MoD. Representative examples include the Data Science in Military Operations Chair at the Faculty of Military Sciences of the MoD in conjunction with the endowed chair in Data Science, Safety, and Security at the Tilburg University in the Netherlands, and the DSCE, which is headed by Chair of the Data Science in Military Operations group (Ministerie van Defensie 2023b).

These chairs contribute to the advancement of data science in the military and security domain. Research of the chair is conducted against the backdrop of a changing world with significant implications of the use of AI and digitization. It focuses on ethical algorithm development and aspects of the use of AI in the security domain, algorithms to support (military) decision-making, and intelligence and cyber security.

The DSCE develops data science courses for different educational programs of NLDA. The research agenda will centre around essential themes crucial for the future of the Defence organisation, spanning strategic, tactical, and operational levels. This approach adopts a multidisciplinary perspective, integrating insights from various research clusters within the Netherlands Defence Academy Faculty of Military Sciences.

7 Conclusion

This chapter provides an overview of the Dutch MoD's approach to AI by highlighting the strategic vision for 2035, the strategic knowledge- and innovation calendar 2021–2025, the Data Science and AI strategy for 2022–2027, and the commitment

to ethical considerations in the development and deployment of defence AI. The Dutch MoD recognizes the pivotal role of AI and data science in safeguarding the Dutch Kingdom and has set three key ambitions: technological advancement, information-centric operations, and becoming a reliable partner and protector. These ambitions align with the commitment to invest at least 2% of expenses of the Defence budget in research and technology development.

Data-driven decision-making and responsible AI use are important for the Dutch MoD, as demonstrated through the creation of ELSA Labs and the hosting of the REAIM 2023 summit on responsible AI in the Military Domain. In terms of developing defence AI, the Dutch MoD is actively engaged in collaborating with EU and NATO partners, knowledge institutions, and industry across various domains, including unmanned autonomous systems, military decision support, logistics, business operations, and security. It is also investing in IT infrastructure, ethical frameworks, and education to ensure responsible AI development and deployment.

The organization of defence AI within the MoD includes steps to facilitate data-driven work, improve data management, invest in knowledge and expertise, and optimise decision processes. The report highlights the practical fielding and operation of defence AI, with a focus on responsible use and adherence to international humanitarian law. It provides insights into specific projects, such as the DataLab, the Robotic and Autonomous Systems, and showcases the Deep Vision team's efforts to utilize AI and data science for national security.

Training for defence AI is a critical aspect, with various educational initiatives aimed at equipping personnel at all levels with the necessary knowledge and skills to navigate the evolving landscape of AI and data science. Overall, this report underscores the Dutch MoD's dedication to adopting AI responsibly while prioritizing national security and defence. It demonstrates a commitment to research, development, collaboration, and ethical principles, positioning the Netherlands as a leader in the responsible use of AI in the military domain.

Some of the challenges that lie ahead emerge from the fact that AI technologies, public sector innovation, and legal and regulatory developments do not evolve in tandem. Innovative techniques to mitigate biases inherent in AI systems are being developed. The increasing intensity of working with machines requires optimal human-machine teaming, interfaces, and processes. Finally, strategic alignment across (inter)national partners is required to guarantee long-term sustainability of current and upcoming AI systems, as they need continuous updates, maintenance, and improvement. Investments into these systems should optimally align with defence strategies and priorities.

References

Alfrink, Kars, et al. 2022. Contestable AI by Design: Towards a Framework. *Minds and Machines*: 1–27.

Antsaklis, Panos. 2020. Autonomy and Metrics of Autonomy. *Annual Reviews in Control* 49: 15–26.

Bharadiya, Jasmin Praful. 2023. A Comparative Study of Business Intelligence and Artificial Intelligence with Big Data Analytics. *American Journal of Artificial Intelligence* 7 (1): 24.

Dragt, David. 2020. *Van exploratie naar realisatie: Implementatiefactoren voor de adaptieve krijgsmacht bij Defensie*. Integratie. Thesis EUR.

Government of the Netherlands. Undated. *REAM 2023 Program*. https://reaim2023.org/. Accessed 30 January 2024.

Hartmann, Philipp, and Joachim Henkel. 2020. The Rise of Corporate Science in AI: Data as a Strategic Resource. *Academy of Management Discoveries* 6 (3): 359–381.

Mattila, Juha Kai. 2022. Governance of Digital Transformation: As Observed in Two Cases of Military Transformations. In *ECMLG 2022 18th European Conference on Management, Leadership and Governance*. Academic Conferences and Publishing Limited.

Ministerie van Defensie. 2020a. *Hoe moet de Nederlandse defensie er in de toekomst uitzien?* Den Haag: Ministerie van Defensie.

———. 2020b. *Defensievisie 2035: Vechten voor een veilige toekomst*. Ministerie van Defensie. https://open.overheid.nl/repository/ronl-cf4bd18b-15e0-4eff-9803-ca88a86e1122/1/pdf/defensievisie-2035-vechten-voor-een-veilige-toekomst.pdf. Accessed 30 January 2024.

———. 2020c. *Strategische Kennis en Innovatie Agenda 2021-2025*. Ministerie van Defensie. https://open.overheid.nl/repository/ronl-52ed0fc2-bddf-4792-9b95-6b13ac087e95/1/pdf/strategische-kennis-en-innovatieagenda-2021-2025.pdf. Accessed 30 January 2024.

———. 2023a. *Defensie Strategie Datascience en AI 2023-2027 - Werken aan een Slimme Krijgsmacht*. Ministerie van Defensie. https://www.rijksoverheid.nl/documenten/rapporten/2023/05/31/defensie-strategie-data-science-en-artificiele-intelligentie-2023-2027. Accessed 30 January 2024.

———. 2023b. *Lindelauf benoemd tot hoogleraar op het gebied van data science en kunstmatige intelligentie*. https://www.defensie.nl/actueel/nieuws/2023/07/01/lindelauf-benoemd-tot-hoogleraar-op-het-gebied-van-data-science-en-kunstmatige-intelligentie. Accessed 30 January 2024.

Ministry of Defence. 2022. *Additional EUR5 Billion in Defence Spending on a Structural Basis*. https://english.defensie.nl/latest/news/2022/05/20/additional-eur-5-billion-in-defence-spending-on-a-structural-basis. Accessed 30 January 2024.

———. Undated. *Netherlands Defence Academy*. https://english.defensie.nl/topics/netherlands-defence-academy. Accessed 30 January 2024.

NATO. 2022. *NATO's Data and Artificial Intelligence Review Board. Summary of the Establishment of the Board*. https://www.nato.int/cps/en/natohq/official_texts_208374.htm. Accessed 30 January 2024.

NL AIC. Undated. *NL AI Coalitie*. https://nlaic.com/. Accessed 16 January 2024.

Reynolds, Nick. 2020. Performing Information Manoeuvre Through Persistent Engagement. *RUSI Occasional Papers*: 19–26.

Rijksoverheid. Undated. *The National Growth Fund*. https://www.nationaalgroeifonds.nl/english/the-national-growth-fund. Accessed 30 January 2024.

Roberts, Huw, et al. 2021. The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation. *AI & Society* 36: 59–77. https://link.springer.com/article/10.1007/s00146-020-00992-2. Accessed 30 January 2024.

TNO. Undated. *Defence, Safety, and Security*. https://www.tno.nl/en/about-tno/organisation/units/defence-safety-security. Accessed 30 January 2024.

Townsend, Stephen J. 2018. Accelerating Multi-Domain Operations Evolution of an Idea. *Military Review*: 4–7. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-18/Townsend-Multi-Domain.pdf. Accessed 30 January 2024.

A Winding Road Before Scaling-Up? Defense AI in France

Kévin Martin and Lucie Liversain

The French Armed Forces treat artificial intelligence (AI) as a disruptive innovation. AI influences belligerents' behavior by accelerating operational pace across multiple domains, thereby creating a combat environment of several simultaneous confrontations. Since the mid-2010s, AI development is progressing more rapidly thanks to advances in deep neural networks, distributed computing, and increased computing capacity.

France recognized the importance of AI in 2017 when it launched a national strategy to become a world leader in AI. The French Ministry of the Armed Forces published the strategy "AI in service of defense" in 2019, outlining ethical frameworks, infrastructure development, research priorities, and international collaboration. This strategy aimed to create trustworthy AI for defense applications while also embracing dual-use advances on AI in the commercial sector.

The first phase of this strategy saw the construction of a sovereign AI ecosystem focused on research and innovation. This ecosystem established connections between the French Ministry of the Armed Forces, research institutions (INRIA, CEA, CNRS, etc.), traditional defense prime contractors (Thales, Airbus, Dassault Aviation, Safran, MBDA, Naval Group, Nexter/KNDS) and non-traditional defense contractors such AI ventures and SMEs. The second phase, launched in 2022, currently focuses on accelerating AI's integration into key application areas such as decision support, collaborative combat, cybersecurity, logistics, intelligence, and robotics.

France's major procurement efforts, AI studies and research (such as the ARTEMIS.IA Program) are earmarked with an average budget of €100M/year.

K. Martin (✉)
Fondation pour la Recherche Stratégique, Paris, France
e-mail: k.martin@frstrategie.org

L. Liversain
Management Research Center, Ecole Polytechnique (I3-CRG*), Paris, France
e-mail: lucie.liversain@polytechnique.edu

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_11

These initiatives seek to harness AI for massive data processing and build a sovereign solution for operational data. But these efforts have faced challenges in integrating non-traditional defense players, aligning timeframes, and addressing varying levels of end-user maturity.

The Armed Forces Ministry is particularly conscious of the ethical and legal issues that may be raised by AI in defense applications. A permanent multidisciplinary ethics committee has been established at the ministry level for emerging technologies in defense. It has already published reports on the use of AI in critical systems.

The French Armed Forces have undertaken various initiatives to integrate and operationalize AI technologies through experimentation. These initiatives aim to help gain operational efficiency and performance, as well as support future organizational change. They explore the challenges of integrating AI on the battlefield, along with accelerating innovation through experimental labs, and co-innovation projects between startups and end-users. Nevertheless, one of the major obstacles to the operationalization of AI in the Armed Forces is the human resource challenge: the ability to attract and retain sufficient AI talent.

Considering the current state of the French defense AI ecosystem, it is possible to imagine several avenues of improvement. These could include supporting efforts to raise awareness for AI investments within defense programs, increasing funding capacities to scale up AI development and a higher R&T budget to fund defense applications of emerging civilian technologies. Finally, it would be possible to facilitate agile co-development between the Armed Forces and industry to build solutions rapidly in response to use cases.

1 Thinking About Defense AI

1.1 A National Strategic Vision Including Defense

The development of AI accelerated worldwide in the mid-2010s, mainly due to related advances in deep neural networks, optimized distributed computing, and the increase in available computing capacity. This new wave of technology has seen the deployment of the first commercial solutions by major digital players, particularly from the United States. Questions related to its impact on the evolution of digital value chains and on the growth of the sector's economic weight have led many countries to reflect on the issue.

France is no exception. French authorities already fully embraced the topic of AI in 2017, launching #FranceIA. One year later, the report "For a meaningful artificial intelligence: towards a French and European strategy" was published (Villani 2018). Using the report as a basis, French President Emmanuel Macron announced the launch of a dedicated national strategy, aimed at making France (and Europe) a leader in AI (Elysée 2018). The strategy primarily focused on France's research

sector, one of France's main strengths and considered to be among the global benchmarks in the field.

While emphasizing research, the preparatory report for the national strategy clearly identified defense as one of the sectors in which the development and deployment of AI should play a key role. "AI in support of Defense," (DGA 2019) constitutes the strategy of the Ministry of the Armed Forces (henceforth the French MoD) for AI, providing an ambitious roadmap around six themes:

- Establish a robust ethical and legal framework for the use of AI
- Develop the infrastructure needed to deploy AI
- Define priority research areas
- Establish an AI governance framework
- Innovation, Research and Development Strategy
- International collaboration and export strategy

In addition, the strategy set out the broad outlines of a ministerial policy in this area, based on three pillars:

- *Governance*

Formalization of a strategic-level departmental data policy, organization and distribution of data-related responsibilities, management of roadmaps.

- *Architecture*

Adoption of specific solutions adapted to the constraints of the Armed Forces in the context of data storage, collection, processing, and exploitation.

- *Culture*

Continuous and/or specific training in the use of AI and its challenges, recruitment of specialized personnel.

Finally, the key objective of this strategy is to develop trusted AI that meets the unique and strict requirements of the defense world.

1.2 The Challenges of Defense AI

The rise of AI not only accelerates defense developments, but it also takes place against the backdrop of intense global competition. The French Armed Forces do not wish to miss out on developments in AI that primarily derive from the commercial sector. As a result, the French Armed Forces dedicated efforts to define a strategy adapted to the constraints and specificities of the defense sector. This strategy is based on two main lines of effort: Integrating new technologies, mainly from the civilian sector, and adapting doctrines and operational concepts to the issues raised by automation, with particular attention to issues of command responsibility.

1.2.1 A Defense AI Strategy Geared Towards Interaction with the Civilian World

The work on defense AI is part of a global review of the French MoD's strategy, aimed at adapting its structure to the accelerating technological cycles coming from the civilian world. Here the focus is on digital technologies (cybersecurity, cloud computing, AI, semiconductors, quantum computing, etc.), as well robotics, energy, and many others.

Digital innovation, including AI, is enabling spin-in technology transfers, i.e., the capture of innovations developed in a civilian context for integration into a defense system. This is a major paradigm shift after a long period in which spin-out transfers tended to benefit national economies (GPS, radar, etc.). Consequently, the French General Directorate for Armament (DGA), which constitutes France's defense planning and procurement authority, set up the new Defense Innovation Agency (AID) in September 2018. AID's mission is four-fold:

- Lead and drive defense innovation
- Stimulate and capture innovation from the non-defense civilian world
- Improve, transfer and accelerate innovation for the benefit of the Department's users and warfighters
- Identify and implement an innovation approach to prevent strategic surprise

AI is naturally one of the agency's technological priorities.

1.2.2 Adapting AI to Defense Constraints

While opening to the civilian world seems inevitable, the establishment of a cognitive framework adapted to the requirements of the defense sector remains paramount. This is particularly vital given that while there are many opportunities for the use of AI applications in defense, their level of integration and maturity remains highly variable.

Elementary applications such as automatic classification and object recognition, that have matured in the civilian world, are now fully integrated into the military domain. However, this is not always true for "functional" or even "system"-level applications. The latter are still at an early stage of technological maturity (e.g., autonomous robots capable of sensing and performing multiple tasks in an uncertain environment).

The timing of technological developments is also tied to the changing nature of conflicts. The move towards high-intensity conflict, with battlefield robotization, AI integration, data/sensor fusion, and the quest to saturate the battlefield through mass effect, have all guided defense technology development in recent years. This applies both to the launch of the latest major multi-application projects as well as to programs started prior to the launch of the defense AI strategy.

These initial efforts and development projects served as a keystone for a national AI defense strategy. Several key success factors were identified:

- The need to increase the maturity and robustness of technologies for critical applications.
- The availability and accessibility of data needed to explore use cases.
- Infrastructure for AI development, such as clouds. As cloud outsourcing presents a risk to the confidentiality, integrity and availability of data, sovereign combat cloud projects are underway within the French Armed Forces, such as within the new generations of air (SCAF/FCAS) and land (SCORPION) programs. Additionally, the digital transformation of the Armed Forces follows a process launched several years ago and formalized in 2017 with the publication of the strategic document "Ambition Numérique for Digital Ambitions" by the French MoD (Bômont 2021).
- The ability to adapt the workforce (recruitment, profile) of the defense ecosystem to not only develop innovative AI-based solutions, but also to debate and measure needs—both with the defense prime contractors for implementation and integration as well as within the Ministry for specification and deployment.

1.2.3 A Clear and Legal Framework to Develop Defense AI

AI raises unique issues when used in defense. Unlike most civilian applications (with a few exceptions, such as health), the use of AI in defense systems requires a particularly rigorous processes to ensure necessary reliability. It also raises questions about responsibility and its division between humans and machines. However, the former French defense minister's speech is very clear about the framework for the development of AI-related technologies:

> We will develop artificial intelligence for defense according to three main principles: respect for international law, the maintenance of sufficient human control, and the permanence of command responsibility (Parly 2019).

Precautions on ethics have been taken from the start, even if they are state-centric and did not come out of a broader social debate. As far as autonomy is concerned, the minister stated in the same speech that "France refuses to entrust the decision of life or death to a machine, a machine that acts in a completely autonomous manner and is beyond any human control." It reaffirms the need for human control in all weapon systems to be developed in the future. This position has been codified through Instruction 1618 on the implementation of programs (Legifrance 2019) and is also supported by the creation of a ministerial ethics committee on defense issues in 2020. The Ethics Committee is made up of 18 members of the Armed Forces as well as external experts. These external experts include a wide range of professions such as lawyers, professors, and researchers. The ethics committee issues advice while ensuring that the red line—"keep the human element in the loop and do not influence the leader's decision"—is respected.

According to the reports of this committee, the degree of autonomy of an AI-integrated system can only be determined by considering several inseparable dimensions: the design, the deployment, and the use of weapon systems. This is

even more important given the length of the operational life cycle of the equipment, which spans a decade for the most agile systems and several decades for the heaviest equipment. Questions about deployment and doctrine arise more frequently in the development loop due to a goal of accelerating digital procurement programs.

The Ethics Committee further added that the design phase requires in-depth reflection on the future use of the system and its rules of engagement. This allows planners and operators to determine the tasks that will be entrusted to AI and the degree of autonomy it will have to perform. As with vehicles and their level of autonomy, this is not a binary characteristic, but a continuum that needs to be quantified according to progressive levels. The definition and relevance of such a scale in defense has not yet been fully debated, but the need is certain to arise.

2 Developing Defense AI

Following Villani's work and the President's speech, France has adopted a national AI research strategy and corresponding funding plan. This strategy is managed by a national coordinator and is part of the management of credits from the "Investment for the Future Program" (PIA) and "France 2030" by the General Secretary for Investment (SGPI). The primary objective of France's AI strategy at the time was to avoid falling behind scientifically. As a result, the investments made were initially (2018–2022) concentrated on research and innovation, with a total investment of €1.5bn (Cour des Comptes 2023).

The second phase of the national AI strategy (France 2030 2021) was launched mid-2022, with the aim of accelerating the diffusion of AI in the economy and arranging it so that AI can meet the need to automate ancillary tasks. To achieve this, the acceleration strategy is based on investment to support the deep tech of embedded AI, trusted AI, and frugal AI. The aim is to remove certain scientific hurdles on decentralized or embedded AI. A prominent example is energy-efficient hardware for data processing with AI models at the near-edge with a high-level of trust on high-risk applications.

2.1 France's AI Innovation Base

France benefits from a relatively dense academic and research base (Ezratty 2021) including institutions such as the National Institute for Research in Digital Science and Technology (INRIA), the French Alternative Energies and Atomic Energy Commission (CEA) or the National Center for Scientific Research (CNRS). Since AI is not considered a discipline, the research component of the French national strategy launched in 2018 has focused on structuring the ecosystem with the creation of AI centers of excellence, through the designation of interdisciplinary AI institutes (3IA), the establishment of individual chairs (43), as well as the

identification of centers of excellence outside the 3IA institutes. Cooperation in AI research not only takes place through research projects with public research institutes, but also with universities and engineering schools.

According to Bpifrance, there are almost 470 French startups specialized in AI. In 2020, the Ministry of Defense reported that around 100 SMEs and AI startups were involved in French MoD projects (Parly 2021). 223 deep-tech AI startups have raised a cumulative €3.7bn between 2017 and mid-2022 through 391 funding rounds, including €2.3bn in 2021 (Cour des Comptes 2023). Despite this, lack of access to this type of investment for French startups, especially those dedicated to AI, is regularly seen as a hurdle, especially at later project stages (late stage and IPO) (FRS 2020). However, measures have been taken to encourage innovative players to emerge, for example, by creating Definvest and Fonds Innovation Défense (FID). Since its creation, Definvest has made 18 investments, including Kalray and Preligens, while FID has made seven public investments (including Outsight and XXII). In both cases, the objective is to invest alongside private funds (Ouest France 2023).

SME's specializing in AI involved in defense programs are mostly spinoffs from French research laboratories like CEA or INRIA. The respective network of French AI startups and SMEs covers all the different technological segments of AI: AI hardware, language processing, data mining systems, voice processing, image processing and data from 3D sensors, right through to autonomy for robotics. The following examples illustrate these capabilities:

- Kalray (founded in 2008) and NanoXplore (2010), for example, specialize in the development of FPGA processors and SoCs.
- Outsight (2019) develops software for LIDAR data analysis.
- XXII (2015) offers a software platform for AI video analysis.
- Numalis (2015) provides tools and services to help design and validate artificial intelligence systems.
- Bloom (2016) develops algorithms for social network investigation.
- Delfox (2018) develops a platform to train AI models to train autonomous decision-making systems.
- Shark Robotics (2016) has rapidly become a key player in the French robotics sector and a benchmark internationally, developing software, hardware and batteries.
- Chapsvision (2019) has established itself as a consolidator in the sector through a highly ambitious external growth policy (more than a dozen company acquisitions in 4 years).

In addition, SME's established in the early 2000s are noteworthy as well. Among them there are, for example, Vocapia Research, a provider of speech-to-text software, and Probayes, specialized in R&D and custom AI engineering. These defense and non-defense SMEs are integrated into the French defense industrial ecosystem, either as partners of French prime contractors or as direct suppliers to the French MoD.

2.2 Adaptation of France's Traditional Defense Players

The reconfiguration of the IT value chain resulting from digital technological developments is leading digital players (majors, software publishers, digital services companies) to capture an increasing share of the added value generated by companies operating in so-called "traditional" business sectors. Defense is no exception as several civilian and specialized digital players are determined to penetrate the defense market. Atos and Sopra-Steria, for example, are involved to varying degrees in the French Ministry of Defense's ARTEMIS.IA program. In 2022, Preligens, created in 2016, had been awarded a 7-year (premium) framework contract by the DGA worth €240M for data processing solutions tailored to defense requirements (DGA 2022).

In response, traditional defense prime contractors have adapted their strategies to consider the changes brought on by digital technologies (cyber, cloud computing, AI, etc.). Most of these companies' digital transformation plans, which date back to the mid-2010s, include action plans or roadmaps for AI and data governance. However, these specific actions appear to be more recent and coincide with national strategies.

While the strategy of external growth seems to have been favored by defense actors with the first wave of digital technologies related to cybersecurity, current approaches emphasize partnerships and initiatives related to open innovation (Martin 2022). To implement a partnership policy, almost all prime contractors have developed corporate venture-type structures or increased their presence within specialized incubators and accelerators. However, there are subtle differences between the different strategies applied by incumbent defense companies:

- Thales is developing its partnership approach with specialized private sector players (start-ups and young SMEs) to ensure long-term collaboration (i.e., move from a prime contractor-subcontractor relationship to a partner relationship). The group has a presence in France at Station F (Cyber) and in Montreal through the Centech incubator (AI). Thales seems to make less use of its corporate venture arm, which is mainly used for strategic actions.
- Airbus Defense & Space has also adopted this approach and has diversified its support mechanisms for its partners, focusing on acquisitions (simplified procedures for subcontractors such as start-ups and SMEs), open innovation (more challenges) and its Airbus Group Development structure (support for actors around the Group's various industrial sites).
- Safran Group uses a lot its corporate venture, which has allowed it to invest in numerous start-ups in the sector (Outsight, Kalray, for example).
- The situation is different for Dassault Aviation. The company benefits from the positioning of Dassault Systèmes (same shareholder, GIMD), France's leading software publisher (2022 revenue €5.67bn), whose offering is based on the 3D experience platform (modeling-simulation) and, more recently, on the development of a trusted cloud offering (Outscale).

Finally, France's "pure defense players" MBDA, Nexter (KNDS Company) and Naval Group lack synergies stemming from comparable civilian activities. They also seem to suffer from different issues related to data management—such as data access or data storage –, which could be detrimental to their defense AI ambitions. As a result, they might interpret defense AI as a niche task only. However, different specialization strategies are taking place:

- In 2017, for example, the European missile maker MBDA adapted its innovation structure by setting up a "Tech Watch" service to provide technology monitoring.
- Like other pure defense players, Naval Group opened its innovation structure and system in 2015 with the creation of its disruptive innovation accelerator, the Naval Group Innovation Booster. Like MBDA or Nexter (KNDS Company), Naval Group seems to be positioning itself around very specific AI technologies.
- Finally, Nexter (KNDS company) has also reviewed its digital transformation strategy with the creation of a digital innovation and transformation department in June 2018 (FOB 2020). Within this framework, predictive maintenance, local and global navigation without GPS, and decision support seem to be priority development areas for the group (Ricaud and Jourdas 2019).

Defense groups can also jointly develop an offer that incorporates AI or big data capabilities. This partnership, which is part of a defined industrial and commercial project, can be carried out with major digital players, contributing to the digital transformation of the group and its businesses, or with innovative and specialized players (large groups, mid-caps companies, SME and start-ups), mainly in application segments. Focusing on partnerships with major digital players, for example, the Airbus Group has embarked on a data collection project that will enable it to add new services related to fleet management and predictive maintenance. The result is the new "Skywise" (for civil aircraft platforms) and "Smartforce" (for military aircraft platforms) offerings, both developed in partnership with specialist players such as Palantir and Alten (Airbus 2018).

In addition, as part of the development of a secure cloud offering for Armed Forces and public institutions, European defense contractors have partnered with key players in the field. Thales, for example, has partnered with Google Cloud to position itself in its national public cloud market (Thales 2021). Thales and Microsoft are also partners in the development of a defense cloud solution, "Nexium Defense Cloud" (Thales 2018).

2.3 Defense AI R&D Strategy

In general, the French MoD focuses on AI-related R&D activities that are underfunded by the civilian sector or require a defense-specific approach. Consequently, R&D activities on AI focus on:

- Handling data produced and collected by specific sensors of the Armed Forces such as infrared imaging, Synthetic Aperture Radar (SAR) imaging, sonar, or hyperspectral sensing;
- Using AI for very specific military missions such as intelligence collection/gathering or collaborative combat applications;
- Developing algorithms for specific tasks such as data and information fusion, heterogenous and multi-source data processing, or weak signal detection;
- Ensuring embedded or operational safety challenges stemming, for example, from operating in unknown or even hostile environment.

The development of defense AI also aims to ensure trustworthiness. This requires the formalization of a dedicated methodological framework and a technological base that allows collection, storage, processing, and exploitation of the necessary data. On the technical side, French MoD has published a guide for the integration of AI in operational defense systems. This provides methodological elements for implementation, specification, and qualification (AID 2021). In addition, an initial technology base has been but the architecture to store, collect, process, and operate solutions remains to be defined. Pending the next defense cloud program, ARTEMIS. IA remains the most structured program in this field.

2.4 Priority Application Areas

The development of AI in French defense systems is aimed at solving technical defense challenges (specific sensors, embeddability, frugal learning, explainability) to ensure operational superiority. As with any emerging technology, it brings higher levels of performance to operational systems based on maturity. For example, it is now possible to provide feedback from operational deployments for intelligence applications, while developments in autonomous robotics still require further development.

The French MoD, through its roadmap, has identified seven main use cases for AI in operations (DGA 2019):

- Decision and planning support;
- Collaborative combat;
- Cybersecurity applications and digital influence;
- Logistics and operational readiness;
- Intelligence;
- Robotics and autonomy;
- AI in support services (administration/health).

In view of developing future AI-enabled defense capabilities, the French MoD also emphasizes the need to cooperate with partners. In this regard France acts upon the belief that AI is a technology field ideally suited for multinational cooperation because of its dual use nature. However, French authorities also perceive defense AI

as a critical technology (French MoD 2017). As a consequence, the French AID mainly focuses on collaboration within the European context with partners who have complementary capabilities. This is done in part to compensate for French AI-related shortfalls, or to build critical mass. In this context, Germany and the UK have been identified as suitable partners. Outside of Europe, France is building on its long-standing innovation cooperation with Singapore to extend it to AI work (French MoD 2023).

2.5 ARTEMIS.IA: Ambition and Reality of Building a Defense AI Ecosystem

ARTEMIS.IA emerged in 2017, in a context where there was a strategic need to build a sovereign solution to exploit the mass of operational data from various sensors while facilitating closer ties with the civilian digital ecosystem. The decision to launch a project, which then became a major procurement program in 2019, was in line with the French MoD's AI strategy goal to harmonize understanding of the issues at stake.

The original ambition of ARTEMIS.IA was to provide shared services for the French MoD's massive data processing applications. This was based on the observation that a single industrial player is unable to meet all user requirements in every context. The technical foundation on which the French MoD's data is hosted has specific features not found in the civilian sector. This includes the need to manage data with different levels of classification, which leads to specific restrictions and multiple security constraints as well as the need to distribute data via networks of varying types, sometimes on embedded platforms.

Alongside this technical ambition, the need to build an ecosystem of applications capable of massive processing around a digital base has raised the need to adjust procurement mechanisms. The innovation partnership, a new feature of the French Public Procurement Code, has made it possible since 2016 to resolve several issues, such as ensuring competitive bidding by contracting the same service to two different manufacturers. It also enables transferring intellectual property from a feasibility contract to a preliminary design and definition contract (Public Procurement Code 2021).

This partnership makes it possible to introduce progressive competitive bidding from the exploration phase through to production, culminating in the construction of a market-standard platform. This platform is open to a plurality of business application suppliers and contains a separation of responsibilities: State operator; industrial players developing software bricks; users exploiting them. Through this project, the French MoD explores new ways to engage with startups.

ARTEMIS.IA is divided in three program phases:

- Phase 1, launched in 2017: Three players competing in parallel, under the aegis of an innovative partnership framework agreement, to define the foundations of the system and carry out the first proofs of concept.
- Phase 2, launched in 2019: ARTEMIS.IA became a program of record. The government selected the ATHEA solution (joint venture between Thales and Atos), a synthesis of the solutions proposed by Thales and Atos in terms of data management, ontology processing and human-machine interface for visualizing the results of data fusion.
- Phase 3, launched in 2022: Opening to a diversity of suppliers, including the ecosystem of French AI startups. This has revealed new challenges of integrating innovations of startups into ARTEMIS.IA.

The original design of the program was intended to identify the best proposal among the competitors. However, this objective was not accomplished, as competitors who were unable to win successive phases were eventually able to reposition themselves as subcontractors (despite a ban on co-contracting, and a ban on keeping more than one player after phase 2, circumvented by the creation of the Athea joint venture). Given the criticism of the program, both in terms of ARTEMIS.IA's operational contribution and the relevance of the technical proposal put forward by Atos and Thales, the integration of AI into weapons programs may be subjected to particular attention. This could include more political pressure to be stricter about the competitive nature of such tenders.

As the role of data supervisor is assigned to the MoD's Digital Directorate (DGNUM) and not to ARTEMIS. IA, the connections to sensor data (e.g., Composante Spatiale Optique (CSO) satellites), the platform for sharing operational data, and the dedicated instances for algorithm training and agile experimentation have not yet been established. This decoupling means that the program has yet to mature. As a result, it does not yet offer a state-of-the-art software platform with genuine integration of innovative building blocks from the civilian ecosystem. Mainly treated as a technical issue, ARTEMIS.IA revealed broader organizational challenges. One big issue encompassed the need by the defense procurement agency to reach out to players in all AI-related programs, from the Armed Forces, directorates, and services to industry, and to agree on a roadmap. As a result, ARTEMIS.IA was transformed into a "platform" project, even though it was originally intended as a "profound transformation in the use of data" project, risking selling technology without reflecting on its uses.

3 Organizing Defense AI

3.1 Defense AI Governance

In 2019, the French MoD created the Defense Artificial Intelligence Coordination Unit (CCIAD) to facilitate the implementation of AI and coordinate the actions of the French MoD. At the time of its creation, the goal was to recruit 200 AI experts and specialists by 2023 (French MoD 2019; Usbek & Rica 2021; DGE 2023), an objective which seems to have been achieved since then. Housed within the AID, CCIAD's mission is to coordinate the defense AI community, raise awareness of the operational value of AI, and bring together the various stakeholders to communicate on relevant initiatives that can lead to the integration of AI into programs. CCIAD created an ecosystem around two functions:

- AI coordinators in the Armed Forces, directorates, and services, are in charge of cross-functional actions that may affect AI and those in charge of thematic groups related to AI.
- Project and action managers integrating an AI solution. On the DGA side, this involves AI function architects, AI experts for an armament operation with an AI module or for any upstream study related to AI; on the Armed Forces side, this involves, directorates, services, officers in charge of AI experiments. However, these coordination functions do not include "data" governance, which is still handled by DGNUM as the ministerial data administrator.

3.2 Data Governance and Data Sharing: A Policy Yet to Be Confirmed

Since the launch of its digital transformation process in September 2017 (DGNUM 2020), the French MoD's digital governance organization has evolved significantly. Thus, DGNUM was created to carry out this transformation. It is responsible for implementing the Ministry's digital policies (and making proposals for their development). Its director is also the minister's data manager. In this way, DGNUM ensures the implementation of the Ministry's data governance, and its policy is then translated into roadmaps and action plans by the Ministry's various bodies.

According to the French MoD's 2021/2023 data roadmap (French MoD 2021), one of the main areas of focus is data exploitation. With a greater variety of data than the civilian sector (e.g., sonar, radar, infrared, electronic warfare, etc.), the defense sector is characterized by its specific constraints (embedded systems, limited networks, non-cooperative environment, very often unstructured data). As the main AI solutions on the market focus on deep learning technologies (in particular, machine learning), the development of AI systems relies on the ability to use adapted training and test data. This requires, among other things, massive data annotation.

To manage and increase the value of the data, the French MoD has decided to act on three levels: strategic to provide a coherent vision of the data; operational to define sharing rules and exchange procedures; and organizational to promote AI culture. DGNUM is responsible for implementing a data policy that will enable the identification of existing data, its tagging, and the definition of exploitation models.

However, this process of data collection produced in the context of French military operations—data that should then be annotated and contextualized to make it available for defense AI developments—still needs to be structured. It raises many questions: who owns the data, how to store it, how to share it? In the absence of a general data policy that has been modernized, formalized at a strategic level and shared various French MoD entities, have set up discussion frameworks to address the issues inherent in data sharing. This was driven primarily by the operational needs of experimentation with industry support.

Moreover, the French MoD's vision of data sharing seems rather restrictive. Environmental data sets collected by the system are considered confidential and can provide information on the use and performance of defense equipment by Armed Forces and, more generally, on activities carried out in theaters of operations. There are still ways to overcome the sensitivity of operational data, such as anonymizing data by design or creating synthetic data from a data model.

4 Funding Defense AI

By 2022, the budget for defense innovation increased by around 20% to €1bn (AID 2023). In 2024, this will rise to €1.2bn, intended to enable the Armed Forces to adequately address new fields of conflict (space, seabed, information, cyber) by 2030 (Assemblée Nationale 2023). With a target of €100M spent per year on defense AI on the French MoD's five-year spending plan for the period 2019–2025 (military programming law), upstream studies currently account for almost 30%, the ARTEMIS.IA program for 30% (with a gradual rise to €30M per year), other programs for around 30% (SCAF, Rafale). The remaining 10% are devoted to capturing innovation from the civilian sector via the RAPID grants and the innovation acceleration projects of the Defense Innovation Agency. Investments are mainly focused on use cases considered currently more mature, such as detection, recognition, and identification. AI brings significant added value here, overcoming challenges in terms of the frugality of AI models and state-of-the-art computing.

The military programming law for the period 2024–2030 earmarks around €10bn to accelerate defense innovation with ten technological priorities, including AI and autonomous systems (Legifrance 2023) In this context, the share dedicated to developing defense AI is set to grow significantly, compared with the more than €700M committed over the previous period 2019–2025 (French MoD 2022). Spending on artificial intelligence is therefore mainly associated with programmatic roadmaps, decided over a long period of time, leaving very little room for capturing open innovation. The low level of investment to attract military applications of civilian AI

innovations therefore complicates the integration of these technologies for the Armed Forces.

As most programs are primarily oriented towards hardware development, there are several challenges to integrate AI:

- The programs leave little room for increments once they have been launched. Exceptions occur primarily when the industrial company which serves as program and system owner, is ready to commit to performance levels (e.g., purchase orders through MALICIA contracts).
- Most of the funding is earmarked for R&D and the corresponding production at the end of these contracts. Potential scale-up is rarely envisioned. The Scale-Up Governance Committee set up by the AID is intended to address this issue for all emerging technologies, but with a still limited budget and a restricted number of projects (Briant 2022).
- ARTEMIS.IA, is the only program to have opened its design phase to an ecosystem of innovative AI players from the civilian sector. It has a budget of €13M to finance the integration of state-of-the-art AI modules, i.e., barely 13% of the annual defense AI spending.

5 Fielding and Operating Defense AI

5.1 A Wide Range of Initiatives

The aim of preparing the Armed Forces for the AI revolution is to help them make the appropriate organizational changes to achieve superior operational efficiency. Initiatives aimed at bringing defense AI to the battlefield take various forms:

- *Operational Data Management*

In 2020, the French Navy set up a Marine Data Service Center within the Naval Programs Expertise Center (CEPN), with the aim of building up databases annotated and contextualized by sailors. The idea was to make them available to entities inside or outside the French MoD and explore the use of AI to provide decision support tools and use cases exploiting massive data.

- *Maintenance, Repair and Overhaul (MRO)*

In the French Air Force, the Directorate of Aeornautical Maintenance (DMAé) is leading the strategy to verticalize maintenance contracts. A prime example is the RAVEL program, which groups most of the support activities for the Rafale airframe and associated equipment (excluding the engine). To this end, Dassault Aviation draws on its experience in the civilian sector and uses the same digital tools to carry out all its "support big data" activities (Dassault Aviation 2023). As part of its military support activities, the French aerospace group benefits from sovereign solutions developed by Dassault Systèmes around the civilian 3D Experience

platform, an evolution of Catia CAD (having benefited from the acquisition of new technological capabilities, particularly in data mining and cloud infrastructures). With the help of these technical tools and a new form of contract, the RAVEL contract has enabled the Armed Forces' data to be more visible and therefore taken into account.

Maintenance contracts are also designed to address the problem of heterogeneous information systems and the difficulty of communicating between them. In March 2021, for example, Sopra-Steria was selected as part of the Brasidas program, which aims to set up a new information system for aeronautical operational maintenance. Software development is based on a proven civil aeronautical maintenance software package (La revue du digital 2021). Thales, the prime contractor for the Command and Control System for Aerospace Operations (SCCOA) program, is developing the VASSCO information and operational management system, which "ensures the integrity and rapid sharing of information between all players involved in systems support" (Thales 2022).

- *Feedback Loops for Concept Development*

Feedback from field experience for the development of doctrine, such as the degree of autonomy of equipment, particularly in the context of denial of action in electromagnetic space, supports concept development.

- *Training for Specialists and Experts*

The French Army is currently considering the creation of a program for senior officers specializing in AI, big data, and robotics to create a senior management corps.

By operationalizing defense AI along these lines of efforts, the Armed Forces also learn and understand what works or not. On the positive side, the experiments have shown that it is possible to achieve "common requirements" that can be shared across domains/environments despite existing constraints. In addition, experiments also help establish user groups that are essential to collect feedback from operators that helps shape common roadmaps. On the critical side, connectivity—in addition to the decompartmentalization of data, storage, and computing capacities—is brittle. Therefore, Armed Forces need to think about "data frugality" and reconsider whether to put algorithms on the edge or on common backbones. In addition, sometimes operational contexts limit the amount of available data. In this case synthetic data can help to train algorithms. This prompts the need to rethink weapon system contracts and data access, so that algorithms can be constantly evolved and retrained based on all available data. Recent examples of software factories in the French Armed Forces and the Software Acquisition Pathway in the United States show how hardware/software development cycles can be truly decoupled, with very short software development loops between manufacturers and Armed Forces (a few weeks, or even a few days, instead of several years).

5.2 Development Through Experimentation: A New Approach to Deploy AI Solutions

Developing AI solutions for the Armed Forces involves a great deal of experimentation. Because of the need to access data, the agile development approach required for this technology, and since the level of technological maturity still varies from one application to another, use cases need to be explored with the respective users. In what follows, we look at challenges and the "Traitement et Analyse d'Images par Intelligence Artificielle" or Image Processing and Analysis by Artificial Intelligence (TAIIA) case to illustrate the approaches of the French Armed Forces.

5.3 Challenges by the Armed Forces' Experimental Labs

Alongside the DGA's technical innovation clusters and the Armed Forces' experimentation centers, the Armed Forces experimental labs play an essential role in accelerating innovation. Despite their differences in terms of size and resources (whether physical or intangible testing grounds, physical or digital modeling capabilities, with or without a specific location), the Ministry's laboratories share the objective of responding to innovation challenges by working on specific projects or problems.

In 2022, to provide the French MoD with the necessary tools for innovation, the DGA set up the Innovation Défense Lab. This lab provides centralized and dedicated support to the Ministry's laboratories, facilitating hackathons, training courses and design thinking sessions. The Agency has also taken steps to federate the "Defense Makers Community." In collaboration with the DGA expertise center on aeronautical techniques (DGA TA), the Agency presented its ambitions in May 2022, followed by a mapping of the French Armed Forces labs. In this context, numerous exchanges have taken place with entities such as FUSCOLAB, Battle Lab Terre, and CEAM confirming the interest of operational staffs and enabling the French MoD to pursue its efforts to structure this community. The current objective is to create a platform for exchanging and sharing best practices in modeling and rapid prototyping. Ideally, this will accelerate innovation within the French MoD. One of the latest challenges to consider the integration of AI on the battlefield is the CoHoMa challenge. Aimed at innovation related to decision-making, this challenge focused on displacement (e.g., forest, urban area, open country) and concealment as well as connectivity. Launched in 2021 (and renewed in 2023) by the Battle Lab Terre, the challenge of cooperation between man and machine aims to unite players in robotics through mixed teams from industry, startups, research labs, and engineering schools around a collaborative challenge. Each challenge envisages a tactical scenario for 2040. Three aspects are of particular relevance: maneuvering and articulating land and air satellites from a master vehicle; crossing terrain

compartments and progressing to the final zone; detecting, identifying and deactivating traps to be able to advance while informing the command post.

5.3.1 Experiments Conducted by Operational Units: The TAIIA Case

The TAIIA project was an experiment hosted by the Directorate of Military Intelligence (DRM) in 2020. It aimed at building a customized tool for the automatic detection of activities on sites of strategic interest. Based on an experimental platform fed by operational images from the new CSO observation satellite constellation, the project was one of the first experiments to industrialize AI in classified environments. To nevertheless deliver high-performance algorithms, Preligens' models have been trained on commercial data. Preligens has invested heavily in building an "AI Factory" which accelerates moving from development to production. This has the potential to drastically reduce the time it takes to produce algorithms.

Over and above the challenge of making AI operational for intelligence purposes, the specificity of the project lies in the co-construction of the product. The technology not only helps the experts in their search for information and clues in the images, but also enables them to improve their analysis of activity at pre-selected geographical sites. This project has had far-reaching organizational consequences (Ceillier 2021):

- It has profoundly transformed the activities of photo interpreters and intelligence analysts, freeing them from a particularly tedious task (counting objects) to concentrate on higher value tasks, such as detecting unknown activity on sites of interest and thus producing usable intelligence (French MoD 2020).
- This co-construction approach, which responds to a strong operational challenge but entails major organizational changes, mirrors the defense sector's unique restraints. The software had to work, heavily restricted, within the Directorate of Military Intelligence infrastructure and premises, with no Internet connection and no remote intervention in the event of a problem. Moreover, the end-users, intelligence analysts, remain discrete and bound by oath to secrecy, despite the product's co-construction approach. Many subjects cannot be discussed, and the knowledge passed on is often taken out of context or diluted, preventing direct access to sensitive information. Other adaptations to the agile software development method are necessary due to the constraints of confidentiality such as delivery rhythm (every eight weeks for example, rather than in a matter of minutes or hours in the commercial sector) and user involvement.
- Finally, despite the operational interest and relevance of the co-innovation approach with AI, this project had to overcome the difficulties associated with scaling up from an R&D budget to industrialization, imposing highly complex contract negotiation phases and specific contractual engineering.
- Initial results have prompted the French Armed Forces to pursue experimentation, with the aim of offering this technological capability to all players in the

field of imagery-based intelligence and analysis. After many months of negotiations, the French MoD decided to pursue the TAIIA project, scaling up the solution for operational deployment within the Joint Intelligence Function (Preligens 2022).

Furthermore, this project also revealed that the historical separation between R&D budgets (P144) and equipment budgets (P146), inherited from the "waterfall" model used for the design and acquire complex hardware systems, was ill-suited for software development in "DevOps", which requires very short loops between design, development, testing and deployment.

6 Training for Defense AI

The human resources challenge remains an important barrier to operationalize AI in the Armed Forces. Beyond the subject of AI, the issue of skills in the digital field is crucial. But this is currently under considerable pressure due to high demand and limited supply. This situation is reflected in the exponential growth in salaries in the private sector compared to the public sector. Several initiatives have been put in place to meet this challenge:

- The French Interministerial Digital Department (DINUM) has introduced a new approach for the management of its contract staff, based on a "quasi-corps" system. This approach offers several advantages, such as shorter recruitment times, better remuneration for the 56 professions concerned, and a more structured career path. Inspired by the model of the National Agency for Information Systems Security (ANSSI), which employs 80% contract staff, the French Ministry of Defense sees this model as a means of rapid staff renewal, where contract staff come to gain rewarding experience before pursuing their careers elsewhere. This approach fosters diversity of career paths and the enrichment of skills within the administration.
- The use of Digital Service Companies is also widespread, and the French MoD is working to industrialize this collaboration with the private sector. Hybrid service centers have been set up, notably at the Joint Directorate of Infrastructure Networks and Information Systems (DIRISI), to bring together public and private skills to develop satellite links, for example.

Recruiting specialized AI experts is also a challenge for the defense industry. To meet this challenge, major defense companies have created in-house training programs ranging from awareness-raising and dissemination of an AI culture to advanced technical certifications. The co-construction of training programs with engineering schools is also a priority. Projects are launched on interactive simulation using AI, among others at the Air Force Experimentation Center.

7 Conclusion

Defense AI now seems to be firmly rooted in the French Armed Forces. There is a plethora of initiatives launched in the context of major programs (FCAS, for example), thematic challenges (robotics with COHOMA), or experiments in operational units (TAIIA).

AI governance has also taken shape around the CCIAD at the Defense Innovation Agency. However, considering the requirements of different military services, the Procurement Agency (DGA) and the new entities created as part of the Armed Forces digital transformation (Defense Innovation Agency—AID, the Digital Directorate—DGNUM, Defense Digital Agency—AND), the French MoD's action can appear very fragmented for the defense ecosystem. This is all the truer given that localized, high-impact initiatives have emerged within each military branch at multiple levels, as discussed, for example, with the creation of the Naval Data Service Center (CSD-M).

This profusion of initiatives at various levels and taken by different military branches may illustrate the lack of a centralized data-sharing policy, favoring ad hoc development frameworks. For the time being, the French MoD's approach to data sharing is restrictive. The latest Defense Innovation Agency activity report suggests that this situation is subject to minor changes, with the declared aim of ensure adequate data supply: "Data at the heart of AI-based processing is all the more valuable for its operational nature. The provision of such data must be compensated fairly by the Ministry, such as through the supply of annotated data or the possibility of testing solutions developed by external players" (AID 2023). This type of negotiation generally concerns the sharing of intellectual property related to algorithms developed on the data made available by the MoD. For the time being, however, the respective compensation seems to be negotiated on a case-by-case basis.

In addition, the French MoD's objective is to promote AI in all programs wherever possible and desirable. Indeed, while the first phase consisted of setting a course and providing resources, the French MoD seems to have adopted a new approach, with the widespread dissemination of AI. According to the head of AI projects at the CCIAD, AI is no longer "identified as a particular object" (Le Monde 2023). This underlines the French MoD's commitment to a new approach that could be interpreted as a sign of maturity. But it seems that the Ministry's policy remains to be confirmed if it is to fully disseminate trusted AI solutions. Indeed, if the ministerial policy of data sharing remains restrictive, then this will force the MoD to continue to rely on the recruitment of scarce skilled labor. Moreover, experiments conducted so far have identified major roadblocks such as the need to develop adequate digital infrastructure including clouds, access to users, and adjusting budgetary and contractual mechanisms to the reality of agile software development. The updated defense AI strategy, which could be published in 2024, will need to take these elements into account to meet the challenges of developing trusted AI techniques and solutions.

The strategy update will also need to reflect upon the fact that—despite the will to integrate defense AI into military operations—large-scale implementation has yet to take place. To achieve this, AI governance needs to be strengthened and strategic investments made to develop programs that can catalyze many successful initiatives in different areas of AI. There are still several open items that can help scale AI development, such as:

- Supporting the work of raising awareness of investments in AI within armament programs;
- Increasing financing capacities to scale up AI developments available to major armament programs;
- Increasing the R&T budget of the Defense Innovation Agency's to finance defense applications of emerging civilian technologies, identified and captured in an open innovation process;
- Formalizing a strategic data-sharing policy for the entire French MoD and defining rules of ownership and use to facilitate access for experimentation purposes;
- Decoupling software and hardware development cycles within weapons programs;
- Facilitating agile co-development between the military and manufacturers (Fedtech 2022) to move forward on the rapid construction of solutions in response to use cases (possibly drawing inspiration from US Armed Forces' software factories).

References

AID. 2021. Le guide pour l'intégration de l'intelligence artificielle (IA) évolue. https://www.defense.gouv.fr/aid/actualites/guide-lintegration-lintelligence-artificielle-ia-programmes-evolue. Accessed 30 January 2024.

———. 2023. Bilan d'activités 2022. https://www.defense.gouv.fr/sites/default/files/aid/Bilan%20d%27activite%CC%81s%202022.pdf. Accessed 30 January 2024.

Airbus. 2018. Airbus Launches SmartForce - Services Bringing the Power of Data to Military Operations. https://www.airbus.com/en/newsroom/press-releases/2018-07-airbus-launches-smartforce-services-bringing-the-power-of-data-to. Accessed 30 January 2024.

Assemblée Nationale. 2023. Compte rendu Commission de la défense nationale et des forces armées, Audition, ouverte à la presse, de M. Emmanuel Chiva, délégué général pour l'armement, sur le projet de loi de finances 2024. https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_def/l16cion_def2324013_compte-rendu. Accessed 30 January 2024.

Bômont, Clotilde. 2021. *Le cloud défense: défi opérationnel, impératif stratégique et enjeu de souveraineté*. Institut français des relations internationales. https://www.ifri.org/sites/default/files/atoms/files/bomont_cloud_defense_2021.pdf. Accessed 30 January 2024.

Briant, Raphaël. 2022. *Open Innovation in Defense: Passing Fad or New Philosophy?* Institut Français des Relations Internationales. https://www.ifri.org/sites/default/files/atoms/files/briant_open_innovation_defense_2022.pdf. Accessed 30 January 2024.

Ceillier, Rugdual. 2021. Une start-up civile dans la défense, les raisons d'un succès. La Jaune et la Rouge. https://www.lajauneetlarouge.com/wp-content/uploads/2021/11/Pages-de-JR_769-4.pdf. Accessed 30 January 2024.

Cour des Comptes. 2023. La stratégie nationale de recherche en intelligence artificielle: une stratégie à structurer et à pérenniser. https://www.ccomptes.fr/sites/default/files/2023-10/20230403-strategie-nationale-recherche-intelligence-artificielle.pdf. Accessed 30 January 2024.
Dassault Aviation. 2023. Dassault Aviation, Annual Report, 2022. https://www.dassault-aviation.com/wp-content/blogs.dir/2/files/2023/06/RA_2022_VA_BD.pdf. Accessed 30 January 2024.
DGA, AI Task Force. 2019. AI in Support of Defence. https://www.decideo.fr/attachment/1702015/. Accessed 30 January 2024.
———. 2022. DGA Orders Data Processing Solutions Tailored to Defense Needs from Preligens. https://www.defense.gouv.fr/dga/actualites/dga-commande-a-societe-preligens-solutions-traitement-donnees-adaptees-aux-besoins-defense-0. Accessed 30 January 2024.
DGE. 2023. L'intelligence artificielle et le monde de la défense. https://www.entreprises.gouv.fr/fr/numerique/enjeux/l-intelligence-artificielle-et-monde-de-la-defense. Accessed 30 January 2024.
DGNUM. 2020. La transformation numérique des Armées, Concepts clés. https://www.defense.gouv.fr/sites/default/files/dgnum/La%20Transformation%20num%C3%A9rique%20du%20minist%C3%A8re%20des%20Arm%C3%A9es_concepts_cl%C3%A9s.pdf. Accessed 30 January 2024.
Elysée. 2018. Discours du Président de la République sur l'intelligence artificielle. https://www.elysee.fr/emmanuel-macron/2018/03/29/discours-du-president-de-la-republique-sur-lintelligence-artificielle. Accessed 30 January 2024.
Ezratty, Olivier. 2021. *The Uses of Artificial Intelligence*. Creative Commons.
Fedtech. 2022. Software Factories for the Military Scale DevSecOps. https://fedtechmagazine.com/article/2022/05/software-factories-military-scale-devsecops-perfcon. Accessed 30 January 2024.
FOB. 2020. Comment Nexter conjugue innovation et transformation digitale depuis un an. https://www.forcesoperations.com/comment-nexter-conjugue-innovation-et-transformation-digitale-depuis-un-an/. Accessed 30 January 2024.
France 2030. 2021. Stratégie Nationale pour l'intelligence artificielle – 2e phase. https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=334FD34F-7844-497E-9551-79EDFF3B2EEF&filename=1645%20-%20DP%20-%20Strat%C3%A9gie%20Nationale%20pour%20l%27IA%202%C3%A8me%20phase.pdf. Accessed 30 January 2024.
French MoD. 2017. Revue stratégique de défense et de sécurité nationale. https://www.diplomatie.gouv.fr/IMG/pdf/2017-revue_strategique_dsn_cle4b3beb.pdf. Accessed 30 January 2024.
———. 2019. Création de la cellule de coordination de l'intelligence artificielle de defense. https://www.defense.gouv.fr/aid/actualites/creation-cellule-coordination-lintelligence-artificielle-defense. Accessed 30 January 2024.
———. 2020. Project TAIIA. https://www.youtube.com/watch?v=KTqXoYe0uho. Accessed 30 January 2024.
———. 2021. Feuille de route de la donnée 2021/2023. https://www.data.gouv.fr/fr/datasets/feuilles-de-route-ministerielles-sur-la-politique-de-la-donnee-des-algorithmes-et-des-codes-sources/. Accessed 30 January 2024.
———. 2022. Lancement de la réalisation du projet Artemis.IA, solution de traitement massif de données et d'intelligence artificielle. https://www.defense.gouv.fr/dga/actualites/lancement-realisation-du-projet-artemisia-solution-traitement-massif-donnees-dintelligence. Accessed 30 January 2024.
———. 2023. France and Singapore Create a Joint R&D Laboratory in the Field of Artificial Intelligence for Defense. https://www.defense.gouv.fr/aid/actualites/france-singapour-creent-laboratoire-conjoint-rd-domaine-lintelligence-artificielle-defense. Accessed 30 January 2024.
FRS. 2020. Web Conference on Funding and Startup Development in Defense Sector. https://www.youtube.com/watch?v=ZKNSIAz2ZYM. Accessed 30 January 2024.
La revue du digital. 2021. Les armées achètent un système d'information pour accroître la disponibilité de leur avion. https://www.larevuedudigital.com/les-armees-commandent-

un-systeme-dinformation-pour-accroitre-la-disponibilite-de-leurs-avions/. Accessed 30 January 2024.
Le Monde. 2023. Défense: les start-ups de l'intelligence artificielle tentent d'investir le champ de bataille. https://www.lemonde.fr/economie/article/2023/06/27/defense-les-start-up-de-l-intelligence-artificielle-tentent-d-investir-le-champ-de-bataille_6179459_3234.html. Accessed 30 January 2024.
Legifrance. 2019. Instruction n°1618/ARM/CAB on Armament Operations. https://www.legifrance.gouv.fr/circulaire/id/44542. Accessed 30 January 2024.
———. 2023. LOI n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la defense. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047914986. Accessed 30 January 2024.
Martin, Kévin. 2022. *Defense Groups and Digital Technologies*. Fondation pour la Recherche Stratégique. https://www.frstrategie.org/publications/recherches-et-documents/groupes-defense-technologies-numerique-2022. Accessed 30 January 2024.
Ouest France. 2023. Le ministère des Armées, via Bpifrance, investit dans les PME stratégiques à l'Ouest. https://www.ouest-france.fr/economie/entreprises/entretien-le-ministere-des-armees-via-bpifrance-investit-dans-les-pme-strategiques-a-louest-6177d838-e4fb-11ed-9757-e35473d4e313. Accessed 30 January 2024.
Parly, Florence. 2019. Déclaration de Mme Florence Parly, ministre des armées, sur l'intelligence artificielle et la défense, à Saclay le 5 avril 2019. https://www.vie-publique.fr/discours/271295-florence-parly-5042019-intelligence-artificielle-et-defense. Accessed 30 January 2024.
———. 2021. Déclaration de Mme Florence Parly, ministre des armées, sur l'intelligence artificielle de défense, à Creil le 10 mai 2021. https://www.vie-publique.fr/discours/279917-florence-parly-10052021-intelligence-artificielle. Accessed 30 January 2024.
Preligens. 2022. France's General Directorate of Armaments (DGA) Contracts with Preligens for Data Processing Solutions to Meet Its Defense Needs. https://www.preligens.com/sites/default/files/2022-10/Press_Release_Preligens_DGA.pdf. Accessed 30 January 2024.
Public procurement Code. 2021. Article R2172-20 on Innovation Partnerships. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000037701019/LEGISCTA000037724640/2021-08-26. Accessed 30 January 2024.
Ricaud, Bruno, and Cécile Jourdas. 2019. *Nexter: AI & Robotic Systems*. Association francaise pour l'Intelligence Artificielle. https://pfia2021.fr/conferences/apia/actes_APIA_CH_PFIA2021.pdf. Accessed 30 January 2024.
Thales. 2018. Thales and Microsoft Partner to Develop a Unique Defense Cloud Solution. https://www.thalesgroup.com/en/worldwide/defence/press-release/thales-and-microsoft-partner-develop-unique-defence-cloud-solution. Accessed 30 January 2024.
———. 2021. Thales and Google Cloud Announce a Strategic Partnership to Jointly Develop a 'Trusted Cloud' in France. https://www.thalesgroup.com/en/group/investors/press_release/thales-and-google-cloud-announce-strategic-partnership-jointly. Accessed 30 January 2024.
———. 2022. Thales Wins VASSCO Contract to Support Air Surveillance Systems. https://www.thalesgroup.com/en/worldwide/defence/press_release/thales-wins-vassco-contract-support-air-surveillance-systems. Accessed 30 January 2024.
Usbek & Rica. 2021. IA: «Il faut en urgence à la France une force de travail pour préparer, comprendre les données et prévenir les limites des machines». https://usbeketrica.com/fr/article/ia-il-faut-en-urgence-a-la-france-une-force-de-travail-pour-preparer-comprendre-les-donnees-et-prevenir-les-limites-des-machines. Accessed 30 January 2024.
Villani, Cédric. 2018. For a Meaningful Artificial Intelligence: Towards a French and European Strategy. https://fichiers.acteurspublics.com/redac/pdf/2018/2018-03-28_Rapport-Villani.pdf. Accessed 30 January 2024.

Waking Up Slowly: Defense AI in Spain

Raquel Jorge Ricart

Defense AI is not a topic that is overtly discussed in Spain. Instead of reflecting on the usage of defense AI, governmental speeches often acknowledge that defense AI is no longer a separate issue. Rather, defense AI is an element that is part of a broader range of issues revolving around a holistic approach to national security.

An analytical assessment of existing national strategies, technology-oriented industrial defense plans, and directives on defense policy show that until around 2020, AI was not a central element in the Spanish defense ecosystem. Until then, the general importance of AI had been acknowledged, while risks and benefits had been generally addressed. However, it was not until the start of the new decade of the 2020s that AI took center stage with specific principles, roadmaps, and several initiatives outlining how AI should be governed and implemented. Public documents also acknowledge that the Spanish ecosystem has lagged in the development of defense AI. This, the documents contend, has negatively affected Spain's international positioning on AI and limited the competitiveness of the local defense industry—something that ought to be addressed.

Spain's governance system for defense AI includes mandates and processes to coordinate stakeholders across relevant institutions. An increase in funding, a diversification of projects, and access to much more publicly available documents on the descriptive plans of projects as well as their final results and impact may be convenient to create a culture of defense AI and are potential policy recommendations to move forward.

A small number of large companies lead the defense AI market and act as leaders of several relevant European Union (EU) projects. Still, this article proposes that a larger focus should be put onto small and medium-sized enterprises (SMEs) to ensure that defense AI emerges from a diversified portfolio of services across different types of firms. This would help increase the defense industry market footprint in

R. J. Ricart (✉)
Technology and International Affairs, Elcano Royal Institute, Madrid, Spain
e-mail: rjorge@rielcano.org

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_12

Spain, expand and deepen existing value chains while also creating new ones across the industry, and increase the level of involvement of Spanish companies in European projects.

Defense AI is fielded and operationalized via different instruments and takes place in many strategic sectors that Spain has flagged for national security (such as aerospace, cybersecurity, and maritime security). However, further activities are needed to fully leverage synergies with other technologies (e.g. quantum) in research and development (R&D) projects.

Finally, there is limited information on the training of systems and human capital. Based on existing national and European regulation as well as the respect for fundamental rights, university programs should more actively include defense AI in their curricula.

1 Thinking About Defense AI

Defense AI is not a topic that is overtly discussed in Spain. Instead of reflecting on the usage of defense AI, governmental speeches often acknowledge that defense AI is no longer a separate issue. Rather, defense AI is an element that is part of a broader range of issues revolving around a holistic approach to national security.

There is no general definition of the meaning and the potential use cases of AI in support of Spain's national security and defense. The lack, however, has not created problems but rather stems from the fact that Spain had been waiting for an EU-wide definition of AI provided by the AI Act adopted under the Spanish Presidency to the Council of the European Union in the second half of 2023. Spain supports a human-centric approach to AI in general, especially a "no harm" policy, respect for personal data privacy and support for human rights. However, Spain has, thus far, hardly addressed the ethics of defense AI as the dominating AI ethics debate excludes defense. Nevertheless, the fact that the whole-of-government approach to AI is human-centric suggests that any defense AI development will need to rely on ethical principles that govern AI in general.

An analytical assessment of existing national strategies, technology-oriented industrial defense plans and directives on defense policy show that, until around 2020, AI did not play a prominent role in Spain's defense discourse. While AI was always acknowledged as an important technology, and most capstone documents underlined the need to address its challenges and opportunities, it was not until the start of the new decade that AI was listed as a central element, and given a set of measures, grounded principles, roadmaps, actions or at least considerations on how it should be governed. In general, Spain has followed a human-centric approach to AI with a strong emphasis on regulation, while guiding the work on the AI Act proposal, but this line of reasoning has been completely separated from defense concerns. Rather, Spain's defense community has developed its own thinking on defense AI via the respective channels in the EU and NATO.

Public documents also acknowledge that the Spanish ecosystem has lagged in the development of defense AI. They also explicitly state that this situation has limited Spain's positioning globally and the development of an economically competitive AI-capable defense industry.

1.1 A Broader Outlook on the National Security Strategy

The role and importance of AI in the defense and national security ecosystem in Spain has evolved in recent years. In the National Security Strategy from 2017 (National Security Department 2017), AI was mentioned only twice and in broad statements that reflected the importance of this topic from an intellectual perspective. No specific policy action, roadmap or initiative was drawn. However, with the renewal of the National Security Strategy (NSS) in 2021 (National Security Department 2021), AI turned from being an intellectual topic into becoming a central element of the ways, means and goals, as well as instruments, that frame, explain and provide guidance to the NSS.

Technology and strategic sectors are ranked second out of three main goals of the 2021 NSS. The strategy broadens (Ricart 2022) the scope and identifies technology, not only as a driver to boost the security and defense dimension, but also an end in itself, which needs to be underpinned with adequate industrial capabilities. The strategy emphasizes the key role of technology but has also been criticized as being too generic and lacking substance on the goals to be achieved and the roadmaps to implement them (Arteaga 2022a, b).

Particularly, AI is perceived as the most strategic technology across all sectors. The 2021 NSS devotes great attention to this technology and approaches it in two ways: as a power tool, and as an enabling, facilitating tool.

As a power tool, AI has become a key geoeconomic challenge. Spain explicitly mentions that China, which has achieved a mature development level in AI, aims to gain a predominant position that allows the country to define international standards and technical and industrial protocols. It wants to become the powerhouse leading foreign direct investments and technology flows into other countries to gain influence and market share in services and network operators. Second, AI is also a power tool because most developments of digital services and infrastructures rely on emerging and disruptive technologies such as cloud computing, quantum technologies, network visualization and the Internet of Things, all of which largely depend on the maturity of AI. Third, AI poses risks that are interrelated. Threats derived from the usage of next-generation technologies, such as AI, add complexity and impinge on individual rights through the illicit usage of AI. Finally, the 2021 NSS makes an explicit reference to the respect for human rights and ethics when designing, developing, deploying, and using AI, such as in the case of lethal autonomous weapons systems (LAWS). Although there is no real public debate about the ethics of LAWS, strategies always refer to the need to support arms control for AI and limit harm while not curtailing necessary military innovation.

Second, as an enabling and facilitating tool, AI is perceived as an opportunity that may be leveraged for specific applications. While the strategy acknowledges that AI may apply to a large range of case uses, it highlights two specific policy areas: counterintelligence, the fight against disinformation campaigns and actions against foreign interference; and maritime security. Regarding counterintelligence, it calls for the human and technological capacities to be strengthened, to continue to reap the benefits linked to proper data management and processing, such as AI, quantum computing and the cloud. In addition, the strategy calls for an update to legislation to guarantee the data protection rights of Spanish citizens, while enhancing the capacity of the Intelligence Services to act in their defense. On maritime security, the strategy sets the safety of the Spanish merchant and fishing fleet in Spanish jurisdictional and international waters as a priority. In this regard predictive analytics supports effective planning for complex operational scenarios. That's why AI plays an increasingly important role in maritime surveillance systems, platforms, and sensors to modernize maritime capabilities.

AI is not only seen as a major element of national security and defense. AI also supports the three objectives of the 2021 NSS:

- Advancing crisis management by adopting an anticipatory approach and supporting data-driven decision-making, across the central government and in co-governance with all regional authorities.
- Strengthening technological capabilities and strategic sectors by adapting and updating strategic sectors to the much-needed quality controls, regulatory adaptation and research and developments (R&D) projects that may be accelerated and facilitated by AI.
- Developing capabilities to prevent, deter, and respond to hybrid threats, where AI may be an active part of malicious hybrid threats, but also an active part in the fight against them.

In a nutshell, the three Ps of the 2021 National Security Strategy are to Protect, Promote and Participate—with AI playing a foundational role across all three elements. To achieve the 3 Ps, the security ecosystem would need to integrate AI across various instruments. However, AI is not explicitly mentioned in the strategy with regards to the other remaining instruments: resources on national security, preparation plans, indicator-based early warning systems, development of special communications from the Government Presidency, and the integration of regional authorities ("Comunidades y Ciudades Autónomas") into the national security system.

1.2 The Directives on National Defense and on Defense Policy

While the national security strategy emphasizes AI as an important topic, the Directive on National Defense (DND) (Ministry of Defense 2020a) does so only limitedly. The DND is Spain's top defense planning document and occupies the main position in Spanish defense policy after the Organic Law on National Defense

5/2005. The common purpose of the DND is to establish the objectives and the main lines of effort pursued by the Ministry of Defense (MoD). Among the fourteen goals mentioned in the document, technology ranks twelfth—behind issues like climate change and gender equality. Descriptions remain vague, encapsulating no specific policy actions or initiatives.

Despite this low position in the list of objectives, the DND highlights the need to foster R&D and innovation in technological capabilities. Also, it stresses the importance to foster capacity to attract technology-skilled talent i.e. through training, education, and skilled immigration policies. While capacity and specialization are needed, the DND highlights the importance of having "availability" of AI to be used, always based on national legislation. However, statements on AI are very limited, and there is no prominent importance given to AI in comparison to other technologies.

In the Guidelines, section 7 speaks of promoting the EU's Common Foreign and Security Policy (CFSP), including industrial and technological cooperation, but only superficially. The second to last guideline (14th) is reserved for promoting the Industrial and Technological Base.

To give a further understanding of the practical implications of the DND, it is important to assess the Directive on Defense Policy (DDP) (Ministry of Defense 2020b), which develops and implements the guidelines derived from the DND in the MoD's area of responsibility. It was published for the first time in 2020 with the goal of providing details on the implementation of the DND, which had already existed since 2010 but without a publicly available roadmap. The DDP fills this void.

Although the DND does not identify technology as a major topic, the DDP considers technology as a cross-cutting phenomenon that needs to be addressed in three ways: through a trust-based approach, by empowering strategic autonomy and reducing dependence in critical value chains, and by fostering a more cooperative European defense industrial and technological base (DITB). Against this background, the DDP's principles fall into two categories. First, the DDP outlines the strengthening of the Spanish DTIB by

1. facilitating the development of dual-use technologies with other ministries, particularly the Ministry of Industry and Tourism, the Ministry of Science, Innovation and Universities, and the Ministry of Treasury and Public Administration, as long as operational requirements allow it;
2. prioritizing the use of technology and training over the large-scale deployment of human resources;
3. accomplishing greater strategic performance with the least personnel and material effort;
4. seeking maximum flexibility in dealing with multi-purpose and multi-domain tasks;
5. advancing the development of capabilities aimed at neutralizing hybrid threats.

Second, it aims to strengthen the internationalization of the national defense industry by

1. promoting industrial and technological cooperation as one of the main elements of Defense Diplomacy;
2. identifying the EU and NATO as priority frameworks for the internationalization of Spain's defense industry;
3. making an integrated and coordinated effort, seeking the collaboration of all ministerial departments.

However, to implement specific measures for defense AI, the Directive acknowledges that the most important asset will be to deploy "reasonable financial resources" and maintain a stable budget. Defense investment should be approached in such a way that it not only meets the needs of public service, but also contributes to innovation, technological development, job creation and the projection of Spain's influence in the world.

1.3 The Specific Focus of the 2020 Strategy on Technology and Innovation in Defense (ETID 2020)

The ETID (Ministry of Defense 2020c) was positively received. It did not produce a novel strategy but updated the one from 2015. The update reflected the need to explore upon new technologies and their impact on defense capabilities. Overall, the document rests on three pillars of

- directing research, development and innovation (RD&I) investments towards achieving the technological objectives set out in the Strategy, drawn from the set of RD&I guidelines of interest for defense;
- promoting actions that advance national and multinational cooperation in RD&I;
- pushing excellence by leveraging the MoD as an RD&I catalyst and integrating talent from all sectors.

ETID also highlights the importance to find a balance between the innovative use of mature technologies and the advances associated with the development of emerging technologies. The innovative use of mature technologies involves a novel idea that combines different mature technologies for impact, greater than the sum of its parts. The ETID supports deep technologies that offer promising technological edge but require longer time to market and significant capital investments. It does not involve radically new or complex RD&I actions, nor does it involve large investments, and the results are obtained in the short or medium term. This is the type of innovation that has the greatest impact on different sectors in the civil sector (transport, communications, etc.). As for the development of emerging technologies, they require intensive efforts in RD&I, with investments that only a few countries or corporations are capable of deploying. The results come in the long or very long term and are helpful to maintain a competitive edge. However, fully understanding the possibilities of these still emerging technologies or the timescales, in which they will really take hold, is a major challenge.

Specific AI use cases are mentioned in the sections below. However, from a strategic planning perspective, it is important to note that the ETID acknowledges the fact that the scientific community and defense-relevant industry players express their frustration with the current system, "much more than in other countries," as stated by the ETID strategy. This may be due to Spain's bifurcated technology ecosystem, with commercial stakeholders focusing on the general application of AI and defense companies and defense-focused research institutes dealing with defense AI. This represents a self-limitation in the field of defense AI.

2 Developing Defense AI

Spain wants to advance national defense AI solutions and looks at the EU and NATO as important frameworks to develop these solutions in cooperation with partners. This section addresses each of the three lines of effort separately. Overall, Spain emphasizes that defense AI development must be rules-based as this reflects the country's general stance on the importance of regulation.

2.1 Developing Defense AI at the National Level

Spain does not yet have a publicly available strategy or roadmap on defense digitalization, defense AI or a defense data policy. However, the ETID provides a roadmap, which aims to develop emerging and disruptive technologies, where AI plays an important role, to address seven challenges: defense applications with high technical exigencies, defense against asymmetric threats, leveraging the civilian technological boost, promotion of skilled labor capabilities, energy sustainability, digital transformation, and initial technological readiness.

The ETID addresses these specific challenges with a set of technological tools, among which AI serves as an important enabling tool. Table 1 includes those areas where AI is mentioned.

RD&I plays a pivotal role in developing technologies to address these seven challenges. In this regard, the ETID outlines what should be accomplished across eleven different areas of activities identified in the document. The following five make particular reference to the role of defense AI:

- *Precision Effects*

The first area is arms and munition; concretely the improvement of munition performance from advanced guidance and control devices, as well as increasing their autonomy through the incorporation of sensor data processing technologies, artificial intelligence, communications links, etc., achieving operational advantages mainly related to improved combat effectiveness, reduced logistical burden, or reduced potential collateral damage.

Table 1 Contribution of defense AI to specific technology development initiatives in Spain

Area of action	Reference to AI
Defense applications with high technical exigencies	• AI-powered guidance technologies and munition control
Defense against asymmetric threats	• Advanced systems for detection of ground-based improvised explosive devices (IEDs)
Leveraging of civilian technological boost	• Automated, smart analysis of large data volumes of sensors • Predictive Maintenance • Smart analysis of multiple information sources for decision-making • Unmanned ground platforms for defense missions • Unmanned underwater vehicles for defense missions • Usage of small satellites in defense applications
Promotion of skilled people's capabilities	• Technologies for infantry • Exoskeletons for defense missions • Advanced simulation training
Energy sustainability	• New forms of propulsion for manned platforms and unmanned systems
Digital transformation	• Technology 4.0 for the digital transformation of the defense department
Initial technological readiness	• Detection technologies for the development of active protection systems

Source: Author's compilation based on ETID 2020

- *Sensors and Electronic Systems*

The second area is sensors and electronic systems. This is divided into three main blocs, where AI plays an important role. First, in radars, AI is expected to be used for identifying non-cooperative objectives and automated reconnaissance, as well as to develop new algorithms for radar processing. The second bloc is the processing of sensors data: concretely, the development of algorithms that analyze the data obtained by different sensors to automatically detect, recognize or identify the presence of entities of significance and interest to the Spanish Armed Forces (SAF), thereby reducing the analysis burden on human operators. The third area is electronic warfare.

- *Data Analytics for Cross-Cutting Technologies*

The third area is typical technologies for bases, installations, platforms, and combatants. Concretely, AI-powered data intelligence is aimed at ensuring predictive maintenance of platforms, such as accurately and reliably predicting the remaining lifetime of each component or system. This is expected to be used for ground-based, naval, and aerial platforms, outer space systems, integrated systems, and to support maritime situational awareness.

- *CBRN Defense*

The fourth area is Chemical, Biological, Radiological and Nuclear defense (CBRN defense), where AI would be useful to assess data provided by unmanned remote detection systems at high speed and for the identification of CBRN atmospheres based on AI-powered data.

- *Information and Communications Technology (ICT)*

The fifth area is the inclusion of AI for ICT development, although this area is less precise regarding the potential of AI.

It is mainly the private sector that drives defense AI developments in Spain, but the private sector constitutes a patchwork of heterogenous actors. The biggest group is represented by a few large defense companies that represent the bulk of activities. These are usually led by Indra Systems (a Spanish information technology and defense systems company), Navantia (a leading maritime security company), and Tecnalia (a private R&D company). In addition, leading foreign defense companies like Thales or Airbus have offices and R&D centers in Spain.

Research institutions constitute the second largest group. Most of them come from the public sector, and some of them are part of the military ecosystem, like the Instituto Nacional de Técnica Aeroespacial Esteban Terradas. Others are a conglomerate of SMEs that have joined forces in clusters, such as the Andalusian CT Ingenieros Aeronauticos de Automocion e Industriales, but these clusters mostly focus on civilian, rather than defense engineering and thus only occasionally contribute to defense solutions. The smaller group consist of start-ups that mainly work for large companies. Some of them have their own portfolios, clients and investors, work individually, and provide services to international clients. One example is Devo, formerly Logtrust, a technology company that developed the first real-time big-data-in-motion software, which collects and analyses big data in real-time. The company became Spain's first cybersecurity unicorn. Devo also provides AI solutions. It secured financial backing from venture capital firm Insight Venture Partners—an investor in tech giants such as X (formerly Twitter), Wix, Shopify, Trivago and many others—and has signed a USD9.5M contract with the U.S. Air Force (Devo 2020).

To grow the small number of start-ups and SMEs working on defense AI in Spain, large companies have taken action to entice more small companies to become active in this technology field. For example, Indra Systems launched the "FCAS Challenge" (Future Combat Air System), to boost the innovation capacity of the entire Spanish industrial ecosystem to the maximum by jointly developing emerging and disruptive technologies within the framework of FCAS. The FCAS Challenge aims to attract SMEs with cutting-edge technologies or highly innovative projects, with the objective of collaborating in the development, promotion, and maturation of their technological proposals. AI, data management in distributed clouds, technologies for low observability sensors, simulation and representation of information, optical technologies, or radio frequency (RF) and microwaves, are some of the technologies of greatest interest to the initiative (Indra 2023).

2.2 Developing Defense AI at the EU Level

The EU is an important reference point for the Spanish defense industry. The DDP, for example, stipulates the ambition to internationalize the Spanish defense industry within the framework of the EU (Arteaga 2022a, b). The main goal for Spain is to

push national solutions abroad through multi-nationalization in areas where the Spanish industry is a leader. The main challenge still is to leverage EU projects to support those Spanish stakeholders that are not leaders in their areas but may benefit from these EU-wide projects to close existing industry capability and capacity gaps.

Strategies presented above show that the development of defense AI is part of the three lines of effort that Spain is contributing to at the EU level. In the research phase, it started with PADR (Preparatory Action on Defense Research 2017–2019) and now with Research Actions under the European Defense Fund (2021–2027). In the development phase, it started with European Defense Industrial Development Programme (EDIDP 2019–2020), and currently with Development Actions under the European Defense Fund (2021–2027). In the acquisition phase, the financial toolbox of contributions remains essential for a joint view on defense AI.

Spain has been an early supporter of the EDF launched in 2021 (Fiott 2023) and has since actively participated in several projects. Under the PADR, Spain led three defense research projects and 19 Spanish entities were involved in projects totaling €70M. Under the EDIDP, Spanish entities led eight projects and 64 of its entities were involved in EDIDP projects, that amounted for a total of €371M.

The naval domain has represented the largest share of the investments over the two EDF calls with an amount of €540M–€449M being invested in ground combat capabilities and €439M in space. The maritime sector is one of the key industries for the Spanish defense ecosystem, and where Spain is a leader worldwide. In particular, the Spanish ecosystem considers that the use of AI will become vitally important as an indispensable support to the decision-making process in the new way of operating at sea and from the sea. Finally, the operational environment of the near future requires fully connected naval forces, across branches and between allies. In this regard, Spain expects AI to play an important role in reinforcing ideas originally developed for network-centric warfare and to advance cross-domain cooperative engagement capabilities.

Although important, it is difficult to assess the specific defense AI development goals for current EDF projects. Based on this author's analysis, the following seven projects seem particularly relevant:

- *Frugal and Robust AI for Defence Advanced Technology (FaRADAI)*

FaRADAI focuses on frugal learning. The consortium includes the Fundaction Tecnalia Research & Innovation, Indra Sistemas, Thales Programas de Electronica y Comunicaciones and the Universidad Politecnica de Madrid.

- *Proactive automatic imagery intelligence powered by artificial intelligence exploiting European space assets (IntSen2)*

IntSen2 develops AI for Imagery Intelligence (IMINT). The consortium is led by Tracasa Instrumental and includes Trabajos Catastrales and Zabala Innovation Consulting from Spain.

- *Knowledge Extraction, Machine Learning, and other AI approaches for secure, robust, frugal, resilient and explainable solutions in Defence Applications (KOIOS)*

KOIOS seeks to improve defense AI, among other things, by defining metrics to measure frugality, robustness, and resilience. Led by CT Ingenieros Aeronauticos de Automocion e Industriales, the consortium also includes the Barcelona Supercomputing Centre, and NTT Data.

- *Convoy Operations with Manned-unManneDSystems (COMMANDS)*

COMMANDS is to develop capabilities for cooperative manned-unmanned land systems. Under the leadership of Sener Aerospacial Sociedad Anonima, the consortium also includes Indra Sistemas and the Instituto Nacional de Tecnica Aerospacial Esteban Terradas and Santa Barbara Sistemas.

- *Digital Ship Structural Health Monitoring (dTHOR)*

dTHOR aims to improve battle damage and structural integrity assessments of ships and includes the National Institute of Aerospace Technology, SAES, and Tecnicas Y Servicios de Ingenieria from Spain.

- *European Digital Naval Foundation (EDINAF)*

EDINAF is about integration of a joint naval operational cloud in cloud-based approaches for Multi-Domain Operations. Led by Spain's Navantia, the consortium also includes Aertec Solutions, Indra Sistemas, and the Universidade da Coruna from Spain.

- *European framework and proof-of-concept for intelligent automation of cyber defence incident management (EU-GUARDIAN)*

EU-GUARDIAN shall create AI-based solutions to automate incident management and cyber defense. Indra Sistemas leads the consortium, which also includes the University of Murcia.

2.3 Developing Defense AI at the NATO Level

Spain's commitments to its NATO allies have made it necessary to double the defense budget until 2029, starting with a 25.8% increase in 2023 (from €9.791bn in 2022 to €12.317bn in 2023). Of this, €5.241bn will be allocated to modernization programs (122A) and special modernization programs (122B) in 2023, €5.908bn in 2024, €5.576bn in 2025 and €5.766bn in 2026 (Fiott 2023). Unlike recently, the budget increase in investment should not only be aimed at providing military capabilities to the armed forces and orders to the defense industry (spend more), but also at adapting the national defense economy to the geostrategic rivalry with Russia and geopolitical competition with China (spend better), including AI.

Spain fully supports and contributes to NATO's recent innovation initiatives, the Defence Innovation Accelerator for the North Atlantic Alliance (DIANA), and the NATO Innovation Fund (Ricart 2023). Spain is home to five test centers, which focus on AI alongside maritime security and defense, neurotechnology, 5G,

quantum communications and energy. Spain expects both NATO defense innovations to stimulate the local AI-related defense innovation ecosystem and to advance interconnections with partners across the Alliance.

3 Organizing Defense AI

The governance of defense AI is managed by the Sub-Directorate General for Planning, Technology, and Innovation (SDG PLATIN) at the Directorate General for Armament and Materials (DGAM), which belongs to the Secretary of State for Defense at the Spanish MoD. The main function of SDG PLATIN is to propose and direct the plans and programs for research and development of weapons systems and equipment of interest for national defense, in coordination with the relevant national and international organizations. The SDG PLATIN is also responsible for:

- Developing defense R&D policy;
- Drawing up the Defense Technology and Innovation Strategy (ETID);
- Coordinating and monitoring the defense R&D activities carried out by the different R&D centers of the MoD and establishing, coordinating, supervising, and evaluating the results achieved by the Department's organizations executing the established R&D policy.

While defense AI is located in SDG PLATIN at the MoD, ETID, which provides guidance on the development of defense technology, is a sector-specific strategy derived from the overall Spanish Strategy on Science, Technology, and Innovation. This latter strategy is managed by the Ministry of Science and Innovation, which coordinates the National Plans of Scientific, Technical and Innovation Research (PEICTI) for the periods 2021–2023 and 2024–2027 that fund the technological goals of different ministries, including those of the MoD.

This means that there are two levels of inter- and intra-ministerial governance. First, ETID is an in instrument of inter-ministerial governance, focusing on defense AI and defense technologies. While the MoD is in lead, it acknowledges the need to promote and facilitate innovation and dual developments in coordination with other ministries, mainly the Ministry of Industry, Trade and Tourism (MINCOTUR), the Ministry of Science and Innovation (MICI) and the Ministry of Finance and Public Administrations (MINHAP).

In addition, the Secretariat of State for Digitalization and Artificial Intelligence also addresses AI. The Secretariat has existed since 2020 under the 1st Vice-Presidency and Ministry for Economic Affairs and Digital Transformation and has been transformed into the Ministry for Digital Transformation in late 2023. The National Strategy on Artificial Intelligence (Ministry of Economic Affairs and Digital Transformation 2020) emphasizes the need to leverage the opportunities and mitigate the risks presented by AI. This strategy does not include defense but earmarked €50M for investment in five flagship AI R&D projects in 2021 in agriculture

and food; health; environment; energy; and employment, thereby covering 78 entities.

Second, intra-ministerial defense AI governance is organized around the SDG PLATIN. In addition, other Secretaries of State as well as other subordinate bodies such as the University Centers for Defense (CUD), the Research Centre for High Studies on National Defense (CESEDEN) and technical R&D centers affiliated to the MoD like the Esteban Terradas National Institute for Aerospace Technology (Instituto Nacional de Técnica Aeroespacial Esteban Terradas) play important roles. As RD&I involves the resources of many different departments, coordination via DGAM must involve many different stakeholders. Therefore, infrastructure-related activities involve coordination with the Directorate General for Infrastructure (DIGENIN), while ICT-related projects need to be synchronized with the Center for Information and Communications Systems and Technologies (CESTIC). Close coordination is not only needed to make best use of limited defense funds, but also in view of making sure that civilian RD&I efforts are not duplicated.

Moreover, Spain's defense AI governance also needs to respect the country's federal structure. Spain's administrative-political system is composed of seventeen autonomous regions ("Comunidades Autónomas") and two autonomous cities (Ceuta and Melilla in North Africa), with both exclusive competencies and competencies shared with the central government in Madrid. Defense is an exclusive competence of the central government. However, when it involves opportunities to perform defense AI R&D, there are several autonomous regions that harbor relevant institutions and research centers. For instance, Madrid hosts the EU Satellite Center. Valencia hosts a High Availability Military Base Camp with a long NATO record. Andalusia counts on a large network of defense companies, mostly in the maritime domain.

Finally, AI governance also includes complex discussions on ownership of sensitive data and involves non-defense entities engaged in dual-use activities. For example, the Government of Spain (Government of Spain 2023) announced the launch of the ADIA Lab, a research lab on AI, data science, machine learning, high-performance computing and quantum that would be based at the University of Granada, Andalusia. It receives funding from the Emirati sovereign wealth fund Abu Dhabi Investment Authority (ADIA). The project will last for four years, until 2027, and the goal is to support this research development to provide market solutions. There are no explicit statements on whether the knowledge transfer is bidirectional or goes to one specific direction. ADIA Lab is part of a bilateral agreement signed by the Presidents of Spain and the United Arab Emirates in February 2022. While there is no publicly available information on the lab's concrete AI agenda and possible future use cases, the signing of the agreement was controversial with civil society organizations voicing concern over the risks of potentially sharing sensitive information with a non-EU and non-NATO country.

4 Funding Defense AI

Spain funds activities in support of defense AI via specific defense programs as well as programs that help to advance the country's technological capabilities in general. In 2020, the new ETID set out the basic goals for promoting defense-related RD&I focusing on

1. maintaining participation in EDA R&T activities, especially in defining research priorities and agendas, and participating in cooperation projects when they effectively complement R&T activities carried out at the national level or in the EDF format;
2. increasing national participation in activities of the NATO Science and Technology Organization (NATO STO) following the main technology trajectories set out in the ETID, and improving the exploitation of their results, exploring and exploiting the possibilities offered by other NATO-promoted research and practical technological cooperation tools in areas other than STO activities, such as partnerships;
3. participating in the elaboration of EDF work programs by submitting proposals relevant for collaborative European defense R&D;
4. Supporting the EDF's research window up to Technology Readiness Level (TRL) 6 and with a focus on domains that ensure sufficient technological capacity for the participation of Spain's DTIB;
5. Supporting the EDF development window with the launch of priority technological developments (above TRL 6) of high cost and complexity, including supporting multilateral programs that offer sufficient opportunities for the Spanish DTIB to play an active role, and promoting standardization and interoperability of systems at European levels.

4.1 Funding Programs on Defense Solutions, Including AI

The MoD leads several funding programs that revolve around solutions for the defense ecosystem. Out of these, the Program for Cooperation in Scientific Research and Strategic Technologies Development (COINCIDENTE) aims to take advantage of civilian technologies developed within the scope of the National R&D Plan to incorporate innovative technological solutions of interest into the defense ecosystem.

COINCIDENTE projects must aim at developing a demonstrator with military functionality and involve significant technological innovation that meets a real or potential need of the MoD. The MoD's co-funding level varies between 20% and 80% depending on general defense interest, the level of innovation of the respective project, its technological maturity, as well as the size of the company presenting the project.

The COINCIDENTE framework was created in 1985, but its calls did not include any reference to AI until 2018, when AI was requested as an essential element in

proposals for projects implementing smart systems for military information analysis and solutions for other military problems. However, what was meant by "military problems" remained unclear. The call in 2020 included a specific requirement for detection technologies for active protection systems. The call in 2023 made a step forward and asked explicitly for solutions for synthetic data generation to train AI algorithms in defense applications.

Apart from the COINCIDENTE program, the MoD and other institutions have opened specific calls for concrete solutions that need short-term applications and responses on a non-annual basis. For instance, they launched Preliminary Market Consultations for the development of dual-use technologies, such as Earth satellite observation in 2023. The Centre for Technological Development and Innovation (CDTI), in collaboration with the Sub-Directorate General for Planning, Technology and Innovation of the DGAM, launched an initiative to promote the process of Innovative Public Procurement, in the form of pre-commercial procurement (PCP) in the field of Earth satellite observation. DGAM identified certain dual technology needs related to those that cannot be met through existing solutions on the market, and which could be addressed through a PCP process. One of the two proposals aims to integrate AI on board the satellites to reduce the necessary data transmission bandwidth.

4.2 Funding Technological Solutions, Including AI, with No Focus on Defense But Potential Alignment or Dual Use

Spanish institutions fund the development and implementation of AI. The CDTI funds several programs for international technological cooperation, including AI. CDTI organizes these international projects in two blocs. First, the Plan for International Calls, amounting to a total of 20 annual calls. Second, multilateral programs, that are made up of three initiatives:

- Eureka is an intergovernmental undertaking that aims to support the development of products, services and processes and help these companies position themselves in third countries' markets. To do so, Eureka establishes a partnership between a Spanish company and, at least, one firm or research center from a country that is part of the Eureka network. In addition to EU member states and associated countries, the Eureka Initiative also includes Ukraine, Argentina, Chile, Singapore, and South Africa.
- IBEROEKA projects are open for partners from Latin American and Caribbean countries, plus Spain and Portugal.
- Projects within the framework of the Partnership on Research and Innovation in the Mediterranean Area (PRIMA) are oriented towards Arab countries in North Africa, Turkey, and Southern European countries.

Out of these initiatives, AI tends to be included in the Annual Plan for International Calls and in then Eureka Initiative. However, it is difficult to assess if and to what extent projects funded under these initiatives generate spin-offs relevant for the Spanish defense ecosystem, as there is no breakdown on the specific applications of joint programs on AI.

5 Fielding and Operating Defense AI

5.1 Positive and Negative Goals

This section argues that the Spanish defense industry is guided by two main goals of the Spanish public administration: a positive goal that strives to seize the benefits of defense AI, and a negative goal that addresses the risks and challenges pertaining to developing and using defense AI. The Spanish government emphasizes both aspects as appropriate solutions for risk mitigation which can also create market opportunities for Spanish industry.

As for the positive goal, representative use cases include:

- Electronic warfare solutions adapted to the current and future electromagnetic environment, inter alia with a focus on developing state-of-the-art electronic warfare systems in the non-communication and communication bands; electronic support (ESM) and electronic countermeasures (ECM), for which technological advances in antennas, components and RF modules will be applied; and advanced warning and intelligence algorithms adapted to the signals present in the electromagnetic (EM) environment.
- Robotics with a focus on unmanned ground platforms for defense missions.
- Industry 4.0 technologies to enhance the digital transformation of the MoD.
- Automatic and intelligent analysis of large volumes of sensor data and technologies to enhance predictive maintenance of defense platforms.
- Intelligent analysis of multiple sources of information for decision support.
- Unmanned ground platforms for defense missions, unmanned surface, and underwater vehicles for defense missions as well as innovative applications of remotely piloted air systems (RPAS) for defense missions, and
- Human Performance Modification with the use of exoskeletons for defense missions.
- The use of AI in combination with sensors, signal intelligence, smart communications, and combat clouds as part of the FCAS Challenge launched by Indra Systems.

The negative goal covers the need for novel technological solutions to mitigate the risks of defense AI, due to the

- lack of clarity in the decision logic of many AI algorithms, in particular deep learning algorithms;

- difficulty in detecting fake multimedia content generated from real multimedia content;
- lack of robustness or malicious introduction of training data that alters or biases the learning process;
- data security and privacy throughout the process;
- unpredictable behavior of algorithms in novel situations for which they have not been prepared;
- possible cascading failures when incorporating multiple AI-based software modules in a complex system, such as those used in defense;
- need for large volumes of data to train algorithms;
- complexity of incorporating ethical criteria into decision-making processes.

Moreover, the ETID 2020 addresses the applications of biometric technologies, and the need to test the applications for speech and text analysis.

5.2 Technology Readiness Levels

For fielding and operating defense AI, there are two levels of action: early-stage technology development, and highly advanced technology maturity. For the first area of action, the main goal is to foster research in emerging technologies for TRL 1–3 (early stages) and achieve a growing level of complementarity with specific instruments managed by the public administration through calls for projects. As for high-technology maturity, the goal is to foster technology demonstrators (TRL 4–6) and prototypes (TRL 7–8) and leverage civilian developments to be incorporated into the military field with dual-use approaches.

However, what seems straightforward in theory looks more challenging in practice as several hurdles prevent the members of the Spanish defense ecosystem from fully exploiting the opportunities of defense AI (Díaz 2020). These hurdles include:

- *Access to Information*

The MoD prepares, in a cyclical process every six years, its defense planning cycle, which results in two documents, the Long-Term Doctrine Objective 2035 (Ministry of Defense 2019) and the Military Capabilities Objective. However, due to classification both documents are not publicly available. Therefore, members of the Spanish DTIB do not have access to the armed forces' short-, medium-, or long-term needs. Consequently, investments and defense development priorities may not be consistent with the needs of the Armed Forces.

- *Access to Requirements*

The detailed set of requirements formulated in operational, functional, technical, logistical, and physical terms to be met by these systems is not available. DTIB developments may not meet these requirements and, consequently, may not be of use to the SAF. Access to data can be included in this group when it is relevant to the design of solutions, such as in the case of systems that include AI.

- *Access to Evidence*

Information about Spanish defense projects are not always available to all members of the national ecosystem. Information asymmetry, however, is a problem as it can stifle competition and prevent the development of defense solutions that meet the requirements of the armed forces. Timely access to information would also help speed up development cycles. But demands for comprehensive information access collide with information classification.

- *Access to Operational Validation Environments*

Quality assessment criteria are needed when developing and deploying new defense solutions. In this regard test and experimentation centers play an increasingly important role to verify what has been developed. The number of these test and experimentation centers is growing in Spain, but they are not yet well spread across the country.

5.3 A Bet on Transparency in Operationalizing Defense Technologies

Although the operationalization of defense technologies projects is evident, there is still a lack of comprehensive awareness of investments undertaken at the national level. To this end, the public sector indicates that it has collaborated with private firms to establish quantitative indicators to assess the level of investments devoted to RD&I projects meeting defense goals, the number of projects and mobilized economic volume in dual-use projects, and the number of projects with private non-governmental funding. In addition, indicators also set out to assess quantitively the number of Spanish entities participating in the European DTIB, the percentage of economic returns generated by Spain's participation in EDF projects, the number of projects that applied to the EDF with Spanish participation, the results (granted, non-granted), and the investments in other multinational initiatives on technology development and investments returns. At the time of writing this chapter, the respective figures are still being collected.

6 Training for Defense AI

There is not much publicly available information on training for defense AI. However, this section aims to divide this topic in two main parts. First, how defense AI systems are trained. Second, how the human capital is trained to design, develop, implement, deploy, and use defense AI.

6.1 Training the Systems

Three lines of effort are worth mentioning to train defense AI systems:

- *Training the Systems for Specific Projects*

First, the public sector develops its own projects. This is the case of the Esteban Terradas National Institute for Aerospace Technology (Instituto Nacional de Técnica Aeroespacial Esteban Terradas, INTA), which conducts self-funded R&D projects in different technology areas (Marín 2019). IDATECT is the project that makes use of AI to improve the competences in the areas of Experimental Aerodynamics and Theoretical and Computational Aerodynamics to contribute to meeting the following technological challenges: new configurations with improved aerodynamic efficiency leading to lower fuel consumption and thus pollution reduction; innovative concepts for aerodynamic efficiency improvement, including active flow control devices, high-lift devices; multilevel and multidisciplinary modelling and simulation methods; robust and reliable design strategies, in order to manage the uncertainties of the models and their input data; and big data and artificial intelligence, including techniques that use data extracted from various sources to enable efficient and fast decision-making.

- *Creating Specific Centers for AI Training*

Training the AI systems for defense is not only a matter of funding specific projects. INTA's 2024 Work Plan (INTA 2023) foresees establishing the new Technological Center for Development and Experimentation (CETEDEX), located in Andalusia (Jaen). CETEDEX will also house three new centers aimed at developing anti-drone technologies, general vehicle and connected vehicle technologies, and AI. In 2024, ongoing work on setting up the main campus will continue, while the Advanced Proving Ground Project and initial technology projects will be launched.

- *Training the Systems to Improve Intra-Institutional Performance*

INTA is working to develop a project aimed at digitalising the Institute's activity. This project is structured into four major blocks with one block focusing on establishing the AI Supercomputing Center to accommodate the needs for modelling and simulation, using the most modern AI techniques on a single platform. The center will also develop a cloud system in both a private and hybrid cloud, which will provide the necessary flexibility and capacity for future INTA digital transformation projects.

6.2 Training the People

There is limited information on specific trainings for defense AI. However, private defense companies offer hands-on training on the usage of AI, inter alia, with a focus on defense AI training related to maritime security, aerospace, and the linkage between cybersecurity and AI. In parallel, the public sector also seeks to reinforce

trainings in practical terms. Already in the ETID 2020, the public administration suggested the creation of challenge programs and hackathons.

Integrating AI into defense solutions will require more technical coordination since AI—as a cross-cutting technology—will depend on the parallel modification of other technologies and specifications to generate added value for the SAF. This increases the level of complexity compared to traditional defense solutions. There is—in particular, against the systemic hurdles mentioned in the preceding section—a risk that unsynchronized development priorities will inevitably lead to imbalances in the technological levels of sophistication. The lack of publicly available information on training goals and activities undertaken by the MoD, the military services, and the defense industry underlines the pressing need to focus more attention on developing the skill sets needed to successfully design, develop, implement, deploy, use, and assess the results generated with defense AI in Spain.

7 Conclusion

Spain is slowly waking up to the realities of defense AI. AI has been considered an important issue across national strategies since the mid 2010s. However, it was not until the 2020s that AI became a centerpiece of strategy and was translated into roadmaps, tailored measures, and specific applications.

Although the governance system is adequately organized and coordinated across many different stakeholders, more needs to be done to advance defense AI in Spain. For example, funding needs to be increased, a broader portfolio of projects should be pursued, and information relevant for long-term force development in Spain needs to be made accessible to the Spanish defense industry. Furthermore, public, and private stakeholders need to engage more closely on setting out the goals that the use of defense AI is expected to accomplish, as well as the results (and the failures) ongoing defense AI development projects generate.

The defense market of defense AI is led by a few large companies that are also leading an important number of defense development projects at the EU level. Still, a larger focus on SMEs should developed to ensure that defense AI can tap into the capacities of a broad set of companies to avoid critical dependency on a few players.

The fielding and operationalization of defense AI benefits from taking place through different instruments, although further activities are recommendable due to the potential opportunities that AI brings into the defense ecosystem. This proposal would help increase the defense industrial footprint in Spain, create cross-company ecosystems, and increase the participation of Spanish companies in European projects. Finally, there is limited information on the training of systems and of human capital. A greater inclusion of curricula on defense AI should be fostered in university programs.

While it is not possible to define the long-term pathway for defense AI in Spain, the current trajectory shows that the ecosystem, the number of activities and the

interest are growing, suggesting a gradual uptick of defense AI activities in the country. However, the main challenge remains sustained investments in the technologies and skillsets needed to develop defense AI.

References

Arteaga, Félix. 2022a. *Estrategia de Seguridad Nacional 2021: más discurso que novedades*. Elcano Royal Institute. https://www.realinstitutoelcano.org/comentarios/estrategia-de-seguridad-nacional-2021-mas-discurso-que-novedades/. Accessed 30 January 2024.

———. 2022b. *La política industrial de defensa, civil y espacio de la Comisión Europea: ¡abran paso!* Elcano Royal Institute. https://www.realinstitutoelcano.org/analisis/la-politica-industrial-de-defensa-civil-y-espacio-de-la-comision-europea-abran-paso/. Accessed 30 January 2024.

Devo. 2020. *Devo Awarded $9.5M U.S. Air Force Contract for Next-Generation SIEM Technology*. Devo. https://www.devo.com/company/newsroom/devo-awarded-9-5m-u-s-air-force-contract-for-next-generation-siem-technology/. Accessed 30 January 2024.

Díaz, L.J.R. 2020. La participación española en la Cooperación Estructurada Permanente: oportunidades y desafíos para la industria de defensa nacional. *bie3: Boletín IEEE* 17: 562–573.

Fiott, Daniel. 2023. *Investing and Innovating? Spain and the European Defence Fund*. Elcano Royal Institute. https://www.realinstitutoelcano.org/en/analyses/investing-and-innovating-spain-and-the-european-defence-fund/. Accessed 30 January 2024.

Government of Spain. 2023. *ADIA Lab elige España como su sede europea para el desarrollo de la Inteligencia Artificial y la computación avanzada*. Madrid: Government of Spain.

Indra. 2023. Indra Launches "The FCAS Challenge" to Involve Spanish Startups and SMEs in the Development of Disruptive Technologies Within the Framework of the Future European Air Combat System. https://www.indracompany.com/sites/default/files/231023_pr_the_fcas_challenge.pdf. Accessed 30 January 2024.

INTA. 2023. *Plan de Actuación Anual 2024*. Instituto Nacional de Técnica Aeroespacial. https://www.inta.es/export/sites/default/.galleries/Galeria-pdfs-de-paginas/Plan-Actuacion-Anual-2024.pdf. Accessed 30 January 2024.

Marín, M. 2019. Reflexiones sobre la adaptación del sector industrial de defensa y seguridad de España a la nueva logística 4.0: la aplicación de modelos de cooperación público-privada. *Economía industrial* 412: 89–100.

Ministry of Defense. 2019. Long-Term Doctrine Objective (ODLP) 2035. https://emad.defensa.gob.es/Galerias/CCDC/files/Long-Term_Doctrine_Objective_ODLP_2035_English_version_JAN22_updt.pdf. Accessed 30 January 2024.

———. 2020a. *Directiva de Defensa Nacional*. Madrid: Government of Spain.

———. 2020b. *Directiva de Política de Defensa*. Madrid: Government of Spain.

———. 2020c. *Strategy on Technology and Innovation in Defense*. Madrid: Government of Spain.

Ministry of Economic Affairs and Digital Transformation. 2020. *National Strategy on Artificial Intelligence*. Madrid: Government of Spain.

National Security Department. 2017. *Estrategia de Seguridad Nacional. National Security Department. Ministry of the Presidency*. Madrid: Government of Spain.

———. 2021. *Estrategia de Seguridad Nacional. National Security Department. Ministry of the Presidency*. Madrid: Government of Spain.

Ricart, Raquel Jorge. 2022. *Critical Technologies and Industrial Capabilities: National Definition and Policy Implications. The Spanish Case*. The French Institute for International and Strategic Affairs. https://www.iris-france.org/wp-content/uploads/2022/06/ARES-76-Comment.pdf. Accessed 30 January 2024.

———. 2023. *NATO Defense Innovation and Deep Tech: Measuring Willingness and Effectiveness*. Carnegie Europe. https://carnegieeurope.eu/2023/08/29/nato-defense-innovation-and-deep-tech-measuring-willingness-and-effectiveness-pub-90314. Accessed 30 January 2024.

Exploring the Benefits of a New Force Enabler: Defense AI in Italy

Andrea Gilli, Mauro Gilli, and Ivan Zaccagnini

In the realm of defense Artificial Intelligence (AI), Italy undeniably finds itself as a latecomer, but it is determined to catch up. Italy's strategy revolves around narrowing its gap with other countries, and it forms an integral component of its wider initiatives for the digitalization and digitization of the country and more specifically of its Armed Forces. The Italian government views AI as both a potential asset that can enhance its capabilities and a potential threat. The former perspective has been instrumental in the government's dedication to preserve human involvement in decision-making processes, a concept commonly referred to as keeping humans in the loop, all while pursuing modernization efforts. However, Italy issues a warning regarding the integration of AI with other disruptive and emerging technologies, such as robotics and unmanned vehicles. Such integration could, on the one hand, be used to enhance national military capabilities, but, on the other hand, it could present new difficulties for the Italian Armed Forces as well as new challenges for the industrial sector and economic stability. Overall, Italy views defense AI as a new force enabler, something that could improve the capabilities of the Italian Armed Forces on the battlefield through sophisticated sensors and automation, data fusion, and decision-making support.

A. Gilli
University of St Andrews, St Andrews, Scotland

M. Gilli
Center for Security Studies, Swiss Federal Institute of Technology, Zurich, Switzerland
e-mail: mauro.gilli@sipo.gess.ethz.ch

I. Zaccagnini (✉)
Department of Political Science, LUISS Guido Carli University, Rome, Italy

Center for Security, Diplomacy, and Strategy (CSDS), Vrije Universiteit Brussels (VUB), Brussels, Belgium
e-mail: izaccagnini@luiss.it

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_13

Italy's commitment to digitize and modernize its Armed Forces dates to early the 2000s. The so-called Forza NEC (Network Enabled Capabilities) program has been running an extensive procurement and digitalization process since 2007 (Nones & Marrone 2011). By integrating new and old military assets "into network," it seeks to modernize, digitize, and integrate the Italian Armed Forces by 2031 to improve their capabilities for computation, information exchange, communication, and situation awareness. Additionally, in 2021, the Italian Ministry of Defense (MoD) allocated €190M for a program focused on AI development and improvement for the period 2021–2035. Even though the design, development, and implementation of defense AI parts and components are included in numerous programs (national and multinational) which Italy funded over the same period, this is probably the only project that is exclusively focused on defense AI. Some programs that involve the partial use of AI or AI-supported technologies are the Global Combat Air Programme (GCAP), the Future Combat Naval System, the Safe Soldier System, and the Robotics and Autonomous Systems Experimentation Campaign (RAS) among others.

It is noteworthy that the Italian Armed Forces are working cooperatively and synergically on their major projects with the country's entire AI ecosystem, which consists of academic institutions, civil and military research labs, startups, and private and public high-tech firms. As a prime contractor, system integrator, and systems authority for the architectural requirements, Leonardo, for instance, has been heavily involved in all phases of the Forza NEC program.

Finally, the majority of Italian defense AI development projects are designed with the goal of optimizing resources and ensuring integrability and interoperability both among the branches of the Italian Armed Forces as well as among NATO allies and platforms—this is also true for AI and training simulations. The Italian Armed Forces have set some specific and very ambitious goals for 2035, but it remains to be seen whether they will be able to meet them by that deadline.

1 Thinking About Defense AI

AI is a critical technology for both commercial and military applications. Commercial companies such as Google, NVIDIA, Alphabet, Amazon, Meta, and IBM are market leaders in AI technologies applied to projects such as autonomous vehicle guidance systems, processing software, e-commerce search algorithms, social networks, targeted advertising, virtual reality, visual tracking systems, and many others. In fact, many experts and practitioners believe that the defense industry and military organizations are lagging (at least in some sectors), but they are catching up quickly. Today, most of the world's medium and great powers recognize that defense AI will be a key strategic technology in future conflicts as well as in global competition in general.

Italy has officially acknowledged the importance of developing and applying AI in defense. Despite being a latecomer, both the Italian government and its Armed

Forces (Esercito Italiano, Marina Militare, and Aeuronautica Militare) have listed AI as one of the key technologies in which the country must invest now and in the future in their official documents. Accordingly, Italy is planning a development and funding program for AI and other related technologies (Ministry of Defense 2021).

Former Defense Minister Lorenzo Guerini issued the Documento Programmatico Pluriennale della Difesa per il Triennio 2021–2023 (Pluriannual Defense Planning Document for the Three Years 2021–2023) in 2021. This document detailed and contextualized Italy's efforts to invest in emerging and disruptive technologies such as AI, augmented reality (AR), robotics, big data, quantum computing, and direct energy systems. It also stated that these technologies are urgent and priority investments, emphasizing the need to exploit and investigate the potential applications of these new technologies to operate efficiently in the cyber-domain.

In 2019, the Italian Army General Plans Department Plans Office (GPDPO) published the document "Future Operating Environment post 2035—Implications for Land Forces," which was part of the "conceptual work conducted by the Army" with the goal of "identifying the principal actors and the nature of the future environment in which land forces may be called upon to operate" (GPDPO 2019: 2). The paper sought to "describe hypothetical scenarios and the main challenges which the Army will confront" and "find possible solutions that will be able to drive the process of capability development in support of Defense" (GPDPO 2019: 2). Furthermore, the document provides a brief overview of the current scenarios and challenges that Italian ground units are likely to face on modern battlefields. The Italian Army views AI as both a technology to be exploited and a potential source of future danger. Italian land units, in particular, may face new threats such as swarms of drones and AI-enabled robots. Simultaneously, AI is listed as one of the "new and potentially revolutionary technologies" or "game changers" that the Italian Army must develop and exploit in the future to enhance its capabilities and the safety of its personnel (GPDPO 2019: 2–13).

The other branches of the Italian Armed Forces share a similar view: both the Italian Air Force and the Italian Navy are committed to developing a new approach for Intelligence, Surveillance, and Reconnaissance (ISR) missions through the integration of manned and unmanned systems, which necessitates the application of AI technology. They specifically foresee the use of AI for autonomous surveillance, automatic target recognition, and teams of manned and autonomous vehicles. In this regard, the participation of Italy in the GCAP is telling (Italian Government 2022; UK Ministry of Defense 2021).

Overall, the Italian Armed Forces, as well as defense companies such as Leonardo, are involved in several programs that necessitate the use of AI to develop and integrate modern sensors and platforms, both manned and unmanned. The Eurodrone MALE RPAS (Medium Altitude Long Endurance remotely piloted aircraft system) and the Future Combat Naval System are two prominent additional examples (PESCO Secretariat Undated-a; Italian Navy 2021). Since 2007, Italy has also been undergoing an ambitious procurement and digitalization process as a result of tight collaboration between the military and industrial sectors (Leonardo Undated-d). For instance, the Forza NEC program integrates the roles of "system

integrator" and "prime contractor" in a single actor—Finmeccanica-SES—and involves a wide number of national companies such as MBDA Italia, Oto Melara, AugustaWestland, Elettronica, Iveco DV, Engineering, CIO—Consorzio Iveco-Oto Melara, Leonardo-Finmeccanica, Beretta, Sistemi Compositi, and Aerosekur.

1.1 Defining AI

> Not humans against AI, but humans working with AI.
> (Defense General Staff 2021: 41)

In 2021, the Italian Defense General Staff (Stato Maggiore Difesa) identified emerging and disruptive technologies such as AI that "are modifying and influencing society, the economy, politics, and the military world" (Defense General Staff 2021: 74). Even though the Defense General Staff did not provide an explicit definition of AI, we can infer it from the Italian Armed Forces' documents. Like some common definitions in the field, the Italian Armed Forces regard AI as a set of hardware and software capable of providing computers with capabilities and performance commonly believed to be the exclusive domain of human intelligence.

Moreover, AI is considered a supportive technology, a sort of force and capacity multiplier that supports the work of soldiers and officers. Despite acknowledging the importance of emerging technologies, particularly in AI applications, the Italian Armed Forces are committed to keeping the human operators at the center of the loop in military operations (GPDPO 2019: 8–9). As a result, the Italian Armed Forces consider AI as an enabler that will improve their performance and decision-making ability (human in the loop), rather than a technology which will completely replace humans. However, the Italian Defense General Staff takes into account the possibility that in the near future some tasks will be carried out autonomously by AI under the supervision of the human being (human on the loop) and, they do not exclude a priori the possibility that in a more distant future, AI could even operate without human action in the management process (human out of the loop).

The Italian Navy shows more concern than the other services in fully automating its operations and platforms. The Navy's core value of multiple redundancies makes it seem impossible to them at the moment to take human control away from some crucial processes and activities. In this regard, according to the Navy, human control is essential due to the maritime domain's unique challenges in comparison to others. The Italian Navy is, on the other hand, gradually implementing drones, modifying current naval units to make use of remotely piloted aerial vehicles (RPAs), and creating new units with these technologies in mind.

1.2 The Role of AI in Italy

The Italian AI ecosystem consists of a wide number of Research Technology Organizations (RTO), defense, and non-defense companies. The complex and varied set of actors also includes universities and research centers, governmental organizations, state-owned as well as private-owned companies, and startups. The Agency for Digital Italy (Agenzia per l'Italia Digitale) in collaboration with the Italian Association for Artificial Intelligence (Associazione Italiana per l'Intelligenza Artificiale) registered in the period between 2017 and 2020 the following data: 20 Universities, 19 Research Centers, 92 Companies, 6 Public Administration entities and 51 startups (Fig. 1).

Additionally, one of the most significant multinational Italian companies, Leonardo, invested in dedicated research facilities for AI and related technologies and processes. In particular, Leonardo is concentrating its effort and resources in areas such as "system autonomy through Swarm Intelligence techniques; algorithms for unmanned systems; command and control systems; cognitive sensors and resilience systems; cyber security systems; signal processing in radars through to war-gaming and simulation systems; industrial process optimization; and predictive maintenance" (Leonardo Undated-c).

The Italian government released its "Strategic Program on Artificial Intelligence 2022–2024" in 2021, outlining its goals for the field as well as discussing the advantages and disadvantages of its AI ecosystem (Italian Government 2021). There are four strengths and weaknesses listed in the document. Regarding the latter, the main issues are the parceled growth of research labs, a poor ability to attract talent, a

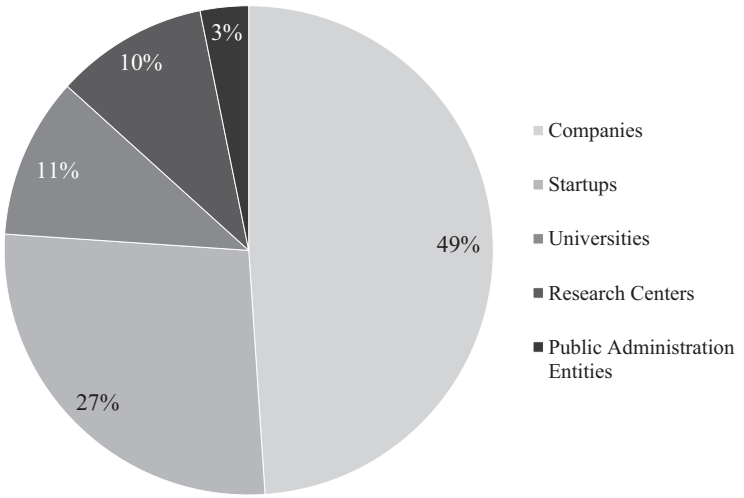


Fig. 1 Relative number of actors in Italy's AI ecosystem. Source: Agenzia per l'Italia Digitale in collaboration with Associazione Italiana per l'Intelligenza Artificiale, 2017–2020. Authors' pie chart

significant gender gap among its members, and finally, a limited number of patents. Research centers, education and training, physical and digital assets, and communities provide some of the advantages of the Italian AI ecosystem:

- First, Italian researchers are very active and primarily employed by public research institutions like the National Research Council (CNR) and research foundations like the Fondazione Bruno Kessler or the Italian Institute of Technology, as well as university research labs. They cover a broad range of AI technologies, including "Machine/Deep Learning, Computer Vision, Natural Language Processing (NLP), Data Mining, Big Data analytics, Embedded AI, Human aspects in AI, Knowledge Representation and Symbolic Learning, Decision Support Systems, Agent-based systems, and Trustworthy AI" (Italian Government 2021: 5).
- Second, the report notes that Italy is making assertive investments in training and education. There are currently more than 200 AI curricula available at 50 different universities across the country. To boost the training of researchers, innovators, and professionals in the field of artificial intelligence, the Italian government recently launched its National "Artificial Intelligence" PhD Program. According to the official document, the program "has awarded 200 PhD scholarships with a budget of €16M" (Italian Government 2021: 5).
- Third, Italy can rely on top-tier research infrastructure and assets including the CINECA-INFN Infrastructure for HPC, CNR-High Performance Artificial Intelligence Center HP-AI, and finally, the new IIT HPC infrastructures that are part of the 2020–2023 Strategic asset in AI and Machine Learning.
- Finally, Italian experts participate in all the major international AI research networks, including CLAIRE, ELLIS, HumanE-AI-Net, TAILOR, AI4ME-DIA, ELISE, and VISION. As a result, Italy has a vibrant and dynamic AI research community. Additionally, Italy is among the founding members of the Global Partnership on AI (GPAI).

The Italian Armed Forces, which are currently focusing on defense AI, fully understand and recognize the need to develop AI-driven and AI-supported military technologies and operate them in modern conflicts. Today, the battlefield is more complex than ever, and soldiers receive a massive amount of data that must be aggregated, fused, filtered, processed, and understood in real-time. This is made possible by the integration of modern sensors and technologies. Military personnel require the assistance of AI and machine learning at every stage of the procedure to achieve this goal and to identify and interpret data that are even larger in volume, faster, and more complex than in the past.

In military operations, AI's computational power will facilitate and support the work of the soldiers, and through simulations and probabilistic calculations, it will also help the officers make decisions. Leonardo, for example, established a research team to AI-enhanced "solutions to develop systems that support forecasting and decision-making processes" (Leonardo Undated-b).

Given that commercial companies are responsible for driving technological innovation, the Italian MoD is aware that collaboration with non-defense businesses

and organizations is essential to facilitating the transfer of know-how and technology. To foster collaborations with civilian and private businesses, the MoD, among others, plans the establishment of AI-dedicated research centers (Pulcini 2022), as will be discussed more extensively in the following sections.

1.3 Concerns and Opportunities

The Italian Armed Forces have acknowledged the opportunities presented by AI and have worked to determine the best strategy for utilizing them. Two key documents have been created in this regard by the Italian Defense General Staff and the Italian Army Headquarters General Plans Department Plans Office.

The former has identified several AI employments. It has acknowledged that, even though AI has grown to be a crucial technology for the military and defense industry, it is still impossible to predict the exact course of this technology. At the same time, however, the Defense General Staff claims that AI will simplify complex logistics and demanding maintenance, improving readiness and agility; increase computational capabilities, enabling armed forces to analyze adversaries' decisions more quickly and more effectively; and enhance the management of remotely piloted vehicles, enabling autonomous and coordinated operations, including the integration of a cyber component such as a network of sensors with IoT (Internet of Things) and with IoBT (Internet of Battlefield Things) (Italian Defense General Staff 2021).

The Italian Defense General Staff has also acknowledged some concerns that AI raises related to how it would make part of the workforce redundant, thus requiring effort to help them reintegrate into the job market. Other issues have been clarified by a document created by the Italian Army Headquarters General Plans Department Plans Office. Accordingly, military personnel will specifically need to learn how to deal with emerging and disruptive technologies (such as robots with artificial intelligence, swarms of drones, nanotechnology, alternative energy, and psychological operations) and how to coexist with them and manage the process of technological innovation (GPDPO 2019).

2 Developing Defense AI

Given the fact that Italy is lagging behind in AI compared to other middle powers, the Ministry of Defense (MoD) has launched a very ambitious program to catch up. Overall, the Ministry of Defense wants to provide the Armed Forces with digital platforms that are integrated with robotic systems and are capable of quickly and effectively receiving, processing, and sharing information at the tactical, operational, and strategic levels (Ministry of Defense 2021).

Within the MoD, the General Secretariat of the Defense, and the National Directorate for Armament, oversee the development of military AI and other military technologies. The MoD is committed to meet the requirements of the various Armed Forces and make sure that the technologies comply with the principles of interoperability, interchangeability, and integration. In addition, it is responsible for outlining which technologies are the most urgent to invest in. For instance, autonomous systems, cyber capabilities, space, command and control, and multi-domain situation awareness technologies are some of the areas recognized as top priorities by the MoD.

Since the 2002 Prague Summit, NATO members have pursued the digitization of their armed forces, through the so-called Network Enabled Capabilities (NEC). With this acronym, "NATO expressed the idea of 'enabling the capability' of combining heterogeneous elements—doctrinal, procedural, technological, organizational and human—into a single network, in order to achieve, through the interaction of these elements, strategic superiority in military operations" (De Zan 2016: 115). Consequently, in 2007 the Italian MoD started a procurement and digitalization inter-force program to meet this requirement and to modernize its armed forces. The Forza NEC program is to be completed by 2031 with an expected cost of €22bn (Table 1).

2.1 Current Defense AI

Italy's defense AI lag has several, technological and economic root causes. There is "an evident gap" between Italian national capabilities and those of comparable countries, such as in AI, quantum computing, cyber defense, and microprocessors, as acknowledged in the Pluriannual Planning Document 2021–2023 of the MoD (Ministry of Defense 2021: 138). Accordingly, the MoD and the Ministry of Homeland Security are committed to catching up with state-of-the-art AI. In 2013, the Center for Advanced Studies in Defense (CASD) reported that Italy was investing relatively little in R&D for defense in comparison to other countries (Lt Col Dotoli 2015). But the same report also emphasized how the government had supported initiatives meant to encourage technological innovation and information

Table 1 Forza NEC program phases

Forza NEC program phases	Year
Feasibility study	2007
Project definition	2007–2010
CD&E (Concept Development & Experimentation)	2010–2013
First phase of implementation	2018
Second phase of implementation	2026
Third phase of implementation	2031

exchanges among various sectors, including research facilities, ministries, the armed forces, universities, and both public and private businesses (Ministry of Defense 2015).

Since 2013, several documents published by the research centers of the Italian Armed Forces have underlined the need to allocate more funds for technological innovation. But only recently, starting in 2019, have the most significant incentives emerged. In this regard, it has not helped that government defense spending decreased between 2008 and 2015, despite an increase in the proportion of government spending on R&D from 0.95% to 1.53% of GDP (Worldbank Data Undated-a, b).

2.2 Defining AI Structure and Organization

The MoD manages, plans, and coordinates military research and development. The General Secretary for the Defense is specifically responsible for facilitating and encouraging collaboration between the government and businesses, whether they are military or commercial, domestic, or international. In addition, the Fifth Directorate of the Secretariat General of and the National Armaments Directorate (SGD/DNA) work to expand the MoD's knowledge base in high-tech fields so that Italy can participate in future national and international defense programs.

The SGD/DNA conduct assessment and planning regarding R&D in defense, which entails gathering and coordinating ideas and proposals from academic institutions, research centers, private companies, and the MoD itself. The SGD/DNA then integrates the National Plan for Military Research is then integrated with these concepts and recommendations. Furthermore, the SGD/DNA also aims to strengthen and broaden international cooperation within the EU and NATO.

Finally, the Center for Innovation in Defense, a significant organization within the Stato Maggiore Difesa (Defense General Staff), is tasked with ensuring and promoting the conceptual and doctrinal development and upgrading necessary to enable the transformation of the military. This center is specifically in charge of fostering innovative strategic thinking to determine the aims, directions, and priorities of technological development.

2.3 Main Defense AI Projects

Before examining the main defense AI projects of the Italian Armed Forces, it is crucial to remember that Italy has been taking part in many multinational projects as a member of NATO and the EU, and that some of the most ambitious and cutting-edge programs are conducted in cooperation with other nations. In this regard Italy's participation in the EU's Permanent Structured Cooperation (PESCO) is telling as it coordinates 8 projects and participates in 26 projects related to developing shared

and enabling capabilities, the cyber sector and the Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) sector. Additionally, Italy participates in projects dedicated to unmanned vehicles, aircraft, naval units, and space systems. In one way or another, all these projects require the support, application, and development of AI tools. Due to its involvement in so many multinational projects and operations, Italy will need to adhere to the interoperability standards set by both the EU and NATO (NATO 2022).

2.3.1 Joint

The Italian Armed Forces' multi-year funding program for AI 2021–2035 is one of their most ambitious projects. The goal of this joint initiative is to connect and network the research and experimentation facilities of the various military services. Additionally, the project seeks to foster and support collaboration between the network and civil research organizations specialized in AI. A portion of the resources allotted for this program will be dedicated to acquiring tools, creating, and modernizing physical spaces, and supporting cooperation agreements between the MoD and non-military research institutions such as universities and specialized centers (Ministry of Defense 2021).

2.3.2 Army

The Future Soldier Program, now known as Safe Soldier System, and the Robotics and Autonomous Systems (RAS) Experimentation Campaign are at the core of the Italian Army's initiatives, and both envision the exploitation of AI and AI-supported technologies.

The Safe Soldier System aims to provide infantry units with enhanced capabilities while also modernizing their weapons and equipment through the implementation of new hardware and software. For example, in 2020 the Army purchased 20,000 electronic systems for individual control and situational awareness to improve its soldiers' capacity to gather, process, and share real-time information while on the battlefield (Ciocchetti 2020). The Safe Soldier System program aims also to improve infantry protection, survival skills, C2 integration, nocturnal mobility, and lethality, providing them with advanced situational awareness capabilities. Furthermore, "the system allows, through digitized C2 devices, the joint use of the platform, ensuring maximum operation in all scenarios, from combat to population support, always remaining 'connected' to the net-centric architecture" (Italian Army Undated).

The RAS experimentation campaign represents the second main project and aims to improve human-machine interaction and manned-unmanned teaming. The goal is to enhance the situational awareness capabilities of ground units, particularly during operations in urban areas, through the cooperation and the synergistic employment of new advanced sensors. The Army Innovation Office oversees the

program. Despite not being directly involved in R&D, this office is in charge of understanding the most effective way to employ the technology that is developed by specialized centers in order to enhance military capabilities. The Army Innovation Office serves as a sort of bridge between technological development and operational activity. The RAS campaign specifically seeks to comprehend how to improve human-machine teaming by determining how robotic and autonomous systems can generate operational advantages in support of the ground forces' core (Lt. Col. Vito Marra 2022). In December 2021, the Italian Army finalized a contract with the Estonian company Milrem Robotics that joined the program as technological partner. In March and May 2022, two training activities have been carried out employing the digital platform models provided by the Milrem Robotics.

2.3.3 Air Force

Italy is involved in the development of two important multinational platforms that will be used by its air force: the MALE RPAS PESCO project, also known as Eurodrone, and the Global Combat Air Program (GCAP), which will merge two previously separated sixth-generation fighter-jet projects.

The GCAP was preceded by the Future Combat Air System (FCAS) program which was led by the United Kingdom with the collaboration of Italy and Sweden. The project, also known as Tempest program, aimed at developing a sixth-generation fighter jet and involving first-tier aerospace companies such as BAE Systems, Rolls-Royce, Leonardo UK and MBDA UK (Leonardo Undated-a). Tempest aspired to be a state-of-the-art jet fighter fully integrated with cutting-edge technologies like deep learning, swarming drones, direct-energy weapons, and more. Some claimed that the Tempest would have become "the most cutting-edge aircraft in the world" given its alleged capabilities and specifications (Kenealey 2020). Specifically, the cockpit would have been revolutionized, and the conventional controls would have been replaced by "augmented and virtual reality displays inside the visor of the helmet, which would be fully customizable" (Kenealey 2020). In addition, the human-machine teaming would have improved pilots' performance, assisting them making instantaneous decision, and carrying out critical flight maneuvers. Finally, Tempest would have embodied the so-called cooperative engagement capability, that is, "the ability to cooperate on the battlefield, sharing sensor data and messages to coordinate attack or defense" with both manned and unmanned systems (Mizokami 2018). However, the UK started a close cooperation with Japan on developing key aircraft components such as engines and radar demonstrators (Kelly et al. 2022). In 2022, the program was officially merged with the Japanese Mitsubishi F-X into the GCAP, envisioning a tight collaboration between UK, Italy, and Japan (Chuter 2022).

The MALE RPAS PESCO project aims to develop a next-generation Medium-Altitude Long-Endurance drone with ISTAR capabilities (European Commission 2021). The Eurodrone will have advanced ISR and data processing capabilities thanks to the application of new sensors and AI-supported technologies. The project involves top-tier European defense firms such as Airbus, Dassault, and Leonardo, as

well as other Italian firms like Avio and Elettronica Group. Thanks to its cutting-edge sensors and communication systems, the Eurodrone will be fully integrated with other military platforms and will improve EU Joint ISR capabilities as well as carry out homeland security operations, international conflict prevention, and crisis management.

2.3.4 Navy

The Italian Navy's primary defense AI initiatives aim to develop and field new technologies for unmanned systems and maritime surveillance. The Navy is trying to reduce the gap with other countries in unmanned and autonomous technologies, as only a few Italian ships have been modernized to host and operate unmanned aerial, surface, and underwater vehicles.

The Navy aims to purse this goal by both developing new platforms that already possess these capabilities and modernize legacy platforms. The Navy emphasizes the need to catch up technologically to protect national interests in both territorial and international waters while acknowledging that Italy is a latecomer in this field (Seminar, Capt. Quondamatteo and Capt. Vignola 2022). Specifically, by integrating, storing, and analyzing a large volume of different types of data (data fusion), the Navy believes that unmanned surface, underwater, and aerial vehicles will improve its ISR capabilities guaranteeing an all-domain all-weather coverage over its operational areas.

The Naval Future Combat System 2035 policy paper outlines the primary threats that the Italian Navy will encounter over the coming years and "summarizes the vision of the Armed Force on the Maritime Instrument of the future." According to this document, future Italian efforts will need focus on AI, big data, quantum, robotics, unmanned systems, innovative materials, hypersonic and direct energy weapons, and biotechnologies (Italian Navy 2021; Ciocchetti 2022).

Among other projects worthy of attention, it is possible to list the new European Patrol Corvette (EPC), the Harbour And Maritime Surveillance & Protection (HARMSPRO) PESCO project, the new offshore vessels, the and the new destroyers. Italy is the coordinator of HARMSPRO, which aims to provide member states with the capabilities to surveil and protect specified maritime areas such as harbors, littoral waters, and sea lines of communication fielding "an integrated system of maritime sensors, software and platforms (surface, underwater and aerial vehicles), which fuse and process data, to aid the detection and identification of a range of potential maritime threats" (PESCO Secretariat Undated-b). With regard to the new destroyer, it aims at the development and deployment in the coming years of a comprehensive anti-ballistic and anti-hypersonic missile capability to defend national territory and population.

3 Organizing Defense AI

As discussed above, the Italian Armed Forces organize current and upcoming projects both jointly and individually (single service) in accordance with the tasks needed to accomplish. On the one hand, the SGD/DNA coordinates the major AI programs, which are jointly developed and operated by the Armed Forces. As a result, they simultaneously serve the Army, the Navy, and the Air Force. On the other hand, other projects designed for specific requirements are developed and organized individually. The Robotics and Autonomous Systems Experimentation Campaign (RAS) of the Army, and the Advanced Recognition and Exploitation System (ARES) of the Air Force, are good examples. While the coordination and centralization of R&D efforts is the primary responsibility of the Secretariat General of Defense, all platforms and systems must also adhere to the requirements for integration, interoperability, and interchangeability. These requirements must be met for the Italian Armed Forces to coordinate their organizational efforts and engage in joint operations with their own different services and allies.

Italy has actively studied the lessons learned and the best practices of its traditional partners and allies, including the United States, United Kingdom, France, and Germany, to improve its organizational and innovation capabilities. As a result, Italy plans to establish a network that will connect all the national players engaged in the development of AI and other technologies deemed to have "strategic value." The ultimate goal of the Italian MoD is to boost and enhance the innovation process and foster "potential technological discontinuity—an objective aggressively pursued abroad by the renowned Defense Advanced Research Program Agency (DARPA)" (Ministry of Defense 2021).

4 Funding Defense AI

The office for General Joint Planning (Pianificazione Generale Interforze), which oversees the national defense plan, states that the goal of the initiative is to "to create and support an efficient, ready and effective military instrument, sustainable in terms of human and financial resources, perfectly balanced and integrated, with significantly interoperable features in its various components and in a multinational and inter-agency context, functional to a credible deterrence and to express concrete operational capabilities with multi-domain effects" (Ministry of Defense 2021). This type of long-term investment and planning is regulated by the Italian Leggi di Bilancio (Ministry of Defense 2021: 54–56).

By 2026–2028, Italy plans to field most of these investment programs. For 2021, the budget law has refinanced the "Fund relating to the implementation of multi-year investment programs for the needs of National Defense" with a budget of €12.35bn and which runs between 2021 and 2035. According to the Italian government, these measures will mark an "epochal turning point" (Ministry of Defense

2021: 56), providing the Italian Armed Forces with the tools they need to support long-term national efforts in defense needs, country digitalization and technological development. Among others, the main programs include the following projects:

- Joint: Joint Maritime Multimission System (J3MS), AI Development and Enhancement Programs, Acquisition of Defense Cloud capacity, Multi Data Link Modernization (MDL), European Cooperation Programs, A/R and air and missile defense enhancement and maintenance of the operational capacity of the defense satellites.
- Army: Infantry Fighting Vehicle (IFV), Leopard Tank Modernization and logistic support, Robotics and Autonomous Systems (RAS), SHORAD GRIFO renovation on CAMM-ER.
- Air Force: EUROPEAN MALE RPAS, TEMPEST (sixth generation "Combat Air System" now merged into the GCAP), C-27J (Jedi and Praetorian).
- Navy: Embarked Unmanned Aerial Systems (UAS), New Destroyers (DDX), New amphibius Units (LXD), European Patrol Corvette (EPC) and the new Offshore Patrol Vessels (OPV).

4.1 Joint Programs

The primary objective of the joint programs outlined in the Documento Programmatico Pluriennale della Difesa 2021–2023 is to develop, modernize, and renew a set of military assets and technologies that are deemed to be of the utmost strategic value by the entire Italian Armed Forces. The document underlines the importance of the development and application of AI to defense platforms and architectures.

Italy has earmarked a €190M budget for the period 2021–2035 to support the development and advancement of AI. This multi-year initiative seeks to establish a network of innovation hubs "that [will] enable the most qualified actors of the technical-operational area of Defense (i.e. the Experimental Centers or in any case the similar realities) to interact synergistically with the world of civilian research specialized in the sector of Artificial Intelligence and, in general, of emerging digital technologies" (Ministry of Defense 2021). These funds will facilitate the establishment of physical spaces and infrastructures, the procurement of tools, and the formalization of partnership agreements with prominent research centers. These agreements, among other benefits, will allow for synergistic collaboration with civilian researchers.

In addition, Italy has allocated funds for other joint programs relevant to develop defense AI applications. Table 2 provides an overview of these programs and the allocated resources.

Table 2 Italian joint programs involving defense-relevant AI applications

Joint program	Amount (in €M)
Emerging Disruptive Tech R&S	60
Data Collection	55
Capacity Acquisition for Data Sharing Based on Defense Cloud Concept	90.7
Upgrade Subsystem Multi Data Link Processor (MDLP)	26.29
Joint Maritime Multimission System (J3MS)	470
Acquisition of Defense Cloud capacity	90
Multi Data Link Modernization (MDL)	312
European Cooperation Programs	90
A/R and air and missile defense enhancement	358
Maintenance of the operational capacity of the defense satellites	100
Loitering Ammunition	3.88

Table 3 Italian army programs involving defense-relevant AI applications

Army program	Amount (in €M)
Remotely-piloted aircraft Mini and Micro	89
Infantry Fighting Vehicle (IFV)	1022
Leopard Tank Modernization and Logistic Support	192
Robotics and Autonomous Systems (RAS)	Unknown
Short-Range Air Defense (SHORAD) GRIFO renovation on CAMM-ER	235
Light tactical multirole vehicle (LMV) "Lince 2"	272

4.2 Army

The Italian Army wants to combine its existing assets (legacy) with cutting-edge platforms and AI technologies. Specifically, by updating and renovating outdated equipment, vehicles, and systems. In addition, the Army intends to improve the abilities of its infantry units by giving them the capacity to receive, share, and process information more quickly and efficiently by equipping them with new sensors and connecting them to the network. Furthermore, through the RAS campaign, the Army is at work to improve the human-machine interaction, through the synergically employment of small tactical unmanned aerial and ground vehicles and infantry units. Table 3 highlights the Army programs that include defense AI applications and the respective allocated resources.

4.3 Air Force

The Italian Air Force is engaged in two major, highly ambitious and most expensive projects involving AI: the development of the EUROPEAN MALE remotely piloted aircraft system and the Global Combat Air Program (GCAP). Italy has earmarked €1.8bn for the development, procurement, and logistical support of the Eurodrone within the scope of the PESCO project and allocated €2bn for the conceptualization, design, development, and procurement of sixth generation combat air systems. These two initiatives alone constitute approximately 31% of the total budget allocated to the "Fund relating to the implementation of multi-year investment programs for the needs of National Defense" for the period 2021–2035. Table 4 provides further details on additional Air Force programs and their respective budget allocations.

4.4 Navy

The Italian Navy's primary initiatives revolve around the construction of next-generation naval vessels and the modernization of existing systems to ensure compatibility with new platforms, especially unmanned systems. Among these, one of the most significant projects is the development of advanced offshore vessels, with a budget allocation of €1.5bn spanning the period from 2023 to 2035. Additionally, Italy holds the role of coordinator and project member in the European Patrol Corvette (EPC) PESCO project. Lastly, Italy has committed €2.3bn for the development and procurement of new destroyers, with a final estimated cost of €2.7bn. These cutting-edge naval units will be equipped with the latest sensor technology, hardware, and software, enabling them to efficiently transmit, receive, and process vast amounts of data in real-time.

Table 4 Italian air force programs involving defense-relevant AI applications

Air force program	Amount (in €M)
Smart Wing/Anti-intrusion	20
Air Defense Radar Digitalization	68
Network Info/Infrastructure (TLC e T-B-T)	29
Interoperability Force Elements C6ISTAR-EW—LND Study	71.40
C27J EW-JEDI and Mission System	27
Ballistic Missile Defense System (BMD+)	408
Implementation of the System for the Generation and Processing of Meteorological Data	22.49
Short Range Air Defense (SHORAD) capabilities	127
C4ISTAR	28

It is also worth to mention that the Italian Navy has also allocated €3M for the Embarked Remotely Piloted Aircraft study and €26M on the Coastal Radar Network.

5 Fielding and Operating Defense AI

At present, the Italian Armed Forces are actively involved in 43 operations across the globe, deploying approximately 16,400 military personnel, with a focus on crisis management and deterring potential threats. Roughly half of these operations are dedicated to the promotion of international security and the maintenance of stability. Italy stands as a significant contributor to missions conducted by NATO and the EU, and it holds the distinction of being the foremost contributor among Western countries to UN missions.

Despite its lag in developing defense AI solutions, Italy's armed forces have already implemented certain platforms that leverage AI applications. For instance, they are currently utilizing unmanned vehicles for ISR operations. Furthermore, the Secretariat General of Defense and National Armaments Directorate has recently allocated resources for the design and creation of a deep learning model intended to analyze aerial images acquired by drones (SGD/DNA 2022). Additionally, even though the incorporation of Defense AI into technologies such as drones, mixed reality, robotics, big data, and data fusion is still in its nascent stages, numerous significant programs are in progress. These initiatives align with Italy's overarching strategy to cultivate "an agile and projectable force, technologically advanced and capable to work with its allies in the context of international missions" (Ministry of Defense 2021: 10).

5.1 Army

The Italian Army is enhancing its capabilities in human-machine teaming through the ongoing development of the RAS campaign. This initiative aims to foster greater integration between unmanned vehicles and ground forces. While certain technologies have been deployed, the overarching concept and primary architecture are still in the process of development. Nevertheless, within the Army, infantry units are already employing a diverse array of mini and micro drones, including models such as Sixton, Asio, Spyball, Crex-B, and Raven (MILEX 2018). Furthermore, the Army has incorporated AI-driven software into various aspects of its operations, including command and communication functions. AI is also a valuable component in virtual and mixed reality training activities, contributing to more effective and immersive training experiences.

5.2 Air Force

During the early 2000s, the Italian Air Force embarked on the acquisition of large unmanned aerial vehicles (UAVs) from the United States. Specifically, Italy procured and subsequently operated cutting-edge platforms such as the Predator, Reaper, and, most recently, the Global Hawk (NATO variant). In a recent development, the MoD has considered investing in the domestically produced Piaggio P2HH UAV, with the aim of potentially replacing the Predator and Reaper in the future.

Moreover, the Italian Air Force is actively engaged in developing the Advanced Recognition and Exploitation System (ARES), which seeks to create and employ an open-source neural network utilizing data gathered by Predator platforms (CESMA Seminar 2022). The project leverages deep neural network algorithms for real-time object detection and acquisition. By training these algorithms on an unclassified dataset, the Air Force has successfully tested and demonstrated the protentional of AI to automatically recognize and simultaneously identify, track, and classify multiple targets in a theater of operations. The next phase of the project aims to enhance predictive capabilities, empowering the system to make forecasts based on the data it has gathered and classified (Col. Del Vecchio/Lt. Col. Diana 2022).

5.3 Navy

While the Italian Navy currently deploys unmanned vehicles, such as the Camcopter S-100, primarily for patrol missions, the integration of these assets into service lags behind comparable initiatives in Turkey or the United States. The principal objective of the Italian Navy is to develop the capacity to employ drones across three distinct domains: on the sea's surface, beneath the sea, and on land in conjunction with amphibious units. Specifically, the Navy relies on a trident of capabilities, encompassing the carrier strike group, the amphibious task group, and underwater units along with special forces. Consequently, the primary aim is to seamlessly integrate unmanned vehicles within this trident, thereby enhancing the naval force's capabilities across all three domains.

6 Training for (and with) Defense AI

The future demands of the Italian Armed Forces envision the ability to collaborate synergistically with machines, harnessing the potential of emerging technologies to elevate the performance of military personnel. Furthermore, this interaction between humans and machines will extend its advantages to training activities within the armed forces. In particular, Italy already relies on a suite of simulation

environments and cutting-edge technologies to train its military personnel through various modalities: live, virtual, and constructive (Ministry of Defense 2021: 43/117).

From an Italian perspective, simulated training exercises enable, and will increasingly enable in the future, the armed forces to enhance personnel readiness by using digital platforms, state-of-the-art software, and robotics systems. Moreover, Italy actively promotes collaborative endeavors among its various military branches to optimize resource management and minimize environmental impact. A notable illustration of this commitment is exemplified by the Rotary Wing Mission Training Center (RWMTC) initiative. This initiative seeks to bolster joint training efforts among Italian pilots, striving to establish a unified and mutually shared virtual and constructive simulated environment.

With respect to Italy's dedicated simulation infrastructure, the armed forces have access to both joint and single-service training facilities and centers. These include the Salto di Quirra Joint Training Area, the Army's Simulation and Validation Center (CESIVA) in Civitavecchia, the Navy's Training Center in Taranto, and the Air Force's Multi-Crew Training Center in Pomezia (Pratica di Mare).

In 2021, Italy initiated the Operational Training Infrastructure (OTI) program, slated for completion by 2033 with an estimated cost of €79.2M. The OTI project is specifically designed to enhance simulated training capabilities by focusing on "the development of an open, modular, persistent, resilient and safe geo-federated architecture aimed at connecting flight simulators, simulation systems and C2 systems to make them interoperable within a single and common synthetic simulation scenario that reproduces operational real, complex, uncertain and highly variable environments" (Ministry of Defense 2021: 130). Furthermore, the program encompasses efforts to enhance and modernize the infrastructure at the Salto di Quirra Joint Training Area.

7 Conclusion

Italy currently trails its counterparts in the realm of defense AI projects. This relative lag can be attributed to several contributing factors, which include a relatively narrow digital base in AI technology overall, a dearth of major AI companies operating within its borders (with very few exceptions), and comparatively limited financial resources. Nevertheless, Italy has intensified its efforts with the objective of narrowing the gap with cutting-edge technology. This endeavor is being pursued through collaborative partnerships with EU and NATO allies, engagement in national digitization programs, and strategic investments in academic research and development.

The Italian approach exhibits both strengths and weaknesses. On the positive side, Italy boasts a network of private and public research institutions with well-established expertise in high-tech fields. Additionally, there exist synergies between government entities, commercial enterprises, and defense companies, along with a

couple of leading educational institutions in Europe. However, on the downside, Italy's public finances limit the availability of substantial funds. Consequently, a question arises as to whether participation in the development of military technologies reliant on AI, such as the GCAP and Eurodrone projects, will provide the country with the requisite experience and know-how to bridge the existing gaps with other countries.

In pursuit of its future capability objectives, Italy has outlined two primary goals: the digitalization (use of digital technologies) and digitization (conversion of information into digital format) of the Italian Armed Forces, to achieve through the Forza NEC program, and the development and modernization of conventional assets, as outlined in the Documento Programmatico Pluriennale 2021–2023. The Forza NEC initiative is focused on establishing networked capabilities across various units, enabling real-time data sharing, seamless transmission, and reception of large datasets, and harnessing advanced computational capabilities. The Documento Programmatico Pluriennale 2021–2023 encompasses a range of investment plans aimed at incorporating AI applications and modernizing legacy assets.

Italy's extensive involvement in multinational defense projects plays a pivotal role in its strategy to fill the AI gap. This broad participation is influenced by both budgetary constraints and the technological complexity associated with the development process of cutting-edge AI and AI-supported technologies. However, it is important to note that Italy's reliance on multinational projects may shape the kind of experience and expertise it acquires. Consequently, this could impact the specific defense AI technologies that Italy will develop in the future, as well as the trajectories these technologies may follow.

References

Agenzia per l'Italia Digitale in collaboration with Associazione Italiana per l'Intelligenza Artificiale. 2017–2020. *Ecosistema Intelligenza Artificiale*. https://ia.italia.it/ia-in-italia/; https://ia.italia.it/ia-in-italia/#elenco-dellecosistema-ia-in-italia. Accessed 30 Jan 2024.

Centro Studi Militari Aeronautici (CESMA). 2022. Seminar. Artificial Intelligence (AI) Autonomous Surveillance, Automatic Target Recognition & Teams of Autonomous Vehicles. Rome

Chuter, Andrew. 2022. Move over, Tempest: Japan pact takes UK-Italy fighter plan 'global'. *Defense News*. https://www.defensenews.com/global/europe/2022/12/09/move-over-tempest-japan-pact-takes-uk-italy-fighter-plan-global/. Accessed 30 Jan 2024.

Ciocchetti, Tiziano. 2020. The Italian Army tries to modernize. *Difesa Online*. https://en.difesaonline.it/mondo-militare/lesercito-italiano-cerca-di-ammodernarsi. Accessed 30 Jan 2024.

———. 2022. Il Future Combat Naval System Secondo la Marina Militare. *Difesa Online*. https://www.difesaonline.it/mondo-militare/il-future-combat-naval-system-secondo-la-marina-militare. Accessed 30 Jan 2024.

De Zan, Tommaso. 2016. Italy and the Forza NEC Program. In *Istituto Affari Internazionali (IAI), Edizioni Nuova Cultura, Technological Innovation and Defence: The Forza NEC Program in the Euro-Atlantic Framework*. https://www.academia.edu/36491366/Italy_and_the_Forza_Nec_Program. Accessed 30 Jan 2024.

Defense General Staff. 2021. *Nuove tecnologie per l'Esercito Italiano.* https://www.esercito.difesa.it/comunicazione/Pagine/Nuove-tecnologie-per-l-Esercito-Italiano20200113.aspx. Accessed 30 Jan 2024.

Del Vecchio, Roberto, and Roberto Diana. 2022. *Air Force Staff*. CESMA Seminar.

Dotoli, Pierpaolo. 2015. *Tecnologie Emergenti e possibili impieghi futuri in campo militare: le prospettive internazionali.* Centro Alti Studi per la Difesa (CASD). https://www.difesa.it/SMD_/CASD/IM/CeMiSS/Documents/Ricerche/AH_T_04_dotoli.pdf. Accessed 30 Jan 2024.

European Commission. 2021. *European Medium Altitude Long Endurance Remotely Piloted Aircraft System (MALE RPAS) – development until Preliminary Design Review (PDR).* https://defence-industry-space.ec.europa.eu/system/files/2021-06/EDIDP_DA_MALE%20RPAS.pdf. Accessed 30 Jan 2024.

GPDOP (Italian Army Headquarters General Plans Department Plans Office). 2019. *Future Operating Environment post 2035 – Implications for Land Forces*. Rome: Army Headquarters General Plans Department Plans Office.

Italian Army. Undated. *Sistema Soldato Sicuro*. https://www.esercito.difesa.it/equipaggiamenti/sistema-soldato-sicuro. Accessed 30 Jan 2024.

Italian Defense General Staff. 2021. *Concetto Scenari Futuri: tendenze ed implicazioni per la Sicurezza e la Difesa*. Rome: Defense General Staff.

Italian Government. 2021. *Strategic Program on Artificial Intelligence 2022-2024*. https://assets.innovazione.gov.it/1637777513-strategic-program-aiweb.pdf. Accessed 30 Jan 2024.

———. 2022. *Dichiarazione Congiunta GCAP (Global Combat Air Programme)*. https://www.governo.it/it/articolo/dichiarazione-congiunta-gcap-global-combat-air-programme/21235. Accessed 30 Jan 2024.

Italian Navy. 2021. *Il Future Combat Naval System 2035 nelle operazioni multi-dominio come affrontare la sfida tecnologica e della sostenibilità.* https://www.marina.difesa.it/media-cultura/Notiziario-online/Documents/Il%20Future%20Combat%20Naval%20System%202035.pdf. Accessed 30 Jan 2024.

Kelly, Tim et al. 2022. EXCLUSIVE Britain and Japan aim to merge Tempest and F-X fighter programmes-sources. *Reuters*. https://www.reuters.com/business/aerospace-defense/exclusive-britain-japan-aim-merge-tempest-f-x-fighter-programmes-sources-2022-07-14/. Accessed 30 Jan 2024.

Kenealey, James. 2020. Team Tempest: Cutting-edge AI and cockpit technologies trialled. *Morson*. https://www.morson.com/blog/2020/11/team-tempest-cutting-edge-ai-and-cockpit-technologies-trialled?source=google.com. Accessed 30 Jan 2024.

Leonardo. Undated-a. *Global Combat Air Programme (GCAP).* https://www.leonardo.com/it/business/gcap. Accessed 30 Jan 2024.

———. Undated-b. *Applied Artificial Intelligence Laboratory Leonardo.* https://www.leonardo.com/it/innovation-technology/leonardo-labs/applied-artificial-intelligence. Accessed 30 Jan 2024.

———. Undated-c. *Artificial Intelligence*. https://www.leonardo.com/en/innovation-technology/technological-areas/artificial-intelligence. Accessed 30 Jan 2024.

———. Undated-d. *Forza NEC Program*. https://electronics.leonardo.com/documents/16277707/18366451/body_FORZA_NEC_LQ_mm07677_.pdf?t=1542837913321. Accessed 30 Jan 2024.

Marra, Vito. Army Staff. 2022. *The Italian Army Robotics and Autonomous Systems (RAS) Experimentation Campaign.* CESMA Seminar.

MILEX – Osservatorio sulle spese militari italiane. 2018. *Droni: Dossier sugli APR militari italiani.* https://www.osservatoriodiritti.it/wp-content/uploads/2018/06/droni-militari-milex-2018.pdf. Accessed 30 Jan 2024.

Ministry of Defense. 2015. *La matrice delle tecnologie abilitanti.* https://www.difesa.it/SGD-DNA/InfoCom/News/Pagine/TheWebsiteMatrix.aspx. Accessed 30 Jan 2024.

———. 2021. *Documento Programmatico Pluriennale della Difesa per il Triennio 2021-2023*. Rome: Ministry of Defense.

Mizokami, Kyle. 2018. *U.K. Introduces New Fighter Jet: The Tempest.* Popular Mechanics. https://www.popularmechanics.com/military/research/a22168844/uk-new-fighter-jet-tempest/. Accessed 30 Jan 2024.

NATO. 2022. *NATO 2020 and 2021 Highlights Science and Technology Organization – Empowering the Alliance's Technological Edge.* https://www.nato.int/cps/en/natohq/news_194749.htm. Accessed 30 Jan 2024.

Nones, Michele, and Marrone, Alessandro. 2011. *La trasformazione delle Forze Armate: il programma Forza NEC.* Istituto Affari Internazionali (IAI). https://www.iai.it/sites/default/files/iaiq_02.pdf. Accessed 30 Jan 2024.

PESCO Secretariat. Undated-a. *European Medium Altitude Long Endurance Remotely Piloted Aircraft Systems – MALE RPAS (EURODRONE).* https://www.pesco.europa.eu/project/european-medium-altitude-long-endurance-remotely-piloted-aircraft-systems-male-rpas-eurodrone/. Accessed 30 Jan 2024.

———. Undated-b. *Harbour & Maritime Surveillance and Protection (HARMSPRO).* https://www.pesco.europa.eu/project/harbour-and-maritime-surveillance-and-protection/. Accessed 30 Jan 2024.

Pulcini, Alessandro. 2022. Savio (Leonardo): Innovazione militare e civile, 2 metà della stessa mela. *Fortune Italia*. https://www.fortuneita.com/2022/05/02/savio-leonardo-innovazione-militare-e-civile-2-meta-della-stessa-mela/. Accessed 30 Jan 2024.

Quondamatteo, A., and E. Vignola. 2022. *Navy Staff*. CESMA Seminar.

UK Ministry of Defense. 2021. *£30-million injection for UK's first uncrewed fighter aircraft.* https://www.gov.uk/government/news/30m-injection-for-uks-first-uncrewed-fighter-aircraft. Accessed 30 Jan 2024.

Worldbank Data. Undated-a. *Italian Military Expenditure 1960-2022*. https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?locations=IT. Accessed 30 Jan 2024.

———. Undated-b. *Italian Research and Development Expenditure 1996-2020*. https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=IT. Accessed 30 Jan 2024.

Harnessing the Potential: Defense AI in Greece

Nikolaos Karampekios, Konstantinos Sakalis, and Iraklis Oikonomou

Greek defense policy officials have acknowledged Artificial Intelligence (AI) as a potential force enabler on the modern battlefield. Considering the country's geostrategic risk landscape and in view of harnessing technological opportunities, the Greek defense ecosystem has launched three main lines of effort to prepare for and adopt defense AI: research and development (R&D) collaboration, procurement of defense AI from key partners, and the provision of a holistic approach to training and education.

First, Greece makes maximum use of its active participation in European defense research, development, and innovation (RD&I) projects. It also launches national R&D initiatives to enable the domestic ecosystem to access cutting-edge knowledge and technologies and/or tests them under real operational conditions.

Second, procuring high-quality defense material that exploits AI will enable the armed forces to understand its operational capabilities. This will significantly expedite the learning curves of both military officers and engineers, close capability gaps that emerged from the country's systematic underinvestment during the 2009–2018 economic crisis and enable the defense industry to benefit as well. As subcontractors for international procurement projects or as main contractors to various export cases, exploiting AI will increase their production capacity and upgrade their list of products.

Finally, Greece is stepping up efforts to advance the education of its military personnel. Within both standard military education and civilian postgraduate

N. Karampekios (✉)
Heat, Innovation and Networking Unit, National Documentation Center (EKT), Athens, Greece
e-mail: nkarampekios@ekt.gr

K. Sakalis
Hellenic Air Force General Staff, Athens, Greece

I. Oikonomou
Independent Researcher, Athens, Greece

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_14

degrees, a growing AI-related educational, research, and entrepreneurial ecosystem to which they can link and get hands-on experience is becoming visible. This is also likely to create beneficial feedback loops.

In line with the platonic phrase "necessity is the mother of invention," the Greek defense establishment has been a quick adopter of AI and its defense promises for several reasons. These include long-standing bilateral problems with neighboring countries, the potential to apply defense-related AI to the civilian realm and vice versa, and an innate understanding of the need to ride the current scientific and technological wave.

1 Thinking About Defense AI

AI is hereby perceived as the next general-purpose technology that will shape the technological and economic evolution of the twenty-first century, affecting a wide range of industries. AI boosts the performance of other cutting-edge technologies, such as robotics, and "educates" decision support systems linked to applications, such as autonomous vehicles, by way of crunching ever-increasing amounts of classifiable data. This reality has been recognized at the top political level in Greece (Mitsotakis 2023: 4) and exercises mapping the domestic AI-related capabilities have been initiated (Sahini et al. 2022).

Defense is a field that cannot remain immune to the potential benefits of AI. Indeed, as this technology poses strains in the conduct of the 'traditional' technology policy and innovation management, by way of making use of large language models in "synthesizing scientific evidence for policymakers" (Tyler et al. 2023) up to 'reinventing the way we invent' (Cockburn et al. 2018), the policymakers responsible for developing new defense products and applications have been pondering how to best exploit the benefits of AI and utilize new advances in AI and machine learning to find new opportunities for defense technology developers (Rickli and Manellassi 2023). This has not evaded Greek policymakers. AI has been recognized as one of the main strategic axes of the Digital Transformation Bible, the flagship digital transformation policy report developed by the Ministry of Digital Governance (2021). As for the definition of AI, the document refers to it as "a collection of technologies that, by combining data, algorithms and increased computing power, is able to learn and make decisions that until recently were made solely by humans, with the aim of achieving defined goals" (Ministry of Digital Governance 2021: 158).

A National Strategy on AI (NSonAI) is scheduled to be published by the Ministry of Digital Governance in 2024 (Van Roy et al. 2021: 70–71). While the NSonAI has not been made public yet, it is believed that it touches upon the relevant security and military challenges and offers strategic outlines for developing a robust defense AI strategy. The NSonAI is expected to "set out the conditions for the development of AI, including the skills and trust framework, data policy and ethical principles for its safe development and use" and "outline national priorities and areas for maximizing the benefits of AI to address societal challenges and economic growth" (Ministry of Digital Governance 2021: 159–160).

Additionally, a high-profile team of experts was created in October 2023, under the auspices of the Prime Minister's office. It has been tasked to propose how Greece should best position itself in relation to AI, exploring avenues for the latter to be incorporated into multiple policy domains, including defense. While announcing the establishment of the advisory team, PM Mitsotakis referred explicitly to "AI and the armed forces" as "a great challenge for the transformation of the deterrent capacity of our country" (Hellenic Republic 2023).

Development and implementation of a Greek defense AI strategy[1] must center on the key specificities and considerations, including external threats, laid out by the Ministry of National Defense (MoD). Indeed, traditional security considerations loom large in the country's decision to embrace AI. As AI is considered a game-changer and Greece's competitors have already adopted and implemented defense AI strategies, Athens has embarked on a path to incorporate AI into defense. Although a comprehensive defense AI strategy has not yet been published, this view is reflected in two preceding MoD documents: the National Defense Industrial Strategy (General Directorate for Defense Investments and Armaments 2017) and the Strategic Analysis of Developments after 2030 (Hellenic National Defense General Staff 2015). Authored in the previous decade, both documents seek to position the domestic defense industrial base and the force structure in relation to cutting-edge technologies that can influence defense affairs. As of September 2023, both are being updated.

While such systemic documents are being re-authored, they indicate an operational reality that domestic defense policy makers have been quick to grasp. In numerous high-profile meetings, AI has been pointed out by high-ranking officials as a key technological objective (Hellenic National Defense General Staff 2022a; Ministry of Defense 2019, 2022) that Greek armed forces should be increasingly aligning with to address the challenges emanating from its geostrategic environment. Greece is preparing to incorporate AI into twenty-first century defense scenarios and attribute robotics and other unmanned vehicles a larger role in multi-domain operations. Or as former Deputy Defense Minister Nikos Hardalias (2023a) pointed out:

> The importance of new technologies, and in particular Emerging and Disruptive Technologies, is crucial, and we need to exploit them at all levels. These technologies, such as quantum technologies, AI, robotics, and autonomous weapon systems can have a catalytic effect on the battlefield as we know it… We see how important weapons systems and technologies such as drones, satellite internet and cyber weapons have become today.

Significantly, this rationale has been taken up by the incoming Minister of National Defense Nikos Dendias who has already signalled his acute understanding of the need for Greek armed forces to continue strengthening their digital and tech-savvy footprint in relation to AI and cybersecurity. Indeed, enhancing the production capabilities of the domestic industrial sector and a much more holistic and institutionally rounded approach on innovation has been indicated. As of November 2023, a dedicated legislation is currently in the workings.

[1] In parallel to working on the defense AI strategy, the MoD is also promoting the digitalization of the armed forces. Accordingly, a Data Protection Officer has been named by the Army, signaling a more up-to-date approach in relation to data protection. However, there is no MoD defense data strategy in place.

Another prominent individual whose strategic thinking can be seen as reflecting the broader understanding of the Greek techno-military establishment is Panagiotis Kikiras, Head of Unit, Innovative Research, at the European Defense Agency:

> AI has the potential to be a game changer for the defence sector (…) reducing the risk of loss of human lives on the battlefields, offering better efficiency than human soldiers, and the cost of its introduction is 10 times less than the corresponding cost of training soldiers. Moreover, today AI technologies are more mature and driven by investments in non-military sectors. This trend (…) has led to the exponential growth of AI technologies, which has allowed its immediate introduction into defence (…) (Kikiras 2017).

As addressed in the following chapters, Greek defense planning has been systematically incorporating AI in its daily business in the form of developing and participating in AI-related RD&I projects to get access to cutting-edge knowledge and testing this new technology under real operational conditions. Policy makers have realized that such cutting-edge technologies are being developed by both the defense and civilian ecosystem, thus trying to "spin-in" commercial solutions into their wider military planning by way of instigating synergies within the domestic civilian R&D ecosystem (Hardalias 2023b).

Also, the Greek armed forces seek to acquire operational applications of AI by way of procuring high quality defense material from global industry players. A third channel is through educating personnel. Seeking to expand knowledge boundaries, personnel of the armed forces are presented with a plethora of study options in relation to AI and a growing AI-related educational, research and entrepreneurial ecosystem to which they can link.

In advancing national defense AI capabilities, Greece takes a slightly different path on one important aspect: ethics. Although ethical considerations on the wider use of AI have been pointed out in Greek society, on its military applications a much more pragmatic approach remains the norm. Overcoming a decade of procurement drought and the continuous strategic rivalry with Turkey are the key considerations for policymakers. These have sidelined any societal debate about ethical questions surrounding defense AI. Nevertheless, the MoD should keep track of the international debate on the ethics of defense AI and generate in-house reflections on the ethical challenges of AI during warfare.

2 Developing Defense AI

2.1 Defense AI Ecosystem

Greek's defense AI ecosystem consists of two broad groups. First is the public administration comprising the national armed forces and the homeland security apparatus (falling under the auspices of the Ministry of Citizen Protection), not least because many foreign threats are inextricably linked with civilian security considerations. The second group consists of private and publicly owned firms engaged in

providing the "tools" for defense. The commonly accepted understanding is that the country

> consistently supports cooperation with the private sector and the academic community to promote innovation and the exploitation of Emerging and Disruptive Technologies to the maximum extent possible, in line with the operational requirements and specifications of the armed forces (Hardalias 2023a).

The armed forces are not just a "consumer" of AI products. With a highly educated profile, increased operational experience and participation in NATO and EU agencies, the armed forces actively shape the AI-related discussion in relation to needs and requirements. Moreover, as an end-user of cutting-edge RD&I projects, officers get to test AI-enhanced equipment and acquire first-hand experience during the development phase.

Defense firms constitute an important aspect of the defense AI ecosystem. Increasingly active in RD&I activities and starting to capitalize on their export potential, Greek firms are engaged in the production of defense services and products of various technological levels and capabilities. With an industry structure having a few large companies that are export-oriented and/or work as contractors for global defense firms, most are SMEs focused on the delivery of specific parts in the domestic defense value chain. Most established companies are active in both civilian and defense markets. The focus on providing dual-use technology and the decision to serve two different markets originate from the fact that during the decade-long economic crisis, firms had to diversify to survive. Moreover, established companies operate parallel to startups and spin-offs offering innovative new products and solutions. Among others, the following defense companies have been active in the field of defense AI:

- Hellenic Instruments (defense electronics)
- Planetek (remote sensing solutions)
- Intracom Defense (missile electronics, tactical communications, C4I systems, and unmanned systems)
- Space Hellas (integrated ICT and security solutions)
- Terra Spatium (remote sensing and geoinformation solutions)
- Eight Bells (consulting on AI, cybersecurity, optical networks, and sensors)
- FEAC Engineering (virtual engineering services through computer-aided engineering and simulation techniques)
- Lambda Automata (advanced sensor-fusion capabilities)
- Olympia Electronics (electronic safety and security solutions)
- Prisma Electronics (smart sensor wireless network technology)
- Spirit Aeronautical Systems (unmanned systems technology)
- Satways (integrated geospatial C2 solutions)

The Greek defense AI ecosystem also includes several leading research institutes, different directorates of the Greek MoD and the armed forces, and international partners as highlighted in Fig. 1 and Table 1.

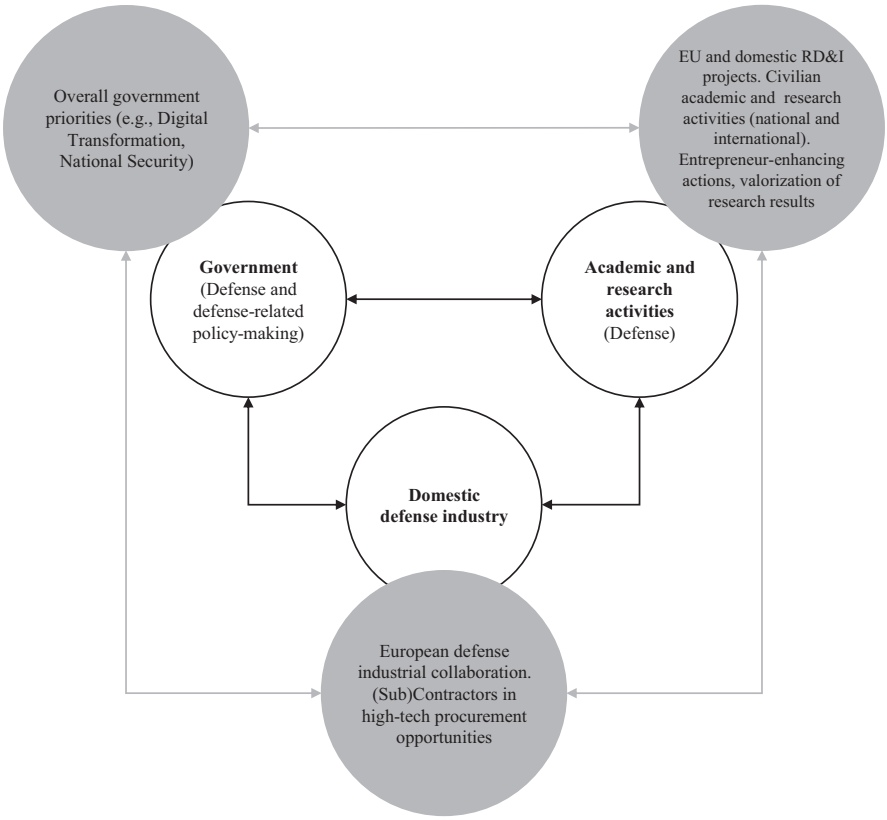


Fig. 1 Conceptualizing the Greek National Defense ecosystem. Source: Authors' Chart

In view of advancing and strengthening networks among defense stakeholders in Greece, DefencEduNet was launched in December 2023. This new framework brings together industry members of SEKPY with leading national academic institutions and research centers. The ambition is to improve the valorization of academic and research expertise by stepping up cooperation with industry, promote collaborative efforts to strengthen the development of defense and dual use technologies, and advance the inclusion scientific experts from Greece in European programs (SEKPY 2023).

2.2 Important Defense AI Projects in Development

Currently, several AI-related defense projects are in various stages of development. They are funded by European competitive funds or co-funded by European and national funds, including the Recovery and Resilience Facility, or nationally funded, including procurement contracts.

Table 1 Actors in the Greek Defense AI ecosystem

	Government	Industry	Research & Academia
International actors	• NATO • EU Directorate-General for Defense Industry and Space (DG DEFIS • European Defense Agency	• Lockheed Martin (USA) • Dassault Aviation (France) • MBDA (France) • Israel Aerospace Industries (IAI) • Rafael Advanced Defense Systems (Israel)	• Defense Innovation Accelerator for the North Atlantic (DIANA) • NATO Defense College • European Security and Defense College
National actors	• General Directorate for Defense Investments and Armaments • Directorate for Defense Investments and Technological Research • General Directorate for Defense Programs and Principle Contracts • General Directorate of National Defense Policy and International Relations • Land Forces: Communications Division • Hellenic Air Force: C' Branch (Support), D' Branch (Policy and Planning • General Secretariat for Research and Innovation • National Documentation Centre	• Hellenic Aerospace Industry • Hellenic Instruments • Planetek • Intracom Defense • Space Hellas • Terra Spatium • Eight Bells • Lambda Automata • Olympia Electronics • Prisma Electronics • Sunlight • Satways • Skytalis • Theon • SAS Tech • Akmon • FEAC Engineering • Hellenic Manufacturers of Defense Material Association (SEKPY)	• Elevate Greece • DefencEduNet (R&D partnership between the Hellenic Manufacturers of Defense Material Association and leading Greek universities and research centers) • Hellenic Army Academy • Naval Cadets School • Hellenic Air Force Academy • Universities such as NTUA, AUTH • Research centers such as NCSR "Demokritos" and CERTH

Source: Authors' Overview

2.2.1 International Development Projects

With respect to international development projects, the lion's share refers to European projects aiming at establishing a common defense R&D and industrial capability. Participation in EU projects is a significant pathway for Greek actors to obtain funds and top-tier know-how, and a pathway wherein these actors exhibit success (Defence Redefined 2022). The following non-exhaustive overview includes projects with Greek partners as coordinators and/or members and is indicative of Greece's emphasis on securing European funding and expanding the network of international partnerships:

- CTIRISP (Cyber Threats and Incident Response Information Sharing Platform).
- DECISMAR (Development of a Decision Support Toolbox for enhancing the feasibility study of the Upgrade of Maritime Surveillance).
- d-THOR (Digital Ship Structural Health Monitoring).
- FaRADAI (Frugal and Robust AI for Defence Advanced Intelligence)

- GEOMETOC (Geo-Meteorological and Oceanographic Support Coordination Element)
- HARMSPRO (Harbour & Maritime Surveillance and Protection)
- LOTUS (Low Observable Tactical Unmanned Air System)
- MAS MCM (Maritime Semi Autonomous Systems for Mine Countermeasures)
- MIRICLE (Mine Risk Clearance for Europe)
- PANDORA (Cyber Defence Platform for Real-time Threat Hunting, Incident Response, and Information Sharing)
- PRIVILEDGE (PRIVacy and homomorphic encryption for artificial intelligence)
- USSPS (Development of Unmanned Semi-fixed Sea Platforms for Maritime Surveillance)

2.2.2 National Development Projects

Through funding programs such as the 2021–2027 Partnership and Cooperation Agreement, the Recovery and Resilience Facility and national funds, Greece has invested in developing systems related to security and defense AI along three lines of efforts: big data and data fusion to enhance situational awareness, unmanned systems, and safety and predictive maintenance.

- *Big Data and Data Fusion*

The THORAX integrated information system (Ministry of Development & Investments 2020; Nedos 2022) will transmit real-time information concerning search and rescue operations, border security, irregular immigration, or earthquakes to the MoD's National Operational Center, thus enabling decision-making commensurate with the needs of emerging crisis situations. AI will be used for real-time data fusion of information obtained through multiple air, land, and sea-based sensors.

- *Unmanned Systems*

Greece aspires to develop unmanned systems to cover its gap with the global use of unmanned systems (Ellinikikos Stratos Undated). Turkey, Greece's strategic competitor, has become highly adept at developing and using these systems. The Greek inability to counter these systems entails a tactical disadvantage in addition to a know-how deficiency in a cutting-edge field. Greece has established a privileged partnership with the United States and Israel to make use of their unmanned systems to cover the country's tactical deficiencies as a stop-gap measure.

Against this background efforts to develop Greek unmanned aerial vehicles (UAV) go back to 1982, with the first flight of the HAI E1-79 Pegasus followed by its second version (Pegasus II) in 2005 which is currently part of the arsenal of the Hellenic Air Force (Undated-a). The HCUAV RX-1 was developed as collaborative project in the 2007–2013 National Strategic Reference Framework, coordinated by the Fluid and Turbine Engineering Laboratory of the Mechanical Engineering Department of AUTH (Defence Point 2019). The DELEAR RX-3 platform which

emerged from RX-1 was produced as part of the LOTUS project (DELAER Undated; Intracom Defense 2020). The RX-3 vehicle will adopt AI to perceive the environment and to autonomously execute parts of its mission.

A second attempt emerged from a joint venture project involving the Naval Cadets School, the National Technical University of Athens and the EFA Group of Companies[2] for the development of the Greek UAV ARCHYTAS (Nikitas 2022). A TRL-8 prototype is expected in Q4 of 2023 and industrial production is expected in Q1 of 2024 (Ministry of Defense 2023).

A third attempt concerns the development of the first Greek UCAV, GRYPAS, which was initialized in January 2023 with the signing of a Memorandum of Cooperation between the Ministry of Finance and the MoD, the Hellenic Aerospace Industry, and several Greek universities (Defence Review 2023). This project corresponds to the operational need of the armed forces for a medium-altitude long-endurance UAV for intelligence or strike missions. AI will be implemented for automated navigation and recognition of certain types of targets.

- *Predictive Maintenance and Safety*

NAVMAT, a project of the Naval Cadet School and the Hellenic Foundation for Research and Innovation, is a platform for recording, indexing, comparing, assessing, and retrieving information, history of operations and maintenance, evidence, and testimony for incidents of failure in the naval environment. Based on materials failure ontology, it makes use of AI algorithms and cutting-edge approaches in data handling, optimizing naval materials failure management, and supporting decision-making in maintenance and repair operations (NAVMAT 2023).

2.2.3 Procurement Projects

During the last 5 years, Greece has signed approximately 200 major defense procurement contracts (e-Amyna 2023), driven mainly by the long-standing strategic rivalry with Turkey and the need to overcome a decade of limited procurement activities. These external drivers have been coupled with a more utilitarian approach: procuring ready-to-use high-tech defense systems from foreign contractors requires the national defense industrial base to be involved to ensure smooth operation. In addition, there is a growing interest in using international procurement projects as avenues to help mature local defense companies and enable them to enter more digital product segments.

Importantly, these objectives are in line with a wider political understanding with the governments of the states where the respective industrial groups, from which the procurement will take place, are headquartered. Countries such as the United States, France, and Israel have recognized the increased geopolitical

[2]This consortium includes Theon (electro-optical sensors), SCYTALIS (data links), and UCANDRONE (design and manufacturing of the aircraft).

significance of Greece and maintain strategic interests that are in line with Greece's objectives. Exploring the possibilities and investing in AI-related systems and technologies "is a security issue that is both national and supranational, and therefore concerns both NATO and the EU. But it can only be carried out effectively through international cooperation with partners with whom we share common principles and values" (Hardalias 2023a).

This has morphed into a more collaborative approach in matters of industrial production. A conscious effort is being undertaken to transform this "one-way street" of high-tech procurement from advanced countries into an industrial production scheme wherein Greek defense industry will participate in product development for the purposes of the specific procurement contract and as part of the production value chain globally. This geopolitical alignment is further exhibited in EU RD&I projects, wherein Greek entities extensively collaborate with French, Italian and Spanish actors.

Regarding industrial production, Naval Group's 3 Belharra-type frigates (FDI-HN), Dassault Aviation's 24 Rafale, the modernization of 4 MEKO-type frigates and the acquisition of 20 Lockheed Martin-made F-35 fighter jets are of special interest as most of these assets are data-powered and sensor-enabled. These projects will require the local industry to make substantial efforts in view of sensor fusion capabilities and other types of decision support tools operators can use for integrating disparate sensor and information data, optronics for target acquisition, and parsing of Failure, Reporting, Analysis, and Corrective Action (FRACAS) data. However, if and to what extent local industry partners can contribute is still under discussion and needs to be assessed in view of local competencies and international supplier requirements. This includes a detailed understanding of the domestic defense industry's research and technological capabilities—a mapping task that is currently being undertaken.

In addition, MBDA's contract to provide ASTER 30 B1 area air defense and MM40 Exocet Block 3C anti-ship missiles for the FDI-HN, and the Meteor air-to-air, the SCALP cruise, the MICA air-to-air and the AM39 Exocet anti-ship missiles for Rafale are linked to collaborating with domestic parties. One such case is the contribution of the National Technical University of Athens to develop AI-relevant technologies. This case and MBDA's "R&D Booster" for the establishment of R&D partnerships with the domestic industry and academia indicate the aforementioned geopolitical alliance between France and Greece, through which France as the supplier is seeking to broaden its footprint in Greece's defense ecosystem (MBDA 2022, 2023).

3 Organizing Defense AI

Greek's defense institutions are reorganizing for the advent of defense AI. Early indications suggest that new NSonAI that will be published later this year will cover defense AI issues in relation to inter-ministerial and cross-departmental arrangements and security and military considerations. These aspects notwithstanding, the MoD currently lacks a single, unitary coordinating authority responsible for defense AI. Rather, the respective policies and the gathering of relevant knowledge are being carried out by multiple centers within the MoD structure:

- The Directorate for Defense Investments and Technological Research (DDITR) at the General Directorate for Defense Investments and Armaments (GDDIA) is responsible for managing state-funded and European R&D projects, including those that are AI-focused. This Directorate is familiar with the EU's AI-related priorities, the capabilities of participating Greek actors, and the respective project results.
- In collaboration with DDITR, the Directorate for Defense Programs and Principal Contracts within the same General Directorate manages major procurement projects, including sub-contracting the domestic industrial base. Given that most—if not all—of the current procurement projects do entail a domestic co-production aspect, GDDIA is highly engaged in organizing technological and industrial actions on defense AI.
- Moreover, given the hybrid security threats posed by both state and non-state actors in Greece's land and sea borders, additional operational centers and assets performing multiple data-collection missions are being operated in tandem by defense, police, and coast guard forces. Thus, the Hellenic National Defense General Staff is also exposed to AI-relevant assets and technologies that are being deployed within the context of security-relevant R&D and procurement projects.
- As of end of October 2023, the new Hellenic Center for Defense Research and Innovation Development (KETAK) has been institutionalized by the MoD, seeking to address real, operational requirements by all branches of the armed forces. Although little has been revealed, one can assume that KETAK will seek to implement a fully blown defense technology policy by taking into consideration the existing domestic, civilian and defense, RD&I ecosystem and the industrial realities of GDDIA. Whether KETAK will incorporate the existing per branch research centers or will administer them in a more streamlined manner is per se an innovation management question to be addressed within the MoD. Defense Minister Dendias (2023) specified the establishment of KETAK as one of the key priorities for 2024, focusing on the mobilization of resources and international collaborations to advance R&T development and defense industry restructuring.
- Lastly, the General Directorate of National Defense Policy and International Relations (GDNDPIR) is responsible for addressing the policy-relevant issues on

AI and other cutting-edge technologies, thereby considering the country's international relations, allied obligations, and requirements stemming from bilateral defense cooperation agreements.

This multiplicity of administrative entities within MoD creates several inroads for the latter to be educated on defense AI. In addition, there are several service-specific inroads via the Communications Division of the Land Forces, the Submarine Directorate of the Hellenic Navy and C Branch (Support) in coordination with the D Branch (Policy and Planning) of the Hellenic Air Force General Staff. Service-specific insights gained through these avenues can inform the set up and implementation of new R&D projects, thus creating a positive feedback loop. Although this decentralized and horizontal approach is beneficial, thought should be given to setting up an overarching single point of entry within the MoD. As our concluding chapter will argue, such an approach could also streamline inter-agency interaction and help overcome institutional inertia.

As argued previously, the defense industry is an important economic and policy actor in relation to defense AI and an essential part of the defense ecosystem. Firms are engaged in several ways in organizing AI-relevant defense activities:

- First, by participating in EU, national and in-house R&D projects, thus acquiring relevant know-how. In addition to funding and know-how, being part of EU RD&I consortia offers significant networking and collaboration opportunities. Indeed, certain private firms have been exhibiting a steady participation in such projects. These companies can serve as national "transmission belts" that help diffuse international experience among national partners and enable them to develop competitive future products and services.
- Second, by participating as a subcontractor to the domestic procurement process. As part of the production pipeline, Greek firms stand to gain by becoming trusted partners of the main contractors on similar procurement contracts globally.
- Third, by participating in global tenders. This is due to in-house innovation and technological prowess. As the GDDIA is responsible to regularly update the Registry of Manufacturers of Defense Material (General Directorate for Defense Investments and Armaments 2023), the MoD is familiar with each firm's AI-related capabilities. This is also relevant for the Hellenic Manufacturers of Defense Material Association (SEKPY), which is the largest national defense cluster with more than 200 member companies. To further promote the commercial interest of their members, industrial associations should undertake all relevant measures to regularly map and disseminate the technological capabilities and skills of its members in relation to such cutting-edge technologies. This syncs with GGDIA's objectives and offers a validated set of data to be incorporated to the country's defense technology and industrial policy. Even though the MoD maintains an overview of available technological capabilities, such mapping would bring added value to the equation. For instance, an industry-led initiative could help faster highlight the strong innovative elements of the sector, thereby informing dual-use industrial policy. Also, mapping will assist with attracting talent and locating skill gaps, enabling the provision of additional

> training/upskilling opportunities. Lastly, potential bureaucratic obstacles in the timely monitoring of industrial capabilities by the MoD can be more effectively bypassed in this way.

Being knowledgeable about the AI capabilities of the domestic defense industrial base is important, as a new AI-focused domestic ecosystem is emerging. Dedicated platforms such as Elevate Greece (Undated) and a renewed emphasis on innovation, as set out by the Minister of National Defense Nikos Dendias and his explicit aim to set up a dedicated Project Management Office in his upcoming legislation, will potentially streamline and boost existing good practices, such as MoD's defense-related start-up competitions (General Directorate for Defense Investments and Armaments 2017: 12) and Defense Innovation Challenge (Ministry of Defense Undated), thus providing a comprehensive overview of the national defense AI ecosystem.

Moreover, the new NATO Defense Innovation Accelerator for the North Atlantic (DIANA) is expected to provide Greece's ecosystem with a further boost. Operating as a start-up incubator/accelerator and building on existing test facilities (NATO 2022a), DIANA has enlisted the Foundation for Research and Technology—Hellas (in Crete and in Patras), the National Centre for Scientific Research Demokritos (in Athens), and the Center for Research and Technology Hellas (in Thessaloniki). These will focus on AI, autonomous technologies, quantum technologies, biotechnology, and novel materials. In combination with the new NATO Innovation Fund, the objective is to kick-start deep-tech startups, including spin offs, and to bring them into technology development projects relevant for NATO.

4 Funding Defense AI

An increase in R&D investment has been the new norm within the Greek RD&I ecosystem. Despite the existing shortfalls originating from the fallout of the economic crisis 2009–2018, political decision-makers agree on the need to increase Greece's participation in European RD&I projects and advancing the proficiency of the local workforce. Or, as the National Defense Industrial Strategy puts it,

> the participation of the armed forces in research programs, funded either by the state budget or externally, as a strategic partner or contractor with significant operational experience, specialized personnel, infrastructure, and means should be encouraged (General Directorate of Defense Investment & Armaments 2017: 2).

This understanding has become the guiding principle to set up the Hellenic Foundation for Research and Innovation, the Deputy Ministry of Research and Technology, and Elevate Greece, a state registry on startups and an informed gateway for potential investors. A large portion of the 2021–2027 Partnership and Cooperation Agreement, the Recovery and Resilience Facility and other national funds are directed towards R&D. A pro-business climate spurred domestic R&D spending (from 0.68% of GDP in 2011 to 1.45% of GDP in 2021), which, in turn, helped renew the attention of global investors to engage in Greece's high-tech sector.

Spending on defense procurement and R&D has been on the rise. Historically, Greek armed forces have been a procurer of foreign defense material, but defense purchases plummeted during the crisis years. Similarly, R&D activities attracted low interest from policy officials. Both trends have been reversed. Procurement has spiked since 2020 with the government signaling its willingness to buy top defense equipment, and awareness of the importance of RD&I as a "vertical" theme of activities has increased. To be part of global value chains and long-term partners of global firms, domestic companies have realized that they need to engage in knowledge-intensive activities that initiate in-house learning processes critical for product/services development. Still, despite a general uptick in defense RD&I spending, it is impossible to provide a financial breakdown of Greece's spending on defense AI as the respective figures are classified.

5 Fielding and Operating Defense AI

Although Greece participates in AI-relevant R&D activities, the production and operation of AI systems is not particularly developed. Based on open-source information we contend that some of the R&D projects discussed previously have been turned into field experiments. Additionally, Greece's purchase of off-the-shelf defense systems and future defense procurement plans include integrated AI components. If these lines of effort serve as indicators for the use cases of defense AI solutions that are about to be fielded, we see three focus areas: improving situational awareness and understanding, augmenting existing defense capabilities, and advancing border security.

5.1 Situational Awareness and Situational Understanding

A case in point here concerns the streamlining and operationalizing of multiple data sources for real-time command and control. This has been the focus of the new Intelligence Fusion Cell (IFC) of the Special Warfare Command. IFC focuses on providing full-spectrum, multi-domain operational and strategic intelligence through AI, thus achieving interoperability and enabling intelligence sharing (Hellenic National Defense General Staff 2022b).

5.2 Augmenting Existing Capabilities

Like other countries, Greece strives to advance existing defense capabilities with the use of defense AI. In this regard, the following projects are worth mentioning:

- Its presence at the 2021 Parmenion exercise (Ministry of Defense 2021) suggests that the ARCHYTAS UAV has matured and is ready for operational demonstration. Transferring this system into the portfolio of the Greek armed forces will significantly advance intelligence collection and assessment capabilities.
- In 2021, the Hellenic Air Force procured HERON UAVs from Israel Aerospace Industries (IAI Undated) to conduct intelligence, surveillance, target acquisition and reconnaissance (ISTAR) missions (Nikitas 2021). These missions are built upon the ability to combine and enhance open-source maritime and other terrain data with AI-driven insights to quickly identify patterns of vessel behavior and anomalies. This advances the tipping and cueing capabilities of the Greek armed forces to identify and track large objects such as ships and calculate mission-relevant risk levels.
- The Hellenic Air Force is using IRIS-T missiles (Hellenic Air Force Undated-b) carried by F-16BLK 52+ and F-16BLK 52+ADV aircraft. They provide improved accuracy as the imaging IR seeker head in conjunction with intelligent image processing allows for autonomously identifying the target to select the best aiming point.
- SPIKE non-line of sight (NLOS) is an advanced electro-optical/infrared missile system that can integrate data through machine-learning techniques, enabling a highly accurate target image acquisition process. The system is coupled with Orbiter 3 UAVs as target designators (Egozi 2023).

5.3 Border Security

At the intersection of defense and national security, border security is a strategic priority for Greece as the prevention of irregular immigration proves challenging. Consequently, Greece is emphasizing deterrence, introducing border surveillance systems that implement automated information management in the field through data collection. Surveillance solutions, which were field-tested in 2021, consist of a network of long-range cameras and radars installed along the Greece-Turkey border, transmitting real-time image and data on border conditions (Soulioitis 2021).

Due to increased pressure by irregular immigration, the land border with Turkey in Evros is heavily populated with advanced technological products exploited by Greek police and border control. For example, REACTION (REaltime ArtifiCial inTellIgence for bOrders surveillance via RPAS data aNalytics to support Law Enforcement Agencies) is a follow-up of multiple EU projects (CERETAB, AIDERS and ROBORDER). Operated by the Ministry of Migration & Asylum and developed by CERTH-ITI, REACTION aims to build a comprehensive platform and intelligence architecture for border surveillance by fusing multiple data streams obtained from UAVs through AI (Ministry of Migration & Asylum Undated). AKRITAS and NESTOR are two other advanced border surveillance systems in use. Both aim to provide pre-frontier situational awareness

beyond maritime and land borders for early warning through thermal imaging and AI-enhanced radio frequency spectrum analysis technologies (Frontex 2022; Cordis Undated-a).

Similarly, sea borders are being monitored by the Hellenic Coast Guard making use of advanced EU projects such as PROMENADE (Artificial intelligence and big data for improved maritime awareness) (Cordis Undated-b). It focuses on automatic vessel detection, tracking and behavior analysis based on machine-learning. This multi-sensor and multi-source environment is streamlined with AI-data fusion techniques to operational rooms operated in tandem by defense, police and coast guard forces to provide for increased situational awareness. A further case in point is ARESIBO, a research project in which the Naval Cadet School participates in conjunction with the National and Kapodistrian University of Athens and CERTH. This project is meant to "enhance the current state-of-the-art through technological breakthroughs in Mobile Augmented Reality and Wearables, Robust and Secure Telecommunications, Swarm Robotics and Planning of Context-Aware Autonomous Missions, and AI, to implement user-friendly tools for border and coast guards" (ARESIBO Undated).

Although these systems mostly concern officials of the Ministry of Citizen Protection, they do not exclude the participation of the MoD, since the Greek Army personnel is involved in joint patrols with the police. This offers the armed forces opportunities to gain first-hand experience in operating non-defense electronic surveillance systems. Additionally, the External Border Control and Surveillance System is aimed at strengthening the national ability to control and monitor the external borders, involving the supply of equipment accompanied by the necessary software. That the officers belonging to the security and defense branches of the Greek state are jointly working in the respective control rooms suggests a need for inter-agency information sharing mechanisms and interoperability requirements. Moreover, the operational deployment of THORAX will advance data sharing as defense, police, and coast guard forces will use a common approach to data dissemination.

6 Training for Defense AI

Training for and with AI has been high on the MoD's priorities list. On several public occasions, top MoD decision-makers have underlined the value of AI (plus quantum technologies, robotics, and autonomous weapon systems) as a means towards enabling military prowess. Also, they have emphasized the value of lifelong learning, continuous education, and training as a means for gearing up for the complexity of modern operations (Hellenic National Defense General Staff 2022a). Against this background, MoD personnel are actively encouraged to seek relevant educational opportunities. Training for and with AI takes place via simulation in operational settings, within the military academies and at the postgraduate level, and through conferences and other entrepreneurial-minded activities.

6.1 Simulation-Based Training

A case in point regarding enhanced operational training has been the inauguration of the Synthetic Training Squadron on Andravida Air Base (Hellenic Air Force 2022, Undated-c). The squadron aims to enhance interoperability between special forces and air power by exploiting the operational characteristics of its 11 simulators. Making use of augmented reality technology coupled with AI offers a richer and more realistic behavior of simulated individuals, teams, and platforms in target-rich and complex environments.

The Hellenic Air Force personnel has completed the operational deployment of the simulators, underlining the proficiency of the staff in using and developing advanced technology systems. Additionally, the establishment of the Flight Training Center (FTC) in Kalamata Air Base with its Mission Training Center will upgrade the operational training of aircrews through new technologies and flight simulators (Mononews 2022). Cutting-edge technologies exploited in FTC will use data-driven tools for optimizing training delivery built on adaptive training platforms powered by AI.

6.2 Military Education

Education in military academies, participation in postgraduate programs on new technologies, the development of educational programs for officer schools and the organization of conferences currently constitute the main avenues for the personnel of the Hellenic Armed Force to acquire new skills related to AI.

The Hellenic Army, Naval, and Air Force Academies provide the basic education of new officers. These academies have incorporated themes of disruptive and emerging technologies in their educational programs. In addition to acquiring advanced mathematical skills in functional analysis, numerical methods, and probability theory, students proceed to advanced AI-relevant topics such as optimization problems by way of using neural networks, distributed systems, signal processing, and data fusion (Hellenic Air Force Academy 2023a; Hellenic Army Academy 2022; Hellenic Naval Academy 2023b). These place emphasis on making use of AI in applied subjects such as the detection of noise propagation, data distribution, and border control systems.

Historically, Greek military officers have been actively seeking postgraduate educational opportunities both within and outside of their operational training necessary for their grade. Officers study at purely civilian universities, obtaining postgraduate degrees that treat the mathematical aspects of AI (Applied Mathematics), optimization in real-life problems, (Machine Learning and Deep Learning in structural, geotechnical and bridge engineering) and core IT-relevant aspects.

The Hellenic Army has formalized cooperation agreements with Greek universities for offering postgraduate opportunities to its personnel. A case in point is the

Hellenic Army Academy's participation in two Masters of Science with the School of Production Engineering and Management of the Technical University of Crete (Hellenic Army Academy & Technical University of Crete Undated). The MSc in Intelligent Systems Engineering and the MSc in Operation Research and Decision-Making treat AI within the scope of computational intelligence, machine learning, big data analytics, and data science in relation to real-life operational conditions such as tracking of unmanned systems. An MSc in Cryptography, Security and Information Systems is offered by the Hellenic Army Academy to its army officers. Herein, analysis and evaluation of symmetric crypto methods using AI and methods for privacy-preserving machine learning and inference are a few domains of cryptography that are addressed through AI (Hellenic Army Academy Undated). Also, the Hellenic Naval Academy (2023a) recently signed a cooperation agreement with the National Centre of Scientific Research "Demokritos" for educational and R&D purposes in the fields of AI, machine learning, big data analytics, and new materials. Lastly, indicative of the increased focus on AI has been the recent foundation of the "Archimedes" Center for Research in Artificial Intelligence, Data Science and Algorithms. Operating as a Research Unit of the Athena Research Center (Athena Research Center Undated), it can provide research capabilities on relevant issues.

The Senior War Colleges of the three military services and other educational institutions—Supreme Joint War College and National Defense College—provide extra avenues to educate active-duty senior officers. These educational institutions provide courses that cover a wide range of topics related to national defense and military strategy in conjunction with defense AI and new technologies.

Another avenue for attaining educational experience is through NATO's post-graduate opportunities. While there is no open-source data on the number of Greek officers attending such courses or the exact subjects of the offered courses, a digital search in Monterey's Postgraduate School indicates that AI has been introduced as a key subject (Naval Postgraduate School Undated; America's Navy 2023). In the EU context, AI-relevant educational opportunities should be explored in the context of the European Security and Defense College (ESDC).

In relation to extracurricular activities, one case has been the Common Module on Unmanned Aerial Systems provided by the Hellenic Air Force Academy (2023b) in collaboration with the ESDC. Therein, the technological principles of Unmanned Aerial Systems and their applications, specifications, and classification of different categories, types, and sensors were presented.

6.3 Conferences and Entrepreneurial-Minded Training Activities

Educational activities in the form of conferences on topics related to defense AI have been taking place. For example, the Hellenic Air Force has been organizing its Annual Air Power Conference, inter alia, to discuss early technology adoption to preserve operational advantage. The topic of AI has received attention in multiple

conferences (Hellenic Air Force Undated-d). In a special section titled "Artificial Intelligence and Man in the Loop: Opportunities—Capabilities—Prospect," the panel discussed how AI could influence developments in military conflicts and delved into relevant topics such as Machine Learning Methods on Noisy and Sparse Data.

A conference titled "Technology—Innovation, Defense, and Strategy," aimed at senior officers, was organized in 2023 by the National Defense College. The purpose was to broaden the participants' knowledge with an emphasis on the impact of innovation and the application of new technologies in the armed forces. The conference also addressed the use of AI in defense (Hellenic National Defence General Staff 2023). The topic was presented by researchers at the National Centre of Scientific Research "Demokritos" further indicating the links between the domestic research ecosystem and armed forces.

In 2022, the MoD conducted the Defense Innovation Challenge, focusing on situational awareness. The overall goal was to stimulate innovative in-house ideas that can help transform the operational horizon (General Directorate for Defense Investments and Armaments 2021). AI-related projects that sought to identify submarines (Submarine Identification with Artificial Intelligence) were shortlisted for future-proofing (Association of Graduates of Hellenic Air Force Technical NCO Academy 2022). The challenge made it clear that officers constitute a valuable source that the MoD should systematically tap into to enhance ongoing force transformation activities.

7 Conclusion

AI presents an innovation challenge for complex organizations such as ministries of defense. Such critical technologies contest existing inter-institutional operational modes and potentially alter 'the way business is conducted' both within these bureaucratic organizations and (most importantly) in relation to their institutional mandate. New technology development for military applications that exploit AI is surely a topic that policymakers and innovation managers must tackle in the coming years for good and bad reasons. Indeed, scholars of defense innovation have started incorporating the latest wave of technological development that AI represents into their analytic thinking and seek to unravel lessons for future leaders (Krepinevich 2023).

This chapter showed that Greek defense policy officials have actively taken steps to harness the potential of the technological and operational "window of opportunity" that AI presents. Several factors—such as long-standing bilateral problems with neighboring countries, looming tactical and operational gaps coupled with technological obsolescence due to the decade-long economic crisis—have prompted the MoD to actively seek industrial and defense materiel upgrades. In combination with the drive to revitalize the dormant defense industry and capitalize upon the highly educated military personnel, these factors have pushed the defense

establishment towards riding the current scientific and technological wave. Still, despite notable progress, several long-term challenges remain to be tackled for the Greek military ecosystem to seize AI's potential.

First and foremost, Greek defense planners should remain alert for scientific breakthroughs in the field. Operating a "black box" where algorithms and key optimization techniques remain unknown to military engineers, data scientists, and mathematicians is problematic for sustaining long-term operational advantages. Enhanced cooperation with the science establishment, focused bibliometric and technometric analysis, and network and centrality analysis to locate knowledge-rich areas of expertise should be the norm.

Second, participating in collaborative RD&I projects is an important avenue to access top-notch know-how and accumulate experience. Importantly, current and future operational requirements should systematically guide the selection of RD&I projects the Greek armed forces want to participate in. While such a future oriented, technology-based, tactical list is currently not publicly available, the aforementioned actions indicate a conscious approach in both closing existing operational gaps and leveraging technologies to leapfrog. Such know-how should start being transposed into the strategic and tactical planning of the country's defense forces and the production lines of Greek firms.

Third, procuring cutting-edge defense material is a significant learning curve for military personnel. Thus, the MoD should move swiftly to become a proficient end user in current and future R&D projects. Greek defense procurement officials should actively negotiate specific conditions with foreign contractors to ensure that Greek armed forces are granted "enhanced" user rights related to new defense equipment. Additionally, domestic defense contractors should be given access to proprietary knowledge when engaging with international partners in co-production agreements. Enabling an operational relationship with domestic civilian universities and the country's highly performant science diaspora is yet another channel to gather cutting-edge scientific and technological information on AI. This will also advance Greece's understanding related to increasing vulnerabilities that are bound to appear in interconnected systems—ranging from cyber-attacks and manipulated and corrupt data to data transmission flows.

Fourth, the MoD should adopt a more systemic view to monitor defense AI-relevant policy discussions in NATO, European agencies, and other multilateral formats. Greek military delegates should "tag" and send AI-related information to a single point within the ministry for the latter to keep track of all concurrent activities. For example, NATO's new Data and Artificial Intelligence Review Board (DARB) is a key forum to exchange best practices and views on AI (NATO 2022b). Greece will be appointing a representative to DARB and should use this forum to systematically gather information on international defense AI developments. The same holds true for European institutions like the European Defence Agency (EDA), the European Space Agency (ESA) and the European Network and Information Security Agency (ENISA) (European Space Agency 2023; ENISA Undated).

Finally, establishing a new function like the US Department of Defense's Chief Digital and Artificial Intelligence Office should be explored. A single administrative

point would help establish and implement a unified defense AI vision, collect all relevant information in a structured manner, and streamline interagency overlap and push back organizational inertia and turf war. Further, this office could push towards greater collaboration with domestic academic and research institutions and international partners.

Apart from being a scientific, technological, and operational challenge, AI constitutes first and foremost a learning challenge. This chapter discussed the Greek defense establishment's ability to 'learning to learn'. While much remains to be done, there is reason to be optimistic.

References

America's Navy. 2023. *Artificial Intelligence Summit at NPS Accelerates Critical Capabilities.* https://www.navy.mil/Press-Office/News-Stories/Article/3272831/artificial-intelligence-summit-at-nps-accelerates-critical-capabilities/. Accessed 30 Jan 2024.

ARESIBO. Undated. *ARESIBO - AR for field and C2 activities*. https://aresibo.eu/. Accessed 30 Jan 2024.

Association of Graduates of Hellenic Air Force Technical NCO Academy. 2022. *ΥΠΕΘΑ: 1ος Διαγωνισμός Καινοτομίας και Τεχνολογίας*. https://sastya.gr/new/item/1595-ypetha-1os-diagonismos-kainotomias-kai-texnologias. Accessed 30 Jan 2024.

ATHENA Research Center. Undated. *ARCHIMEDES Unit*. https://www.athenarc.gr/en/archimedes. Accessed 30 Jan 2024.

Cockburn, Iain M., Rebecca Henderson, and Scott Stern. 2018. *The impact of artificial intelligence on innovation*. National Bureau of Economic Research, NBER Working Paper Series. https://www.nber.org/system/files/working_papers/w24449/w24449.pdf. Accessed 30 Jan 2024.

Cordis. Undated-a. *aN Enhanced pre-frontier intelligence picture to Safeguard The EurOpean boRders - Project Description.* https://cordis.europa.eu/project/id/101021851. Accessed 30 Jan 2024.

———. Undated-b. *imPROved Maritime awarENess by means of AI and BD mEthods - Project Description*. https://cordis.europa.eu/project/id/101021673. Accessed 30 Jan 2024.

Defence Point. 2019. *Αερόχημα HCUAV RX-1 από την ελληνική εταιρία Space Sonic με ηλεκτρονικά IDE.* https://www.defence-point.gr/news/aerochima-hcuav-rx-1-apo-tin-elliniki-space-sonic-me-ilektronika-tis-ide. Accessed 30 Jan 2024.

Defence Redefined. 2022. *Greece in 5th place for funding from European Defence Fund.* https://defenceredefined.com.cy/edf-greece-in-5th-place-for-funding-from-european-defence-fund/. Accessed 30 Jan 2024.

Defence Review. 2023. *Το ελληνικό UCAV με την ονομασία «Γρύπας» ανακοίνωσαν από κοινού τα Υπουργεία Εθνικής Άμυνας και Υπουργείο Οικονομικών*. https://defencereview.gr/new-hellenic-ucav-grypas/. Accessed 30 Jan 2024.

DELAER. Undated. *The DELAER concept. DELAER project website.* https://delaer.gr/portfolios/the-delaer-concept/. Accessed 30 Jan 2024.

Dendias, Nikos. 2023. Οι στόχοι και η στρατηγική του Υπουργείο Εθνικής Άμυνας για το 2024. *Parapolitika newspaper*. https://www.mod.mil.gr/arthro-ypoyrgoy-ethnikis-amynas-nikoy-dendia-afieroma-tis-efimeridas-parapolitika/. Accessed 30 Jan 2024.

e-Amyna. 2023. *Συμβάσεις - συμφωνίες ΥΠΕΘΑ/ΓΔΑΕΕ 2019-2023, List of major defense contracts awarded in the period 2019-2023, compiled by e-Amyna.* https://twitter.com/e_amyna/status/1658400669752074241?ref_src=twsrc%5Etfw%7Ctwcamp%5Eembeddedtimeline%7Ctwterm%5Escreen-name%3Ae_amyna%7Ctwcon%5Es1. Accessed 30 Jan 2024.

Egozi, Arie. 2023. *Aeronautics to deliver Orbiter 3 drones to Greece.* Defence Industry Europe. https://defence-industry.eu/aeronautics-to-deliver-orbiter-3-drones-to-greece/. Accessed 30 Jan 2024.

Elevate Greece. Undated. *Registered Startup Database.* https://elevategreece.gov.gr/startup-database/. Accessed 30 Jan 2024.

Ellinikikos Stratos. Undated. *Προγράμματα ανάπτυξης ελληνικών UAV.* Ellinikos-Stratos.com. https://www.ellinikos-stratos.com/arthra/uav-greek. Accessed 30 Jan 2024.

ENISA. Undated. *Ad-Hoc Working Group on Artificial Intelligence Cybersecurity*. https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence/ad-hoc-working-group. Accessed 30 Jan 2024.

European Space Agency. 2023. *Artificial intelligence in space.* https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/Artificial_intelligence_in_space. Accessed 30 Jan 2024.

FRONTEX. 2022. *Horizon projects, NESTOR.* https://frontex.europa.eu/innovation/eu-research/horizon-projects/nestor-MDU4gJ. Accessed 30 Jan 2024.

General Directorate for Defense Investments and Armaments. 2017. *National Defence Industrial Strategy.* https://www.gdaee.mil.gr/wp-content/uploads/2021/09/NDIS-ENGLISH.pdf. Accessed 30 Jan 2024.

———. 2021. *1st Competition of Innovation and Technology of the Ministry of National Defence to highlight solutions, ideas and applications in the field of defence.* https://www.gdaee.mil.gr/en/1st-competition-of-innovation-and-technology-of-the-ministry-of-national-defence-to-highlight-solutions-ideas-and-applications-in-the-field-of-defence/. Accessed 30 Jan 2024.

———. 2023. *Registry of Manufacturers of Defense Material.* https://www.gdaee.mil.gr/en/registry-of-manufacturers-of-defense-material/. Accessed 30 Jan 2024.

Hardalias, Nikos. 2023a. *Ομιλία ΥΦΕΘΑ Νικόλαου Χαρδαλιά στην Ημερίδα «Τεχνολογία-Καινοτομία, Άμυνα & Στρατηγική» της Σχολής Εθνικής Άμυνας.* Ministry of National Defence. https://www.mod.mil.gr/omilia-yfetha-nikolaoy-chardalia-stin-imerida-technologia-kainotomia-amyna-amp/. Accessed 30 Jan 2024.

———. 2023b. *Ομιλία ΥΦΕΘΑ Νικόλαου Χαρδαλιά στην ημερίδα «Συνδέοντας την Έρευνα με την Αμυντική Βιομηχανία».* Ministry of National Defence. https://www.mod.mil.gr/omilia-yfetha-nikolaoy-chardalia-stin-imerida-syndeontas-tin-ereyna-tin/. Accessed 30 Jan 2024.

Hellenic Air Force. 2022. *Εγκαίνια των Εγκαταστάσεων της Μοίρας Επιχειρησιακής Συνθετικής Εκπαίδευσης του Κέντρου Αεροπορικής Τακτικής.* https://www.haf.gr/2022/12/egkainia-ton-egkatastaseon-tis-moiras-epicheirisiakis-synthetikis-ekpaideysis/. Accessed 30 Jan 2024.

———. Undated-a. *Pegasus II.* https://www.haf.gr/en/equipment/pegasus-ii/. Accessed 30 Jan 2024.

———. Undated-b. *AIM-2000 (IRIS-T) Infrared Imaging Seeker – Tail.* https://www.haf.gr/en/equipment/aim-2000-iris-t-infrared-imaging-seeker-tail/. Accessed 30 Jan 2024.

———. Undated-c. *Μοίρα Επιχειρησιακής Συνθετικής Εκπαίδευσης*. https://www.haf.gr/structure/ata/keat/squadrons-schools/moira-epicheirisiakis-synthetikis-ekpaideysis/. Accessed 30 Jan 2024.

———. Undated-d. *8ο Συνέδριο Αεροπορικής Ισχύος*. https://www.haf.gr/news/air-power/. Accessed 30 Jan 2024.

Hellenic Air Force Academy. 2023a. *Undergraduate Study Programme 2022-2023.* https://drive.google.com/file/d/1vCAa5yNM3aGdbqjAESe9aHakIAP6Tbas/view. Accessed 30 Jan 2024.

———. 2023b. *Common Module on Unmanned Aerial Systems (UASs) at Hellenic Air Force Academy (HAFA).* https://hafa.haf.gr/en/2023/04/common-module-on-unmanned-aerial-systems-uass-at-hellenic-air-force-academy-hafa-2/. Accessed 30 Jan 2024.

Hellenic Army Academy. 2022. *Undergraduate Study Programme 2022-2023.* https://sse.army.gr/odigos-proptychiakon-spoydon/. Accessed 30 Jan 2024.

———. Undated. *Postgraduate Study Programme.* https://master.sse.gr/html/?page_id=32. Accessed 30 Jan 2024.

Hellenic Army Academy & Technical University of Crete. Undated. *Master in Intelligent Systems.* http://www.sse-tuc.edu.gr/en. Accessed 30 Jan 2024.

Hellenic National Defence General Staff. 2015. *Στρατηγική Ανάλυση Εξελίξεων για την Ελλάδα μετά το 2030, ΣΑΕ 2030.* https://geetha.mil.gr/wp-content/uploads/2019/11/sae2030.pdf. Accessed 30 Jan 2024.

———. 2022a. *Ομιλία του Αρχηγού ΓΕΕΘΑ στο Πανεπιστήμιο Πειραιώς με θέμα «Σύγχρονες Απειλές και Προκλήσεις Ασφάλειας».* https://geetha.mil.gr/omilia-toy-archigoy-geetha-sto-panepistimio-peiraios-me-thema-sygchrones-apeiles-kai-prokliseis-asfaleias/. Accessed 30 Jan 2024.

———. 2022b. *Εγκαίνια του Κόμβου Πληροφοριών Δυνάμεων Ειδικών Επιχειρήσεων της Διοίκησης Ειδικού Πολέμου του ΓΕΕΘΑ.* https://geetha.mil.gr/egkainia-toy-komvoy-pliroforion-dynameon-eidikon-epicheiriseon-tis-dioikisis-eidikoy-polemoy-toy-geetha/. Accessed 30 Jan 2024.

———. 2023. *Ημερίδα με Θέμα «Τεχνολογία – Καινοτομία, Άμυνα και Στρατηγική».* https://geetha.mil.gr/imerida-me-thema-technologia-kainotomia-amyna-kai-stratigiki/. Accessed 30 Jan 2024.

Hellenic Naval Academy. 2023a. *Υπογραφή Πρωτοκόλλου Συνεργασίας μεταξύ Σχολής Ναυτικών Δοκίμων και ΕΚΕΦΕ «Δημόκριτος».* https://www.hna.gr/el/activities/recent-activities/item/20230421b. Accessed 30 Jan 2024.

———. 2023b. *Πρόγραμμα Σπουδών ΣΝΔ - Κατεύθυνση Μάχιμων - Έτος Εισαγωγής 2023-2024.* https://www.hna.gr/sites/default/files/hna_docs/programma_spoudon/max_2023_2024.pdf. Accessed 30 Jan 2024.

Hellenic Republic. 2023. *Ενημερωτικό σημείωμα για τη συνεδρίαση της Συμβουλευτικής Επιτροπής για την Τεχνητή Νοημοσύνη υπό του Πρωθυπουργό Κυριάκο Μητσοτάκη.* https://www.primeminister.gr/2023/10/25/32870. Accessed 30 Jan 2024.

IAI. Undated. *Heron Multi-Role MALE UAS.* https://www.iai.co.il/p/heron. Accessed 30 Jan 2024.

Intracom Defense. 2020. *LOTUS: Next Generation Tactical UAV from INTRACOM DEFENSE for ISR missions.* https://www.intracomdefense.com/lotus-next-generation-tactical-uav-from-intracom-defensefor-isr-missions/. Accessed 30 Jan 2024.

Kikiras, Panagiotis. 2017. Interview to Giannis Mouratidis. *Netweek*. https://netweek.gr/%CF%80%CE%B1%CE%BD%CE%B1%CE%B3%CE%B9%CF%8E%CF%84%CE%B7%CF%82-%CE%BA%CE%AF%CE%BA%CE%B9%CF%81%CE%B1%CF%82-%CE%B5%CF%80%CE%B9%CE%BA%CE%B5%CF%86%CE%B1%CE%BB%CE%AE%CF%82-%CF%84%CE%B7%CF%82-%CE%BC%CE%BF/. Accessed 30 Jan 2024.

Krepinevich, Andrew. 2023. *The Origins of Victory: How Disruptive Military Innovation Determines the Fates of Great Powers*. New Haven: Yale University Press.

MBDA. 2022. *MBDA awarded two contracts by Greece for naval and aircraft weaponry.* https://www.mbda-systems.com/press-releases/mbda-awarded-two-contracts-by-greece-for-naval-and-aircraft-weaponry/. Accessed 30 Jan 2024.

———. 2023. *MBDA to boost cooperation with Greek Defence industry*. https://newsroom.mbda-systems.com/mbda-cooperates-closely-with-greek-defence-industry/. Accessed 30 Jan 2024.

Ministry of Defense. 2019. *Συμμετοχή ΥΕΘΑ κ. Νίκου Παναγιωτόπουλου στην Άτυπη Σύνοδο Υπουργών Άμυνας της Ε.Ε. στο Ελσίνκι.* https://www.mod.mil.gr/symmetohi-yetha-k-nikoy-panagiotopoyloy-stin-atypi-synodo-ypoyrgon-amynas/. Accessed 30 Jan 2024.

———. 2021. *Παρουσία ΥΦΕΘΑ Νικόλαου Χαρδαλιά στην τελική φάση της ΤΑΜΣ 'ΠΑΡΜΕΝΙΩΝ-21' στη Χίο – Επίσκεψη σε ΕΦ 'Οινουσσών', 'Παναγιάς' και 'Αγίας Ελένης'.* https://www.mod.mil.gr/paroysia-yfetha-nikolaoy-chardalia-stin-teliki-fasi-tis-tams-parmenion/. Accessed 30 Jan 2024.

———. 2022. *Συμμετοχή ΥΕΘΑ Νικόλαου Παναγιωτόπουλου στη Σύνοδο Υπουργών Αμύνης του ΝΑΤΟ στις Βρυξέλλες (16-17 Φεβ 22).* https://www.mod.mil.gr/symmetochi-yetha-nikolaoy-panagiotopoyloy-sti-synodo-ypoyrgon-amynis-nato-stis/. Accessed 30 Jan 2024.

———. 2023. *Απάντηση ΥΕΘΑ Νικόλαου Παναγιωτόπουλου σε ερώτηση Κοινοβουλευτικού Ελέγχου (υπ. Αριθμ. 1901/24-01-2023) με θέμα: «Προβληματισμοί σχετικά με την υλοποίηση του πολύ-προβεβλημμένου προγράμματος ανάπτυξης UAV Αρχύτας».* https://www.mod.

mil.gr/apantisi-yetha-nikolaoy-panagiotopoyloy-se-erotisi-koinovoyleytikoy-elegchoy-yp-arithm-313/. Accessed 30 Jan 2024.

———. Undated. *Defence Innovation Challenge.* https://crowdhackathon.com/defencetech-bootcamp/en/. Accessed 30 Jan 2024.

Ministry of Development & Investments. 2020. *Μνημόνιο συνεργασίας μεταξύ των Υπουργείων Ανάπτυξης & Επενδύσεων και Εθνικής Άμυνας για την υλοποίηση του προγράμματος 'ΘΩΡΑΞ – THORAX'.* https://www.mindev.gov.gr/%CE%BC%CE%BD%CE%B7%CE%BC%CF%8C%CE%BD%CE%B9%CE%BF-%CF%83%CF%85%CE%BD%CE%B5%CF%81%CE%B3%CE%B1%CF%83%CE%AF%CE%B1%CF%82-%CE%BC%CE%B5%CF%84%CE%B1%CE%BE%CF%8D-%CF%84%CF%89%CE%BD-%CF%85%CF%80%CE%BF%CF%85/. Accessed 30 Jan 2024.

Ministry of Digital Governance. 2021. *Digital Transformation Bible 2020-2025.* https://digitalstrategy.gov.gr/en/vivlos_pdf?page=158. Accessed 30 Jan 2024.

Ministry of Migration & Asylum. Undated. *Reaction - Call: BMVI/2021/SA/1.5.4: Support to comply with the implementation of the relevant interoperability legal framework.* https://migration.gov.gr/en/ma/reaction/. Accessed 30 Jan 2024.

Mitsotakis, Kyriakos. 2023. *Η Ελλάδα το 2040, μια χώρα στην πρώτη γραμμή της Ευρώπης. Βουλή - Επί του Περιστηλίου* (pp. 4–5). https://www.hellenicparliament.gr/userfiles/ebooks/periodiko_t061/4/index.html. Accessed 30 Jan 2024.

Mononews. 2022. *Elbit Systems: Προχωρά το έργο του Διεθνούς Κέντρου Εκπαίδευσης Πιλότων στην Καλαμάτα.* https://www.mononews.gr/business/elbit-systems-prochora-to-ergo-tou-diethnous-kentrou-ekpedefsis-piloton-stin-kalamata. Accessed 30 Jan 2024.

NATO. 2022a. *NATO sharpens technological edge with innovation initiatives.* https://www.nato.int/cps/en/natohq/news_194587.htm. Accessed 30 Jan 2024.

NATO. 2022b. *NATO's Data and Artificial Intelligence Review Board: Summary of the establishment of the Board.* https://www.nato.int/cps/en/natohq/official_texts_208374.htm. Accessed 30 Jan 2024.

Naval Postgraduate School. Undated. *AI for Military Use Certificate.* https://nps.edu/web/ciser/ai-certificate. Accessed 30 Jan 2024.

NAVMAT. 2023. *AI-powered NAVMAT prototype at ICEAF VII.* https://www.navmat.gr/news/ai-powered-navmat-prototype-iceaf-vii-june-23. Accessed 30 Jan 2024.

Nedos, Vassilis. 2022. *'Thorax' κατά υβριδικών απειλών – Νέο σύστημα στο ΓΕΕΘΑ. Η Καθημερινή.* https://www.kathimerini.gr/politics/561722623/thorax-kata-yvridikon-apeilon-neo-systima-sto-geetha/. Accessed 30 Jan 2024.

Nikitas, Giannis. 2021. *UAV Heron: Άριστη η πρώτη εμπειρία επιχειρησιακής αξιοποίησης με επίκεντρο τη διακλαδικότητα στην ΤΑΜΣ 'ΠΑΡΜΕΝΙΩΝ 2021'.* Defence Review. https://defencereview.gr/hellenic-armed-forces-operational-experience-uav-heron/. Accessed 30 Jan 2024.

———. 2022. *Το ελληνικό UAV 'ΑΡΧΥΤΑΣ' της EFA VENTURES: Πολλαπλασιαστής ισχύος των Ελληνικών Ενόπλων Δυνάμεων.* Defence Review. https://defencereview.gr/to-elliniko-uav-archytas-tis-efa-ventures-pollapl/. Accessed 30 Jan 2024.

Rickli, Jean-Marc, and Federico Manellassi. 2023. Artificial intelligence in warfare: military uses of AI and their international security implications. In *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*, ed. Michael Raska and Richard A. Bitzinger, 12–36. London: Routledge.

Sachini, Evi, Nena Malliou, Charalambos Chrysomallidis, Nikos Karampekios, Konstantinos Siouma-las-Christodoulou, and Stefanos Christopoulos. 2022. *Εντοπισμός και ανάλυση των ελληνικών επιστημονικών δημοσιεύσεων στον τομέα της Τεχνητής Νοημοσύνης με τεχνικές Μηχανικής Μάθησης.* National Center of Documentation. https://metrics.ekt.gr/publications/633. Accessed 30 Jan 2024.

SEKPY. 2023. *«DefencEduNet»: Ίδρυση της «Εταιρείας Διασύνδεσης Αμυντικής Βιομηχανίας, Ανώτατης Εκπαίδευσης και Έρευνας».* https://sekpy.gr/defencedunet-idrysi-tis-etaireias-diasyndesis-amyntikis-viomichanias-anotatis-ekpaidefsis-kai-erevnas/. Accessed 30 Jan 2024.

Souliotis, Giannis. 2021. *Ηλεκτρονική ασπίδα στον Εβρο – Σε λειτουργία κάμερες και ραντάρ, Η Καθημερινή*. https://www.kathimerini.gr/society/561551092/ilektroniki-aspida-ston-evro-se-leitoyrgia-kameres-kai-rantar/. Accessed 30 Jan 2024.

Tyler, Chris, K.L. Akerlof, Alessandro Allegra, Zachary Arnold, Henriette Canino, Marius A. Doornenbal, Josh A. Goldstein, David Budtz Pedersen, and William J. Sutherland. 2023. AI tools as science policy advisers? The potential and the pitfalls. *Nature*. https://www.nature.com/articles/d41586-023-02999-3. Accessed 30 Jan 2024.

Van Roy, Vincent, Fiammeta Rossetti, Karine Perset, and Laura Galindo-Romero. 2021. *AI Watch - National Strategies on Artificial Intelligence: A European perspective*. Luxemburg: Publications Office of the European Union.

Enabling Technology of Future Warfare: Turkey's Approach to Defense AI

Çağlar Kurç

Defense artificial intelligence (AI) development in Turkey focuses primarily on improving the capabilities of autonomous systems, sensors, and decision support systems because Turkey believes autonomous systems are the future of modern warfare. Increasing autonomous systems' capability in intelligence gathering and fighting, as well as enabling swarm operations, are prioritized in developing defense AI. While Turkey enhances the capabilities of autonomous systems, humans will continue to be critical for decision-making in the foreseeable future.

Currently, the fast pace of developing and deploying autonomous systems exacerbates the dilemma of human-machine interaction. As Turkish defense industry representatives contend, it is easier to make machines talk to each other than to add humans into the mix, because existing structures are not yet suitable for effective human-machine interaction. However, these defense industry representatives also believe that AI enhancements to decision-making systems would help humans to make faster decisions and ease human-machine interactions.

Turkey's intentions and plans for the development of AI can be traced in official strategy documents, as well as R&D focus group reports. Prominent documents include the following:

- The 11th Development Program, which sets out Turkey's economic development goals and critical technology investments;
- The National Artificial Intelligence Strategy 2021–2025, which sets the framework for AI development in Turkey;
- Focus Technology Network Reports, which lay out technology roadmaps for specific defense technologies. These documents provide insight into how Turkey approaches AI, defense AI, and related technologies.

Ç. Kurç (✉)
Department of Political Science and International Relations, Abdullah Gül University, Kayseri, Turkey

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_15

- The 2023–2027 Defense Industry Sector Strategy Document, which describes the relations between defense AI development and the sub-sectors within the Turkish defense industry and sets the goals for defense AI development.

Turkey specifically focuses on AI-related technologies like machine learning, computer vision and natural language processing with an application focus on autonomous vehicles and robotics. Autonomous systems, mainly uncrewed aerial vehicles (UAVs), remain a priority in Turkish AI development since 2011. This focus has since expanded to include all types of uncrewed vehicles. In parallel, enhancing these vehicles with AI is gaining traction. The intertwined development of AI and related technologies form the core of Turkey's AI ecosystem.

Turkey's AI ecosystem is nascent but growing. As of September 2023, there are 350 AI startups listed in the Turkish AI Initiative (TRAI) database. Turkey aims to create synergies between its defense and civilian industries, academic institutions, and government through various ecosystem initiatives. Since many organizations are involved, these initiatives enhance the repetition and redundancy that often arises from AI technology itself.

Turkey currently has a distributed organizational approach to AI. Each government agency sets up its own AI organization with overlapping responsibilities. Recently, the Defence Industry Agency (Savunma Sanayi Başkanlığı, SSB) established an AI-specific organization, the Artificial Intelligence Talent Cluster of Defence Industry (SAYZEK). SSB aims to foster defense innovation by centrally coordinating stakeholders in defense AI.

Turkey seeks to increase its R&D spending on AI, aiming to increase employment and grow the ecosystem. The SSB would grant more AI-based projects in the future and be willing to buy more autonomous systems, encouraging an upward trend in R&D spending. However, although Turkey would like to increase spending, the financial crisis may hinder current efforts.

Training and managing a skilled workforce are essential to building the indigenous AI development capacity that Turkey is looking for. This includes two components. First is the fostering of human resources that can develop and produce defense AI. Turkey is therefore investing in new university programs, researcher training, open-source platforms, and employment while supporting technology competitions. Second is the training of military personnel that would use defense AI. Defense AI is also slowly becoming part of the Turkish Armed Forces' (Türk Silahlı Kuvvetleri, TSK) training activities. Currently, there is very little open information on how Turkey intends to train military personnel in using defense AI.

1 Thinking About Defense AI

Turkey's approach to AI revolves around other emerging technologies. In other words, Turkey views AI as an enabling technology that would improve the capabilities of emerging systems, such as autonomous systems, and aid decision-making

systems through improving human-machine interfacing and enhancing training. This can be seen in how AI is defined in the National Artificial Intelligence Strategy 2021–2025. According to the document, AI is "in a very general sense, the ability of a computer or computer-controlled robot to perform various activities in a similar way to intelligent living things" (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 2021: 12). AI-supported systems use advanced algorithms that learn from patterns contained in the data and make predictions (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 2021: 12). The main thrust of the defense AI development in Turkey focuses on improving the capabilities of various autonomous systems such as sensors and decision support systems. Turkey believes the future of warfare will be defined by using autonomous systems, increase the operational tempo.

AI will usher in a new era of fighting in which swarms of systems gather intelligence and fight. As the information gathered from the battlefield increases, it goes beyond the capabilities of human cognition. Thus, AI emerges as the facilitator for information fusion and data evaluation. Information from different locations about a single target needs to be fused and delivered to decision-makers. Likewise, swarm operations require various systems to operate in seamless coordination with each other, requiring a high level of autonomy. The necessary autonomy is believed to be realized by incorporating AI into these systems. However, future warfare would continue to include human-controlled systems as well, at least in the foreseeable future. As a result, autonomous systems need to communicate with human decision-makers.

Turkish scholars expect two main consequences of AI on future warfighting (Kasapoğlu and Kırdemir 2018: 16). The first is the increased speed of the Observe, Orient, Decide, Act (OODA) loop. AI-supported systems will increase the rate of intelligence gathering, surveillance, target acquisition, and reconnaissance. Consequently, the military's decision-making processes will accelerate as the commanders' access to information increases. Combined with AI-enhanced decision-making systems, commanders would make faster decisions. Second, related to the increased capability of gathering information, militaries and intelligence agencies could advance predictive analysis.

Turkey's defense capstone documents reflect these expectations. Focus Technology Networks (Odak Teknoloji Ağı, OTAĞ) reports provide insight into Turkey's approach to defense AI and related technologies, while the 11th Development Program and the National Artificial Intelligence Strategy 2021–2025 inform about Turkey's approach to AI in general and related fields of activity.

The 11th Development Program is the foundational document that determines the overall framework for area-specific strategy documents. It focuses on Turkey's overall economic development and sets out respective goals. The document also sets out the technologies that are deemed critical for Turkey's continued development (Strateji ve Bütçe Başkanlığı 2019).

The National Artificial Intelligence Strategy 2021–2025, meanwhile, sets out the goals for developing AI in parallel with the overall economic development strategy. It lays out the current state of Turkey's AI capabilities, which various government organizations and the private sector are pursuing to enhance Turkey's AI proficiency

and discusses the necessary steps to be taken to improve Turkey's capabilities (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 2021).

In parallel with the overall AI strategy, various government organizations are expected to produce their own area-specific AI strategies. Although SSB recently organized a focus meeting for a national defense AI strategy (Işık 2022), the author does not know whether the document will be made public. Furthermore, SSB is currently working on an AI OTAĞ report (STM ThinkTech 2022: 12), which has not yet been published at the time of writing of this chapter. However, an investigation of completed OTAĞ reports provides ideas on the possible focus of the defense AI strategy concerning research and development priorities and the technologies that Turkish defense industries will likely focus on developing.

OTAĞ reports are a foundation for the defense R&D development roadmap for a given focus area. Through these reports, Turkey determines the critical technologies that need to be indigenized, prioritizes those critical technologies, and initiates the basic technology projects (Savunma Sanayii Başkanlığı 2022a). However, this can only be done with assumptions about future war. While these documents do not tell us definitively what the TSK think about the future of warfare, they provide detailed discussions by defense industry and academia, providing some insight into how the armed forces may be thinking.

Of the various OTAĞ reports, two of them are very important. The first one is the Swarm Intelligence Development report, which mainly focuses on developing and using swarms of autonomous weapons. The second document focuses on developing radio frequency technologies that would enhance the information-gathering capabilities of military systems (İncel et al. 2021). A third report focuses on cyber security, in which AI is mentioned but not as prominent as the other two documents (Savunma Sanayii Başkanlığı and Türkiye Siber Kümelenmesi 2019). As the OTAĞ reports suggest, AI is closely intertwined with other emerging technologies and seen as a facilitator to increase these capabilities.

Turkey expects to acquire capabilities mainly in autonomous systems and data collection and management. Currently, STM-produced Alpagu and Kargu tactical loitering munitions utilize computer imaging for targeting and machine-learning algorithms to optimize target classification, tracking, and attack capabilities without the requirement of GPS. Turkey's other UAVs, such as Bayraktar TB2, could have similar capabilities (BaykarTech 2022). Thus, developing defense AI and integrating it with uncrewed systems would advance their capabilities, both when operating alone and as a swarm. Further gains result from collecting battlefield data, such as data fusion, prioritization, and aiding the decision-maker.

Every capability gain also comes with new concerns. Current literature on autonomy and AI in Turkey reveals four main concerns about the prospective impact of defense AI:

- *Aligning Concepts and Technology Development*

The first concern is about how to manage expectations. Can Kasapoğlu, director of the security and defense studies program at the Istanbul-based Center for

Economics and Foreign Policy Studies (EDAM), points out that although the main expectation is that defense AI would simplify tasks and operations, in reality, new weapon systems and their newfound capabilities will add to the complexities of modern warfare. Rather than a one size fits all approach, the proliferation of different weapon systems, their interconnected capabilities, and increased electromagnetic capabilities would increase the complexity, resulting in problems in managing these systems and the data they produce. New technologies would open new mission spaces that come with their own unique set of problems. Thus, militaries must find new ways to deal with these emerging problems and develop new concepts and doctrines that would fit the new operational environment (Kasapoğlu and Kırdemir 2018: 15). To this end, for example, the Turkish Navy, in cooperation with various defense companies, is experimenting with autonomous systems, which have different mission packages, both in national and NATO exercises (İnsansız Deniz Sistemlerinin Geleceği ve Türkiye Potansiyeli 2022).

Although there is no open-source information on the specifics of how these concepts and doctrines would look in the Turkish case, Havelsan's future warfare vision provides an insight on, at least, how industry thinks about future doctrines and concepts. The company has been developing a variety of uncrewed systems for operations on land, in the air, and at sea in parallel with its future warfare concept, Digital Troops. The concept has three pillars: (1) training and preparation for battles, (2) wearable technologies and (3) integrated autonomous robotic systems. Havelsan aims to integrate autonomously operating uncrewed air, land and naval systems with the new generation of wearable military technologies and the command and control (C2) center, thus enabling full integration between different systems with soldiers and commanders (Köprülü 2021: 7). This vision seems to be in line with the research and development as well as defense AI priorities of Turkey. Although the concept hints at the future direction of Turkish plans, it is easier to imagine this future vision than to implement it as the military and the defense industry face difficulties in developing autonomous systems and integrating them into the existing military structures.

- *Handling Human-Machine Interaction*

The second concern refers to human-machine interaction. Despite the development of AI systems, they are not mature enough to deploy in fully autonomous systems that can coordinate independent of human control. And even when full autonomy can be reached, there is still a need for human oversight. Thus, human-machine interactions sit at the center of the development of AI-enabled autonomous systems (STM ThinkTech 2021b: 13). Yet, it seems that this is the most challenging part. Industry representatives argue that coordinating a group of uncrewed systems is far easier than making machines and humans work together because adding machines into the C2 mix alters the established human-to-human command and control behavior of the military personnel (İnsansız Deniz Sistemlerinin Geleceği ve Türkiye Potansiyeli 2022).

- *Integrating Uncrewed Systems into Existing Force Structures*

The third concern is about organizing and managing uncrewed systems within the overall military system. Currently, every service pursues its own uncrewed system projects. Yet, Gökhan Uçar, the former Head of the Uncrewed and Smart Systems Department at SSB, contends that the proliferation of autonomous systems requires a new type of organization. He argues that Turkey needs to establish an "Uncrewed Systems Command," composed of military officers and civilians focusing solely on using autonomous and uncrewed systems. The new command should have uncrewed land, air, sea, and robotic soldier branches (STM ThinkTech 2021a: 11). While the specifics of the new organization have not been elaborated, the suggestion of a new organization points out an awareness for the need to think differently about uncrewed systems. Such an organization could enable a more focused and coordinated approach to the development, procurement, and use of uncrewed systems as well as the development of defense AI.

- *Addressing AI-Induced Vulnerabilities*

The final concern is dealing with new vulnerabilities that emerge with interconnected systems. One of the common security concerns regarding autonomous systems and AI is hacking. In other words, as the systems become more connected and computerized, they increasingly become vulnerable to cyber-attacks. Thus, the question becomes how to prevent AI-enabled systems from input manipulation, which would alter how the AI behaves (Kasapoğlu and Kırdemir 2018: 18; Bülbül et al. 2021: 79).

Turkey's capstone research and development documents and the discussions on defense AI also reveal how international partners influence the country's approach to defense AI. Although Turkey tries to learn from the experiences of many states, the United States emerges as the main source of influence. The research and development documents mainly reflect the developments and discussions in the United States, as highlighted by the references quoted in these documents (Bülbül et al. 2021). Similarly, discussions about the need to protect defense AI solutions against outside interference reflect and sometimes reiterate ongoing US discussions. This explains why publicly available information as well as ongoing debates seem to be generic. Yet generic discussions reveal whose discourse impacts Turkey's approach to defense AI. However, this does not imply that Turkey is seeking to fully emulate the United States. Rather, as we will discuss in the following sections, the US serves as a point of departure, and through testing and experimenting, Turkey strives to construct its own path in developing defense AI.

2 Developing Defense AI

Turkey is seeking to become a powerhouse in emerging technologies. This is reflected in general R&D priorities, which are connected to its defense AI development programs. According to the 11th Development Program, AI, the Internet of Things, Augmented Reality, Big Data, and Sensor Technologies are the priority

R&D areas that would elevate the Turkish economy (Strateji ve Bütçe Başkanlığı 2019: 81). In line with the R&D priorities determined by the 11th Development Program, Turkish companies are also focusing on AI and AI-related technologies such as Machine Learning, Computer Vision, Natural Language Processing, Autonomous Vehicles, and Robotics (Strateji ve Bütçe Başkanlığı 2019; TRAI 2023). Again, the general R&D priorities show how interconnected AI development is with other emerging technologies.

Robotics is Turkey's current prime R&D focus. Since 2011, defense R&D in robotics, especially autonomous weapons, has focused on autonomous command and control. According to the UAV Technology Roadmap, automation, AI, distributed command, control, and communication technologies sit at the heart of the technology roadmap (Savunma Sanayii Müsteşarlığı 2011). In parallel with the focus on robotics and autonomy, the same document also refers to swarm technologies (Savunma Sanayii Müsteşarlığı 2011: 57), which have recently gained prominence, as observed in OTAĞ documents and the National AI Strategy.

The defense AI R&D projects focus on developing underlying technologies that increase the capabilities of AI-enabled systems. In this regard, SSB currently has the following priorities (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 2021: 55):

- Social media anomaly detection
- Event analysis
- Deep learning, the big data analysis platform
- Social media analysis performance enhancement
- GPS-independent, autonomous navigation
- Identification and classification of radar-detected naval targets
- Swarm robots and autonomous reconnaissance
- Guidance and navigation
- Operational AI command assistant
- AI-based fire support and autonomous driving for land systems
- AI-based risk detection and prevention in software-based networks
- Global risk analysis

OTAĞ reports and Defense Industry R&D Broad Topic Calls (Savunma Sanayi Ar-Ge Geniş Alan, SAGA) analyze in more detail, which technologies Turkey would pursue in the future. AI SAGA calls for prioritized projects focusing on explainable AI learning methods, reinforced learning methods, learning with sparse data, robust learning methods against data poisoning, and innovative (third generation) learning methods (Savunma Sanayii Müsteşarlığı 2018: 4). Building on the earlier SAGA call, the Swarm Intelligence OTAĞ report argues that distributed AI, AI-based electronic warfare, and AI-based cognitive modeling should be prioritized for swarm systems (Bülbül et al. 2021: 193). The Radio Frequency OTAĞ report focuses on signals processing and underlines the importance of cognitive signal processing-based systems and cognitive signal processing systems for distributed systems networks (İncel et al. 2021: 203). Finally, the Cyber OTAĞ report prioritizes the development of an AI-based risk information sharing platform and AI-supported command and control system to increase cyber security defenses

(Savunma Sanayii Başkanlığı and Türkiye Siber Kümelenmesi 2019: 39). Completed and ongoing research projects reflect these priorities.

2.1 Current Defense AI Projects

Turkey currently has nine defense AI-related projects, which also represent Turkey's ongoing defense AI procurement priorities:[1]

- *AI Commander Assistant Developing Course of Action Project (HAMLE)*

HAMLE is an AI-based war gaming platform developed by ASELSAN. It uses reinforcement learning and AI algorithms to provide operational suggestions for corps, brigades, and battalions at the tactical level through different game modes. The system learns from wargames and assumes the role of an instructor in personnel training. As the system learns, it could be used in military decision-making (Aselsan 2022).

- *AI-Assisted Fire Control Support and Autonomous Driving for Land Vehicles Project (Karagöz)*

The system uses information from Lidar, radar, ultrasonic sensors, and electro-optic sensors to enable autonomous driving (route planning, moving/stationary target detection, geographical information systems integration, passage recommendation in confined spaces, and collusion detection), observation (tracking, 360 degrees vision and friend-or-foe identification), and fire support (target range detection, target, and target class detection, and ammunition recommendation). The system is based on machine and deep learning, sensor fusion, and computer vision (Savunma Sanayii Başkanlığı 2022b).

- *Autonomous Discovery, Guidance, and Navigation with Collaborative Robots Project (Robo-Tim)*

This project aims to develop a heterogenous swarm system that integrates three UAVs and three UGVs to engage cooperatively in adaptive exploration and autonomous navigation. The system would enable swarm systems to simultaneously position themselves and operate in GPS-denied areas. It uses AI-based work sharing and object and friend/foe recognition to facilitate the cooperation of UAVs and UGVs and improve operational swarm capabilities. The project aims to enable UAVs to land on moving UGVs. Automatic charging would allow UAVs to continue their operations. Finally, the project will form a foundation for swarm communication capabilities (STM ThinkTech 2021b: 27).

[1] There is no publicly available information about the SSB-backed Social Media Analysis Performance Development Project (PEGEL). See Kökçü (2020).

- *Identification and Classification of Radar-Identified Surface Targets Project (GÖRÜ)*

The project aims to develop AI to detect, classify and identify surface targets based on data from synthetic-aperture radar (SAR) sensors (Savunma Sanayi 2020).

- *Image Analysis and Automatic Target Recognition System Project (HASAT)*

The project aims to develop an image recognition system that could identify, recognize, and classify targets. It will be able to analyze and evaluate the image and detect targets based on the data acquired from electro-optic systems and SAR of satellite and air platforms (Savunma Sanayii Müsteşarlığı 2017b).

- *Advanced Imagining Technologies Project (TUYGUN)*

The project aims to develop multispectral and hyperspectral imaging software and target analysis for various platforms (Savunma Sanayii Müsteşarlığı 2015).

- *Artificial Intelligence Technologies for Swarm vs Swarm Air Engagement Development Project (SUMRU)*

Led by İTÜNOVA TTO (Savunma Haber 2022), this project aims to develop an AI-based guidance system that would enable swarms to operate independently of central command and control and disable the adversary's swarm systems (Kaplan 2022).

- *Detection of Border Violations by Artificial Intelligence Enhanced UAVs Project (AHLAT)*

The project, led by Bitlis Eren University (Savunma Haber 2022), aims to develop an observation system based on mini-UAV swarms with deep reinforced learning. At the optimum time and route along the border, these swarms would conduct area sweep and detect illegal activities around military units (Kaplan 2022).

Technologies developed with the help of these projects are likely to be integrated into Turkey's other autonomous system projects. TUYGUN and HASAT seem to be service and system-agnostic. Others seem to be service-related but platform-agnostic. GÖRÜ is for the Turkish Navy, while Karagöz and AHLAT are for the Turkish Army. Robo-Tim technology has the potential to be used by all three services to integrate their autonomous systems, although the project in its current form mainly focuses on cooperation between UAVs and UGVs. SUMRU could also be used by all three services as an air defense solution. Some of these technologies are likely to be integrated into and form the basis of autonomous capabilities developed with the following three weapon system projects:

- *Bayraktar Kızılelma*

Bayraktar Kızılelma is a Turkish uncrewed fighter aircraft (Cenciotti 2022). Conceptually, it is unclear whether it will operate like a Loyal Wingman or be controlled from a ground station (Newdick 2022). If it was operationalized like a Loyal Wingman—as foreseen by other countries developing similar

technology—Kızılelma would work with Turkey's TF-X fifth-generation fighter plane and be used for dangerous air operations that require penetration of heavily defended areas to conduct suppression of enemy air defense (SEAD). In addition, it is planned to conduct intelligence, surveillance, and reconnaissance (ISR) and counter-air missions (Newdick 2022). It has a stealth design and is powered by turbofan engines. There will be different versions of Kızılelma, which would use various engines and engine configurations and thus have additional capabilities. Furthermore, Baykar Technology also plans to have a naval version capable of operating from the TCG Anadolu, an amphibious assault ship (Kasapoğlu 2022).

Kızılelma is also expected to be AI augmented (Jennings 2022). It is argued that the system can learn from its environment, detect new patterns, develop new behavior, and facilitate human-machine integration (Kasapoğlu 2022). Yet, apart from these generic expectations, not much is clear about how Kızılelma would use AI. However, Baykar Technology's previous work on AI suggests that Kızılelma would have visual posture detection, basic object detection, landmark recognition and operate beyond the line of sight (BLOS) (BaykarTech 2022). These technologies have not only been developed for Kızılelma, but also for other systems, such as TB2, Akıncı, and other Baykar UAVs. Kızılelma would have more advanced versions of these technologies—an important test for Baykar's AI capabilities. Other SSB-funded technologies discussed above could be integrated into the system.

- *FNSS Shadow Rider UGV*

FNSS Shadow Rider is an optionally manned UGV based on the M113 platform. Its AI-based autonomy kit enables the system to patrol, track and return to the military base. It could be used in reconnaissance and surveillance, logistic support, tactical deception, fortified position reconnaissance, communication relay, medical evacuation, and fire support missions. The armed versions do not fire on targets autonomously, but as argued earlier, always keep the man-in-the-loop. Its autonomous capabilities include leader-follower capabilities in GNSS-denied areas and obstacle detection and avoidance (FNSS 2022). We can expect Robo-Tim technology to be integrated into the Shadow Rider.

- *Aselsan-Sefine Marlin USV*

Turkey has been investing in various types of USVs (Ozberk 2022a). With its electronic warfare capabilities, Marlin USV emerges ahead of other competitors in its class. The system can be fitted with different payloads such as lightweight torpedoes, light guns, medium-range surface-to-surface missiles, electronic warfare modules, sonobuoys, satellite, line of slight, and underwater communication (Ozberk 2022b). AI could enhance the system's autonomous capabilities if needed (Yanık 2022). The system is also capable of conducting anti-submarine warfare. During NATO exercises "Robotic Experimentation and Prototyping Exercise by Maritime Uncrewed Systems" (REMPUS) and "Dynamic Messenger 22," Marlin detected the undersea target simulator through the processing of signals from different sonobuoys and reported back to NATO Headquarters (Aksan et al. 2022).

Although these examples are not exhaustive, they show that Turkey's defense AI approach is inherently linked to robotics and uncrewed systems. Increasing production capabilities and recent successes of Turkish weapon systems, such as Bayraktar TB2 drones, resulted in an increased focus on the development of autonomous weapon systems. We expect that SSB-funded, as well as company-funded, AI technologies will be integrated into these systems. Although there is little information on which technologies would be integrated and how, the growing AI-related industry shows the direction of future Turkish expectations.

Increased focus on uncrewed systems also led to more companies entering the market (See Presidency of Defence Industries 2019: 44–49, 102–103, 141–151; Defense Here 2021b), resulting in more systems that could be tested. Thus, Turkey currently engages in constant experimentation to construct new concepts and doctrines for autonomous systems. For example, Arda Mevlütoğlu, a Turkish engineer and scholar, contends that Turkey's use of UAVs for electronic warfare in coordination with multirole aircraft and artillery, as highlighted during the spring 2019 operation in Idlib, signifies novel battlefield tactics that result from exploring and developing new concepts by the TSK (Türk tipi İHA Operasyonu: Arda Mevlütoğlu anlatıyor 2020; Mevlütoğlu 2021). Thus, Turkey is increasingly focusing more on its specific needs and limitations while developing new weapon systems. Hence, the author expects that there will be a divergence between the United States and Turkey in terms of development and concepts in the deployment of autonomous systems and, therefore, defense AI.

2.2 Defense AI Ecosystem

Turkey has a nascent but growing AI ecosystem. While some AI companies are working with the defense industry in developing defense AI, the overall management of the ecosystem is decentralized. The National AI Strategy aims to encourage AI clusters that would increase the synergy and cooperation between different companies and industries. Consequently, various organizations seek to improve the relations between industrial partners, universities, and government institutions. For example, TÜBİTAK Artificial Intelligence Institute seeks to encourage cooperation and technology transfer between universities, state research centers and the private sector through establishing clusters focusing on financial technologies, smart production systems, smart agriculture, food and husbandry, climate change, and e-trade technologies (Yapay Zekâ Enstitüsü 2022a, b). SSB also seeks to construct an ecosystem focusing on defense through the Defense Industry Artificial Intelligence Platform (Savunma Sanayii Yapay Zekâ Platformu 2022) and newly established SAYZEK. Furthermore, the Turkish AI Initiative (TRAI), a non-governmental organization, also seeks to improve the AI ecosystem in Turkey. The effectiveness of these disparate groups is questionable because of structural duplication, but SSB aims to prevent redundancy through centralizing the coordination in Defense AI.

Overall, the defense AI ecosystem comprises a few prominent companies, including STM, Havelsan, Aselsan, Bites, and Baykar, which research and develop primarily uncrewed platforms. These companies have already fielded AI-based uncrewed systems and are working on developing new technologies. Havelsan is especially important as it is very competent in developing AI-based wargaming, which could also be transformed into an AI-based decision support system. However, it is difficult to separate neatly between pure defense and civilian companies due to the dual-use nature of AI and robotics technologies. Furthermore, defense companies that focus on AI development also cooperate with other defense partners, such as the shipyards of Sefine and Yonca-Onuk, as well as civilian companies to develop and field AI-integrated platforms.

Turkey has a primarily dual-use AI technology ecosystem. As of September 2023, there were 350 AI startups listed in the TRAI database (TRAI 2023). Since AI is a general-purpose technology that could be applied to different settings, various companies have products for both civilian and defense sectors. Thus, it is not surprising to see civilian companies also cooperating with defense companies and partnering in defense AI research. Some prominent examples include Selvi Technology, OBSS, Kuartis, and Titra. Universities also play an essential role in developing defense AI and acting as centers for guidance and knowledge transfer. METU Center for Image Analysis and METU-TAF Modsimmer are the two most prominent research centers with close links to Turkey's defense and military sectors, but there are many more. In parallel with the development goals and the National Artificial Intelligence Strategy, the number of AI-focused programs and research has increased.

In line with its push for greater self-sufficiency Turkey does not seek international partners in developing its local defense AI capabilities but is willing to participate in NATO initiatives. In 2022, TÜBİTAK BİLGEM and SAGE have been selected as test centers under NATO's Defense Innovation Accelerator for the North Atlantic (DIANA) initiative (Gökkoyun 2022; TÜBİTAK SAGE 2022).

Civilian AI initiatives, by contrast, are encouraged to seek and increase international partnerships. Turkey mainly cooperates with the United States and European Union member states, in particular Germany (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 2021: 52). International cooperation is essential for Turkey's overall AI ecosystem. However, due to the transferability of the skills, experience gained through these partnerships could be transferred to building defense AI.

Although Turkey does not partner with other countries on developing defense AI, interoperability is nonetheless a major concern. Interoperability of swarming systems is particularly important as interoperable swarm communication is said to increase operational effectiveness. To this end, the Swarm Intelligence OTAĞ report suggests (Bülbül et al. 2021: 182–183):

- Determining software and hardware requirements
- Choosing common components and interface requirements
- Securely controlling and managing data links

- Establishing package structures for the communication between uncrewed systems that have different characteristics and data
- Analyzing the optimum bandwidth values and frequency based on data package and size based on standards
- Bringing different characteristics from NATO standards and STANAG documents for control station functional architecture and data link systems.

Turkey seeks to incorporate NATO standards while integrating different Turkish autonomous weapon systems. This suggests that Turkey considers the need for allied interoperability while developing autonomous systems as this could also improve the export prospects of Turkey's autonomous system to NATO allies. Overall, Turkey appears to follow a structured and project-based technology development path to incorporate defense AI into its emerging technologies.

3 Organizing Defense AI

Turkey currently has a distributed organizational approach to AI. Each government agency is setting up its own AI organization with overlapping responsibilities. Here is a list of established agencies:

- Department of Big Data and Artificial Intelligence Application under the Digital Transformation Office of the Presidency
- General Directorate of National Technology under the Ministry of Industry and Technology
- TÜBİTAK Artificial Intelligence Institute
- General Directorate of Health Information System under the Ministry of Health
- Unit of Artificial Intelligence and Wearable Technologies under National Projects Management Coordinatorship
- Branch Office of Process Management and Artificial Intelligence Application under the Directorate of Communication and Information Technologies of the Ministry of National Defense

SSB aims to sustain the efficient development of AI technologies and foster defense innovation in the AI sector through centralized guidance and cooperation of stakeholders (SSB 2023: 160). To this end, recently, SSB established the Artificial Intelligence Talent Cluster of Defence Industry (Savunma Sanayii Yapay Zeka Yetenek Kümelenmesi—SAYZEK) (Savunma Sanayii Başkanlığı 2023). The cluster aims to bring AI companies, academia, and other stakeholders together to foster cooperation and product development in the security and defense sector (SAYZEK 2023). In addition to SAYZEK, the SSB Department of R&D manages AI-related R&D projects and the SSB Department of Uncrewed and Smart Systems manages platform-related projects. Apart from the SSB strategy documents, the author does not have any information on how military services approach defense AI and how they plan to change their organizational structure.

4 Funding Defense AI

Turkey has been increasing its R&D budget since 2006. According to TurkStat, Turkish R&D spending has increased from TL4.399bn (USD3.081bn) in 2006 to TL198.669 billion (USD12.004bn) in 2022 (TurkStat 2023).[2] While state funding remains low, the primary funding source comes from private industry, which is also leading most R&D projects. Most private R&D spending is in the production sector, with TL122.027bn (USD7.373bn) in 2022 (TurkStat 2023). While the recent data on sectoral spending is not available, in 2020, the information and communication sector was the second biggest spender, with TL11.144bn (USD1.260bn) in 2020. R&D in this sector involves research on AI and machine learning, big data, and data analytics, among others. While the specific R&D budget for AI is unclear, the National AI Strategy shows that large companies are leading the AI development (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 2021: 46).

In 2021, TÜBİTAK determined eight areas as priority R&D and innovation topics. These were information and communication technologies, energy, agriculture and food, machine production, automotive, health, and other areas (mining, advanced metallurgy, and chemistry). Within information and communication technologies, big data and data analytics, robotics, and mechatronics, and AI were the prioritized research areas. AI research areas prioritize AI technologies (a very general term) and artificial vision, image, and video processing (more specific technology). Within the robotics area, AI is also prioritized with the new generation AI-based robots as one among different topics (TÜBİTAK 2022). Even though TÜBİTAK mainly focuses on developing technologies for civilian use, with the notable exception of defense-specialized institutes, we can assume that the TÜBİTAK-funded AI R&D projects would spill over to the defense area.

Against this background, it can be assumed that Turkey seeks to increase R&D spending on AI as it wants to grow its AI ecosystem and create jobs for highly qualified experts. Thus, SSB could buy more autonomous systems and lift its overall R&D spending. However, the biggest challenge is the current economic crisis, which limits the government's financial leeway. At this point, private sector initiatives would become important, especially for defense companies. Growing arms trade volumes could facilitate more R&D investments, but still, companies would look for a return on investment to justify growing R&D spending.

[2] Current prices. Based on OECD exchange rates: 2006 1USD = TL1.428, 2022 1USD = TL16.549 TL https://data.oecd.org/conversion/exchange-rates.htm. Accessed 30 January 2024.

5 Fielding and Operating Defense AI

Turkey seeks to augment a variety of capabilities with the development of defense AI. The first set of priorities emerged in 2018. According to the AI SAGA call, Turkey prioritizes the improvement of Smart Decision Support (including Command and Control, Risk Assessment and Prioritization, Fast Decision Making, Intelligence, Reconnaissance and Surveillance Systems, Identification of Friend or Foe vehicles and people), Cyber Security, Border Security, Electronic Warfare and Radar, New Generation Guided Systems, and Learning Through War Gaming (Savunma Sanayii Müsteşarlığı 2018: 4).

In addition, OTAĞ reports illustrate how developing defense AI would augment specific national capabilities. For example, Swarm Intelligence reports focus on improving autonomy by leveraging Turkey's recent success in robotic systems (Bülbül et al. 2021). The Radio Frequency OTAĞ report focuses on using defense AI to improve signals processing to enhance Turkey's intelligence-gathering capabilities through distributed sensors and the ability to operate under electronic warfare (İncel et al. 2021: 26).

While these priorities show future intentions and act as future roadmaps, we currently observe that Turkey is taking initial steps that would create the building blocks for future capabilities. Six currently deployed systems show how Turkey is building future capabilities:

- *STM Loitering Munitions*

STM Alpagu and Kargu tactical loitering and attack systems use machine learning algorithms "to optimize target classification, tracking, and attack capabilities without the requirement for a GPS connection" (Kasapoğlu and Kırdemir 2018: 26) and use computer imaging for targeting. These loitering munitions can operate autonomously, but the human operator decides to attack the target.

- *Multi-Dimensional Radio Communication Signal Analysis Platform Project (Kaşif)*

The system is a signals intelligence platform that captures communication signals between 10 MHz and 6 GHz and detects the direction, distance, and movement of the signal source using AI algorithms (TÜBİTAK Bilgem 2021).

- *Defense Industry Capability Inventory (YETEN)*

YETEN aims to facilitate cooperation and technology transfer between different defense companies and improve defense production and procurement management. The system collects data on financials, human resources, products, and production and testing infrastructures of defense companies and organizations. The system provides an overall capability inventory of Turkish defense industries, which will be used to meet TSK demands locally and determine technology areas that need to be improved. Its AI-based suggestion system identifies candidate companies that could produce required parts and components locally with or without a technology transfer. Furthermore, the system helps peacetime defense management and supports

decision-making mechanisms during mobilization and wartime (Savunma Sanayii Başkanlığı 2022c).

- *Data Tagging Platform (Veri Kovani)*

The platform provides fundamental tagged data (video, images, text, voice) that would be used to develop AI-based algorithms in areas such as robotics, autonomous driving, remote sensing, and biomedicine. The platform will act as a qualified data pool, which will help to increase workforce efficiency in AI development while reducing project time (SavunmaSanayiST 2020). The platform uses crowdsourced data tagging and also acts as a central source for disseminating these data clusters (Savunma Sanayii Başkanlığı 2022d).

- *Virtual Forces with Learning Artificial Intelligence Project (FIVE-ML)*

FIVE-ML is an AI-based simulator that will be incorporated into the T-129 ATAK helicopter, ATAKSIM, ANKA, and UMTAS simulators. It will replace rule-based behavior infrastructure with AI-based behavior infrastructure (HAVELSAN 2020).

- *Global Positioning System Independent Autonomous Navigation System Project (Kerkes)*

The Kerkes project is a navigation system that enables UAVs to continue operating when GPS and datalinks are unavailable. The system uses data acquired from platform optic systems and fuses the incoming data to determine the platform's location. It uses image recognition and deep learning to recognize landmarks to determine the platform's position and enable effective navigation (Savunma Sanayii Başkanlığı 2022e). In July 2022, the project was completed and accepted by SSB.

These projects show that Turkey is building its defense AI capabilities from the ground up and it is not limited to uncrewed weapon system development. Another important aspect is that ongoing projects are a source of gaining experience and developing new concepts and doctrines. For example, continuing projects on USVs are tested during military exercises, which help to experiment and understand how autonomous systems could be used and integrated into the existing military structures and crewed systems. Furthermore, Turkey is also experimenting with different payloads for different mission sets. Thus, experimenting before deploying provides valuable information in shaping the future force structure. Most importantly, the use of defense AI is not limited to weapon systems. Turkey also seeks to increase its effectiveness in managing defense industry capabilities through projects such as YETEN. This is vital for developing a sustainable and robust defense AI industrial base and shows that the use of defense AI impacts the overall military structure and defense planning.

6 Training for Defense AI

Training and managing a skilled workforce are essential to building the indigenous AI development capacity that Turkey is looking for. This has two components. First are the human resources that would develop and produce defense AI capability. Second is the training of military personnel that would use defense AI.

6.1 Academic and Workforce Training

In training human resources to develop and produce defense AI, different organizations pursue various programs to improve Turkey's education and increase employment in the AI sector. The Higher Education Council prioritizes AI research under an interdisciplinary 100/2000 Ph.D. project, which aims to increase the employment of research assistants and faculty members in Turkish universities. Since 2018, Turkey has initiated 4 undergraduate, 14 graduate, 1 Ph.D. program(s) in AI, and 24 graduate and 5 Ph.D. programs in big data, robotics and smart systems. Turkey's Open-Source Platform encourages projects focusing on natural language processing through peer learning. To increase employment, the Ministry of Treasury and Finance initiated the "1 million employment" project, which would provide free online training in IT, including AI, and an open CV database for employers (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 2021: 41).

Apart from these initiatives, the following two competitions are important to grow and develop defense AI talents:

- *Teknofest*

Teknofest is an all-inclusive technology competition focusing on high-technology areas deemed necessary for Turkey's defense and civilian sectors. There are a variety of Teknofest competitions, such as smart transportation, helicopter design, mixed swarm robots, fighter UAV, AI in healthcare, AI in transport, and Turkish language processing. Teknofest also has a broad participation base ranging from students (primary school level to graduate level) to private sector professionals. Its wide reach facilitates the development of human resources in high-technology sectors by igniting interest in younger generations, encouraging innovative ideas, and supporting the winners of competitions. For example, winners of the fighter UAV competition will be provided with internship opportunities in Turkey's technology institutions. In other words, these competitions not only work for experimenting with new ideas but also act as a talent pool for Turkey's technology companies. As Vice-Minister of the Ministry of National Defense Muhsin Dere contends, Teknofest will serve as one of the critical sources for the future workforce of Turkish defense industries (Defense Here 2021a).

- *Yenilikçi Yazılımlar Yarışıyor Y3 (Innovative Software Competition)*

Y3, a part of SSB's Defense Industries AI Platform, has a similar goal to Teknofest, though its audience and participants are more limited. Its competitions are open to companies, organizations, and researchers focusing on AI applications to encourage sustainable cooperation between them. Competitions show similarities with SSB's continuing projects and future goals. For example, the UYDU 2019 and 2020 competitions focused on automatic object recognition (such as buildings, ships, helipads, aircraft, bridges, tunnels, and runways) from electro-optic satellite images. GAG 2020 was also an automatic object recognition (person, large vehicles, and automobiles) competition based on large field observation images. The 2022 competitions focus on swarm strategy development with reinforcement learning (SÜRÜ 2022), synthetic data production with generative adversarial networks (GAN 2022),

and route fusion for moving target tracking (GEZİNGECİK 2022) (Savunma Sanayii Başkanlığı 2022f).

6.2 Military Training

Against this broader national background, defense AI is also slowly becoming part of the TSK's training activities. The HAMLE and FIVE-ML projects are the best examples of how AI is integrated into military training. Furthermore, the author expects that number of AI-based training systems in the military's inventory will increase. In line with the goal to accelerate the OODA loop, the increasing integration of data and advanced data-sharing among different platforms would necessitate a new approach to the military decision-making hierarchy. Military decision-makers will have to evaluate the situation from multiple perspectives to succeed in future battlefields (Mevlütoğlu 2014). To prevent data from overwhelming the decision-makers, we expect militaries to use AI-based systems and take some of the cognitive load from the decision-makers.

The increasing use of AI-based systems will require new training approaches especially to prepare military personnel for human-machine interactions, as these constitute a very challenging part of developing and integrating autonomous systems into the overall military systems. For example, it is expected that in future multi-domain operations both autonomous and crewed platforms would interact with each other. While ensuring interaction among platforms might be relatively straightforward, integrating the human elements proves to be more difficult (İnsansız Deniz Sistemlerinin Geleceği ve Türkiye Potansiyeli 2022: 23;26–30;28) because the existing command and control systems are not suitable for managing the integration of machines. The core problem for all states is the lack of concepts and doctrines for human-machine interactions. Turkey is currently experimenting with different concepts on its own and in cooperation with NATO allies. However, as far as the author knows, there isn't any open resource on how these expectations of future warfare, integration of autonomous systems, and defense AI reflect on Turkey's approach to defense AI-specific training in the military. The author expects that the training will evolve as new concepts and doctrines emerge with the further integration of autonomous systems into the military.

7 Conclusion

AI, as Michael C. Horowitz contends, is a general-purpose technology, an enabler, that can operate in several dimensions, such as to direct physical objects to assist in processing and interpreting information and to create new forms of command and control (Horowitz 2018: 39–41). Turkey's approach to defense AI reflects upon the enabling nature of AI. In Turkey, developing defense AI is closely linked to advances in autonomous weapon systems—Turkey's current defense priority.

Recent successes of Turkish drones in contemporary conflicts encourage Turkey to invest in this niche market. Turkey's usage of drones increased the combat effectiveness of the Turkish military as well as the users of Turkish drones. Especially following the Second Nagorno-Karabakh War, international interest in Turkish drones has been on the rise. Thus, the successes in the operational area result in increased exports, which is critical for sustaining the Turkish defense industrial base. Encouraged by operational successes and increased sales, Turkey is now significantly investing in autonomous systems, as reflected in the growing number of projects. In the long run, however, Turkey's ambition to boost its arms exports could be subject to change as defense AI is increasingly integrated into Turkey's autonomous weapon systems.

Turkish arms trade decision-making remains opaque. Turkey strives to advance arms exports to sustain its indigenous defense industrial base. As a part of its export policy, Turkey actively incentivizes its companies to participate in NATO-supported projects as well as committees and working groups of the Conference of National Armaments Directors (CNAD) (Savunma Sanayii Müsteşarlığı 2017a: 8–9). Yet, except for compliance with international agreements, we do not know the clear principles for arms exports. Based on the sale of armed drones, Turkey is willing to sell to any state, except to states that are in direct conflict of interest with Turkey, such as Egypt and Russia. But it is not clear if current arms export logic would also underpin future exports of AI-enhanced autonomous systems or other defense AI products.

While Turkey likely seeks to sustain or even expand current levels of supplying foreign customers with export versions of state-of-the-art weapon systems, NATO countries could emerge as the most likely customers of AI-enhanced systems. Turkish defense industry already follows NATO standards and is aware of the significance of interoperability, which is reflected in the development of new weapon systems and technologies. All the services seek interoperability with each other, between the different assets, and with NATO members.

Regarding concept development on defense AI, it is difficult to say which service is leading as detailed information about service-specific approaches is missing. Based on existing uncrewed systems projects, each service pursues AI-based systems and seeks to integrate these systems. Each service is experimenting with new technologies in cooperation with the defense industry. As these systems enter service, we will have a clearer picture of concept development.

Proper human-machine interaction remains one of the key challenges in developing and fielding AI-enhanced systems. Industry representatives and government reports underline the pressing need to tackle this challenge. Industry, in particular, highlights how difficult it is to integrate autonomous systems into existing structures that rely on existing paradigms of human-human interaction. Moving forward, human-machine interaction would be one of the core issues that needed to be solved through a combination of organizational change and the development of new technologies.

References

Aksan, Sertaç, Özge Güngürmüş, and Resul Daban. 2022. *NATO tatbikatında şov yaptı: Marlin'e tam not*. TRT Haber.

Aselsan. 2022. *Hamle Hareket Tarzı Geliştiren Yapay Zekalı Komutan Asistanı.* Aselsan. https://www.aselsan.com.tr/tr/inovasyon/haber-detay/hamle-hareket-tarzi-gelistiren-yapay-zekali-komutan-asistani-6361. Accessed 30 Jan 2024.

BaykarTech. 2022. *Yapay Zeka.* Baykar Teknoloji. https://baykartech.com/tr/yapay-zeka/ baykartech.com. Accessed 30 Jan 2024.

Bülbül, Ahmet Bahadır, Aytaç Ceylan, Büşra Aparı, Cem Boran Erdoğan, Uğur Güngör, Yücelen Bahadır Yandık, Tolga İmamoğlu, et al. 2021. *Sürü Zekası Odak Teknoloji Ağı Sonuç Raporu. OTAĞ*. Ankara: Savunma Sanayii Başkanlığı.

Cenciotti, David. 2022. *Turkey's First Indigenous Unmanned Fighter Aircraft Carries Out Autonomous Taxi Tests. The Aviationist.* https://theaviationist.com/2022/11/22/kizilelma-unmanned-fighter-aircraft-tests/. Accessed 30 Jan 2024.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. 2021. *Ulusal Yapay Zeka Stratejisi 2021-2025.* Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.

Defense Here. 2021a. *Milli Savunma Bakanı Yardımcısı Muhsin Dere ile röportaj* (2.bölüm: TEKNOFEST). Defense Here.

———. 2021b. *Türkiye'nin yerli ve milli insansız kara araçları hünerlerini sergiledi*. Defense Here.

FNSS. 2022. *Shadow Rider Unmanned Ground Vehicles*. FNSS. https://www.fnss.com.tr/products/shadow-rider-unmanned-ground-vehicles. Accessed 30 Jan 2024.

Gökkoyun, Ceren. 2022. TÜBİTAK BİLGEM ve TÜBİTAK SAGE, NATO tarafından test merkezi olarak seçildi. Anadolu Ajansı, April 8.

HAVELSAN. 2020. *HAVELSAN Yapay Zekâlı Simülatör Geliştirecek*. HAVELSAN.

Horowitz, Michael C. 2018. Artificial intelligence, international competition, and the balance of power. *Texas National Security Review* 1: 37–57. https://doi.org/10.15781/T2639KP49.

İncel, Bilge, Ekmel Özbay, Erdal Saygıner, İrfan Yıldız, Mehmet Ünlü, Mustafa Fatih Akbostancı, Mustafa Özen, et al. 2021. *RF Odak Teknoloji Ağı Sonuç Raporu. OTAĞ*. Ankara: Savunma Sanayii Başkanlığı.

İnsansız Deniz Sistemlerinin Geleceği ve Türkiye Potansiyeli. 2022.

Işık, Yusuf Emir. 2022. *SSB'den yapay zeka çalıştayı*. DefenceTurk.

Jennings, Gareth. 2022. *Turkish 'loyal wingman' conducts taxi and take-off trials ahead of first flight.* Janes. https://www.janes.com/defence-news/news-detail/turkish-loyal-wingman-conducts-taxi-and-take-off-trials-ahead-of-first-flight. Accessed 30 Jan 2024.

Kaplan, Süleyman. 2022. *SSB'de 13 Ar-Ge Projesi için imza töreni yapıldı*. DefenceTurk.

Kasapoğlu, Can. 2022. *Bayraktar Kızılelma yeni bir harekat tasarısının habercisi*. Anadolu Ajansı.

Kasapoğlu, Can, and Barış Kırdemir. 2018. *The rising drone power: Turkey on the eve of its military breakthrough.* EDAM. http://edam.org.tr/wp-content/uploads/2018/06/CAN-the-rising-drone_word.docx.pdf. Accessed 30 Jan 2024.

Kökçü, Ata Ahmet. 2020. *SSB'den 17 yeni Ar-Ge projesi*. DefenceTurk.

Köprülü, Tacettin. 2021. Warriors of the future world: Digital troops. *Havelsan* 3: 6–13.

Mevlütoğlu, Arda. 2014. Sorunlar... Ve Çözüm? *Siyah Gri Beyaz*.

———. 2021. *Türkiye'nin SİHA deneyimi: Devrim mi, dönüşüm mü?* Yetkin Report | Siyaset, Ekonomi Haber-Analiz, Yorum.

Newdick, Thomas. 2022. Turkey's fighter-like drone emerges for taxi tests. *The Drive*. https://www.thedrive.com/the-war-zone/turkeys-fighter-like-drone-emerges-for-taxi-tests. Accessed 30 Jan 2024.

Ozberk, Tayfun. 2022a. Here are the four USV programs Turkiye is working on. *Naval News*. https://www.navalnews.com/naval-news/2022/08/here-are-the-four-usv-programs-turkiye-is-working-on/. Accessed 30 Jan 2024.

———. 2022b. MARLIN USV: Meet Turkiye's latest drone ship. *Naval News*. https://www.navalnews.com/naval-news/2022/09/marlin-usv-meet-turkiyes-latest-drone-ship/. Accessed 30 Jan 2024.

Presidency of Defence Industries. 2019. *Turkish Defence Industry Product Catalogue*. Ankara: MİLDATA Prodüksiyon.
Savunma Haber. 2022. *Siber Güvenlikten Kompozit Teknolojilerine: SSB, 13 Yeni Ar-Ge Projesini Daha Hayata Geçirdi*. Savunma Haber.
Savunma Sanayi. 2020. *Görü Projesiyle Su Üstü Hedefler Yapay Zekayla Tespit Edilecek*. Savunma Sanayi.
Savunma Sanayii Başkanlığı. 2022a. *Odak Teknoloji Ağı (OTAĞ) Süreci*. Ar-Ge ve Teknoloji Yönetim Portalı. https://arge.ssb.gov.tr/TeknolojiYolHaritalari/Sayfalar/OTAGSURECLER.aspx. Accessed 30 Jan 2024.
———. 2022b. *Robotik/Otonom/Sürü Zekası Teknolojileri - Ar-Ge İnfografikler.* Ar-Ge ve Teknoloji Yönetim Portalı. https://arge.ssb.gov.tr/Kurumsal/Documents/POSTER%20-%20Robotik.pdf. Accessed 30 Jan 2024.
———. 2022c. *YETEN*. Yetenek Envanteri. https://yeten.ssb.gov.tr/haberler/savunma-sanayii-2021-degerlendirme-ve-2022-hedefler-toplantisi. Accessed 30 Jan 2024.
———. 2022d. *Veri Kovanı*. Veri Kovanı. https://verikovani.ssb.gov.tr/home.html. Accessed 30 Jan 2024.
———. 2022e. *Alternatif Konum Bulma - Ar-Ge İnfografikler.* https://arge.ssb.gov.tr/Kurumsal/Documents/POSTER%20-%20Alternatif%20Konum%20Bulma.pdf. Accessed 30 Jan 2024.
———. 2022f. *Yenilikçi Yazılımlar Yarışıyor.* Savunma Sanayii Yapay Zekâ Platformu. https://y3.ssyz.org.tr/. Accessed 30 Jan 2024.
———. 2023. *Savunma Sanayii Yapay Zeka Yetenek Kümelenmesi Tanıtım Töreni ve Çalıştayı Gerçekleştirildi.* Savunma Sanayii Başkanlığı.
Savunma Sanayii Başkanlığı and Türkiye Siber Kümelenmesi. 2019. *Siber Güvenlik Teknolojileri OTAĞI Sonuç Raporu. OTAĞ*. Ankara: Savunma Sanayii Başkanlığı.
Savunma Sanayii Müsteşarlığı. 2011. *Türkiye İnsansız Hava Araçları Sistemleri Yol Haritası (2011-2030). Technology Roadmap*. Ankara: Savunma Sanayii Müsteşarlığı.
———. 2015. *İleri Görüntüleme Teknolojileri (TUYGUN) Projesi*. Government. Savunma Sanayii Müsteşarlığı.
———. 2017a. *2017-2021 Uluslararası İşbirliği ve İhracat Stratejik Planı [2017-2021 International Cooperation and Export Strategic Plan]*. Ankara: Savunma Sanayii Müsteşarlığı.
———. 2017b. *Görüntü Analizi Ve Otomatik Hedef Tanıma Sistemi (HASAT) Projesi*. Government. Savunma Sanayii Müsteşarlığı.
———. 2018. *Ar-Ge Geniş Alan Çağırısı Duyurusu: Yapay Zeka Teknolojilerinin Geliştirilmesi*. Savunma Sanayii Müsteşarlığı.
Savunma Sanayii Yapay Zekâ Platformu. 2022. *Yetenekler ve Altyapımız.* Savunma Sanayii Yapay Zekâ Platformu. https://ssyz.org.tr/. Accessed 30 Jan 2024.
SavunmaSanayiST. 2020. *SSB'den yapay zeka için "Veri Kovanı" hamlesi.* SavunmaSanayiST.com. Accessed 30 Jan 2024.
SAYZEK. 2023. *Hakkımızda*. Government. SAYZEK. https://sayzek.org.tr/hakkimizda. Accessed 30 Jan 2024.
SSB. 2023. *2023-2027 Savunma Sanayi Sektörel Strateji Dokümanı [2023-2027 Defense Industy Sector Strategy Document]*. Ankara: Savunma Sanayii Başkanlığı.
STM ThinkTech. 2021a. *Kuvvet Çarpanı Olarak Otonom Sistemler. Odak Toplantısı*. Ankara: STM ThinkTech.
———. 2021b. *Entegre Harekat Ortamında İnsanlı ve İnsansız Sistemlerin Birlikte Kullanılması. Araştırma Raporu*. Ankara: STM ThinkTech.
———. 2022. *Türk Savunma Sanayiinin Adaptasyon ve Dönüşümünde Küresel Oyuncularla Rekabet. Odak Toplantı*. Ankara: STM ThinkTech.
Strateji ve Bütçe Başkanlığı. 2019. *On Birinci Kalkınma Planı (2019-2023)*. Türkiye Cumhuriyeti Cumhurbaşkanlığı.
TRAI. 2023. *TRAI Startup Ecosystem Map*. Türkiye Yapay Zekâ Inisiyatifi.
TÜBİTAK. 2022. *BTY İstatistikleri*. TÜBİTAK. https://www.tubitak.gov.tr/tr/kurumsal/politikalar/icerik-bty-istatistikleri. Accessed 30 Jan 2024.
TÜBİTAK Bilgem. 2021. Çok Boyutlu Telsiz Haberleşme İşaret Analiz Platformu. *Bilgem Teknoloji* 39.

TÜBİTAK SAGE. 2022. *TÜBİTAK SAGE, NATO DIANA Test Merkezi Seçildi.* Savunma Sanayii Araştırma ve Geliştirme Enstitüsü. https://www.sage.tubitak.gov.tr/tr/haber/tubitak-sage-nato-diana-test-merkezi-secildi. Accessed 30 Jan 2024.
Türk tipi İHA Operasyonu: Arda Mevlütoğlu anlatıyor. 2020.
TurkStat. 2023. *Statistics on research and development activities.* Government. TÜİK İstatistik Veri Portalı.
Yanık, Tolga. 2022. *MARLIN SİDA, üstün teknoloji yetenekleriyle sınıfında rakip tanımıyor*. Anadolu Ajansı.
Yapay Zekâ Enstitüsü. 2022a. *Ekosistem Yapısı*. Yapay Zekâ Enstitüsü.
———. 2022b. *Hakkımızda*. Yapay Zekâ Enstitüsü.

High Hopes Amid Hard Realities: Defense AI in Russia

Katarzyna Zysk

Notwithstanding mounting troubles on the battlefield in Ukraine and economic hardships at home, Russia has been pursuing AI and other emerging and disruptive technologies (EDT) with an increasing sense of urgency. Traditionally, advanced technology has been considered in Russia of critical importance for military effectiveness and strategic advantage. From Moscow's perspective, gaining or losing ground in the contest for cutting-edge military technology and more effective weapon systems will have far-reaching consequences for warfare and, thus, for national security, sovereignty, and economy. Hence, AI development appears to have a major impact on Russia's position and corresponding influence in the international system.

Furthermore, Russia's sustained focus on defense AI under Vladimir Putin's leadership has been driven by other key forces working in conjunction: first, the expectation that AI may provide a major military boost to narrow the capability gap with the West; and second, a fear that new vulnerabilities created by AI could be exploited by adversaries to undermine Russia's security, sovereignty, and place in the international hierarchy of power. The war in Ukraine has further increased the country's emphasis on pursuing AI. Public statements by Russian authorities, including President Putin, suggest that one of the lessons Russia has been learning is that AI-enabled weapons systems and infrastructure provide clear battlefield advantages.

This chapter begins with an examination of the Russian understanding of AI and the incentives for engaging in what is seen in Moscow as an international technology race. Subsequently, it examines how the evolving Russian approach to defense AI is reflected in a range of key strategic documents providing the framework for Russia's AI strategy and policy. Next, it analyses how Russia goes about developing defense AI. With its traditional state-driven, top-down innovation model, Russia is

K. Zysk (✉)
Norwegian Institute for Defence Studies, Oslo, Norway

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_16

an outlier among global AI contenders. However, to exploit advances achieved in the civilian sector, Russia has modified its model to partly emulate the US's and China's approaches.

An assessment of Russian funding for defense AI is complicated by its sensitive nature, which is rarely made public, and because AI technology is not a single product but rather a component applied in almost all the Russian military EDT programs. Hence, it comes from different financing sources and cooperation platforms involving other sectors. Still, this chapter examines the general economic trends and selected available figures pertaining to civilian AI funding that shed light on Russia's defense research & development (R&D) environment and the relationship between declared ambitions and economic realities. Finally, this chapter examines major Russian priorities related to fielding and operating defense AI systems. Russia faces numerous systemic problems and practical limitations that this chapter considers before drawing tentative conclusions about the current state and prospects of defense AI in the country. Despite the severe impediments, Russia's government will likely continue to prioritize AI development in selected defense applications to gain a rapid battlefield advantage.

1 Understanding Defense AI and Driving Forces

The focus on AI in Russia has significantly intensified, particularly in the early 2010s. According to the official Russian definition, AI is "technological solutions capable of mimicking human cognition and performing intellectual tasks similarly to, or better than, humans" (Presidential Decree 2019). The Russian military dictionary defines it in greater detail (Military Encyclopedic Dictionary Undated) as a network of cybernetic devices that replaces human intelligence activity; provides the foundation for building an automated control system; and is applied for the search, recognition, and analysis of information, for developing of recommendations and decisions, for automatically creating and issuing commands, and as a tool for analyzing large volumes of data. AI is seen as key to improving decision-making and complex analysis in situations where there is a high degree of uncertainty, inconsistent real-time data, and severe time pressure (Military Encyclopedic Dictionary Undated).

There is, nonetheless, a certain level of confusion about the understating of what AI is. It derives from the varying degrees of autonomy and intelligence found in different systems. Russian discourse distinguishes between automation (avtomatizatsiya), as employed in automated, remotely controlled, and semi-autonomous weapon systems, and "intellectualization" (intellektualizatsiya), which refers to the integration of machine learning and other sub-elements of AI technology (Fink 2021; Nadibaidze 2022a).

Automation and weapons systems capable of operating automatically have existed in Russia since Soviet times and are, therefore, more advanced than Russian systems integrating machine learning and other sub-elements of AI-related

technology (Nadibaidze 2022a). Examples include the P-700 Granit anti-ship cruise missile, introduced in 1983, which featured AI algorithms in an on-board computer (Gazeta.ru 2021); the more precise and complex P-800 Onyx rocket; and the Don-2N radio-electronic facility in Sofrino near Moscow, designed to provide automatic detection of nuclear warheads, transmission of information to anti-missile system launchers, and offering options for action (Poroskov 2022). In contrast, the process of "intellectualization" involves critical elements of adaptability, self-learning, self-improvement, and self-programming as well as "the ability to make decisions in various and rapidly changing situations, similar to a person" (Fink 2021).

Seen from Moscow, advances in AI development may propel weapon systems towards further autonomy, ultimately replacing humans on the battlefield (Military Encyclopedic Dictionary Undated). However, the Russian government's approach to full autonomy and to weapons and target selection without human intervention appear ambiguous. In its 2019 national AI strategy (Presidential Decree 2019), Russia highlighted the importance of developing ethical norms to govern the interaction between humans and AI. Russia recognizes the dangers in using lethal autonomous weapon systems (LAWS) and emphasizes the need for humans to stay in control. The official stance is that the loss of meaningful human control of LAWS is unacceptable. The responsibility for the use of LAWS and for any unintended consequences rests with the operator of the robotic system or programming (Belousov 2022).

However, Russia simultaneously argues that developing the criteria to define meaningful human control will be difficult without politicizing the issue. Moreover, the Russian government has systematically avoided agreeing to legally binding international instruments that would prohibit the use and development of LAWS (Hoffberger-Pippan et al. 2022; GGE 2019; Nadibaidze 2022b). One notable reason is that restrictions could hamper Russia in the global AI race (Presidential Decree 2019). In July 2022, Russia's official representation to the UN argued that LAWS also confer several benefits. Such systems, it said, do not suffer from human weaknesses, including moral and religious attitudes or feelings of revenge, panic, exasperation, prejudice, and fear. Moreover, highly automated technologies can increase strike accuracy and thus reduce harm to civilians and civilian facilities (Belousov 2022).

While the latter argument may sound hollow given the systematic Russian targeting of civilians in Ukraine, the Russian authorities seem certain about the advantages of LAWS. Two years after the 2019 national AI strategy highlighted the importance of ethical norms to govern human-AI interaction (Presidential Decree 2019), Russia approved a national code of AI ethics. It is important to note, however, that it does not carry the weight of law as these are only recommendations. Moreover, it is designed for civilian AI systems and non-military purposes only (Novyi 2021). Indeed, defense AI development under the current Russian regime is unlikely to be significantly constrained by ethical considerations.

Two key forces have driven Russia's pursuit of defense AI: the expectation of a major military boost and the fear of new vulnerabilities AI may create.

On the one hand, the Russian authorities expect AI can help them to narrow, if not close, the capability gap with the West that has grown larger because of extensive losses suffered in the period since Russia's reinvasion of Ukraine in February 2022. Indeed, AI-enabled weapons systems and other EDTs promise to accelerate Russia's military build-up and modernization in a non-linear manner, providing a military edge, if not superiority, in selected areas.

On the other hand, the Russian decision-makers are concerned about new vulnerabilities and security threats that AI can create, and that Russia's adversaries can exploit. Some Russian officials worry that AI could help enemies win a conflict even before it officially erupts (Cheberko 2018). AI technologies are expected to have the potential to change the character of warfare and the dynamics of crisis escalation in ways that could undermine strategic balance and pose an existential threat to Russia (Sergeantov et al. 2022). Engaging in the AI race therefore appears not to be a matter of choice, but of necessity.

The Russian authorities argue that competing with the US and NATO symmetrically would take a long time due to limited Russian resources. Breakthrough technologies by contrast are seen as force enablers and multipliers that can give Russia an advantage relatively quickly (Zysk 2020). In 2021, Putin argued that AI could provide a qualitative leap to Russian weapons systems, including hypersonics, while enhancing other key capabilities such as lasers and robotics (Ria Novosti 2021; Vzglyad 2020).

The experiences Russia has gained by reinvading and occupying parts of Ukraine have added a sense of urgency to its development of a range of AI capacities, including command, control, communications and high-speed decision-making at all levels; high-precision weapons and nuclear weapons; unmanned systems for surveillance, reconnaissance, situational awareness, search and rescue, target acquisition and strike; air defenses, early warning, electronic warfare and space-based systems; logistics and manufacture; and offensive cyber and influence operations to shape the psychological domain.[1]

2 Developing Defense AI

A series of strategic documents, concepts, and policy papers since the early 2010s testify to Russia's rising interest in pushing AI forward. Many of the documents remain classified and this chapter does not aim to provide an exhaustive list. The examples below, however, shed light on the focus areas and extent of Russian AI development.

Key documents include the "Concept of development and combat use of robotic complexes for the period until 2025" (Newsru.com 2014) and the "Concept of the

[1] The Russian AI development priorities are explored in more detail below, in the Sect. 5—"Fielding and Operating Defense AI."

use of robotic systems for military purposes for the period 2030" (MoD 2014), both adopted in 2014. In 2016, Russia developed the "Strategy for scientific-technological development of the Russian Federation" (Presidential Decree 2016), which defines the "transition to advanced digital, intelligent production technologies, robotic systems, new materials and design methods, the creation of systems for big data processing, machine learning and artificial intelligence" as a priority.

Russian defense AI development has been closely connected to national economic development, as expressed in a batch of strategic policy documents released in 2018. In a follow-up, Russia created a series of national projects, such as the Digital Economy, which includes a development program for the 2021–2024 period called Artificial Intelligence (Markotkin and Chernenko 2020). To accelerate Russia's development, innovation and investment climate, the focus has been on removing regulatory obstacles in public administration, healthcare, transport, medicine, education, construction communications, agriculture, fuel and energy and other fields (Markotkin and Chernenko 2020). In addition, Russia launched the federal Digital Technologies project, which focuses more broadly on advanced technologies such as robotics, quantum computing, virtual reality, blockchain, wireless communications and others (Petrella et al. 2021). The growing interest of the Russian authorities in AI has also been expressed in the form of conferences hosted by the Ministry of Defense (MoD) to facilitate contact between stakeholders across sectors (MoD 2018a; Voennoe Obozrenie 2018).

In connection with a Russian government order issued to state-owned companies to draft a variety of "roadmaps" for developing key technologies (including quantum computing and 5G implementation), Sberbank's German Gref led work on the AI roadmap (MoD 2018a). Completed in October 2019, it identifies sub-technologies and transitional timing between stages of research, development, and commercialization. It also provides examples of target use cases and points out major obstacles and measures to overcome them (Ministry of Digital Development 2019).

Sberbank was also instrumental in preparing the draft of Russia's first official AI strategy, which was finalized and signed by Putin in October 2019. This "National Strategy for the Development of Artificial Intelligence for the period until 2030" defines strategic goals in investment, R&D, infrastructure, educational and training programs, legal frameworks, and recruitment of talent to the military and security services. It also calls for streamlining actions to advance AI development across various sectors (Presidential Decree 2019).

One of the strategy's main objectives is to significantly improve AI development in Russia by 2024 and to catch up with competitors in the field. While the document recognizes that Russia lags behind the AI front-runners, the United States and China, it argues that Russia could become a global leader in AI development and utilization (Presidential Decree 2019; Petrella et al. 2021). The strategy aims to increase the number of state and private entities engaged in technological innovation by 50% and to create high-performance export-oriented industries equipped with advanced technologies, primarily in manufacturing and agriculture (Markotkin and Chernenko 2020).

During the high-level Artificial Intelligence Journey Conference in Moscow in November 2022, President Putin noted several measures the Russian authorities plan to take to accelerate AI development. These included the development of new federal industrial robotics projects; the establishment of an AI development maturity index to evaluate practical results of AI implementation by Russian industries; and the development of sovereign cloud technologies. The ambition, he added (Putin 2022a), is to introduce AI technologies into every national development project and every state program as well as into the investment programs of Russian companies.

In July 2022, Russia adopted a concept for the development and use of weapons systems using AI though the document appears to be classified (Russiaun.ru 2022). In December 2022, to further accelerate AI development and large-scale implementation, the Ministry of Economic Development approved a roadmap titled "Development of the high-tech direction Artificial Intelligence for the period up to 2030." To help implement this roadmap, Deputy Prime Minister Dmitry Chernyshenko signed an agreement on 16 January 2023 with 30 parties, including Sberbank, RDIF, and the Skolkovo Foundation (Kommersant 2023). Russian businesses that buy and deploy Russian-made solutions, including AI-enabled systems, were to be offered tax incentives and additional direct funding for upgrades starting in January 2023 (Putin 2022a).

An additional program to support the development of domestic import substitutes was launched in response to Western sanctions. Initial sanctions imposed after the Russian annexation of Crimea in 2014 led Russia to find some components in China (Gressel 2020). The more extensive sanctions that followed Russia's reinvasion of Ukraine, together with a massive withdrawal of Western companies, have made the situation more precarious. While Russia is searching for technology partnerships in various parts of the world, including among ASEAN members, the Sino-Russian technology collaboration remains one of the largest and most promising for the Kremlin in the face of the restrictions. AI-related research collaboration between China and Russia has systematically expanded since 2016 and includes robotics, biotech, telecommunications, cyberspace, machine tools, and microelectronics (Petrella et al. 2021), as well as uses of outer space. In 2020, a 2-year initiative for scientific, technical, and innovation cooperation brought the two countries even closer (Konaev et al. 2021; Lee 2022; Bendett and Kania 2019).

3 Organizing Defense AI

As a part of the large-scale modernization program launched in 2008, Russia has gradually expanded its AI R&D ecosystem. While dominated by the traditional top-down approach that relies on state leadership and funding, it has also increasingly involved the civilian sector with the objective is to generate synergies and accelerate development by increasing the state's access to resources, talent, and experience (Zysk 2020). Simultaneously, in line with a long-standing argument peddled by

Putin (Putin 2012, 2013), the expectation is that defense innovation will stimulate the whole economy. Andrei Morozov, the Deputy Head for Scientific and Educational Activities at the Military Technopolis ERA, has similarly emphasized the dual-use nature of advanced military technology (Zakvasin 2019). The Head of the Department for the Development of Artificial Intelligence Technologies in the Russian Ministry of Defense, Vasilii Yelistratov, argued that while the MoD adapts civilian technologies for the army, the army also provides transfer in the opposite direction. This is increasingly important in the face of sanctions depriving Russia of solutions it once obtained from the West (Rosinform.ru 2022).

Over the years, the Russian authorities have created a large number and variety of cooperation platforms between the military and security services on the one hand and academic, industrial, commercial, and other private actors on the other. According to the state-owned Zvezda media group (Poroskov 2022), which is run by the Russian MoD, in 2022, more than 150 domestic industrial enterprises and research and educational organizations participated in joint military-civilian networks and collaborative platforms working on AI for weapons systems and combat operations. Overall, the MoD in cooperation with the Russian Academy of Sciences, financial institutions, leading research centers and universities has created and operates an R&D ecosystem that interacts with more than 1200 entities from 25 regions (MoD Undated-a).

Among the key Russian institutions with AI as an R&D priority are those known as "radical innovation centers," "technopolises," or "technoparks." Their main objective is to join theory and practice by assembling scientists and experts who normally would not cross paths to accelerate progress from invention to full implementation (Zysk 2021).

The Advanced Research Foundation (Fond perspektivnykh issledovanii—FPI), created in 2012, focuses on developing new and potentially disruptive dual-use technologies, such as unmanned vehicles, including the Marker unmanned ground vehicle (UGV) and the Udar unmanned tank; autonomous systems and automated decision-making systems; superconductors (Liman); additive technology for polymetallic products (Matritsa); autonomous deep-submergence vehicles (Vityaz'-D); and ultra-thin materials (Tavolga) for improving camouflage and protection (Advanced Research Foundation Undated).

One of the most prominent Russian military AI R&D centers is the ERA Technopolis, which was inaugurated in 2018 to create EDTs to serve the Russian armed forces. In September 2019, a dedicated AI laboratory was established at ERA (Sosnitskii 2022). As Morozov has put it, AI cuts across almost all of ERA's R&D activities, thus its development is seen as more of a means than an end (Zakvasin 2019).

ERA's prioritized R&D fields have expanded over the years to include robotics, information security, small spacecraft, energy efficiency, pattern recognition, nanotechnology, nanomaterials, information and telecommunications systems, information technology and computer science, hydrometeorological and geophysical support, hydroacoustic object detection systems, geographic information platforms for military use, radiolocation and targeting for high-precision weapons, automated control & IT and "weapons based on new physical principles," i.e. directed energy,

radiological, genetic and electromagnetic weapons (MoD 2021b, MoD Undated-b; Zysk 2022).

There are three activity clusters at ERA: research, education, and production. Production is represented by the Kulibin Research and Production Centre and the Lomonosov Microelectronics Design Centre. Kulibin conducts experimental and small-scale accelerated production of prototypes of weapons and other military and special equipment from design samples created at ERA and by its partners. Focal points include metal processing, battery testing and development, and small spacecraft. The mini-factory has special workshops that can utilize 3D printing of plastics, photopolymer, metal, and ceramics as well as carbon processing (MoD 2021b, MoD Undated-b; Zakvasin 2019; Zysk 2022).

ERA has an extensive network of civilian partners, including engineering centers, financial development institutions and leading Russian universities and research institutes such as the renowned Kurchatov Institute and Rosatom's research and production complex Dedal (Voennoe Obozrenie 2018; Zysk 2021). The Russian MoD also operates several other scientific and testing centers focused on AI, autonomy, and robotics to serve the needs of the armed forces and defense industry. These include the Main Research and Development Centre for Testing Robotics (Patriot-export.ru 2017; MoD 2018b) and the 46th Central Research Institute (MoD Undated-c). AI R&D is also taking place in laboratories of the Russian military-industrial complex focused on weapon systems, smart munitions, unmanned vehicles and systems, radio communications systems, machine learning of deep neural networks, VR technologies, facial recognition, big data, and others. Rostec State Corp. and many of its subsidiaries (e.g. Kalashnikov, Kamaz and Ruselectronics Holding) are among the most prominent actors (Rostec State Corp. 2019; Poroskov 2022).

Russia's extensive R&D innovation infrastructure is coordinated by the MoD's Main Directorate of Innovative Development (GUIR), which was created in February 2013 (MoD Undated-d, 2021a). Its objectives are to organize development, support scientific, technical and innovation programs and foster conditions favorable to the creation of advanced weapons and other military and special equipment. GUIR also monitors new technologies, both in Russia and abroad, not least those that could pose a threat to national security (MoD Undated-e). To further strengthen the Ministry of Defense's role in the practical application of AI, a special department dedicated to the development of AI technologies was created in 2021 (Tass 2022b). The head of the department, Vasilii Yelistratov, highlighted the need for a database of relevant AI technologies to be assessed for potential recommendation onward to the defense sector (Tass 2023). Projects that pass the assessment are to be tested at ERA (Kashemirov 2020).

Commercial companies also play an important role in supporting AI development. Under the leadership of Gref and Sberbank, several of them that excel at AI development in their respective fields (VKontakte, Yandex, Mail.ru Group, MTS, Gazprom Neft and the Russian Direct Investment Fund) formed the AI Russia Alliance in November 2019. Their stated objective is to "facilitate and accelerate the

development of AI in Russia for education, research and practical applications, and to foster a competitive market for AI solutions" (AI Alliance Russia Undated).

Furthermore, the Russian AI R&D infrastructure also extends to various academic institutions that have created AI centers and laboratories, such as the Neural Networks and Deep Learning Lab at the Moscow Institute of Physics and Technology, the Higher School of Economics, the Ivannikov Institute for System Programming of the Russian Academy of Sciences, the Skolkovo Institute of Science and Technology, Zhukovskii Institute, the iPavlov Conversational Intelligence and Dialogue Agents project, the National Centre for Cognitive Technologies at the Information Technologies, Mechanics and Optics University in Saint Petersburg, the National Research Nuclear University and the ITMO University (iPavlov Undated; CTII Undated; Ministry of Science and Higher Education 2019; Agit Polk 2018).

To improve implementation of the national AI strategy and activities under the federal project titled Artificial Intelligence (part of the national Digital Economy program), Russia created in September 2022 the government-affiliated National Center for the Development of Artificial Intelligence with nearly 9500 organizations from 15 sectors of the economy (Cnews.ru 2022). Its objective is to provide expert support and coordination for AI implementation, monitor key indicators of AI development, provide a platform for selecting prospective AI solutions for business, science, and government, and assist in implementing important infrastructure programs (NCRII Undated; Interfax 2022; Poroskov 2022).

4 Funding Defense AI

The Russian spending on defense AI is not publicly available. In addition, AI technology underlies most of the country's military EDT programs, which further complicates the estimates of AI funding (Zysk 2020). The diversity of cooperative platforms involving AI R&D outside of the defense sector adds to the complexity (Zakvasin 2019). General economic and financial trends, as well as figures available for the civilian AI sector may, nonetheless, shed some light on financial conditions in the Russian defense AI R&D environment.

The AI development is predominantly funded by the state. Having the support of the top political and military leadership has been a key to overriding the traditional institutional conservatism that pervades Russia's military organization, increase its responsiveness to policy change and open to innovation. Yet relying on preferential and centrally controlled state funding has also constrained competition, risk-taking and incentives for innovation. The projects to be pursued and funded are more likely to be chosen based on political criteria than true competitive merit (Zysk 2015). Bureaucratic red tape, widespread corruption and limited intellectual property rights are additional factors stifling innovation. R&D funding has also come under pressure due to an increasingly constrained economic environment, including periods of stagnation and low-level recession since 2014.

For instance, the budget of the Advanced Research Foundation (FPI) in 2013 was RUB3.8bn (about €90M). In 2014, it was reduced to RUB3.3bn (about €80M). The budget was then supposed to increase to RUB4.5bn annually (about €110M) for 2015–2016, yet instead it was reduced by 10%. Moreover, instead of remaining at about that level as intended in 2017–2018, it decreased from RUB3.8bn to RUB3.4bn. Ambitions to boost FPI spending significantly in the following years again came up short (Ria Novosti 2016; Nikol'skii and Bocharova 2018). Russian EDT investments amount to only a fraction of the billions of dollars invested by the United States and China (OECD Undated). For comparison, in 2022, the United States allocated about USD3.8bn (about €3.57bn) to its Defense Advanced Research Projects Agency (Zysk 2021).

In addition, the COVID-19 pandemic and Western sanctions have had a significant negative impact on Russian AI funding. In August 2020, Russian media reported (Cnews.ru 2020b) that the budget for the federal AI project to support implementation of the national AI strategy was slashed from RUB124.8bn for a 4-year period (about €1.78bn) to RUB27.7bn (about €400M). In April 2020, the Russian Ministry of Finance sought to block the budget of the national Digital Economy program (of which the AI project is a part) to redistribute funds to the reserve fund. The 2020 budgets of several other ministries and departments also declined. The Ministry of Communications, headed at that time by Konstantin Noskov, was unable to spend more than RUB26bn (about €370M) in budget funds on Digital Economy, according to Russian media. It is not clear why, but the department used only 73.3% of the budget allocated for the program in 2019 (Cnews.ru 2020a, b).

The 2019 AI roadmap's assessment was that Russia would need to allocate RUB56.8bn (about €799M) for AI development over a 4-year period through 2024. However, the updated AI roadmap published in December 2022 called for only about RUB24.6bn (about €346M) through 2030, i.e., a 7-year period. The volume of expected extra-budgetary financing decreased even more dramatically: from RUB334bn (about €4.69bn) through 2024 to RUB111bn (about €1.73bn) through 2030. Similarly drastic reductions are seen in the expected volume of the domestic market for AI-based technology: while the 2019 AI roadmap had projected RUB160bn (about €2.25bn) by 2024, the figure given in 2022 was less than 10% of that: RUB14bn (about €218M) (Kommersant 2023).

While lobbying in Western capitals to end the sanctions imposed in 2014, Russian officials often claimed that the sanctions provided an excellent opportunity to strengthen Russia's independence by creating domestic technological solutions (Kommersant 2022b, 2023). Likewise, in January 2023, the Ministry of Digital Development argued that the sanctions imposed in 2022 did not complicate the AI work of Russian companies, because most algorithms were public open-source projects available for download and modification. Still, the Ministry acknowledged that some developers experienced difficulties: their accounts were blocked, and there was an "ambiguous" attitude towards Russians programmers in various specialized communities. Most of those carrying out federal AI development projects in Russia are under sanctions and likely to encounter difficulties accessing

sophisticated technology. Access to microprocessors in particular is a matter of concern (Zysk 2022). Another example is the decision of Nvidia to suspend sales in Russia, thus restricting access to graphics processing units used to power a host of AI products (Kommersant 2023).

To some degree, Russia has been able to evade sanctions and exploit loopholes in the exports control regime. For instance, the country has managed not only to continue but to double missile and tank production when compared to the pre-February 2022 figures (Barnes et al. 2023). Another illustration is the launching of a new supercomputer by Moscow State University in August 2023 (MSU 2023). It is to be used for training large AI models and a variety of AI and high-performance computing applications.

Yet there is no doubt about the detrimental effects of the war in Ukraine on Russia's defense innovation environment. This includes the sharp decline in competition faced by domestic technology companies due to the departure of Western corporations and the withdrawal of their investments. In Gref's assessment (Myl'nikov 2022), this exodus from the Russian market will cause losses to the national economy over the long run because "no Russian companies will be able to maintain the level of competition"—and—"where there is no competition, there is no innovation."

5 Fielding and Operating Defense AI

Russia has been pursuing a wide range of programs to leverage AI technologies in the armed forces and security services. According to official sources, as of September 2022 the MoD's Main Directorate of Innovative Development had accompanied over 500 projects for subsequent implementation, 222 of which were planned for completion and implementation in 2022 (Poroskov 2022).

Russia has been seeking to integrate AI into a range of key applications, including command, control, communications, and decision-making; unmanned vehicles for missions such as surveillance, reconnaissance, situational awareness, search and rescue, target acquisition and attack; nuclear, high-precision and other weapons systems; air defense, early warning, electronic warfare, and space-based systems; training, logistics, and manufacturing; and cyber operations and influence operations to shape the psychological domain.

The development of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) has long been defined as critical to gaining and maintaining information superiority (Sukhankin 2019a). The ability to selectively collect large amounts of data from the various domains and to analyze it and make rapid decisions, especially under time pressure, is seen as increasingly important to outperform the adversary in contemporary warfare. Russia's top political and military leaders, including President Putin and Defense Minister Sergei Shoigu, have regularly highlighted the crucial value of rapid decision-making and of improving command and control (C2), communications

and transmission systems (Ria Novosti 2021; Vzglyad 2020; Tass 2023; McDermott 2020b). The National Defense Management Center, established in 2014, that provides the main joint all-domain C2 structure, reportedly applies AI to support information collection, selection, analysis, and decision-making (Regnum.ru 2020; Edmonds et al. 2021). There are other examples of the Russian pursuit of the use of AI with large data sets to integrate C4ISR capabilities, such as in the ISBU command and control system (informatsionnaya sistema boevogo upravleniya), reportedly tested for the first time during the Tsentr-2019 strategic exercise (Markotkin and Chernenko 2020). It is to be designed to propose alternative courses of action based on its assessments of the situation on the ground. To speed decision-making, Russia is working to apply elements of AI in control, reconnaissance, navigation, and situational analysis technology (Sergeantov et al. 2022).

Among top Russian priorities for defense AI applications—defined as an "urgent task" (Putin 2022b)—are unmanned vehicles (UVs). Programs have gradually expanded to include more than 100 types of UVs at different stages of R&D, testing and implementation (Ria Novosti 2021; Vzglyad 2020; Tass 2023). Among conclusions Putin has drawn from the battlefield in Ukraine to date is that the most effective weapons systems are those that operate at high speed and almost automatically. He stressed the necessity of creating a wide range of AI-enabled UVs for missions such as reconnaissance, target acquisition and strike, and of being able to deploy the vehicles in various ways, including swarming and networked reconnaissance (Putin 2022b).

The Russian MoD sees the development of AI-enabled unmanned vehicles for air, ground, and sea-based missions as an important element of C4ISR. The focus is on expanding the speed, range, endurance, and scope of missions for the armed forces and other services, such as the Federal Security Service (FSB) border guard. Missions include surveillance and reconnaissance as well as air, ground, and underwater attack roles, including by kamikaze drones. ZALA Aero Group (a subsidiary of Kalashnikov) claims its KUB-LA kamikaze drone can use AI to select and engage targets. Likewise, the Lancet-3 loitering munitions used in Ukraine, are to be highly autonomous, including the ability to locate and destroy a target without human guidance and return to the operator if a target is not found (Hambling 2022a). Russia has also shown interest in counter drones AI technology, bomb identification and de-mining, anti-submarine warfare, deep-water missions involving hydroacoustics, air-defense detection, electronic warfare (EW) and situational awareness. Various developers are also working on drones for search and rescue, transportation, and logistics (Edmonds et al. 2021; McDermott 2020a, 2022; Palavenis 2022).

Russia also pursues autonomy to strengthen the credibility of its nuclear forces. Here the attention is on increasing the speed of assessment and decision-making, as well as force protection and penetration of missile defenses. This is illustrated by Putin's "wonder weapons", i.e., the Poseidon nuclear-powered and nuclear-capable unmanned underwater vehicle (UUV); the Burevestnik nuclear-powered and nuclear-capable cruise missile; and hypersonic weapons such as the Avangard boost-glide vehicle. AI and autonomy elements are also to be applied in the

guidance systems of the Sarmat intercontinental ballistic missile and the Kinzhal air-launched ballistic missile.

Russia has also shown an interest in AI applications in the Aerospace Forces. A major objective is to disrupt or degrade communications, critical infrastructure, satellites, and other networks that the US and NATO depend on (Work and Grant 2019). For instance, the RB109-A Bylina system aims to collect large amounts of data and uses AI to prioritize and jam electronic signals. AI has also been tested for application in aircraft such as the MiG-35, the SU-35, and possibly the SU-57 to enhance their operations, including on-board information management and target recognition (Palavenis 2022; Tass 2021). Russia is reportedly studying AI-equipped autopilot systems, including in connection with domestic helicopters (Poroskov 2022). Furthermore, in focus are weapons based on "new physical principles," such as electromagnetic, radiological, geophysical, and directed-energy weapons for missions such as countering unmanned aerial vehicles (UAVs) and satellites (Rossiiskaya Gazeta 2018). Scientists are also pursuing AI enhancement of air defense, such as the Pantsir-S (Tass 2022a).

Notably, various Russian weapons systems are to be upgraded with elements of AI, including high-precision weapons, the T-14 Armata tank (Izvestiya 2021); or the Uran-9 tracked UGV vehicle and the Nerekhta reconnaissance UGV that are to be introduced as a part of the Russian ground forces to carry out "experimental military service" (Cranny-Evans 2021). AI is also a component in combat robots, for instance, a fighting vehicle based on the BMP-3 infantry vehicle and Sinitsa remote-controlled combat module (Argumenty i Fakty 2022). Russia is working as well on AI projects to improve control of artillery targeting and on new-generation infantry combat systems such as the Ratnik, whose advanced elements include software linked to small UAVs and other AI-enabled systems (Sukhankin 2019b).

AI is also seen as a critical capability in offensive cyber operations, as well as cybersecurity and cryptography. The objective is to strengthen Russian information security and leverage AI on a broader scale to enhance cyber capabilities. The list of known Russian offensive cyber operations is extensive (CISA Undated; Hakala and Melnychuk 2021), including in Ukraine. Despite initial claims that Russia failed to launch cyberattacks during its invasion, research findings indicate that they have figured prominently alongside the invasion. Only in the first 5 weeks of the war, Russia conducted an intensive campaign in the cyber domain, with some 800 attacks against Ukrainian targets. The impact of Russian cyber operations has been minimized through a combination of Ukrainian preparedness and support provided by the U.S. Cyber National Mission Force, which arrived before the invasion, together with the international cooperative cyber defense task force (Corera 2022).

Furthermore, AI-enabled systems figure prominently as a tool for creating new opportunities and augment traditional methods of influence, including in disinformation, demoralization, and propaganda both abroad and domestically. One example is ERA's project (Zakvasin 2019): a search and rescue drone with an onboard AI-enabled system capable of analyzing situations and recognizing persons that "pose a threat to society," such as "terrorists." Technologies such as facial and pattern recognition enhance information collection, assessment, and prediction to more

effectively influence a population's behavior. Notably, the 2022 AI roadmap published by the Ministry of Digital Development requires the regions to collect large, anonymized data sets for the purpose of training AI systems (Kommersant 2022a).

It is important to note that AI applications are also being explored to heighten productivity in the defense industry. Some production lines reportedly feature applications capable of recognizing details, tools, and human action. The objective is to reduce the role of the human factor in manual operations in the production of weapons and military equipment, such as the production of rocket engines (Poroskov 2022). The Russian United Aircraft Corporation plans to use an AI-based digital system to automatically quality-control aircraft parts for MiG fighter jets (Poroskov 2022). Likewise, state-owned Rostec has been testing the Zyfra Industrial Internet of Things Platform, which uses AI to track the engine manufacturing process and conduct simulated testing in a virtual environment. The objective is to reduce the number of tests, improve quality, and accelerate production (McDermott 2020a).

6 Training for Defense AI

The Russian authorities argue (Presidential Decree 2019) that the country's strong intellectual traditions and high level of education in science, technology, engineering, and mathematics (STEM) will help it join the club of global AI leaders. In reality, while Russia was ranked fourth in the OECD's 2019 global index of education, less than 1% of Russia's graduates earned an IT, communications, or other technology-based degree. The Lomonosov Moscow State University—considered Russia's highest-ranked computer science research institution—was listed 43rd globally in 2017, 60th in 2018, and 78th in 2019 (Dear 2019). Overall, Russia ranked 47th in the 2022 Global Innovation Index (GII 2022).

The 2019 national AI strategy highlighted the importance of education and training in AI (Dear 2019). To improve the pool of specialists in new technologies, Russia tests various strategies to train and retain a new generation of specialists. AI centers offering professional education have been established at the top Russian universities and research institutes. Many offer participation in real development projects by corporate partners, such as Gazprom Neft, MTS, Sberbank, Russian Railways, and others (Ministry of Science and Higher Education 2019; MoD 2018a). A partnership agreement was signed by FPI and the Ministry of Science and Higher Education to facilitate the creation of new scientific schools and centers of expertise focused on EDTs (Tass 2019).

The Russian authorities organize a variety of events that aim to attract university students and even schoolchildren. More than 3000 students enrolled in AI master's programs in 2022. Medical doctors, teachers, and lawyers as well as employees in manufacturing, communications and transport can take a special AI educational module to improve their qualifications. In November 2022, to ensure training quality, President Putin ordered the ranking of universities in the AI field. He also highlighted (Putin 2022a) the need to introduce elements of AI into mathematics and

computer science curricula. In October 2022, more than 19,000 schoolteachers from different regions of Russia took part in an online AI course (Ria Novosti 2022). The Ministry of Defense also organizes high-level conferences devoted to setting the AI agenda and develops AI training programs in a wargame style with tactical, operational, and strategic levels to illustrate the effect of AI on warfare and stimulate further development (MoD 2018a). Still, the Russian war in Ukraine has exacerbated long-standing problems with shortages of professional expertise. An exodus of qualified scientific personnel, including IT specialists, accelerated after Russia announced a mobilization of reservists in September 2022 (Kommersant 2023; Metz and Satariano 2022; Washington Post 2022).

Known measures to recruit and retain talent in the armed forces include the creation of "military scientific units" (nauchnye roty). Staffed by conscripts, these units have developed since 2013 on the foundation of Russian military research and higher educational institutions (MoD 2016). The MoD has gradually been transferring the units to ERA (MoD 2016), and in 2022 eight of them[2] were operating there in various R&D priority fields (MoD Undated-f; Zysk 2021), and supporting needs of several units such as the Aerospace Forces and the 12th Main Directorate. The expectation is that conscripts in these units will continue military-scientific careers working at ERA when their service period ends, either as civilian specialists or with the rank of lieutenant.

To address the problem of brain drain, the Russian authorities also resort to decrees and resolutions as well as the introduction of certain privileges and incentivized funding for academic and scientific institutions, state support for the purchase of domestic replacements of foreign technology, labor market incentives, and streamlining of procedures to employ foreigners (CNA 2022). However, with the deteriorating socioeconomic situation and increasingly repressive authoritarian rule, it is unlikely that bureaucratic measures will be sufficient to make a significant difference.

7 Conclusion

The overall development of Russian defense AI appears to be in the early stages of maturity. The primary focus is on incremental evolution: upgrading legacy systems—nuclear, strategic non-nuclear, and non-military methods and means of warfare—with new technologies. AI is being tested and used in data analysis and decision support, loitering munitions, electronic warfare, communications analysis, cyber warfare and information confrontation, to name but a few applications. Simultaneously, Russia is experimenting with "risky projects", i.e., novel systems, materials and approaches to warfare that could potentially yield significant battlefield advantage—if not superiority—in selected areas.

[2] The plan had been to transfer 20 scientific units by 2020 (Zakvasin 2019).

Still, the high-tech development in Russia has been undermined by extended periods of economic stagnation and recession, aggravated by the COVID-19 pandemic, sanctions and a massive outflow of international corporations halted cooperation. The poor investment climate is further undermined by long-standing unfavourable demographic trends and weak educational foundations. The full impact is yet to come, but dramatic spending cuts on AI in the civilian sector have already occurred. Beyond funding, several other factors will influence the future of Russian AI. One is the extent of Russia's ability to continue circumventing sanctions and moderating its dependence on Western technology. While Russia is reluctant to create new dependencies that can turn into a source of vulnerability, the Kremlin has little choice but to supplement AI development efforts with foreign technology, including drones purchased from Iran and electronics and various other dual-use technologies from China (Kuo 2022; Lo 2023). The pervasive structural problems plaguing Russia's defense sector and the political and economic system at large are an additional factor hobbling AI development and innovation. Systemic reforms will be required to buoy the competitive research environment but are unlikely under the current regime.

All the same, Russia's 2024 state budget clearly demonstrates that the Kremlin is willing to prioritize the defense sector. Despite the deteriorating national economic environment, Russia plans to increase defense spending by 25% in the 2024–2026 period (AP 2023; Wiśniewska 2022). Extensive failures during the Russia's full-scale 2022 invasion of Ukraine have prompted a major reassessment and reforms in the Russian armed forces. How much attention will be paid to R&D in that reckoning remains to be seen. To date, the combination of optimism about significant advantages AI and fear of strengths it can provide adversaries is likely to keep Russia's attention on selected AI applications, not least given Putin's personal interest in this development. Indeed, the experiences from Ukraine have encouraged Russia to double down on its AI commitment. Because Russia's constrained socio-economic and industrial circumstances make a swift military build-up in linear fashion harder, AI development in selected areas may be the best hope to rapidly gain advantage.

To take full advantage of AI, Russia must not only harness the technology but also adapt doctrines, concepts, force structures, and recruitment patterns accordingly. The conflict in Ukraine has exposed a high degree of institutional conservatism in the Russian military. There are, nonetheless, clear patterns of Russia's ability to learn and adapt, however slow in the initial phase of the war (Konaev and Daniels 2023). The extent to which Russia's leadership will be able to draw the right conclusions and increase the military organization's ability to change amid an ongoing war is yet to be seen.

Important to the US, NATO and EU countries is that major Russian weapons programs aim to either match or undermine key Western military capabilities. Simultaneously, Russia is investing in a range of AI-supported indirect and non-miliary methods and means of warfare, including offensive cyber and influence operations to undermine or bypass opponents' strengths and exploit their vulnerabilities. These focus areas are poised to gain importance, especially during the interim period, as the militarily weakened Russia is rebuilding its armed forces.

References

Advanced Research Foundation. Undated. *Fond perspektivnykh issledovanii.* Proekty. https://fpi.gov.ru/projects/. Accessed 30 Jan 2024.

Agit Polk. 2018. *Kak razvivaetsya iskusstvennyi intellekt v Rossii.* https://agitpolk.ru/3918-kak-razvivaetsya-iskusstvennyj-intellekt-v-rossii/. Accessed 30 Jan 2024.

AI Alliance Russia. Undated. *Al'yans v sfere iskusstvennogo intellekta.* https://a-ai.ru. Accessed 30 Jan 2024.

AP. 2023. *Russia's parliament approves budget with a record amount devoted to defense spending.* Associated Press. https://apnews.com/article/russia-budget-duma-economy-ukraine-07e66c23e1f47097de2348325f39dd6f. Accessed 30 Jan 2024.

Argumenty i Fakty. 2022. *Chto za BMP-3 s iskusstvennym intellektom sozdali v Rossii?* https://aif.ru/society/army/chto_za_bmp-3_s_iskusstvennym_intellektom_sozdali_v_rossii. Accessed 30 Jan 2024.

Barnes, Julian E., Eric Schmitt, and Thomas Gibbons-Neff. 2023. Russia overcomes sanctions to expand missile production, Officials say. *New York Times*. https://www.nytimes.com/2023/09/13/us/politics/russia-sanctions-missile-production.html#:~:text=Russia%20subverted%20American%20export%20controls,shipped%20to%20Russia%20more%20easily. Accessed 30 Jan 2024.

Belousov, Andrey. 2022. *Letter to Flavio S. Damico, Chair of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapon Systems (GGE on LAWS), Geneva, Russia's Permanent Representative to the UN Office at Geneva*. https://documents.unoda.org/wp-content/uploads/2022/07/WP-Russian-Federation_EN.pdf. Accessed 30 Jan 2024.

Bendett, Samuel, and Elsa Kania. 2019. *A New Sino-Russian High-Tech Partnership: Authoritarian Innovation in an Era of Great-Power Rivalry*. Australian Strategic Policy Institute Policy Brief, Report No. 22/2019. https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership. Accessed 30 Jan 2024.

Cheberko, Ivan. 2018. Pochemu v Rossii ne poluchilsya analog DARPA. *RBK Daily*. https://www.rbc.ru/opinions/politics/12/04/2018/5ace03ea9a79475603462ad7. Accessed 30 Jan 2024.

CISA. Undated. *Russia cyber threat overview and advisories.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/uscert/russia. Accessed 30 Jan 2024.

CNA (Center for Naval Analysis). 2022. *Artificial intelligence and autonomy in Russia: A year's reflection*. CNA Russia Studies Program. https://www.cna.org/reports/2022/09/Artificial-Intelligence-and-Autonomy-in-Russia-A-Years-Reflection.pdf. Accessed 30 Jan 2024.

Cnews.ru. 2020a. *Tsifrovaya yekonomika' pri Noskove ostavila IT-biznes bez 26 milliardov*. https://www.cnews.ru/news/top/2020-02-20_tsifrovaya_ekonomika_v_chisle. Accessed 30 Jan 2024.

———. 2020b. *Finansirovanie iskusstvennogo intellekta v Rossii urezano na 100 milliardov*. https://www.cnews.ru/news/top/2020-08-17_finansirovanie_iskusstvennogo. Accessed 30 Jan 2024.

———. 2020. *V Rossii nachal rabotat' gosudarstvennyi tsentr razvitiya II*. https://www.cnews.ru/news/top/2022-09-09_chernyshenko_v_rossii_nachal. Accessed 30 Jan 2024.

Corera, Gordon. 2022. Inside a US military cyber team's defense of Ukraine. *BBC News*. https://www.bbc.com/news/uk-63328398. Accessed 30 Jan 2024.

Cranny-Evans, Samuel. 2021. *Russia to conduct mass testing of Uran-9 UGV in 2022.* Janes. https://www.janes.com/defense-news/news-detail/russia-to-conduct-mass-testing-of-uran-9-ugv-in-2022. Accessed 30 Jan 2024.

CTII. Undated. *Tsentr Tekhnologii Iskusstvennogo Intellekta NIC imeni N.E. Zhukovskogo (CTII).* https://ctii-nrc.ru/#aboutus. Accessed 30 Jan 2024.

Dear, Keith. 2019. Will Russia rule the world through AI? Assessing Putin's rhetoric against Russia's reality. *Rusi Journal* 164 (5): 36–60.

Edmonds, Jeffrey, Samuel Bendett, Anya Fink, Mary Chesnut, Dmitry Gorenburg, Michael Kofman, Kasey Stricklin, and Julian Waller. 2021. *Artificial Intelligence and Autonomy in*

Russia. Arlington, USA: Center for Naval Analyses. https://www.cna.org/reports/2021/05/Artificial-Intelligence-and-Autonomy-in-Russia.pdf. Accessed 30 Jan 2024.

Fink, Anya. 2021. *Russian thinking on the role of AI in future warfare*. Russian Studies Series 5/21. NATO Defense College. https://www.ndc.nato.int/research/research.php?icode=712. Accessed 3 Feb 2023.

Gazeta.Ru. 2021. *Pochemu Rossyja massovo vnedryaet iskusstvennyi intellekt v boevye sistemy.* https://www.gazeta.ru/army/2021/11/18/14218657.shtml?updated. Accessed 30 Jan 2024.

GGE. 2019. *Potentsial'nye vozmozhnosti i ogranicheniya voennogo primeneniya smertonosnyh avtonomnykh sistem vooruzhenii*. Submission of the Russian Federation to the Group of Government Experts (GGE) of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (CCW). Geneva. UN Office for Disarmament Affairs, Documents Library. https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_(2019)/CCW.GGE.1.2019.WP.1_R%2BE.pdf. Accessed 30 Jan 2024.

GII. 2022. *Global Innovation Index 2022, Russian Federation.* World Intellectual Property Organization. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_2000_2022/ru.pdf. Accessed 30 Jan 2024.

Gressel, Gustav. 2020. *The sanctions straitjacket on Russia's defense sector.* European Council on Foreign Relations. https://www.ecfr.eu/article/commentary_the_sanctions_straitjacket_on_russias_defense_sector. Accessed 30 Jan 2024.

Hakala, Janne, and Jazlyn Melnychuk. 2021. *Russia's strategy in cyberspace*. NATO Strategic Communications Center of Excellence. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf. Accessed 30 Jan 2024.

Hambling, David. 2022a. Russia steps up Kamikaze drone strikes as it targets Ukraine's American Artillery (Updated). *Forbes*. https://www.forbes.com/sites/davidhambling/2022/07/21/russia-steps-up-kamikaze-drone-strikes/. Accessed 30 Jan 2024.

Hoffberger-Pippan, Elisabeth, Vanessa Vohs, and Paula Köhler. 2022. *Autonomous weapons systems: UN expert talks facing failure, time to consider alternative formats*. SWP (German Institute for International and Security Affairs). https://www.swp-berlin.org/10.18449/2022C43/. Accessed 30 Jan 2024.

Interfax. 2022. *Natsional'nyi tsentr razvitiya iskusstvennogo intellekta nachal rabotu v Rossii*. https://www.interfax.ru/russia/861318. Accessed 30 Jan 2024.

iPavlov. Undated. *Unique iPavlov intelligent platforms.* AI company iPavlov. https://ipavlov.ai. Accessed 30 Jan 2024.

Izvestiya. 2021. *The T-14 Armata tank will receive artificial intelligence*. https://vpk.name/en/536835_the-t-14-armata-tank-will-receive-artificial-intelligence.html. Accessed 30 Jan 2024.

Kashemirov, Maksim. 2020. *Na forume 'Armiya' obsudili budushchee iskusstvennogo intellekta*. Krasnaya Zvezda. https://tvzvezda.ru/news/2020829848-yAWFx.html. Accessed 30 Jan 2024.

Kommersant. 2022a. *Plyus aytifikatsiya vsei strany*. https://www.kommersant.ru/doc/5218247. Accessed 30 Jan 2024.

———. 2022b. *Gosplany zaputalis' v neyrosetakh*. https://www.kommersant.ru/doc/5294266. Accessed 30 Jan 2024.

———. 2023. *Iskusstvennyi intellekt poshel na ubyl*. https://www.kommersant.ru/doc/5773647. Accessed 30 Jan 2024.

Konaev, Margarita, and Owen J. Daniels. 2023. The Russians are getting better. *Foreign Affairs*. https://www.foreignaffairs.com/ukraine/russians-are-getting-better-learning. Accessed 30 Jan 2024.

Konaev, Margarita, Andrew Imbrie, Ryan Fedasiuk, Emily Weinstein, Katerina Sedova, and James Dunham. 2021. *Headline or trend line? Evaluating Chinese-Russian collaboration in AI*. Center for Security and Emerging Technology Issue Brief. https://doi.org/10.51593/20210033. Accessed 30 Jan 2024.

Kuo, Mercy A. 2022. How China supplies Russia's military. *The Diplomat*. https://thediplomat.com/2022/05/how-china-supplies-russias-military/. Accessed 30 Jan 2024.

Lee, John. 2022. *China-Russia cooperation in advanced technologies: The future global balance of power and the limits of 'unlimited' partnership*. Australia-China Relations Institute. https://

www.australiachinarelations.org/content/china-russia-cooperation-advanced-technologies-future-global-balance-power-and-limits. Accessed 30 Jan 2024.
Lo, Kinling. 2023. Chinese satellite start-up named in US sanctions aimed at Wagner group denies aiding Russia in Ukraine war. *South China Morning Post*. https://www.scmp.com/news/china/diplomacy/article/3208451/chinese-satellite-start-named-us-sanctions-aimed-wagner-group-denies-aiding-russia-ukraine-war. Accessed 30 Jan 2024.
Markotkin, Nikolai and Elena Chernenko. 2020. *Developing artificial intelligence in Russia: Objectives and reality*. Carnegie Endowment for International Peace. https://carnegiemoscow.org/commentary/82422. Accessed 30 Jan 2024.
McDermott, Roger. 2020a. Moscow's pursuit of artificial intelligence for military purposes. *Eurasia Daily Monitor*. https://jamestown.org/program/moscows-pursuit-of-artificial-intelligence-for-military-purposes/. Accessed 30 Jan 2024.
———. 2020b. Tracing Russia's path to network-centric military capability. *Eurasia Daily Monitor*. https://jamestown.org/program/tracing-russias-path-to-network-centric-military-capability/. Accessed 30 Jan 2024.
———. 2022. *Russia's path to the high-tech battlespace*. Washington, DC: The Jamestown Foundation. https://jamestown.org/wp-content/uploads/2022/07/Russias-Path-to-the-High-Tech-Battlespace-full-text-web.pdf. Accessed 30 Jan 2024.
Metz, Cade, and Adam Satariano. 2022. Russian tech industry faces 'Brain Drain' as workers flee. *New York Times*. https://www.nytimes.com/2022/04/13/technology/russia-tech-workers.html. Accessed 30 Jan 2024.
Military Encyclopedic Dictionary. Undated. *Iskustvennyi intellekt. Dictionary entry for "artificial intelligence"*. Ministry of Defense, Russian Federation. Accessed January 30, 2024, from https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5271@morfDictionary
Ministry of Digital Development, Communications and Mass Media. 2019. *Dorozhnaya karta razvitiya "skvoznoi" tsifrovoi tekhnologii "neirotekhnologii i iskusstviennyi intellekt"*. Russian Federation. Accessed January 30, 2024, from https://digital.gov.ru/uploaded/files/07102019ii.pdf
Ministry of Science and Higher Education. 2019. *AI is for active involvement... of Russian students in artificial intelligence research*. Russian Federation, Academic Excellence Project. https://5top100.ru/en/news/115622/?sphrase_id=16842. Accessed 30 Jan 2024.
MoD. 2014. *Na voenno-nauchnoi konferentsii po robototekhnike vpervye pokazhut unikal'nye razrabotki voennogo naznacheniya*. Ministry of Defense of the Russian Federation. https://z.mil.ru/spec_mil_oper/news/more.htm?id=12077702@egNews. Accessed 30 Jan 2024.
———. 2016. *Okolo 400 nobobrantsev vesennogo prizyva otobrany dlya sluzhby v nauchnykh rotakh*. Ministry of Defense of the Russian Federation. https://function.mil.ru/news_page/country/more.htm?id=12089407@egNews. Accessed 30 Jan 2024.
———. 2018a. *Konferentsiya 'Iskusstvennyi intellekt: problemy i puti ikh resheniya – 2018'*. Ministry of Defense of the Russian Federation. http://mil.ru/conferences/is-intellekt.htm. Accessed 30 Jan 2024.
———. 2018b. *Spetsialisty GNIIC robototekhniki Minoborony RF sosredotochili usiliya na razrabotke i sozdanii sistem tekhnicheskogo zreniya*. Ministry of Defense of the Russian Federation. https://function.mil.ru/news_page/country/more.htm?id=12169550@egNews. Accessed 30 Jan 2024.
———. 2021a. *Glavnomu upravleniyu nauchno-issledovatel'skoi deyatel'nosti Minoborony Rossii – 8 let*. Ministry of Defense of the Russian Federation. https://function.mil.ru/news_page/country/more.htm?id=12343872@egNews. Accessed 30 Jan 2024.
———. 2021b. *V voennom innovatsionnom tekhnopolise 'year' nachal rabotat' Nauchno-proizvodstvennyi tsentr 'Kulibin'*. Ministry of Defense of the Russian Federation. https://function.mil.ru/news_page/person/more.htm?id=12353521@egNews. Accessed 30 Jan 2024.
———. Undated-a. *Struktura i realizatsiya innovatsionnoi deyatel'nosti*. Ministry of Defense of the Russian Federation. https://mil.ru/mission/innovacia/struct.htm. Accessed 30 Jan 2024.
———. Undated-b. *Nauchno-proizvodstvennyi tsentr 'Kulibin'*. Ministry of Defense of the Russian Federation. https://mil.ru/era/npc-kulibin.htm. Accessed 30 Jan 2024.

———. Undated-c. *46 Tsentral'nyi nauchno-issledovatel'skii institut Ministerstva oborony Rossiiskoi Federatsii*. Ministry of Defense of the Russian Federation. https://ens.mil.ru/science/SRI/information.htm?id=11391@morfOrgScience. Accessed 30 Jan 2024.

———. Undated-d. *Glavnoe upravlenie innovatsionnogo razvitiya Ministerstva oborony Rossiiskoi Federatsii*. Ministry of Defense of the Russian Federation. https://structure.mil.ru/structure/ministry_of_defense/details.htm?id=11376@egOrganization. Accessed 30 Jan 2024.

———. Undated-e. *Vyderzhka iz polozheniya o glavnom upravlenii nauchno-issledovatel'skoi deyatel'nosti i tekhnologicheskogo soprovozhdeniya peredovykh tekhnologii (innovatsionnykh issledovanii) Ministerstva oborony Rossiiskoi Federatsii*. Ministry of Defense of the Russian Federation. https://doc.mil.ru/documents/quick_search/more.htm?id=11919505@egNPA. Accessed 30 Jan 2024.

———. Undated-f. *Nauchnye roty*. Ministry of Defense of the Russian Federation. https://recrut.mil.ru/for_recruits/research_company/companies.htm. Accessed 30 Jan 2024.

MSU. 2023. *V MGU otkryli novyi superkompyuter, reshayushhii zadachi II*. Moscow State University. https://www.msu.ru/news/v-mgu-otkryli-novyy-superkompyuter-reshayushchiy-zadachi-ii.html. Accessed 30 Jan 2024.

Myl'nikov, Pavel. 2022. Glava "Sberbanka": Ukhod firm iz RF grozit poteryami yekonomike. *DW News*. https://www.dw.com/ru/glava-sberbanka-gref-uhod-inostrannyh-firm-grozit-poteramiekonomike-rf/a-63707677. Accessed 30 Jan 2024.

Nadibaidze, Anna. 2022a. *Russian Perceptions of Military AI, and Automation, and Autonomy*. Foreign Policy Research Institute. https://www.fpri.org/wp-content/uploads/2022/01/012622-russia-ai-.pdf. Accessed 30 Jan 2024.

———. 2022b. Great power identity in Russia's position on autonomous weapons systems. *Contemporary Security Policy* 43: 3. https://www.tandfonline.com/doi/full/10.1080/13523260.2022.2075665. Accessed 30 Jan 2024.

NCRII. Undated. *Natsional'nyi tsentr razvitiya iskusstvennogo intellekta pri Pravitel'stve Rossiiskoi Federatsii (NCRII)*. National Center for the Development of Artificial Intelligence. https://aicenter.hse.ru. Accessed 30 Jan 2024.

Newsru.com. 2014. *Minoborony RF utverdilo plan boevogo primeneniya robotov do 2025 goda*. https://www.newsru.com/hitech/06nov2014/roboty_rf.html. Accessed 30 Jan 2024.

Nikol'skii, Aleksei, and Svetlana Bocharova. 2018. *Novoe litso voennykh innovatsii*. Vedomosti.

Novyi, Vladislav. 2021. *Rossiya budet kontrolirovat' sozdanie 'sverhrazuma'*. Vedomosti. https://www.vedomosti.ru/technology/articles/2021/10/26/892915-sozdanie-sverhrazuma. Accessed 30 Jan 2024.

OECD. Undated. *Investments in AI*. Live data, OECD.AI Policy Observatory. https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data. Accessed 30 Jan 2024.

Palavenis, Donatas. 2022. *The use of emerging disruptive technologies by the Russian Armed Forces in the Ukrainian War*. Air Land Sea Space Application Center. https://www.alsa.mil/News/Article/3170285/the-use-of-emerging-disruptive-technologies-by-the-russian-armed-forces-in-the/. Accessed 30 Jan 2024.

Patriot-export.ru. 2017. *Sergei Popov o sovremennom sostoyanii robototekhniki v vooruzhennykh silakh*. http://www.patriot-expo.ru/520/. Accessed 30 Jan 2024.

Petrella, Stephanie, Chris Miller, and Benjamin Cooper. 2021. Russia's artificial intelligence strategy: The role of state-owned firms. *Orbis* 65: 1. https://sites.tufts.edu/hitachi/files/2021/02/1-s2.0-S0030438720300648-main.pdf. Accessed 30 Jan 2024.

Poroskov, Nikolai. 2022. *Iskustvennyi intellekt: novoe soderzhanie voennoi moshchi*. Yezhenedel'nik Zvezda. https://zvezdaweekly.ru/news/2022921178-RPjfz.html. Accessed 30 Jan 2024.

Presidential Decree. 2016. *O strategii nauchno-tehnologicheskogo razvitiya Rossiiskoi Federatsii*. Presidential Decree No. 642. http://kremlin.ru/acts/bank/41449. Accessed 30 Jan 2024.

———. 2019. *O razvitii iskusstvennogo intellekta v Rossiiskoi Federatsii*. Presidential Decree No. 490. http://www.kremlin.ru/acts/bank/44731. Accessed 30 Jan 2024.

Putin, Vladimir. 2012. *Presidential Address to the Federal Assembly*. Presidential Library. https://www.prlib.ru/en/node/359175. Accessed 30 Jan 2024.

———. 2013. *Presidential Address to the Federal Assembly*. http://en.kremlin.ru/events/president/news/19825. Accessed 30 Jan 2024.

———. 2022a. *Speech at Artificial Intelligence Journey 2022 conference in Moscow*. http://en.kremlin.ru/events/president/news/69927/print. Accessed 30 Jan 2024.
———. 2022b. *Speech at the annual meeting of the Board of the Ministry of Defense of the Russian Federation*. Office of the President of Russia. http://kremlin.ru/events/president/news/70159. Accessed 30 Jan 2024.
Regnum.ru. 2020. *Natsional'nyi tsentr upravleniya oboronoi RF primenyaet iskusstvennyi intellekt*. https://regnum.ru/news/polit/2836730.html. Accessed 30 Jan 2024.
Ria Novosti. 2016. *Byudzhet Fonda perspektivnykh issledovaniii na 2018 godu ostanetsya prezhnim*. https://ria.ru/20160706/1459588542.html. Accessed 30 Jan 2024.
———. 2021. *Putin otsenil rol' iskusstvennogo intellekta v proizvodstve vooruzheniya*. https://ria.ru/20211103/vooruzhenie-1757590645.html. Accessed 30 Jan 2024.
———. 2022. *Bolee 19 tysyach pedagogov obuchilis' tekhnologiyam iskusstvennogo intellekta*. https://ria.ru/20221103/tekhnologii-1829017067.html. Accessed 30 Jan 2024.
Rosinform.ru. 2022. *Vasilii Elistratov: 'Nasha zadacha – sohranit' zhizni lyudei s pomoshchyu intellektual'nykh mashin*. https://rosinform.ru/forum-armiya-2022/654572-vasiliy-evstratov-nasha-zadacha%2D%2D-sokhranit-zhizni-lyudey-s-pomoschyu-intellektualnykh-mashin/. Accessed 30 Jan 2024.
Rossiiskaya Gazeta. 2018. *Putin: Boyevye lazery uzhe postupayut na vooruzhenie voisk*. https://rg.ru/2018/03/01/putin-boevye-lazery-uzhe-postupaiut-na-vooruzhenie-vojsk.html. Accessed 30 Jan 2024.
Rostec State Corp. 2019. *Rostec will start exporting face recognition technology to the armed forces*. https://rostec.ru/en/news/rostec-will-start-exporting-face-recognition-technology-to-the-armed-forces/. Accessed 30 Jan 2024.
Russian Government News. 2022. *Speech by Deputy Head of the Russian Delegation to the UN, K. V. Vorontsov, to the First Committee, 77th session of the UN General Assembly*. https://russiaun.ru/ru/news/201022_v. Accessed 30 Jan 2024.
Sergeantov, A.V., A.V. Resin, and I.A. Terent'iev. 2022. Transformatsiya soderzhaniya voiny: kontury voennykh konfliktov budushhego. *Voennaya Mysl* 6: 19–30.
Sosnitskii, Vladimir. 2022. *Innovatsii otsenivaet praktika: Tekhnopolis YeRA stal yeffektivnoi ploshchadkoi konstruktivnogo issledovatel'skogo dialoga*. Krasnaya Zvezda. https://dlib.eastview.com/browse/doc/78978635. Accessed 30 Jan 2024.
Sukhankin, Sergey. 2019a. Russia adopts national strategy for development of artificial intelligence. *Eurasia Daily Monitor*. https://jamestown.org/program/russia-adopts-national-strategy-for-development-of-artificial-intelligence/. Accessed 30 Jan 2024.
———. 2019b. *'Special Outsider': Russia joins the race for global leadership in artificial intelligence*. *Eurasia Daily Monitor*. https://jamestown.org/program/special-outsider-russia-joins-the-race-for-global-leadership-in-artificial-intelligence/. Accessed 30 Jan 2024.
Tass. 2019. *Minobrnauki i FPI podpisali soglashenie o sotrudnichestve po proryvnym razrabotkam*. https://nauka.tass.ru/nauka/6645611. Accessed 30 Jan 2024.
———. 2021. *MiG-35 fighter to have smart system of target recognition*. https://tass.com/defense/1276477. Accessed 30 Jan 2024.
———. 2022a. *Pantsir systems demonstrated effectiveness in Ukraine — Rostec*. https://tass.com/defense/1427385. Accessed 30 Jan 2024.
———. 2022b. *V Minoborony RF sozdali upravlenie po rabote s iskusstvennym intelektom*. https://tass.ru/armiya-i-opk/15492531. Accessed 30 Jan 2024.
———. 2023. *Shoigu: sistemu upravleniya i svyazi VS RF usovershenstvuyut s primeneniem tekhnologii II*. https://tass.ru/armiya-i-opk/16766. Accessed 30 Jan 2024.
Voennoe Obozrenie. 2018. *Shoigu prizval voennykh i grazhdanskikh uchenykh obedinit'sya dlya raboty nad iskusstvennym intellektom*. https://topwar.ru/137827-shoygu-prizval-voennyh-i-grazhdanskih-uchenyh-obedinitsya-dlya-raboty-nad-iskusstvennym-intellektom.html. Accessed 30 Jan 2024.
Vzglyad. 2020. *Putin otsenil rol' iskusstvennogo intellekta v vooruzhenii*.
Washington Post. 2022. *To Hobble Putin, accelerate the brain drain*. https://www.washingtonpost.com/business/energy/to-hobble-putin-accelerate-the-brain-drain/2022/05/10/3f50127a-d061-11ec-886b-df76183d233f_story.html. Accessed 30 Jan 2024.

Wiśniewska, Iwona. 2022. *Russia's 'war' budget for 2023–2025*. Center for Eastern Studies. https://www.osw.waw.pl/en/publikacje/analyses/2022-12-12/russias-war-budget-2023-2025. Accessed 30 Jan 2024.

Work, Robert O., and Greg Grant. 2019. *Beating the Americans at their own game: An offset strategy with Chinese characteristics*. Center for a New American Security. https://www.cnas.org/publications/reports/beating-the-americans-at-their-own-game. Accessed 30 Jan 2024.

Zakvasin, Aleksei. 2019. *'Iskusstvennyi intellekt — sredstvo, a ne samotsel': v tekhnopolise 'Yera' rasskazali o rabote unikal'nogo klastera*. RT. https://russian.rt.com/russia/article/686954-tehnopolis-era-intervyu. Accessed 30 Jan 2024.

Zysk, Katarzyna. 2015. Managing military change in Russia. In *Security, strategy and military change in the 21st century: Cross-regional perspectives*, ed. Jo Inge Bekkevold, Ian Bowers, and Michael Raska, 155–177. London: Routledge.

———. 2020. Defense innovation and the 4th Industrial Revolution in Russia. *Journal of Strategic Studies* 44 (4): 543–571. https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090. Accessed 30 Jan 2024.

———. 2021. Military R&D, innovation and breakthrough technologies. In *Advanced military technology in Russia: Capabilities and implications*, ed. Samuel Bendett, Mathieu Boulègue, Richard Connolly, Margarita Konaev, Pavel Podvig, and Katarzyna Zysk, 11–22. London: Chatham House. https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-23-advanced-military-technology-in-russia-bendett-et-al.pdf. Accessed 30 Jan 2024.

———. 2022. *Is Russia a threat in emerging and disruptive technologies?* NATO Defense College Policy Brief 09-22. https://www.ndc.nato.int/news/news.php?icode=1704. Accessed 30 Jan 2024.

Survival of the Smartest? Defense AI in Ukraine

Vitaliy Goncharuk

Before Russia's full-scale invasion in February 2022, Ukraine had an advanced ecosystem to produce artificial intelligence (AI) solutions for commercial use. The country also ranked first in the number of AI companies in Eastern Europe (Oxford Insight 2020) with more than 7000 AI engineers and hosting research and development (R&D) offices of multinational companies like Amazon, Lyft, Google, Samsung, Grammarly and many others. In addition, the country approved its first national AI strategy (Cabinet of Ministers 2020) in 2020, which, among other priorities, also identified the importance of implementing AI in the field of security and defense. However, Ukraine's defense sector only used AI sporadically, as the defense industry was primarily state-owned, focused on traditional hardware, and was not known as a "hotbed" for innovative, especially software-driven solutions.

The current war between Russia and Ukraine has changed almost all these parameters. Unlike other conflicts over the last 30 years, this is a war among technologically advanced countries. Therefore, both sides began developing and fielding AI solutions for tasks like geospatial intelligence, operations with unmanned systems, military training, and cyber warfare. Consequently, the war in Ukraine became the first conflict where both parties compete in and with AI, which has become a critical component of success.

In 2022, Ukraine's resilience originated from a more active use of awareness systems, volunteer and private AI initiatives as well as the crowdsourcing of data, the use of open-source platforms, and advances in the decentralized use of the respective assets. As of 2023, the Cabinet of Ministers began to launch policy initiatives more systematically to advance defense AI, to advance the respective national industrial base, creating a new ecosystem, and advancing public and

V. Goncharuk (✉)
AI Committee of Ukraine, Kyiv, Ukraine

TechWise Society Foundation, Washington, DC, USA
e-mail: hello@wiseregulation.org

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_17

private funding solutions. The ecosystem of information technology (IT) companies also began to shift its focus from developing civil products to dual-use products and actively recruit the best talents in the AI field. Foreign AI solution developers are using the war as a testbed to evaluate the performance of their solutions on the battlefield. Some defense observers even contend that AI solutions that have not been tested for use in Ukraine's combat environment won't be fit for purpose.

This war poses challenges not only to AI solutions providers but also to AI regulation as battlefield experience prompts the need to reconsider the appropriateness of the "human in the loop" principles and other core assumptions. It seems that many of the existing regulatory principles will be hard to sustain as they have not been designed for war and thus hamper countries in their need to defend against aggressors. Consequently, Ukraine is turning into a most valuable test case for the development and regulation of war-proof defense AI solutions.

1 Thinking About Defense AI

At the time of writing this chapter, Ukraine is at war. Almost all investments, intellectual and material resources are directed toward survival and enhancing defense capabilities to ensure success on today's battlefield, not in 2 or 3 years.

This focus also drives defense AI in Ukraine. According to the national AI strategy, AI is understood as

> an organized set of information technologies, with the use of which it is possible to perform difficult complex tasks by using a system of scientific research methods and algorithms for processing information obtained or independently created during work, as well as to create and use own knowledge bases, decision-making models, algorithms for working with information and determine ways to achieve the tasks (Cabinet of Ministers 2020).

Ukraine's current efforts are geared towards using AI to establish a competitive edge vis-à-vis Russia and build an ecosystem that will sustain this technological advantage to withstand aggression and rapidly develop much-required defense solutions. While both sides benefit from using defense AI to advance the processing of information, support decision-making, and enhancing existing equipment with defense AI, the question is how to get the upper hand in this technology-driven "tit for tat" game. In this regard, the accumulation of knowledge and experience could become a future strategic currency for Ukraine to advance national force development and share insights with allies and partners. The battle use of defense AI also yields valuable lessons for the future regulation of defense AI. Considering the situation, Ukraine has started to explore how warfighting insights on defense AI could be transitioned from the current state of war into a future state of peace as it is particularly important that data, which has been collected during wartime, would henceforth not be used in ways detrimental to human rights and democratic values.

1.1 Regulating Defense AI

The Ministry of Digital Transformation of Ukraine (Cabinet of Ministers 2023) is the main body responsible for policies in the field of AI and robotics development. Within the Ministry, a separate department has been established, and since 2020, there is an expert committee on developing and deploying AI.

So far, the national AI strategy (Cabinet of Ministers 2020) is the country's capstone document, which also foresaw the use of AI for national security and defense as a key area of application. According to the strategy, AI solutions must ensure the protection of human rights and adhere to ethical standards. To this purpose, the strategy also includes developing an ethical code on AI but work in this direction has not yet started.

National security and defense are key use cases for AI in Ukraine. According to the strategy (Cabinet of Ministers 2020), the government wants to develop solutions for the use of AI for

- Command and control (C2);
- Weapons and military equipment including unmanned systems and unmanned demining solutions;
- Collection and analysis of information during combat operations;
- Analysis in support of intelligence activities including the processing of cartographic information;
- Defense against cyber threats including applications that allow for the quick detection of cyberattacks, preliminary scanning, and subsequent avoidance of malicious codes;
- Simulation and cognitive modeling of the combat situation.

These use cases suggest that Ukraine sees AI as integral to its attempt to develop unmanned systems and advance cyber defense solutions as envisioned by the country's 2021 Military Security Strategy (President 2021). To this end, the Cabinet of Ministers has also adopted an implementation plan (Cabinet of Ministers 2021). The plan outlines a series of initiatives such as adopting legal regulation on issues of forming state policy in the field of AI, providing state support to use AI in priority sectors of the economy, implementing AI to enhance national cybersecurity systems, and defining priority tasks and directions for the current and future use of AI for defense.

In addition, Ukraine participates in international initiatives to regulate the development and use of AI. In particular, the Ukrainian Parliament ratified the agreement with the European Union (EU) on joining the "Digital Europe" program in February 2023 (Verkhovna Rada 2023) and signed the November 2023 Bletchley Declaration on AI Security at the AI Safety Summit (Ministry of Digital Transformation 2023a). As an official candidate for EU membership, Ukraine clearly signals its will to synchronize legislative efforts to advance digitalization with the EU's policy initiatives. But while the Ministry of Digital Transformation has outlined a roadmap for regulating the civilian and

commercial use of AI in Ukraine (Ministry of Digital Transformation 2023b), the respective capstone document for the use of AI in support of national security and defense is missing.

1.2 Re-evaluating "Human in the Loop" in Modern Warfare

In recent years, civil society organizations and AI experts have become increasingly concerned about the emergence of lethal autonomous weapons systems (LAWS), which may use AI to identify targets and thus could harm individuals if used without direct human control (Kahn 2022a). Consequently, there has been a collective initiative at the United Nations to prohibit or impose limitations on using these systems. So far, however, these discussions have not yielded significant results.

Proponents of the "human in the loop" principle, which advocates the ultimate role of humans as decision makers, have noble intentions. But technical solutions envisaged to ensure ultimate human control are challenging to implement in war without overly limiting a defender's space for action. First, on the battlefield, the distinction between solutions to find, fix, track, and engage targets with a "human in the loop" or in fully autonomous mode is almost impossible to make as the same technology operates in different modes. In practice, there are only 2–5 s between target identification and engagement, which is hardly enough for a human operator to make a balanced decision. This bears the risk that involving a "human in the loop" becomes a "formality," that might render the target-engagement cycle more difficult. Second, implementing "human in the loop" via mechanisms that ensure remote control of assets not only increases the costs of the respective devices. Russia's frequent use of electronic warfare (EW) also makes connectivity with the platform and the payload unfeasible. Third, there are no effective international mechanisms to verify or ensure that both sides refrain from using weapons without a "human in the loop," as it is challenging—if not impossible—to ascertain after a mission has been executed, whether an unmanned asset has been piloted or flown autonomously. Under these conditions, fully autonomous AI solutions would provide the defender with significant advantages in executing its tasks more effectively and more precisely than, for example, with traditional artillery or conventional weapons (Goncharuk 2020).

In sum, the use of AI in the current war is very likely to shape the future regulatory debate in two different ways. First, war experience will test the binding power of norms and rules when aggressors feel unrestricted by the normative principles that guide a defender's actions. In addition, this will also prompt the need to rethink how the human in the loop logic—which depends on connectivity between operators and unmanned assets—would be ensured under adversarial electromagnetic spectrum dominance.

2 Developing Defense AI

Before the full-scale invasion in 2022, Ukraine's defense sector was considered non-prestigious and corrupt (Bondar 2023). The defense-industrial complex of Ukraine consisted mainly of state-owned enterprises with only a handful of private defense manufacturers getting state defense orders (Kolomychenko 2023). The main AI development centers were concentrated in a few state institutes that historically worked with the main customer UkrOboronProm and dozens of private companies.

In 2022, most AI initiatives, including data collection and processing, neural network training for weapon detection, and social media analysis to fight disinformation campaigns, were spearheaded by private companies and volunteers. These private and volunteer-led efforts incorporated advanced technologies such as AI-enhanced detectors and trackers in drones and robots for localization, adapting rapidly to the evolving demands of the conflict, whereas the state continued to focus on conventional weapons production. However, as will be discussed below, systemic changes at the state level, including the development of funding programs and the creation of new structural units with a focus on AI development, began in 2023.

2.1 AI's War Stimulus

Russia pays significant attention to the development of AI technologies in defense. The arsenal of the Russian armed forces already includes a wide range of weapons using AI technologies (CNA 2022). As Katarzyna Zysk (Zysk 2023) shows, Russia's political and military decision-makers understand the importance of AI and are therefore actively investing in its military application, involving state and private development centers.

Given that Russia is ramping up its industrial production of drones and robotic systems, autonomous robots with AI may begin to be used massively from 2025 to 2026, which could provide a significant advantage on the battlefield. These systems may be EW-proof due to AI's capability to autonomously process and react to electronic threats, dynamically adapt to changing electronic environments, and operate independently without the need for remote signals, which are often targets of electronic jamming. Consequently, Ukraine is forced to compete and develop AI solutions that provide adequate responses to Russia's challenges.

From 2023, the Government of Ukraine began actively stimulating the development of innovative defense solutions. The Ministry of Strategic Industries and the Ministry of Digital Transformation are at the forefront of these efforts. Technological defense developments in the field of AI receive organizational and financial support through specialized platforms and projects. In addition, volunteers—who joined to help the Ukrainian armed forces by raising funds for the purchase of weapons, special equipment, transport, communication means, and training—are of pivotal importance in strengthening the country's defense.

This combination also helps explain Ukraine's success in implementing AI on the battlefield, which is driven by the motivation of Ukrainian troops, a high level of technical training of military specialists (who are recruited from the private sector), and the involvement of private companies in spearheading novel defense solutions. Crowdsourcing, involving ordinary citizens collect important information about military operations shared with Ukrainian authorities, also plays an important role. Together, these aspects illustrate the broader trend of democratizing military power, which goes far beyond the current war (Kahn 2022b).

Moreover, the unprecedented speed of implementing AI technologies into military systems and their use on the battlefield became possible thanks to the simplification of bureaucratic mechanisms to approve new technologies for use in the defense sector. So far, however, neither Russia nor Ukraine has officially acknowledged deploying fully autonomous weapon systems using AI. This also highlights, that it is "impossible to know, based on open-source materials, whether and what type of AI and autonomous technologies are being used in classified tasks and missions, and to what effect" (Konaev 2023).

2.2 Ukraine's New Defense AI Priorities

In September 2023, the Expert Advisory Committee on AI Development at the Ministry of Digital Transformation (Expert Committee 2023) provided recommendations for directing state and private investments to accelerate the development of defense AI solutions between 2023 and 2026. Among other things, the committee identified the following defense AI priorities:

- *AI for Domestic Unmanned Systems (e.g., Drones and Robots)*

The use of AI is meant to support navigation systems (without Global Positioning System, GPS), coordinated task execution management systems, autonomous task performance systems, enemy weapon and equipment detection (identification) systems, and data collection and storage systems for unmanned systems. These AI applications will be important to augment the "Army of Drones," that the General Staff of the Armed Forces and the Ministry of Digital Transformation intend to establish to leverage Ukraine's experience in using unmanned systems to repel Russia's aggression (Saballa 2023).

- *AI to Combat Disinformation*

AI shall be used for interactive solutions based on generative AI, deep voice and deepfake technologies for special law enforcement agencies, automatic detection systems for sources of disinformation and bots involved in foreign influence operations (FIMI), automation/standardization of information threat description and data exchange, labeling and detecting enemy generative AI to prevent the spread of disinformation, and creating datasets and data collection for generative AI development.

- *AI for Defense and Security-Relevant Logistics Systems*

AI is used to support predictive maintenance of equipment based on operating conditions, simulation analysis of supply logistics operations, systems for predicting supply and logistics needs and risks, management and automation systems for military warehouses, autonomous robots for military cargo delivery and personnel evacuation during active military operations.

- *AI for Mine and Ammunition Detection and Neutralization*

AI should support data collection and accumulation systems from satellites, drones, robots, and other sources (e.g., thermal sensors) for minefield detection, identification of combat sites for demining planning, robotic management systems for demining (urban, field, underwater), and quality control of demining systems.

- *AI for Cybersecurity and Information and Communications Technology (ICT) Protection in the Defense Sector*

AI should support systems for radio reconnaissance and advanced EW, modern data encryption and exchange systems, generative AI (voice) for pentesting (e.g., to verify military authorization procedures), countering sophisticated social engineering using generative AI (e.g., voice, 3D video), research focused on developing necessary innovative cybersecurity systems to protect critical digital infrastructures using advanced AI technologies for automatic threat analysis and classification.

- *General Conditions for Rapid Development of AI Solutions for Security and Defense*

Accelerating the use of AI for national security and defense foresees simplifying import and licensing procedures for components needed for AI solution training and development, deregulating and simplifying data acquisition procedures from the battlefield for drone, robot, and other AI system developers, simplifying testing processes for innovative products "on the battlefield" by domestic and foreign companies, advancing transparency and accessibility of information for defense tech participants, implementing universally accepted data exchange and storage standards, providing legal-regulatory provision for data exchange between different market participants and state bodies.

- *General Infrastructure and Solutions*

Moreover, Ukraine also wants to push for automated combat management systems (automated and AI assistance), simulation modeling solutions for military operations (wargames and military operations research), data analysis and classification systems from surveillance cameras, data collection and accumulation systems from media resources (as part of intelligence data), facial recognition and identification systems, AI-based damage assessment systems with various data types, advanced physical data transmission systems (for drones, robots, between different agents), datasets accessible to market participants for AI training and data collection systems, testing ranges for domestic and foreign developers, data exchange

systems between different departments, integration with government business intelligence production of domestic sensors such as stereo cameras, thermal cameras and others.

2.3 *Ukraine's New Defense AI Ecosystem*

Many state agencies, private companies, and volunteer initiatives are involved in developing defense AI. As Ukraine's defense ecosystem grows, it also becomes more complex thus prompting the need for coordination and synchronization. This is an aspect that will need to be strengthened in the future to make sure that ongoing development efforts meet current—and future—warfighting needs.

In addition to the leading Ukrainian ministries, which will be discussed in the next chapter, several para-governmental agencies, a growing number of domestic defense startups as well as international AI companies flocking to Ukraine constitute the country's defense AI ecosystem. Adjacent to the public sector is the state-influenced defense industrial complex that harbors many of the traditional defense companies. The following entities are of particular relevance:

- *JSC Ukroboronprom*

JSC Ukroboronprom is a strategic manufacturer of weapons and military equipment in Ukraine, uniting enterprises in the strategic sectors of the state's defense industry (Ukroboronprom Undated). Ukroboronprom includes the state enterprise Antonov, which developed more than 100 types of passenger, transport, and special aircraft, like the Ruslan and Mriya platforms (Skorobogatova and Kalko 2016). Ukroboronprom also includes the enterprise State Kyiv Design Bureau Luch, which is one of Ukraine's leading developers of components for aviation and anti-tank weapon systems (State Kyiv Design Bureau Luch Undated).

- *Brave1 Platform*

The Brave1 Platform (Brave1 Undated), established by the leadership of the Ministry of Digital Transformation, acts as an accelerator and an incubator. The main goal of the platform is to assess and promote technological products that can be integrated into various state sectors. In addition, Brave1 offers grants to accelerate the development of technologies considered critically important for Ukraine (Pylypiv 2023). Brave1 supports research projects in the field of AI in priority areas like systems and weapons, protection and security, support and logistics, unmanned systems, cybersecurity, intelligence, and navigation. Based on the military cluster of Brave1, the Griselda system was developed using AI to collect intelligence data. This technology is already in use with other systems like Delta (situational awareness), Bronya (artillery fire support), Kropyva (planning support), and GISArta (C2 for artillery fire) (Denisova 2023).

- *Innovation Development Accelerator*

Under the auspices of the Ministry of Defense of Ukraine, the Innovation Development Accelerator (Undated) was created to combine and develop the capabilities of different units inside the Ministry of Defense. This program is designed as a channel for rapid deployment of innovations in the military sphere.

- *Ukrainian Startup Fund*

The Ukrainian Startup Fund (Ukrainian Startup Fund Undated) was established to promote the development of early-stage technological startups in Ukraine. Since the beginning of the full-scale invasion, the fund has focused on supporting defense tech and deep tech projects. The fund allocated USD8.2M in grants, funding 352 startup teams, and conducted over 330 events like hackathons, boot camps, educational lectures, or mentoring sessions with 119 startups. The fund has also provided support to attend some of the world's largest technology events and enabled close to 200 pro bono experts to join the fund's work (Tarasovsky 2023a, b).

Private funds and non-profit organizations complement the government's efforts to advance Ukraine's defense industrial base. The following organizations play a key role:

- *D3 military tech Accelerator*

The D3 military tech Accelerator supports investments in early-stage startups, acceleration, and mentorship (Boshnyakov 2023).

- *Flyer One Ventures*

Flyer One Ventures (Undated), located in Ukraine, invests in Ukrainian startups from Europe and North America.

- *Aerorozvidka*

Aerorozvidka (Undated) is a non-profit organization that promotes the creation and implementation of networked and robotic military capabilities for the Ukrainian security and defense forces.

- *"Come Back Alive" Army Assistance Fund*

The "Come Back Alive" Fund, established in 2014, has already raised over UAH 5.2bn (USD 138M) for the needs of the Armed Forces of Ukraine. This fund specializes in the procurement of technical means and was the first in Ukraine to obtain permission to import dual-use goods from abroad (Melezhik 2022).

- *Prytula Foundation*

Serhiy Prytula's charity fund provides aid to the Armed Forces of Ukraine and humanitarian aid to civilians (Serhiy Prytula Charitable Foundation Undated).

- *Ukraine Defense Fund*

The Ukraine Defense Fund (Ukraine Defense Fund Undated) provides supplies and supports to people fighting on the front lines of Ukraine.

Ukrainian ministries and programs are meant to strengthen Ukraine's defense industrial base. Consequently, the number of Ukrainian startups that provide solutions for defense and national emergency management is growing rapidly. Some of these companies also work on defense AI as the following examples illustrate:

Artellence, an IT company, has developed neural networks for text analysis, face profile search, and algorithms for cleaning and structuring large data.

- Athlon Avia, a Ukrainian research and production company, develops unmanned aerial systems for tactical military missions such as intelligence, surveillance, target acquisition, and artillery fire adjustment (A1-CM "Furia").
- Saker develops affordable AI for small businesses, including drone-based vision systems for plant protection. The SAKER SCOUT drone, equipped with AI, is used in Ukraine for autonomous target detection and engagement.
- UA Damage developed a platform for analyzing damage and pyrotechnic contamination using AI, satellites, and drones. Its comprehensive analysis allows visual inspection of unexploded rockets and mines, detecting them in grass and underground, and even localizing explosive objects and marking them on maps.
- Zvook company creates neural networks of acoustic sensors for detecting aerial objects. The network helps conventional air defense systems detect and destroy enemy cruise missiles and drone attacks and provides alerts to civilians. Zvook technology is trained on a unique dataset of acoustic imprints for most modern Russian weaponry (Ministry of Digital Transformation of Ukraine 2023).

Finally, a unique aspect of military operations in Ukraine lies in the unprecedented support offered by foreign companies. In general, defense collaboration with the United States has been essential for Ukraine. For example, Ukraine has benefited from SpaceX providing access to real-time data transmission in areas where IT infrastructure had been damaged. General Atomics and AeroVironment contributed to advancing surveillance, reconnaissance, and precision strikes. CrowdStrike and FireEye helped advance Ukraine's digital defense in cyberspace. In addition to financial support, collaboration is meant to advance Ukraine's domestic defense industrial base and includes agreements on data-sharing and co-production of defense solutions, also with European partners.

Moreover, foreign AI solutions support and enhance Ukraine's situational awareness and situational understanding regarding Russian threats (Fontes and Kamminga 2023). One notable contributor is Palantir, which played a pivotal role during the conflict by providing extensive data sharing capabilities to the military leadership. Through its MetaConstellation too, Palantir facilitated large-scale data integration, encompassing sources ranging from commercial satellites to classified information from foreign intelligence services. This empowered Ukraine and its allies to utilize commercial data pertaining to specific battlegrounds, enabling the analysis of combat operations and the strategic planning of military endeavors. Notably, during the liberation of Kherson, the Ukrainian military benefited from accurate intelligence on the movements of Russian forces, allowing precise long-range strikes. The information, processed by NATO outside Ukraine, was then transmitted to the Ukrainian command (Ignatius 2022).

American companies such as Planet Labs, BlackSky Technology and Maxar Technologies also contribute significantly by generating satellite imagery of ongoing combat operations and sharing the data with the government and Armed Forces. Furthermore, Primer, an IT company, adapted its voice-to-text program to efficiently process intercepted messages from the Russian military. This innovative approach spares the Ukrainian military from spending extensive hours manually deciphering intercepted conversations. The Primer Command technology facilitates the creation of AI models that swiftly process substantial volumes of data derived from enemy radio communications (Fontes and Kamminga 2023).

3 Organizing Defense AI

Ukraine's war effort leverages decentralized organizational structures and volunteer initiatives to create a vibrant ecosystem of actors that jointly work on complex systems. This approach also nurtures competition for the best ideas and products between different actors. Although beneficial in principle, decentralized efforts create additional layers of complexity related to coordination and synchronization of activities. In this context, several ministries are involved in setting the course for long-term force planning, operational planning to conduct the war, and strengthening the local defense industrial base. Among the public stakeholders, the following are of particular relevance:

- *Ministry of Defense of Ukraine*

In 2021, a Joint Directive of the Minister of Defense of Ukraine and the Commander-in-Chief of the Armed Forces of Ukraine led to the creation of the Center for Innovation and Defense Technologies (Ministry of Defense 2021a). Among other things, the Center has been tasked to develop, test, and provide support for new software that meets the needs of the Armed Forces of Ukraine (Defense Express 2021).

The General Staff of the Ministry of Defense is responsible for military management and develops the country's defense plans. The General Staff is also in charge of strategic planning of the use of the Armed Forces of Ukraine and certain elements and resources of other parts of the Armed Forces. In addition, the Office for the Development of Automation has been set up within the General Staff. This office has been tasked to organize, coordinate, and execute efforts to advance automated defense solutions, create a unified automated control system, and advance the digitalization of Ukraine's Armed Forces (Ministry of Defense 2021b).

The Main Intelligence Directorate complements these activities with a focus on conducting intelligence operations relevant for capability development, military construction as well as cybersecurity and military-technical security (Verkhovna Rada 2020).

- *Ministry of Digital Transformation*

The Ministry of Digital Transformation implements the state's digitalization policy and is responsible for policies in robotics and AI. In 2020, the Ministry had established an Expert Advisory Committee on AI Development, whose goal is to enhance Ukraine's AI competitiveness. This committee, initially the only governmental body with AI expertise, played a significant role before the war. It focused on educational activities, organizing conferences and training sessions to educate military personnel and other agencies about AI applications relevant to their tasks. With the onset of the war, the Expert Advisory Committee shifted its focus to providing consulting support for various tasks. Additionally, some committee members joined the frontline, contributing directly to the defense efforts.

- *Ministry of Strategic Industries*

The Ministry of Strategic Industries is intended to manage the military-industrial complex with a focus on producing drones and robots and boosting Ukraine's indigenous missile program (Press Service of the Office of the Verkhovna Rada of Ukraine 2023).

Ukraine's organizational setup to advance defense AI evolves commensurate with the threat landscape that shapes and refines the country's defense AI understanding. As argued above, Ukraine's defense AI priorities have become more focused reflecting a maturing understanding of the benefits of AI on the battlefield. Nonetheless, as the war goes on, more emphasis will need to be put on how to synchronize the short cycles of battlefield adaptation, that quickly turn instant lessons identified into product upgrades, with the more medium and long-term cycles that look at the necessary changes of concept and capability development that are indispensable to sustain warfighting. This will also have an impact on defense AI governance and the role of coordinating entities that bring the decentralized group of stakeholders together to make sure that everybody understands, supports, and further develops the long-term defense AI priorities discussed above.

4 Funding Defense AI

According to the Stockholm International Peace Research Institute (SIPRI), Ukraine significantly increased its military spending in 2022 by 640% to USD44bn (Tarasovsky 2023a, b). For comparison, Russian military spending grew by 9.2% to USD86.4bn, which is 4.1% of its GDP (Radio Svoboda 2023). Especially as of 2023, Ukraine accelerated funding for AI development. However, due to the war, some program details cannot be disclosed:

- On 19 October 2023, Ukraine's Parliament approved the first reading of the 2024 state budget, allocating nearly UAH 56bn (USD1.5bn) for the Ministry of Strategic Industries (Minstrategprom 2023). The 2024 budget also provides UAH2.55bn (USD60M) for the Ministry of Digital Transformation's digitaliza-

tion, six times more than in 2023. The approved budget for 2024 includes an increase in funding for defense industry development, specifically for weapon production worth UAH51bn (USD1.3bn) as well as unmanned aerial, surface, and underwater systems worth UAH43.3bn (USD1.1bn) (Ministry of Finance 2023).

- BRAVE1 launched an AI startup funding program in 2023, awarding 84 defense tech grants worth USD1.53M for AI and other technologies. The platform aims to fund Ukrainian startups with over USD2M by the end of 2023. The 2024 budget foresees a significant increase of the budget to more than USD39M. As of late 2023, an average grant is about USD 5000–25,000, and in 2024, grants will reach amounts of USD50,000, USD100,000, and USD250,000 (TechUkraine 2023).
- The State Innovative Financial Credit Institution (State Innovative Financial Credit Institution Undated) systematically invests in innovative developments through competitions among universities, institutes, and other state structures. As of 2022, it started including AI projects in dual-use sectors, but specific data is not available.
- International VC Funds (Stojkovski 2023) are actively monitoring the Ukrainian market, as it serves as a testing ground for creating and testing new weapons, with the goal of investing or engaging on mergers and acquisitions (M&A). Among others, Ukrainian AI startup "Swarmer" secured funding from D3 Accelerator, a fund co-managed by Eric Schmidt. Swarmer's flagship product AI Copilot enables a single operator to fly a swarm of drones thus boosting battlefield capacities (Yarova 2023).
- In addition, international companies open local branches in Ukraine to speed up technology development initiatives. German drone manufacturer Quantum Systems, for example, attracted substantial funds with its recent Series B funding round and has decided to join the special economic zone in Diia City to shift parts of its production to Ukraine (Crumley 2023).

Overall, the funding infrastructure for defense innovations focused on AI in Ukraine is in its early stages, actively engaging in processes to establish international cooperation. Considering the high value of local players' experience, a wave of small and medium-sized M&A of Ukrainian developers by global defense market players is likely to occur within the next years.

5 Fielding and Operating Defense AI

Ukraine's AI defense ecosystem operates within a rapid development-to-deployment cycle, characterized by the integration of government and military efforts to recruit top engineering talent. This strategy offers engineers an alternative to frontline service, allowing them to contribute to defense projects in secure settings. The

approach indicates a strategic use of civilian expertise in military applications, balancing defense development needs with the protection of skilled personnel.

There's a notable cultural and operational shift as engineers and managers from the civilian IT sector adapt to the traditional military culture. This transition is significant, blending civilian technological expertise with military operational practices, which is essential for developing relevant and practical AI solutions.

A key feature of the ecosystem is the real-time combat testing of AI technologies. Unlike controlled environments, this rigorous testing allows for immediate feedback and rapid iteration, crucial for practical application and improvement of AI in military contexts. It underscores a focus on developing solutions that can withstand the dynamic and unpredictable nature of modern warfare.

However, the ecosystem faces challenges in system integration due to the diversity of systems and standards, affecting the speed and efficacy of AI implementation. This complexity points to a need for standardized protocols and integration strategies to streamline the process.

Many AI solutions, while showing promise, are still in their early developmental stages. This immaturity can lead to increased long-term operational costs, emphasizing the ongoing development, refinement, and investment required to fully realize the potential of these technologies. The ecosystem's characteristics reflect a strategic blend of civilian and military expertise, rapid adaptation in real-world scenarios, and the ongoing challenge of integrating diverse technologies into a cohesive defense strategy. Key projects and initiatives include:

- *Situational Awareness Solutions*

The Delta platform is a situational awareness and battlefield management system (Rosengren 2023). It consolidates information from various sources, including personnel, officials, sensors, and drones. This system is crucial for planning military operations, coordinating unit movements, and securely exchanging enemy location data. Delta was created at the Center for Innovation and Development of Defense Technologies of the Ministry of Defense. The platform is used by intelligence to recognize and identify objects such as enemy soldiers or military equipment. Delta played a pivotal role in destroying the Russian Cruiser "Moskva" in April 2022 (Krasnomovets 2022), as the system enabled the military command to assess the situation in a short period of time and decide to destroy the military target. The Delta system was created according to NATO standards and is compatible with similar situational awareness systems of NATO members (Dobrovolsky 2022).

"Kropyva" is another situational awareness system developed by the volunteers of "Army SOS." Based on target localization by drones, Kropyva provides fire supports to gunners by computing ballistic calculations. The system receives daily updates on frontline developments. The Ukrainian Army uses Kropyva in combination with other systems like GISArta and more (Melnyk 2022).

- *Data Set Collection Projects*

Students at the Ukrainian Catholic University's Faculty of Applied Sciences (APPS UCU) prepared a specific dataset for object recognition. Data is collected from open sources and can be used by experts to prototype and validate hypothesis (Applied Sciences Faculty of UCU Undated). Kaggle, another database of more than 50,000 public datasets such as equipment losses, for example, can be used for AI training (Kaggle Undated).

- *Disinformation and Bots*

With the help of AI, the Mantis analytics platform monitors and analyzes the information space to detect disinformation (Sobachynskyi 2023).

In sum, Ukraine's AI defense sector is rapidly evolving, marked by a shift towards accelerated development cycles and a focus on integrating advanced AI technologies into defense strategies. Defense AI and other novel defense solutions benefit in particular from

- easier access to combat data, which manufacturers need to negotiate with the government, to continually refine their products and train AI more effectively.
- the efforts of the Ministry of Defense to support a community-driven response to streamline the streamline certification processes that significantly reduce the time from an average year to just 1–2 months for drone certification.
- international companies that establish service and development centers in Ukraine, enabling quick resolution of issues and reduced maintenance time.
- the fact that key end-users are creating general requirements for defense solutions, providing clear long-term development objectives, and reducing market uncertainty.

6 Training for Defense AI

Amid the ongoing conflict with Russia, Ukraine's educational landscape has been significantly disrupted. The constant destruction of educational institutions and private residences, coupled with frequent power outages and the tragic loss of family members, have profoundly impacted the quality and accessibility of education. As of June 2023, Russian bombardments have damaged 3290 Ukrainian educational institutions, destroying 262 of them (Ministry of Education and Science 2023). This destruction accounts for about 10% of the country's educational infrastructure (Center for Economic Strategy 2023).

Despite these challenges, Ukraine trained over 7000 experienced AI developers as of 2022, with its education system producing about 27,000 science, technology, engineering, and mathematics (STEM) graduates each year. Before the full-scale invasion in 2022, AI education in Ukraine typically distinguished between civilian and defense applications. However, the onset of the war prompted a significant shift, with almost

all academic programs incorporating military-related components. This shift led to close collaborations between universities and the military sector on various projects.

A noteworthy aspect of Ukraine's educational response to the war has been the grassroots development of numerous training programs and courses, such as drone operations. These initiatives were often driven by charitable foundations and volunteers, rather than state funding. This approach reflects a unique, community-driven response to the urgent need for specialized training in war time.

Ukraine's higher education institutions, including the Ukrainian Catholic University, Taras Shevchenko National University of Kyiv, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv School of Economics, and American University Kyiv, have adapted their programs to meet these new challenges. These adaptations include offering courses and degrees in Data Science, machine learning, and AI that are increasingly tailored to address defense needs.

Given the destruction of the civilian education infrastructure, the military training ecosystem for drone pilots and users of systems like Delta and Kropyva has become even more important. The rapid development of these programs, primarily facilitated by volunteers, underscores the agility of Ukraine's response to the evolving demands of the war. Military units of the Air Defense Forces, for example, use a Virtual Reality (VR) simulator for military training. This synthetic training environment ensures a more effective preparation of pilots to shoot down enemy cruise missiles, drones, and aircraft (Press Service ODA 2023).

Based on current war experiences, Strata-22 has developed immersive multimedia platforms to train infantrymen, gunners, and tankers. Military operators learn how to handle weapons with the help of largescale models using VR glasses. This simulation environment is built according to NATO standards (Ossipova 2022). In addition, Ukrainian IT company Logics7 has created a universal training system for the fire training of Ukrainian military units. Right now, the system provides digital replicas of different weapon systems like the Next Generation Light Anti-Tank Weapon (NLAW), Javlin anti-tank systems, as well as Stinger and Ingla anti-aircraft systems (Pylypiv 2023). Finally, the war has also highlighted the effectiveness of AI laboratories established at universities, under the aegis of the Ministry of Digital Transformation and the AI Expert Committee. These labs have become instrumental in developing AI tools for wartime use.

In summary, the war has catalyzed a significant transformation in Ukraine's educational system. Traditional university programs have swiftly pivoted to focus on AI applications in military contexts. Meanwhile, the private sector and non-profit initiatives have stepped in to fill the immediate needs for specialized training and program development, demonstrating remarkable adaptability and resilience in the face of war.

7 Conclusion

War needs require Ukraine to focus on what works best on the battlefield while considering future warfighting requirements as well. This has prompted a clear focus on delivering the best solutions to the frontline and making sure to nurture the

talent pipeline for technology development. By contrast, ineffective concepts and burdensome procedures and regulation are pushed aside.

After 2 years of intensive war fighting, it becomes more and more obvious that Ukraine and Russia actively compete in enhancing existing defense solutions with AI and providing new AI-enhanced systems. Against this background, Ukraine is increasingly focusing on (Committee on AI of Ukraine 2023):

- investing in AI to enhance the autonomy and effectiveness of drones and robotic systems, in particular by enabling these systems to operate without GPS and engage adversarial drone systems;
- expanding the use of sophisticated sensors, including thermal and real-time satellite video feeds, thereby using for data analysis and data fusion to support decision-making for complex combat operations;
- developing fully autonomous systems to engage autonomous adversarial systems, thereby using AI to enhance autonomy;
- establishing new research and development centers to underline the government's commitment to advancing AI and other defense technologies;
- integrating AI into all levels of military operations, and
- making AI solutions more affordable to accelerate a broader and quicker adoption of defense AI by the country's Armed Forces.

It is important to note that in the ongoing war, Ukraine's defense AI solutions will be significantly improved thanks to continuous training based on battlefield experience and data. The Ukrainian AI ecosystem has evolved rapidly due to the war, transitioning from grassroots volunteer and commercial efforts to more organized government-backed initiatives and funding. This shift reflects the government's strategic commitment to leveraging AI for defense. The ecosystem now robustly incorporates R&D, academia, private sector collaboration, and significant government investment, focusing on dual-use technologies for military and civilian benefits. This approach underlines a comprehensive, multi-faceted advancement in AI capabilities driven by the urgency of war.

These advancements are also very likely to shape the future international discussion on the use of defense AI on the battlefield. In this regard, NATO countries should first monitor AI developments in Ukraine and Russia during the war and reflect upon the likely consequences for their own capability planning as well as R&D priorities. Second, it can be assumed that violent non-state actors will also closely follow this war and consider how to best benefit from defense AI. This prompts the need to reconsider how to prevent and limit the proliferation of AI-relevant technologies to non-state actors, which broadens the regulatory debate. Third, countries will also need to be aware that many of the existing data and privacy protection ideas are unfit for warfighting when the comprehensive collection, assessment, fusion, and sharing of public and private data might produce distinct advantages in fighting an adversary. Fourth, this should also lead to a more realistic understanding and reconceptualization of the "human in the loop" principle that will be essential for future certification standards as well defense AI compliance and verification regimes.

Finally, even advanced countries should not underestimate the benefits of crowdsourcing, open-source technology, decentralization, and volunteer efforts that tend to be overlooked in a more mature institutional environment. As these efforts have been crucial in Ukraine's early and ongoing defense efforts it would be worth analyzing how these efforts can infuse defense innovation elsewhere.

References

Aerorozvidka. Undated. https://aerorozvidka.ngo. Accessed 30 Jan 2024.

Applied Sciences Faculty of UCU. Undated. *Building a dataset for prototyping ideas for object detection*. https://apps.ucu.edu.ua/projects/stvorennya-naboru-danyh-dlya-prototypuvannya-idey-shhodo-vyyavlennya-ob-yektiv/. Accessed 30 Jan 2024.

Bondar, Kateryna. 2023. *Arsenal of democracy: Integrating Ukraine into the West's defense industrial*. Carnegie Endowment. https://carnegieendowment.org/2023/12/04/arsenal-of-democracy-integrating-ukraine-into-west-s-defense-industrial-base-pub-91150. Accessed 30 Jan 2024.

Boshnyakov, Ilya. 2023. D3 military tech accelerator is to launch in Ukraine. Ex-Google CEO Eric Schmidt is among the LPs. *ain.capital*. https://ain.capital/2023/05/11/d3-military-tech-accelerator-is-to-launch-in-ukraine-ex-google-ceo-eric-schmidt-is-among-the-lps/. Accessed 30 Jan 2024.

Brave1. Undated. https://brave1.gov.ua. Accessed 30 Jan 2024.

Cabinet of Ministers of Ukraine. 2020. *On the approval of the Concept for the development of artificial intelligence in Ukraine*. Order of the Cabinet of Ministers of Ukraine No.1556-p. https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text. Accessed 30 Jan 2024.

———. 2021. *On the approval of the action plan for the implementation of the concept for the development of artificial intelligence in Ukraine for 2021-2024*. Order of the Cabinet of Ministers of Ukraine No. 438-p. https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text. Accessed 30 Jan 2024.

———. 2023. *On making amendments to the Regulation on the Ministry of Digital Transformation of Ukraine*. Order of the Cabinet of Ministers of Ukraine No. 916. Ligazakon.ua; https://ips.ligazakon.net/document/MN027216?hide=true. Accessed 30 Jan 2024.

Centre for Economic Strategy. 2023. *10% of Ukraine's educational infrastructure was damaged by Russian shelling. How much damage has Russia caused to Ukrainian education?* https://ces.org.ua/en/10-of-ukraines-educational-infrastructure-was-damaged-by-russianshelling-how-much-damage-has-russia-caused-to-ukrainian-education/. Accessed 30 Jan 2024.

CNA. 2022. *Artificial intelligence and autonomy in Russia*. Special Issue. https://www.cna.org/Newsletters/Ai%20and%20Autonomy%20in%20Russia/AI-and-Autonomy-in-Russia-Special-Issue-September-2022.pdf. Accessed 30 Jan 2024.

Committee on AI of Ukraine. 2023. *Regarding critical development priorities of artificial intelligence technologies in the field of security and defense of Ukraine*. https://ai.org.ua/wp-content/uploads/2024/01/criticaldevelopment-prioritiesinAI-1.pdf. Accessed 30 Jan 2024.

Crumley, Bruce. 2023. *Quantum-Systems' Ukraine drone, enterprise tech attracts $63M in Series B funding*. Drone DJ. https://dronedj.com/2023/10/25/quantum-systems-ukraine-drone-enterprise-tech-attracts-63m-in-series-b-funding/. Accessed 30 Jan 2024.

Defense Express. 2021. *The Ministry of Defense will create an Innovation Center, its own 'light analog' of the American DARPA*. Defense Express. https://defence-ua.com/news/minoboroni_stvorit_tsentr_innovatsij_svij_vlasnij_lajt_analog_amerikanskoji_darpa-4975.html. Accessed 30 Jan 2024.

Denisova, Kateryna. 2023. *Griselda. A system of intelligence based on artificial intelligence has been developed in Ukraine*. NV. https://nv.ua/ukr/ukraine/events/v-ukrajini-na-bazi-shtuchnogo-intelektu-rozrobili-sistemu-rozvidki-50362114.html. Accessed 30 Jan 2024.

Dobrovolsky, Vadim. 2022. *Ukraine showed NATO a unique battle management and enemy surveillance system*. Speka. https://speka.media/ukrayina-pokazala-nato-unikalnu-sistemu-stezennya-za-protivnikov-9g1zd9. Accessed 30 Jan 2024.

Expert Committee on the Development of Artificial intelligence in Ukraine under the Ministry of Digital Transformation of Ukraine. 2023. http://ai.org.ua. Accessed 30 Jan 2024.

Flyer One Ventures. Undated. https://flyerone.vc/. Accessed 30 Jan 2024.

Fontes, Robin, and Jorrit Kamminga. 2023. Ukraine a living lab for AI warfare. *National Defense Magazine*. https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare. Accessed 30 Jan 2024.

Goncharuk, Vitaliy. 2020. *War in Ukraine: AI weapons and the debate over 'Human in the Loop'*. Medium. https://vactivity.medium.com/war-in-ukraine-ai-weapons-and-the-debate-over-human-in-the-loop-ba2e48a97390. Accessed 30 Jan 2024.

Ignatius, David. 2022. How the algorithm tipped the balance in Ukraine. *The Washington Post*. https://www.almendron.com/tribuna/how-the-algorithm-tipped-the-balance-in-ukraine/. Accessed 30 Jan 2024.

Kaggle. Undated. *2022 Russia Ukraine War*. Dataset. https://www.kaggle.com/datasets/piterfm/2022-ukraine-russian-war. Accessed 30 Jan 2024.

Kahn, Jeremy. 2022a. A.I. is on the frontlines of the war in Ukraine. *Fortune*. https://fortune.com/2022/03/01/russia-ukraine-invasion-war-a-i-artificial-intelligence/. Accessed 30 Jan 2024.

Kahn, Lauren. 2022b. How Ukraine is remaking war. Technological advancements are helping Kyiv succeed. *Foreign Affairs*. https://www.foreignaffairs.com/ukraine/how-ukraine-remaking-war. Accessed 30 Jan 2024.

Kolomychenko, Tetiana. 2023. "Army of drones:" How private drone manufacturers "master" the defense budget. *Biznes Tsenzor*. https://biz.censor.net/r3448681. Accessed 30 Jan 2024.

Konaev, Margarita. 2023. *Tomorrow's technology in today's war: The use of AI and autonomous technologies in the war in Ukraine and implications for strategic stability*. CNA. https://www.cna.org/reports/2023/10/Use-of-AI-and-Autonomous-Technologies-in-the-War-in-Ukraine.pdf. Accessed 30 Jan 2024.

Krasnomovets, Pavlo. 2022. 'Neptune' struck 'Moscva.' How the Ukrainian missile system paid itself off tenfold. *Forbes*. https://forbes.ua/inside/neptun-uraziv-moskvu-yak-ukrainskiy-raketniy-kompleks-okupiv-sebe-desyatikratno-14042022-5449. Accessed 30 Jan 2024.

Melezhik, Tetiana. 2022. *Ukrainian volunteers and funds that help the country the most during the war*. TSN. https://tsn.ua/ukrayina/top-volonteriv-ta-fondiv-yaki-zaluchili-naybilshe-groshey-dlya-shvidshoyi-peremogi-ukrayini-2181787.html. Accessed 30 Jan 2024.

Melnyk, Taisa. 2022. Stinging "Nettle." How Ukrainian software for artillery affects the course of the war. *Forbes*. https://forbes.ua/innovations/zhalyucha-kropiva-yak-ukrainske-programne-zabezpechennya-dlya-artileristiv-vplivae-na-khid-viyni-22072022-7054. Accessed 30 Jan 2024.

Ministry of Defense. 2021a. *Automation Development Department*. https://www.mil.gov.ua/ministry/struktura-generalnogo-shtabu/upravlinnya-rozvitku-avtomatizaczii.html. Accessed 30 Jan 2024.

———. 2021b. *The Ministry of Defense has established the Center for Innovation and Defense Technologies: the relevant joint Directive was signed by the Minister of Defense of Ukraine and the Commander-in-Chief of the Armed Forces of Ukraine*. https://www.mil.gov.ua/special/news.html?article=64623. Accessed 30 Jan 2024.

Ministry of Digital Transformation. 2023a. *Incredible Tech: Investors guide to Ukrainian IT*. https://itukraine.org.ua/files/ITIGUIT.pdf. Accessed 30 Jan 2024.

———. 2023b. *Roadmap for the regulation of artificial intelligence in Ukraine*. https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%94%D0%BE%D1%80%D0%BE%D0%B6%D0%BD%D1%8F_%D0%BA%D0%B0%D1%80%D1%82%D0%B0_%D0%B7_%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%A8%D0%86_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96_compressed.pdf. Accessed 30 Jan 2024.

Ministry of Digital Transformation of Ukraine. 2023. *Ukraine signed an international declaration dedicated to the safety of using AI*. Kmu.gov.ua. https://www.kmu.gov.ua/news/ukraina-pidpysala-mizhnarodnu-deklaratsiiu-prysviachenu-bezpetsi-vykorystannia-shi. Accessed 30 Jan 2024.

Ministry of Education and Science. 2023. *Education in emergency*. https://saveschools.in.ua/en/. Accessed 30 Jan 2024.

Ministry of Finance. 2023. *Verkhovna Rada of Ukraine adopted the state budget for 2024*. Government Portal. https://www.kmu.gov.ua/news/verkhovna-rada-ukrainy-pryiniala-derzhbiudzhet-na-2024-rik. Accessed 30 Jan 2024.

Minstrategprom. 2023. *The draft budget-2024 provides for almost 56 billion UAH for the development of the defense industrial complex in Ukraine*. https://www.kmu.gov.ua/news/na-rozvytok-opk-v-ukraini-proektom-biudzhetu-2024-peredbacheno-maizhe-56-mlrd-hrn. Accessed 30 Jan 2024.

Ossipova, Viktoriia. 2022. *We reduced the cost of training a soldier by at least 30 times. The developer of Strata 22 on how the Armed Forces of Ukraine are acquiring combat skills in AR and VR. DOU*. https://dou.ua/lenta/interviews/multimedia-systems-for-military-training/. Accessed 30 Jan 2024.

Oxford Insight. 2020. *The Government AI Readiness Index 2020*. https://oxfordinsights.com/wp-content/uploads/2023/11/AIReadinessReport.pdf. Accessed 30 Jan 2024.

President of Ukraine. 2021. *On the strategy of military security of Ukraine*. Decree of the President of Ukraine No. 121/2021. President.gov.ua. https://www.president.gov.ua/documents/1212021-37661. Accessed 30 Jan 2024.

Press Service ODA. 2023. *Air Defense Forces 'West' received a VR simulator for practicing the skills of destroying enemy aerial targets*. LOVA. https://loda.gov.ua/news/57059?fbclid=IwAR1hnl-kdPGUCkLAB1fsR22kFQcs1SvrJPQTAHGWTwX55jMrr6kPJBrMoew. Accessed 30 Jan 2024.

Press Service of the Office of the Verkhovna Rada of Ukraine. 2023. *Minstrategprom was conceived as a powerful center for coordinating industrial policy and the military-industrial complex - Dmytro Kysilevsky*. Verkhovna Rada of Ukraine. https://www.rada.gov.ua/news/news_kom/234613.html. Accessed 30 Jan 2024.

Pylypiv, Ihor. 2023. *Drones at sea and on land, artificial intelligence and the Javelin simulator: how military-tech developments bring Ukraine closer to victory. The EP talks about projects that help the Defense Forces beat the enemy. Which of them are already working to win? Economic truth*. https://www.epravda.com.ua/rus/publications/2023/07/5/701912/. Accessed 30 Jan 2024.

Radio Svoboda. 2023. *SIPRI: Ukraine's military spending in 2022 increased by 640% of GDP compared to 2021*. https://www.radiosvoboda.org/a/news-viiskovi-vydatky-ukraina-sipri/32376625.html. Accessed 30 Jan 2024.

Rosengren, Oscar. 2023. *Network-centric warfare in Ukraine: The Delta System*. Grey Dynamics. https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/. Accessed 30 Jan 2024.

Saballa, Joe. 2023. Ukraine's 'Army of Drones' destroys 200 Russian targets in one week: Minister. *The Defense Post*. https://www.thedefensepost.com/2023/09/14/ukraine-drones-russian-targets/. Accessed 30 Jan 2024.

Serhiy Prytula Charitable Foundation. Undated. *Official Site*. https://prytulafoundation.org/. Accessed 30 Jan 2024.

Skorobogatova, N.Ye., and Yu.V. Kalko. 2016. Development of a strategy for forming the export potential of Ukrainian aviation enterprises on the example of the state enterprise 'Antonov'. *Effective Economy* 11. http://www.economy.nayka.com.ua/?op=1&z=5247. Accessed 30 Jan 2024.

Sobachynskyi, Rostyslav. 2023. Ukrainian-made AI platform Mantis Analytics detects Russian fakes in the news. *AIN*. https://ain.capital/2023/09/15/ukrainian-mantis-analytics-detects-russian-fakes/. Accessed 30 Jan 2024.

State Innovative Financial Credit Institution. Undated. https://sfii.gov.ua. Accessed 30 Jan 2024.

State Kyiv Design Bureau 'Luch'. Undated. *Official website*. https://www.luch.kiev.ua/ukr/. Accessed 30 Jan 2024.
Stojkovski, Bojan. 2023. *The Recursive*. https://therecursive.com/can-ukraine-become-the-silicon-valley-of-defense-tech/. Accessed 30 Jan 2024.
Tarasovsky, Yuriy. 2023a. Grants worth millions of dollars, hundreds of events, and projects. The Ministry of Digital Transformation showed the results of the work of the startup fund. *Forbes*. https://forbes.ua/news/granti-na-milyoni-dolariv-sotni-iventiv-ta-proektiv-mintsifri-pokazalo-rezultati-roboti-fondu-startapiv-11072023-14732. Accessed 30 Jan 2024.
———. 2023b. Ukraine's military spending increased by 640% in 2022, to 34% of GDP – SIPRI. *Forbes*. https://forbes.ua/news/viyskovi-vitrati-ukraini-zosli-na-640-u-2022-rotsi-do-34-vvp-sipri-24042023-13245. Accessed 30 Jan 2024.
TechUkraine. 2023. Ukraine's Defense Tech Cluster BRAVE1 Plans to Invest $39M in Startups in 2024. *TechUkraine*. https://techukraine.org/2023/11/30/ukraines-defense-tech-cluster-brave1--plans-to-invest-39m-in-startups-in-2024/. Accessed 30 Jan 2024.
The Innovation Development Accelerator. Undated. http://mil-tech.gov.ua/en. Accessed 30 Jan 2024.
The Innovation Development Accelerator. Undated. https://mil-tech.gov.ua/en/aboutaccelerator. Accessed 30 Jan 2024.
Ukraine Defense Fund. Undated. *Official Site*. https://ukraine defense fund.org/. Accessed 30 Jan 2024.
Ukrainian Startup Fund. Undated. https://usf.com.ua/#usf-sc-2. Accessed 30 Jan 2024.
Ukroboronprom. Undated. *About the company*. https://ukroboronprom.com.ua/en/pro-koncern. Accessed 30 Jan 2024.
Verkhovna Rada of Ukraine. 2020. *On intelligence*. Law of Ukraine. https://zakon.rada.gov.ua/laws/show/912-20#n73. Accessed 30 Jan 2024.
———. 2023. *Agreement between Ukraine and the European Union on Ukraine's participation in the European Union program "Digital Europe" (2021–2027)*. Law of Ukraine No. 2926-IX. Zakon.rada.gov.ua; https://zakon.rada.gov.ua/laws/show/984_005-22#Text. Accessed 30 Jan 2024.
Yarova, Maia. 2023. Ukrainian AI startup Swarmer secures funding from D3 Accelerator. *ain.capital*. https://ain.capital/2023/11/16/ukrainian-swarmer-secures-funding-from-d3/. Accessed 30 Jan 2024.
Zysk, Katarzyna. 2023. *High hopes amid hard realities*. Defense AI in Russia. Defense AI Observatory. https://defenseai.eu/daio_study2311. Accessed 30 Jan 2024.

Embracing the Organized Mess: Defense AI in Israel

Inbar Dolinko and Liran Antebi

Israel has emerged as a prominent player in the field of artificial intelligence (AI), particularly in the realm of defense and security. The role of this technology goes beyond its traditional defensive functions and extends to its impact on the Israeli economy and its reputation on the global stage. To utilize AI's full potential, Israel must face both common and distinct challenges.

Some unaddressed challenges have led to deterioration in Israeli leadership; most notably are the challenge of competing in a fiercely aggressive global race for dominance in the field of AI, without a proper national strategy or budget and central management to support it. Israel's relative smallness and limited resources available for AI can be considered additional limiting factors. Despite its shortcomings, the country is still among the most advanced in the field of defense AI, relaying on the Israeli ecosystem's distinctive advantage, born out of structural and organizational aspects.

Mandatory and reserve services at the Israeli Defense Forces (IDF) nurture and facilitate a unique exchange of personnel and knowledge. Moreover, IDF units, such as Unit 8200 and LOTEM, the unit for Operational Technological Intensification, indirectly support the AI ecosystem by supplying skilled personnel to academia and industry. These processes create a trained and familiar talent pool and enable collaborative AI development in Israel, involving the Israel Ministry of Defense

This paper has been finalized in June 2023. It has been shortened for publication but not updated in the aftermath of the attack on Israel on 7 October 2023.

I. Dolinko
Independent Researcher and Consultant, Tel Aviv, Israel

L. Antebi (✉)
Advanced Technologies and National Security Program, Institute of National Security Studies, Tel Aviv, Israel

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_18

Directorate of Defense Research & Development (IMOD DDR&D), the defense industry, academia, and civil companies.

Currently, there is no single Israeli body responsible for overseeing the field of defense AI. Nonetheless the Ministry of Defense (IMOD) and Israel Innovation Authority are shaping it by launching several key initiatives aimed at improving the necessary infrastructure and enabling further advancement in defense AI. For example, the Israel Innovation Authority, IMOD DDR&D, and the Ministry of Innovation, Science and Technology have together set up the National Natural Language Processing Plan. This initiative specifically focuses on tackling the unique challenges posed by Semitic languages like Hebrew and Arabic in the context of developing Natural Language Processing (NLP) models. In addition, bottom-up initiatives and organizational changes are being made to support defense and security-related AI applications in Israel. For instance, in 2023, a new directorate was established at IMOD DDR&D focusing on innovative technologies, including AI. The IDF is also creating new units and roles that leverage AI's immediate operational value in combat contexts and everyday needs.

Israel's investment in AI for defense and security purposes is challenging to quantify due to the lack of transparency regarding its defense budget. However, the significance of investing in AI has been recognized, resulting in the allocation of NIS550M (around 140 million euros) to several critical projects.

Throughout the years Israel's leading position in defense AI has emerged from the ongoing security challenges it faces, requiring the Israeli security and defense establishment, defense industry of Israel, and academia to stay alert and continuously evolve, and as a result contributing to its rapid advancement. Israel's implementation of AI extends beyond its traditional areas of expertise, such as unmanned military systems, air defense, and cyber warfare. Its prowess in AI for intelligence is evident in its diverse range of applications, which have contributed significantly to its military successes in recent operations, for example, against Hamas in Gaza.

Despite notable progress and achievements, Israel's approach to defense AI is the result of an "organized mess," triggered by Israel's informal culture, the country's tendency to let market forces push technology forward, a demanding security environment, and the need to be able to respond to new threats in a quick and flexible manner. This approach has yielded benefits in the past and enabled Israel to become a prominent player in various technology fields. However, as the international competition for defense AI (and AI in general) grows, Israel should adopt a more robust approach to extend its leading role. In so doing, overcoming the "organized mess" with the help of a more institutionalized set up and the definition of a comprehensive national plan, oversight and budget would be important steps into the right direction.

1 Thinking About Defense AI

1.1 Definition of AI

As in many other countries and organizations around the world, Israel has struggled to formulate one encompassing definition for AI. Furthermore, the country tends to let market forces push technology forward, which means formal definitions sometimes follow practice. Nevertheless, a few definitions have been suggested by Israeli governmental agencies, due to the increasing role of AI in all areas of life and defense specifically.

One definition can be found in the recommendations of the TELEM forum (National Infrastructure for Research and Development) for a national AI strategy:

> A machine or system that performs tasks that usually require human thinking, such as understanding natural language, learning behaviors or problem solving. There is a wide range of such behaviors, but most involve computers running algorithms, which are often based on data (Committee for the Advancement of AI and Data Science 2020: 16).

Furthermore, the definition recognizes the acceleration of the field due to "technological, algorithmic and computational advancements, and due to the availability of big data" (Committee for the Advancement of AI and Data Science 2020: 16). Another definition can be found in a recent publication by the Ministry of Innovation, Science and Technology—a draft detailing principles, regulations, and ethics for AI. The writers distinguish between two types of common definitions for AI: technical ones, which focus on AI's capabilities and the methods to achieve those, and practical ones, which compare AI's abilities to those of humans. The ministry offers the following definition for the purpose of the publication:

> The field of AI is a general name for development in the field of information and communication technologies and data science that enables decision-making, making predictions, or performing actions by a computer at a high level of independence, in a way that simulates or is able to replace human intelligence (Ministry of Innovation, Science and Technology 2022).

Both definitions are broad, touching briefly on technical aspects and emphasizing AI's independence. AI is perceived as a versatile tool that can replace humans in a variety of tasks. The underlining approach allows for flexibility and does not require frequent updates depending on technological advancement. This is important due to the nature of AI as a dynamic emerging technology that affects all dimensions of warfare.

1.2 The Role of AI in Israel

Technology is holding critical importance to Israeli defense and security, ever since the days when Israel's first prime minister, David Ben-Gurion, shaped the foundations of the country's "Security Concept." As a small state with few natural resources and many defense and security challenges, Israel has always focused on cultivating its technological edge to maintain its economic, international, and security status. With AI being a general-purpose technology that impacts every aspect of life, including defense, as well as enabling many opportunities, it appears to be an essential technology for Israel (Antebi 2021).

The global "competition for superiority" that has been increasingly shaping all technology areas including AI also influences Israel. This competition impacts the global balance of power, countries' standing, and their ability to operate in the international arena. Israel is affected by this competition both in "hard" military aspects such as military force buildup, battlefield capabilities, and counterterrorism capabilities counterterrorism; as well as in "soft" aspects such as the export of civilian and military technologies that affect the economy, jobs in the economy, and the ability to employ soft power in the international arena.

Hence, AI has been recognized as a crucial technology for Israel's economy, not just in defense. Israel was an early leader in this field compared to many other countries, as reflected in its industry, defense, and academia. However, there was no proper national strategy or budgeting to support this, as will be discussed below. Israel's leadership in AI has diminished in the past few years due to various reasons. One reason is the challenge of competing in a fiercely aggressive global race for dominance in the field, without a proper national strategy or budget and central management to support it. In addition, Israel's relative smallness and limited resources available for AI can be considered additional limiting factors.

Nonetheless, Israel is ranked fifth on the 2023 Global AI Index, which is reflected in different benchmarks (Tortoise Media n.d.). The number of start-ups active in the field of AI, for example, has risen in recent years. According to Start-Up Nation Central, as of March 2023, there are 2039 Israeli companies focusing on AI as a core technology (out of 6995 active start-ups registered in the database) (Start-Up Nation Central n.d.-a). Additionally, many international companies have established R&D centers in Israel. Furthermore, in academia, the number of academic publications on AI has been on the rise over the last decade, based on OECD data (OECD. AI Policy Observatory n.d.). In 2018, a study identified 273 Israeli researchers specializing in AI and its related fields such as natural language processing (NLP), computer vision, and big data, across various academic institutions (Samuel Neaman Institute for National Policy Research 2018).

The vibrant business and research environment has helped establish a well-functioning ecosystem, in which the Israeli defense and security establishment works closely with local institutes and companies. The Israeli academia contributes to the development of AI research, while the leading industries and giant technological companies establish research centers and work alongside thousands of

innovative startups. Moreover, the Israeli defense and security establishment has undergone impressive development, especially for military intelligence and operational activities. Several factors explain close public-private cooperation in Israeli ecosystems (Antebi 2021):

- *Familiarity*

Connections between academia, the civil–commercial industry, and the defense and security establishment emerge quickly at the organizational, social, and professional level. There is a great sense of familiarity, which fosters innovation and creativity.

- *Proximity*

The short physical distance between a significant number of regional technology clusters and Israel's government as well as defense and security centers facilitate strong cooperation.

- *Culture*

As Israel faces many defense and security challenges, many professionals both in academia and industry, have a sense of "partnership of fate," encouraging their collaboration with defense and security agencies, especially the IMOD and the IDF. Moreover, an open and entrepreneurial character of Israeli culture (in comparison to countries where it is more hierarchical and bureaucratic) help move ideas and gain achievements.

- *IDF Service Model*

The IDF is composed of mandatory service personnel, professionals from the standing army, and military reserves. As a result of this interaction, knowledge is exchanged from different sources and at different stages of a professional career—in the industry, academia, or defense and security establishment. By working together, the three pillars can remain up to date on the advances in the field and leverage each other's strengths. Furthermore, military experience of Israeli academics and industry professionals enhances their ability to contribute to civilian roles through familiarity with defense and security needs and system operations.

To sum up, Israel's unique ecosystem has contributed to its impressive achievements in the field of AI and has helped position the country as one of the global leaders in this rapidly growing field, despite the erosion of its leadership.

1.3 Defense Opportunities and Concerns

Israel acknowledges the immense potential of utilizing defense AI, just as it has successfully done with cyber technologies and unmanned aerial vehicles (UAVs) in the past. AI is viewed as a versatile and empowering technology that can greatly augment Israel's capabilities. It has the ability to revolutionize various aspects such

as logistics and command and control systems, while also enhancing fields in which Israel has already established significant expertise. Leadership in AI has a profound impact on Israel's economy, international standing, and defense capabilities.

Despite the benefits and opportunities, challenges remain. Technological challenges and scarce human capital are two challenges that are of particular relevance for Israel.

1.3.1 Technical Challenges

AI presents numerous technical challenges. Historically, the military has led technological development, and many of these innovations have later been adopted for civilian use. However, nowadays, the private sector has taken the lead in developing new technologies, with the military adapting them for their purposes. Adapting AI algorithms to the military context can be challenging due to differences in training data, environments, and standards. These differences can impact the algorithm's performance and safety and make it difficult to utilize commercially available AI in the defense sector.

One specific technical challenge stem from semitic language and has direct consequence for using AI techniques like Natural Language Processing (NLP). NLP focuses on enabling computers to comprehend human languages and perform tasks such as speech recognition, natural-language understanding, and natural-language generation. In the past year, NLP has gained significant traction due to advancements like ChatGPT and demonstrates impressive progress in English and Indo-European languages. However, the progress in Semitic languages, such as Hebrew and Arabic, is much slower. As these are Israel's two national languages and Semitic languages play an important role in its intelligence efforts, there is a need for advancement in this field. Therefore, the Israel Innovation Authority, IMOD DDR&D, and the Ministry of Innovation, Science and Technology have together set up the National NLP Plan (The State of Israel n.d.-a). The plan proposes multiple approaches to tackle the challenges in Semitic language NLP. This includes initiatives such as establishing language corpora, facilitating access to Hebrew and Arabic datasets; developing generic NLP algorithms for Semitic languages; training a comprehensive language model rooted in Semitic linguistics. The aim is to enhance accessibility and adaptability of these capabilities using open-source infrastructure when possible, catering to diverse applications.

1.3.2 Human Capital

Due to its small size and limited resources, Israel faces challenges in competing with global AI leaders like the US and China in terms of funding and talent pool. The country's smaller GDP means it cannot allocate the same level of funding to national AI efforts. Recruiting and retaining skilled personnel capable of developing, adapting, and implementing AI systems for military and national security

purposes is challenging due to intense competition from the private sector, which provides more favorable employment conditions. While Israel's economy benefits from a flourishing private sector, competition on human capital challenges the ability of the Israel defense and security establishment to retain skilled professionals. Additionally, confidentiality and compartmentalization requirements limit the ability of personnel to move between defense organizations. Therefore, it becomes difficult to establish a career path that will encourage qualified individuals to stay in government service.

Additional concerns complement these two key challenges. These include, among other aspects, the requirement for explainable AI, ethical considerations regarding AI, bias and fake news in the defense environment, and the impact of AI on the pace of war and operations (Antebi 2021). The IDF and IMOD have not publicly disclosed their position on these matters. The only public document on AI ethics in Israel, published by the Ministry of Innovation, Science, and Technology, suggests that Israel aims to align its ethical standards with those established by other prominent nations, rather than taking a leading role in this domain.

2 Developing Defense AI

The research and development of AI in Israel is the result of a collaborative effort among the IMOD DDR&D, the defense industries, and academia as well as startup companies, as elaborated in the preceding chapter. Below we discuss several defense AI R&D projects that exemplify how the relevant stakeholders contribute at different levels of the national ecosystem.

Despite delivering successful defense AI applications, the lack of national funding and appropriate institutional provisions to plan and execute defense AI projects is a serious shortfall. This shortfall constitutes one of the biggest hurdles Israel will need to address in the future.

2.1 Ecosystem Cooperation

Two particular examples illustrate how ecosystem partners cooperate to provide and advance defense AI capacities in Israel:

- *MAFAT Challenge*

This challenge[1] organized by DDR&D includes a series of prize competitions in the field of data science that are open to the public, academia, and industry. It aims at

[1] A challenge is a common high-tech industry practice, allowing companies to quickly find solutions to problems, identify qualified human capital, and sometimes support certain communities and social goals.

exploring "the potential of advanced data science methods to improve and enhance IMOD current data products. The winning method may eventually be applied to real data and the winners may be invited to further collaborate with IMOD on future projects" (Ministry of Defense n.d.). As of April 2023, one challenge is ongoing, three challenges were completed, and another three are planned (Ministry of Defense n.d.).

- *Projects Stargate and Startrack*

Out of ten planned projects these two focus on developing and using AI tools for intelligence. They include participants from Israeli startups, the Israeli defense industry, and academics. They are joined by soldiers from the Israeli Military Intelligence Directorate, the Israeli Computer and IT Directorate, the Israeli Ground Forces, the Israeli Air Force, and soldiers from Project "See Far," that enable young people on the autistic spectrum to join the IDF. This collaboration allows the quick development of AI tools tailored specifically to the IDF's needs (Cohen 2019).

2.2 IDF Contribution

Inside the IDF, specialized units work on defense AI research and development. These include Unit 8200 and Unit 81 in the Israeli Military Intelligence Directorate and LOTEM, the unit for Operational Technological Intensification in the Israeli Computer and IT Directorate. Tools are developed to serve the needs of these units, as well as other users within the IDF. The newly established Information and Artificial Intelligence Division in the Computer and IT Directorate utilizes the large amount of data in the IDF to conduct meaningful operational projects that benefit other departments. One such project is a system that warns soldiers in the Western Negev of threats from anti-tank missiles from the Gaza Strip. Another project uses algorithms that recognize suspicious patterns in the field and prioritize videos for human observers in Division 210 on the Israel-Syria border (Bohbot 2023).

Furthermore, some new units and roles are being established to accommodate needs arising from the use of big data in defense. The Analytics Lab of Shahar Unit—a cooperation between the Computer and IT Directorate and the Personnel Directorate—is a notable example of this process. In the lab, the first of its kind, data analysts and researchers use AI and machine learning models to recognize patterns and predict needs of the IDF's manpower. The analysts and researchers are soldiers with a relevant background who undergo special training. Three notable research projects include predicting the likelihood of soldiers extending their service, identifying potential outstanding commanders early on, and creating personalized training programs for combatants to prevent injuries (Greenberg-Cohen 2021).

In addition, each year, hundreds of experienced soldiers enter the technological ecosystem at existing companies or as founders of new AI startups. This process reinforces the capabilities and capacities of the Israeli tech industry as a whole (Lt. Col. G., Major G., and Major L. 2021). A notable example is Unit 81 as one hundred

graduates of this unit have established about fifty companies from between 2003 and 2010. Some of them, such as Innoviz and D-Fend, offer solutions used for defense (Shulman 2021). The startup Exodigo was also founded by Unit 81 graduates, who won the Israel Security Award during their service. This startup developed a system combining a drone, ground sensors and AI to map in 3D what is happening underground (Alxalsi 2022).

2.3 Industry Contribution

Several prominent projects were developed by the Israeli Defense companies. One example is CARMEL, the future Ground Combat Vehicle (GCV) of the IDF, which is being developed by ELTA systems, a subsidiary of Israel Aerospace Industries (IAI). The CARMEL program will improve the GCV's AI, autonomous, and automatic capabilities for future combat scenarios, urban maneuvering, and operating with only two soldiers (The Marker 2021). Another example is SOI ("Standoff In"), a secret project in development by the IAI. This program uses unmanned air and ground vehicles that are controlled from a safe distance to protect Israeli soldiers during combat.

Most Israeli defense industry projects cater to Israel's own needs, but part of the systems emerging from national projects are sold to other countries as well. For instance, Elbit's Seagull system, an unmanned surface vessel, has been sold to a state in East Asia. It is believed that the system incorporates AI capabilities to facilitate its operation. This suggests that defense industries generate revenue and contribute to AI development through international collaborations. However, information on budgeted defense AI collaborations between Israel and its key partners, like the USA, remains scarce, indicating a high level of secrecy in the field (Frantzman 2022).

3 Organizing Defense AI

Right now, Israel has no single body to guide the development and use of AI in general and for specific defense and military purposes. However, several significant organizations are involved in leading and funding the field, including the IMOD and Israel Innovation Authority, which is affiliated with the Ministry of Innovation, Science and Technology.

Over the past few years, several committees have been established to address the organization of the AI field in Israel. These committees have recognized the importance of AI in defense and security matters. However, due to political instability, the matter has not been fully prioritized or budgeted.

Consequently, a new program has been established which focuses on national infrastructure related to AI. The program operates through the Ministry of

Innovation, Science and Technology, though it may encounter difficulties in asserting authority over other government ministries. Despite this, IMOD DDR&D maintains strong relationships with academic institutions and the defense industries in R&D. At the same time diverse AI initiatives led by academia, industry, and the military continue to emerge.

These new AI initiatives are primarily focused on enhancing the country's defense capabilities through the development of advanced technologies, including autonomous systems, cybersecurity, and intelligence gathering and processing. The IDF, in collaboration with IMOD, leads most of these programs, which are designed to serve all branches of the IDF, including the Israeli Ground Forces, Navy, and Air Force. However, some specific projects are developed and managed independently inside the forces themselves.

Over the past several years, the widespread use of AI has led to a growing recognition among high-ranking officials in the IDF and the IMOD that data is a critical asset, much like traditional weapons. This shift in mindset has significant implications for how the military operates in regard to data. Given the abundance of advanced technology available, there are significant opportunities to fully leverage its potential. Therefore, the IDF and IMOD must adopt proactive strategies to harness these opportunities (Maariv Online 2022).

Consequently, the IDF is undertaking significant efforts to promote connectivity and knowledge sharing among its various units. These projects are designed to facilitate collaboration, enhance communication, and streamline the exchange of information, ultimately improving the effectiveness and efficiency of the IDF's operations (Tzafarir 2021).

Israel's focus on digital transformation has led to the announcement of Project Nimbus, aimed at establishing national cloud centers. The IDF is a key participant in this project, and Amazon AWS and Google Cloud have won the bid to set up and operate the project. It is a state tender at an investment of roughly NIS4bn (around 1 billion euros) (Ziv 2021). This initiative reflects a commitment to enhancing the country's technological capabilities and promoting innovation in the public sector, including within the IDF (Berkowitz/Levy-Weinreeve 2021).

In addition, the IDF's technology units also adopt a civilian tech sector mindset and approach. This involves building a collaborative environment where researchers from diverse backgrounds cooperate towards achieving a common goal. This fosters an environment that functions more like an incubator, putting a premium on continuous improvement and constant development to deliver "products" rather than "projects." This approach propels R&D to a new level needed to successfully compete in the ever-evolving technological landscape (Bohbot 2018).

Furthermore, the IMOD is also implementing significant organizational changes to retain its leadership role on defense AI. In February 2023, Major General (MG) (ret.) Eyal Zamir, the new director general of the IMOD announced the establishment of a dedicated administration within IMOD DDR&D to focus specifically on the development of future technologies. The aim of this initiative is to position Israel as the "world's leader in futuristic technologies." The new administration will oversee the development of AI technologies in Israel and provide the necessary

management to ensure their progress and contribution to the country's advancement (Azoulai 2023).

In line with this effort, MG (ret.) Zamir also recently addressed the 2023 Herzliya Conference to unveil a new multi-year plan, a strategic initiative aimed at enhancing Israel's military capabilities. Highlighting the significance of AI, Zamir emphasized its potential to revolutionize Israel's intelligence and targeting systems. He argued that by harnessing AI technologies, including group and swarm operations and independent combat systems, Israel aims to gain a significant advantage on the battlefield. In conjunction with this plan, the Defense Ministry will establish a dedicated organization focused on AI and robotics, operating under the DDR&D. Zamir also announced a substantial increase in the defense R&D budget, with investments directed towards secure production lines, ensuring independence from potentially hostile powers. Despite his clear statements and broad references to AI and his intention to invest funds and administrative resources in it, no specific numbers regarding the investment size were revealed (Berman 2023).

4 Funding Defense AI

Neither the amount of funding dedicated to developing and using AI for defense and security purposes in Israel, nor the national budget allocated to defense organizations such as the Mossad and the Shin Bet are made public. The budget articles of the IMOD and the IDF are classified and not available to all members of the Knesset, the Israeli parliament (Schwartz and Harosh 2015). Therefore, unlike other nations, Israel does not have one comprehensive document that would lay out the country's defense AI investments. However, some information can be gleaned from recent attempts to formulate a national AI strategy. Those point to the fact that while the funding of defense AI is still decentralized and lacks national oversight, its importance is not lost on decision makers and progress is slowly made.

Over the last 5 years, two national committees have been formed to address the need for a national AI strategy. Each of them identified areas in need of budgets and resources. In 2018, a government committee chaired by Professor Isaac Ben Israel and Professor Eviatar Matania was established. Its goal was to formulate a plan that would position Israel as a leading force in AI worldwide. Over 300 experts and 15 different sub-committees made up the committee, which examined the impact of AI on all aspects of life in Israel. Among its recommendations, the committee called for an annual investment of NIS1-2bn (around €250-500M) per year for 5 years.

Given that Professor Ben Israel is regarded as one of the key figures behind the strategy that transformed Israel into a formidable cyber power, the findings of the committee were awaited with anticipation. But the proposals put forth by the committee were not officially endorsed, primarily due to the political uncertainty that prevailed during its tenure. Israel held a total of five national elections between April 2019 and November 2022 (Israel Democracy Institute n.d.). For 3 years no

state budget was approved, and no resources could be allocated to finance the committee's vast recommendations (Zarchia 2021).

The visible deterioration of Israel's leading position in the international AI competition, exemplified by its declining rankings in the global AI index (Tortoise Media n.d.), has been linked to the inadequate allocation of government resources and the lack of a comprehensive national strategy. As a result, it seems imperative to deal with these issues promptly, even outside of direct government involvement.

This understanding has led the TELEM forum to establish an independent committee in December 2019 chaired by Dr. Orna Berry. TELEM included representatives from the Israel Innovation Authority; Council for Higher Education; IMOD DDR&D; Ministry of Innovation, Science and Technology; and Ministry of Finance. The committee examined where Israeli industry stands in the field of AI, what barriers can be removed, and how the government can contribute to the field's development. The recommendations were submitted a year later. TELEM's narrow plan requested a budget of a billion NIS for 5 years (Ziv 2019/Committee for the Advancement of AI and Data Science 2020). TELEM's recommendation was to start by investing NIS550M (around €140M) into urgent projects, which include infrastructure building, personnel training, and prioritizing R&D projects with significant national importance (Orbach 2020). When eventually a state budget was approved in November 2021, resources were allocated to the program and the rest of the budget should be approved in the current government budget (Halperin 2022).

5 Fielding and Operating Defense AI

Israel is recognized as a leader in the development and implementation of AI in military operations. The country has developed various AI-powered systems that help with early warning of potential attacks, planning and executing military operations, and situational assessment. Israel's expertise in AI also extends to other defense-related areas as we discuss below.

5.1 Logistics

From 2021, IDF started to establish three logistics centers in Israel, costing NIS5.5bn (around €1.4bn). The centers will be constructed and managed by an external civil contractor over a period of 20 years, as the IDF aims to implement a significant transformation in the logistics field. The primary objectives of this initiative are to achieve substantial personnel savings and enhance equipment and inventory optimization. The project leaders assert that the plan will incorporate cutting-edge technologies, including some specifically designed for this project, which are currently unavailable. The project comprises automated warehouses and robots to carry out

picking operations, all of which are powered by AI technologies (Binstock 2021). In addition, there are several further projects within the IDF that relate to the management of munitions and other operational warehouses, which make use of AI while connecting to systems that assist in the planning and management of operations (Heller 2023).

5.2 Intelligence

Intelligence is one of the prominent fields in which AI is being used in Israel's defense. In recent years, Israel has been utilizing AI to collect and analyze vast amounts of data, making the intelligence-gathering process more efficient and effective. This has allowed the country to stay ahead of potential threats and protect its citizens.

5.2.1 General Intelligence

The Israeli defense and security establishment has been utilizing AI to enhance its intelligence-gathering and processing capabilities. One notable example is the facial recognition technology developed by AnyVision, which is being used in two primary applications. The first is for checkpoints where Palestinians pass on their way to work inside Israel. The system enables quick identification of visa holders and shortens queues, facilitating movement and reducing waiting times. The second application is a more secretive project based on a network of cameras spread throughout the area. The system is used to track and identify potential threats, even outside the checkpoints. The use of AnyVision's technology in the Israeli-Palestinian conflict has been controversial, but it has also been praised for its potential to enhance security (Solon 2019).

In addition to facial recognition technology, Israeli defense and security establishments are also utilizing AI capabilities to analyze encrypted content, track suspicious parties, and handle vast amounts of information in the cyber dimension. The IDF, the Shin Bet, and the Mossad have each developed their own set of technologies for gathering, processing, and analyzing different types of data such as voice, image, and text. These advanced technologies allow Israel defense and security establishment to monitor potential threats more effectively and respond quickly to any suspicious activity. With the ongoing development of AI technologies and the increasing use of big data, Israel defense and security establishment is likely to continue expanding its use of AI in intelligence operations:

- The Shin Bet, for example, established in recent years an accelerator for companies that develop technologies for its use, including, among others, a company in the field of Speech Recognition by AI (Pick 2019).

- The Mossad has created Libertad, a fund for technological innovation that invests in breakthrough technologies. The fund has expressed a specific interest in AI and NLP technologies (Orbach 2019). The Mossad has also been reported to use AI for a range of purposes. The agency's use of AI is largely classified, but it is known that they work with Israeli startups and academic institutions to develop and integrate advanced technologies into their operations (Devori 2021).

5.2.2 Intelligence for Operations

AI has improved real-time targeting, and increased accuracy as well as efficiency. The IDF uses AI for intelligence analysis and distribution, for example, with a trio of applications. "The Alchemist" provides real-time visual detection of targets, while "The Gospel" generates target recommendations based on AI capabilities. Another albeit classified project is "The Depth of Wisdom."

These programs helped enhance the efficiency and accuracy of intelligence analysis and distribution, thereby contributing to the IDF's overall operational effectiveness (Antebi 2022). During Operation Guardian of the Walls, the Israeli Air Force attacked 50% of the 200 high-quality targets that the IDF produced in 12 days. A huge improvement, because prior to this operation it took the IDF almost 1 year to produce such number of high-quality targets.

Overall, improved accuracy also reduced the number of enemy multi-barreled rocket launchers and halved the number Kornet launchers, both count as a problematic threat by the IDF (Bohbot 2021). Unit 8200 developed the AI programs, while Unit 9900 used AI technologies for visual intelligence analysis, creating "dual maps" for accurate fire plans and executing the "Lightning Strike" operational program. AI also helped detect "ground violations" for hidden rockets, building tunnels, and bunkers, producing additional targets for attack.

5.3 Command and Control

The IDF has developed several AI-powered systems, such as the one created by the Israeli Computer and IT Directorate, which provides early warning of potential attacks and helps plan the IDF's attacks while coordinating all different military units. Additionally, there are systems that can prioritize hundreds and thousands of targets, examining armaments and officials who can act against them, which would be time-consuming or even impossible for humans to do. These systems combine information from various sources, including tanks, surveillance cameras, airplanes, UAVs, and ships, to provide a comprehensive situational assessment to the Commanders. This allows them to quickly understand the situation and make decisions. The system's data and insights are also available to attack units and even to the Chief of the General Staff, who is Israel's Commander-in-Chief, if necessary (Heller 2023).

5.4 AI in Fielded Air, Sea, and Land Systems

5.4.1 Unmanned Systems

Israel is a prominent provider of unmanned systems across all domains and plays a leading role in developing, producing, operating, and exporting unmanned systems that utilize AI. These systems are designed to perform with different levels of autonomy. AI allows these systems to operate independently, reducing human intervention. Israel has used the respective expertise in particular to develop unmanned air power with UAVs for intelligence, reconnaissance, and surveillance (ISR) as well as strike missions. Israel also holds the top position in loitering weapons.

In the land domain, project SOI ("Standoff In") provides a glimpse into the future, although this development project, for which IMOD contracted IAI, is top secret. This program aims to reduce risk to Israeli soldiers in direct combat with enemy forces by using an armed vanguard of unmanned air and ground vehicles controlled by human soldiers from a safe distance. The SOI program builds on prior Israeli programs, including Rafael's SmartTrigger system, which automates the process between identifying a target and assigning it to a weapon. The first SOI capabilities are scheduled to become operational within 3 years, but experts question the ability of unmanned systems to effectively operate in densely populated areas (AviationWeek 2022).

At sea, the Seagull unmanned surface vessel (USV) highlights the combination of unmanned technology with AI for underwater and surface warfare, including anti-submarine warfare, electronic warfare, and mine detection, and has participated in the Digital Horizon exercise led by the U.S. Navy (Frantzman 2022).

5.4.2 AI-Enabled Military Manned System

The IDF is utilizing AI technology in its advanced military systems such as the F-35 fighter jet and the future Ground Combat Vehicle (GCV) named CARMEL. ADIR, the Israeli version of the American F-35 fighter jet, incorporates advanced AI systems to enhance its combat capabilities. The IDF's F-35 aircraft have been operational since December 2017 and have already played a significant role in intercepting two Iranian drones and participating in various operational missions (The Jerusalem Post 2022; Tor-Paz 2022).

CARMEL is being developed by ELTA. The program aims to improve the AI, autonomous, and automatic capabilities of the GCV to handle present and future combat situations, maneuver in urban environments, and operate with only two soldiers. Right now, similar systems operate with a crew of eleven fighters. Reducing the number to two suggests a significant reduction of human risk on the battlefield while maintaining combat power (The Marker 2021).

The GCV is equipped with a comprehensive set of situational awareness, force protection sensors, target acquisition, weapon stations, electronic counter measures

(ECM), as well as autonomous navigation and maneuvering features. Although the GCV has not yet been deployed for operational use, it is considered a vital element in bolstering the IDF's military capabilities and is being evaluated for its potential use in future conflicts (Ministry of Defense 2019).

5.4.3 Air Defense Systems

Israel's air defense systems rely on AI features to enhance their capability to advance protection against various air threats. In use since 2011, the Iron Dome systems is a crucial element of Israel's air defense umbrella, designed to intercept short-range rockets, mortar shells, and UAVs (Uzi 2021). This active air defense system has undergone upgrades, making it more effective in addressing multiple rocket barrages in a short period. Additionally, the Drone Dome system disables drones, while the new David's Sling system supplements Iron Dome using an interceptor missile that maneuvers quickly and directs itself using a radar and an electro-optical sensor (formerly known as "Magic Wand").

During the 2021 operation "Guardian of the Walls" involving Israel and Hamas, the Iron Dome system intercepted 1660 rockets with a 90% success rate, despite firing heavy barrages of 100-150 rockets in the same area. This remarkable accomplishment is due to the high level of autonomy combined with AI and full integration into Israel's air defense systems (Levin/Bustan 2021).

5.5 Cyber

Israel is a global leader in the cybersecurity industry, with over 450 cybersecurity companies (as of September 2021), many of them using AI and machine learning technologies to provide advanced threat detection and response capabilities (Start-Up Nation Central n.d.-b). Israeli companies such as Cybereason and Cynet use AI to identify and respond to cyber-attacks in real-time. Other leading companies like ActiveFence detects and protects against disinformation, terror, and other malicious content and activities online.

The Israeli government has also recognized the importance of AI in cybersecurity. In 2018 it has launched the National Cybersecurity Agency and has made significant investments in developing the country's capabilities in this area (The State of Israel n.d.-b). The IDF is also a leading developer and user of AI for cybersecurity purposes, with several units dedicated to this task, including Unit 8200 and the Israeli Computer and IT Directorate. The IDF has established a dedicated research center, the Artificial Intelligence and Big Data Research Center, to develop cutting-edge AI algorithms for threat detection and response. Israel's commitment to staying at the forefront of technological innovation in defense and security underscores its position as a global leader in the field of AI-powered cybersecurity (Forbes 2022).

5.6 Conclusion

Israel has been integrating AI not only in traditional fields—such as unmanned military systems or cybersecurity—but also in other areas like logistics and intelligence. Although some major AI projects like the SOI and CARMEL are still under development, operational applications of AI in unmanned ground and naval systems are not yet widespread. This is similar to the situation in other leading countries. At the same time, Israel's leadership in the field of intelligence is evident, with a wide range of capabilities and applications. These capabilities have contributed to significant military achievements in recent operations against Hamas in Gaza. It is likely that Israel possesses even more advanced capabilities that it has not yet revealed.

6 Training for Defense AI

6.1 Training Human Capital

As part of the mandatory service customary in Israel, high school graduates are recruited for a service that ranges from 24 to 32 months. An appropriate training program is needed to allow the IDF to reap the benefits of their service before their release, especially when it comes to technological roles that require complex and expensive training.

Leading military technology units such as Unit 8200 of the Israeli Military Intelligence Directorate and the LOTEM unit in the Israeli Computer and IT Directorate recruit talented high school graduates in a series of exams prior to their enlistment. Training generally lasts 2–6 months and is sometimes incorporated into pre-military training programs. The young recruits learn computing and software skills, as well as professional tools used in civilian and defense environments (Israel Defense Forces n.d.). Their demanding role requires them to constantly improve their skills and to be able to cope with complex issues in a quick and efficient manner.

The IDF school for computer and cyber professions is the main unit to train soldiers for various technological roles: developers, DevOps, data analysts, cybersecurity, and many others. The courses combine theoretical studies with practical exercises, encouraging trainees to study independently and find the method that suits them (Israel Defense Forces 2019). The school incorporates concepts from the civilian tech industry and offers personalized learning areas as well as meetups and hackathons in collaboration with academia and civilian industries (Tal 2022).

The growing role of AI in all areas of life led to the need for additional training to all military personnel, especially commanding officers. A new program—a collaboration between the Shiloh Brigade (Combat Methods and Innovation) with the Maltak (Tactical Command College) and Microsoft—aims to answer this need. This program has two parts: The first is available to any soldier through their phone or computer and offers soldiers lectures and material on AI, the means to integrate it to

governmental organizations and how to create a culture and strategy for AI. The second is under higher classification and is open to Majors and above in the IDF internal system. This part discusses AI in operational contexts, considers its potential and reflects upon use-cases relevant to the IDF (Revivo 2021).

6.2 Training Models

Another important aspect is the training of AI models. AI is an ever-improving technology, requiring an iterative process of learning and adjusting. In this context data plays an important role, as it enables training the algorithms and preparing them for autonomous action. A lack of data challenges the ability to improve and use AI. This issue is relevant both to civilian companies in the private sector, and even more so to the defense sector where data is scarce and costly. There are several challenges regarding data in the defense sector:

- *Secrecy and Compartmentalization*

As the defense agencies are traditionally not connected to external networks and cloud technology, they are unable to use the data centers of other entities, sometimes even within the same organization. Due to national security and safety concerns the Israel defense and security establishment avoids sharing data, algorithms and even results due to fear of exposing data through reverse engineering. Therefore, these agencies are compelled to operate using only their own hardware capabilities and internal databases, with limited ability to collaborate.

- *Lack of Data*

In the intelligence and operational world insufficient data can impede the training of vital algorithms needed to solve problems. For instance, one image or a few images of strategic importance is not enough to train the algorithm properly to act on a specific subject or phenomenon.

- *Training for the Previous War*

Israel's defense and security establishment primarily gather information in routine, but statistical changes in emergencies or combat need to be addressed. However, databases cannot fully represent future operational realities, so training data is based on past routine or emergency scenarios. This poses a challenge as it's like preparing for a war that has already happened, while the operational arena is constantly changing and unpredictable.

- *Technical Challenges*

In addition, there are technical challenges that may not be unique to the defense sector but present a meaningful hurdle for any data-oriented organization. The cost of storage and lack of space sometimes leads to the erasing of data. Moreover, the information collected over the years may not always be suitable for processing

within the framework of AI, and it is necessary to "clean it" and rearrange it to accommodate its use with an AI model.

Some work has been aimed at addressing these challenges. Private and local cloud infrastructure has been developed in the IDF as part of Momentum (Tnufa) Multiyear Plan since 2018 (Htoni 2019). In addition, the previously mentioned Project Nimbus aims to provide the Israeli government, the Israeli defense establishment, and others an all-encompassing cloud solution (Ziv 2021). The move towards a shared operational cloud service could solve technical challenges relating to storage and enable a secured connectivity within the defense apparatus that in turn could facilitate more collaboration and sharing of data and algorithms.

7 Conclusion

AI has become a cornerstone of Israel's national security strategy, serving as a critical tool for enhancing defense capabilities, driving economic growth, and bolstering the country's international standing. While Israel has reaped numerous benefits from leveraging AI in defense and security applications, it also faces distinctive challenges that set it apart from other leading countries in this field. Nonetheless, these challenges have not prevented Israel from emerging as one of the world's foremost AI innovators and leaders in the defense and security domain, as described above.

Israel successfully uses defense AI in the absence of coherent management and explicit budget allocation. Its relentless defense and security challenges enable its position as a global AI powerhouse, which is further based, among other things, on the uniqueness of the Israeli ecosystem in the field. The defense and security establishment, defense industry, and academic institutions of Israel have contributed significantly to the rapid progress of AI in various domains, including logistics, intelligence gathering, command and control, unmanned and manned systems, air defense, and cyber warfare. Additionally, Israel's remarkable capabilities and applications in the field of intelligence have played a pivotal role in recent military successes, further solidifying its position as a leader in AI.

Due to the significant impact of AI on Israel's defense and security, it becomes evident that Israel is obliged to take proactive measures to uphold its position as a world leader in this field. To accomplish this, the Israeli government must allocate a dedicated budget and management resources at the national level, rather than relying on the advantages of the unique Israeli ecosystem to compensate for any shortcomings in governance. Israel could reap additional benefits from allocating extra resources from relevant organizations like the military and IMOD towards enhancing the "soft aspects" of defense AI. This could involve activities like formulating and advocating suitable doctrines, increasing involvement in international forums, and dedicating more comprehensive consideration and expert attention to legal and ethical concerns that may emerge in relation to the operational use of AI for defense and security objectives.

In a fiercely competitive environment and amidst a global arms race, it is essential to recognize that relying on an organized mess approach may no longer guarantee the same level of success. However, by embracing this challenge as an opportunity for growth and innovation, Israel can adapt its strategies, foster collaboration, and harness its technological prowess to stay competitive and to keep its position as a leader in defense AI.

References

Alxalsi, Osheri. 2022. A year ago they were released from 81 and now they are exposed with one of the largest Seed Round in Israel. Geektime. https://www.geektime.co.il/israeli-startup-wants-to-map-the-underground-with-a-few-sensors-and-a-drone-exodigo/. Accessed 30 January 2024

Antebi, Liran. 2021. Artificial intelligence and national security in Israel. Memorandum No. 207. Institute for National Security Studies. https://www.inss.org.il/publication/artificial-intelligence-and-national-security-in-israel/. Accessed 30 January 2024

———. 2022. Has artificial intelligence triumphed over terrorism? Lessons learned from the IDF's use of advanced technology in Operation Guardian of the Walls?. Vortex. Studies on Air and Space Power, pp. 103–120. https://en.calameo.com/cesa/books/00694028836ec273548b7. Accessed 30 January 2024

AviationWeek. 2022. Israel Plans to field advanced autonomous combat unit by 2025. AviationWeek. https://aviationweek.com/defense-space/missile-defense-weapons/israel-plans-field-advanced-autonomous-combat-unit-2025. Accessed 30 January 2024

Azoulai, Yuval. 2023. The Ministry of Defense is planning: the establishment of an administration for the development of future technologies. Calcalist. https://www.calcalist.co.il/local_news/article/hklxszhcs. Accessed 30 January 2024

Berkowitz, Uri, and Levy-Weinreeve, Ella. 2021. Now it's official: the state chose Amazon and Google in the Nimbus cloud tender. Globes. https://www.globes.co.il/news/article.aspx?did=1001368315. Accessed 30 January 2024

Berman, Lazar. 2023. Defense Ministry to invest heavily in AI in bid to improve intel on Iran. The Times of Israel. https://www.timesofisrael.com/defense-ministry-to-invest-heavily-in-ai-in-bid-to-improve-intel-on-iran/. Accessed 30 January 2024

Binstock, Neta-Lee. 2021. Amazon, behind you: the IDF replaces the Warehouses with artificial intelligence. Calcalist. https://www.calcalist.co.il/local/articles/0,7340,L-3904473,00.html. Accessed 30 January 2024

Bohbot, Hagar. 2018. Sneak peek: The IDF's Unit 3060 is leading a revolution in intelligence information. Ynet. https://www.ynet.co.il/articles/0,7340,L-5361168,00.html. Accessed 30 January 2024

Bohbot, Amir. 2021. The destruction of the metro and the thwarting of launches: the technological means that the IDF first operated in Gaza. WALLA. https://news.walla.co.il/item/3438217. Accessed 30 January 2024

———. 2023. A game-breaking weapon: the technology that will decide the IDF's next campaign. Walla. https://news.walla.co.il/item/3559347. Accessed 30 January 2024

Cohen, Sagi. 2019. No longer satisfied with 8200: this is how the army develops artificial intelligence in cooperation with high-tech companies. The Marker. https://www.themarker.com/technation/2019-09-26/ty-article/.premium/0000017f-dee8-df9c-a17f-fef8df750000. Accessed 30 January 2024

Committee for the Advancement of AI and Data Science. 2020. The State of Israel/TELEM Forum. https://innovationisrael.org.il/sites/default/files/%D7%93%D7%95%D7%97%20%D7%A1%D7%95%D7%A4%D7%99%20

%D7%A1%D7%99%D7%9B%D7%95%D7%9D%20%D7%95%D7%95%D7%A2%D7%93%D7%AA%20%D7%AA%D7%9C%D7%9D%20%D7%9C%D7%AA%D7%9B%D7%A0%D7%99%D7%AA%20%D7%9E%D7%95%D7%A4%20%D7%9C%D7%90%D7%95%D7%9E%D7%99%D7%AA%20%D7%91%D7%91%D7%99%D7%A0%D7%94%20%D7%9E%D7%9C%D7%90%D7%9B%D7%95%D7%AA%D7%99%D7%AA%20-.pdf. Accessed 30 January 2024

Devori, Nir. 2021. The Mossad is stepping into a more technological future. N12. https://www.mako.co.il/news-columns/2021_q4/Article-b88cd6b5b5d1d71026.htm?sCh=31750a2610f26110&pId=173113802. Accessed 30 January 2024

Forbes. 2022. Deputy commander of elite intelligence unit 8200 reveals its secret weapon. Forbes Israel. https://forbes.co.il/e/deputy-commander-of-elite-intelligence-unit-8200-reveals-its-secret-weapon/. Accessed 30 January 2024

Frantzman, Seth J. 2022. Israel's Elbit sends Seagull USV to Digital Horizon event in Bahrain. C4ISRNet. https://www.c4isrnet.com/unmanned/2022/12/13/israels-elbit-sends-seagull-usv-to-digital-horizon-event-in-bahrain/. Accessed 30 January 2024

Greenberg-Cohen, Einav. 2021. Based on data: the IDF laboratory that determines who is suitable to sign permanently. MAKO. https://www.mako.co.il/pzm-magazine/Article-92c8c2573912871026.htm. Accessed 30 January 2024

Halperin, Yaniv. 2022. Will the national artificial intelligence program be delayed because of the elections?. People and Computers. https://www.pc.co.il/news/367237/. Accessed 30 January 2024

Heller, Or. 2023. Changes the rules of the game: a first look at the IDF's artificial intelligence. RESHET 13. https://13tv.co.il/item/news/politics/security/izp5v-903457413/. Accessed 30 January 2024

Htoni, Yossi. 2019. Everything you wanted to know about the operational IDF cloud and didn't dare to ask. People and Computers. https://www.pc.co.il/news/303311/. Accessed 30 January 2024

Israel Defense Forces. 2019. The School of Computer and Cyber Professions. Israel Defense Forces. https://www.idf.il/%D7%90%D7%AA%D7%A8%D7%99-%D7%99%D7%97%D7%99%D7%93%D7%95%D7%AA/%D7%90%D7%92%D7%A3-%D7%94%D7%AA%D7%A7%D7%A9%D7%95%D7%91-%D7%95%D7%94%D7%94%D7%92%D7%A0%D7%94-%D7%91%D7%A1%D7%91-%D7%A8/%D7%9B%D7%9C-%D7%94%D7%9B%D7%AA%D7%91%D7%95%D7%AA/%D7%9B%D7%AA%D7%91%D7%95%D7%AA-%D7%9B%D7%9C%D7%9C%D7%99%D7%95%D7%AA/%D7%91%D7%A1%D7%9E-%D7%97/. Accessed 30 January 2024

———. n.d. Get to know LOTEM unit. Israel Defense Forces. https://www.idf.il/%D7%90%D7%AA%D7%A8%D7%99-%D7%99%D7%97%D7%99%D7%93%D7%95%D7%AA/%D7%9C%D7%95%D7%98%D7%9D/. Accessed 30 January 2024

Israel Democracy Institute. n.d. About the elections for the 25th Knesset. Israel Democracy Institute. https://www.idi.org.il/policy/parties-and-elections/elections/2022-1/. Accessed 30 January 2024

Levin, Alon, and Bustan, Yuval. 2021. The stick and the laser: the IDF's impressive technological capabilities will not suffice in the next round. Forbes Israel. https://forbes.co.il/idf-tech-abilitie/. Accessed 30 January 2024

Lt. Col G., Major G., and Major L. 2021. On network intelligence and artificial intelligence: the artificial intelligence transformation of the information processing and analysis center in 8200. IDF Dado Center. 2021. https://www.idf.il/%D7%90%D7%AA%D7%A8%D7%99-%D7%99%D7%97%D7%99%D7%93%D7%95%D7%AA/%D7%9E%D7%A8%D7%9B%D7%96-%D7%93%D7%93%D7%95/%D7%9E%D7%90%D7%9E%D7%A8%D7%99%D7%9D-%D7%95%D7%AA%D7%95%D7%9B%D7%9F-%D7%9E%D7%A7%D7%95%D7%95%D7%9F/%D7%A2%D7%9C-

%D7%91%D7%99%D7%A0%D7%94-%D7%A8%D7%A9%D7%AA%D7%99%D7%AA-%D7%95%D7%91%D7%99%D7%A0%D7%94-%D7%9E%D7%9C%D7%90%D7%9B%D7%95%D7%AA%D7%99%D7%AA-%D7%A1%D7%90-%D7%9C-%D7%92-%D7%A8%D7%A1-%D7%9F-%D7%91%D7%9E%D7%99%D7%9C-%D7%92-%D7%95%D7%A8%D7%A1-%D7%9F-%D7%91%D7%9E%D7%99%D7%9C-%D7%9C./. Accessed 30 January 2024

Maariv Online. 2022. Artificial intelligence is a weapon for everything: the IDF's plans for the new battlefield. Maariv Online. https://www.maariv.co.il/business/tech/Article-896771. Accessed 30 January 2024

Ministry of Defense. 2019. 'Carmel' revealed: what will the IDF's vehicle of the future look like?. Ministry of Defense. https://www.mod.gov.il/Defence-and-Security/articles/Pages/4.8.19.aspx. Accessed 30 January 2024

———. n.d. MAFAT challenge. https://mafatchallenge.mod.gov.il/. Accessed 30 January 2024

Ministry of Innovation, Science and Technology. 2022. Principles of policy, regulation and ethics in the field of artificial intelligence – Draft for public reference. https://www.gov.il/BlobFolder/news/most-news20223110/he/Regulatory%20and%20ethics%20policy%20document%20in%20the%20field%20of%20artificial%20intelligence%20in%20IsraelAI.pdf. Accessed 30 January 2024

OECD. AI Policy Observatory. n.d. AI in Israel. OECD. https://oecd.ai/en/dashboards/countries/Israel. Accessed 30 January 2024

Orbach, Meir. 2019. Mossad's venture arm to diversify portfolio. CTECH. https://www.calcalistech.com/ctech/articles/0,7340,L-3762567,00.html. Accessed 30 January 2024

———. 2020. There is a national program for artificial intelligence, but there is no budget. Calcalist. https://www.calcalist.co.il/internet/articles/0,7340,L-3883198,00.html. Accessed 30 January 2024

Pick, Adi. 2019. Israel's Shin Bet, Tel Aviv University Announce Third Accelerator Cohort. CTHEC. https://www.calcalistech.com/ctech/articles/0,7340,L-3776316,00.html. Accessed 30 January 2024

Revivo, Gal. 2021. Meet the new IDF artificial intelligence course. Israel Defense Forces. https://www.idf.il/%d7%9b%d7%aa%d7%91%d7%95%d7%aa-%d7%95%d7%a2%d7%93%d7%9b%d7%95%d7%a0%d7%99%d7%9d/2021/%d7%91%d7%99%d7%a0%d7%94-%d7%9e%d7%9c%d7%90%d7%9b%d7%95%d7%aa%d7%99%d7%aa-%d7%91%d7%9b%d7%a3-%d7%94%d7%99%d7%93-%d7%9c%d7%9b%d7%9c%d7%9c-%d7%97%d7%99%d7%99%d7%99%d7%9c%d7%99-%d7%95%d7%9e%d7%a4%d7%a7%d7%93%d7%99-%d7%a6%d7%94%d7%9c-%d7%a7%d7%95%d7%a8%d7%a1/. Accessed 30 January 2024

Samuel Neaman Institute for National Policy Research. 2018. Artificial intelligence, data science and intelligent robotics: first report. Samuel Neaman Institute for National Policy Research. https://www.neaman.org.il/Files/Artificial-Intelligence-Data-Science-and-Smart-Robotics_20181204151647.206.pdf. Accessed 30 January 2024

Schwartz, Eliezer, and Harosh, Yoni Ben. 2015. The process of approving the defense budget and its supervision in Israel and other countries. The Information Center of the Knesset of Israel. https://fs.knesset.gov.il/globaldocs/MMM/8e2669be-c5bd-e511-80d6-00155d0204d4/2_8e2669be-c5bd-e511-80d6-00155d0204d4_11_8685.pdf. Accessed 30 January 2024

Shulman, Sophie. 2021. An army of startups. Calcalist. https://newmedia.calcalist.co.il/magazine-07-01-21/m01.html. Accessed 30 January 2024

Solon, Olivia. 2019. Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians. NBC News. https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116. Accessed 30 January 2024

Start-Up Nation Central. n.d.-a. Startups: AI companies. Start-Up Nation Central. https://finder.startupnationcentral.org/company/search?&sort=name-asc&coretechnology=agxzfmlsbGlzdHNpdGVyJAsSF0Jhc2VDbGFzc2lmaWNhdGlvbk1vZGVsGICA4Lu1rJEIDA%7CRbmqmksX733j5CtxKDoXKAlJOiX11qFZmHFTAfFaP47PbnvrXrLWt1%7CagxzfmlsbGlzdHNpdGVyJAsSF0Jhc2VDbGFzc2lmaWNhdGlvbk1vZGVsGICA4Lu-u8oLDA%7CagxzfmlsbGlzdHNpdGVyJAsSF0Jhc2VDbGFzc2lmaWNhdGlvbk1vZGVsGICA4Ie8rfEKDA%7Cag

xzfmlsbGlzdHNpdGVyJAsSF0Jhc2VDbGFzc2lmaWNhdGlvbk1vZGVsGICA4PuDl6YLDA%7Cagxzfmls-bGlzdHNpdGVyJAsSF0Jhc2VDbGFzc2lmaWNhdGlvbk1vZGVsGICA4L-u81fgLDA&status=Active&savedsearchid=zRyAigyGjMiJY9FXWVIKLHOS1zhQwl7KOe1KgZCaTQaviLj62mGtmn. Accessed 30 January 2024

———. n.d.-b. The Israeli Cybersecurity Sector. Start-Up Nation Central. https://startupnation-central.org/wp-content/uploads/2021/09/2-pager-Cybersecurity_screen.pdf. Accessed 30 January 2024

Tal, Yuval. 2022. The base of the computer science school has moved to the south - get a special look inside. Israel Defense Forces. https://www.idf.il/%D7%90%D7%AA%D7%A8%D7%99-%D7%99%D7%97%D7%99%D7%93%D7%95%D7%AA/%D7%90%D7%92%D7%A3-%D7%94%D7%AA%D7%A7%D7%A9%D7%95%D7%91-%D7%95%D7%94%D7%94%D7%92%D7%A0%D7%94-%D7%91%D7%A1%D7%91-%D7%A8/%D7%9B%D7%9C-%D7%94%D7%9B%D7%AA%D7%91%D7%95%D7%AA/2022/%D7%91%D7%A1%D7%9E-%D7%97-%D7%91%D7%A1%D7%99%D7%A1-%D7%91%D7%93%D7%A8%D7%95%D7%9D-%D7%94%D7%90%D7%A8%D7%A5-%D7%94%D7%A6%D7%A6%D7%94-%D7%97%D7%93%D7%A9%D7%A0%D7%95%D7%AA-%D7%90%D7%92%D7%A3-%D7%94%D7%AA%D7%A7%D7%A9%D7%95%D7%91-%D7%95%D7%94%D7%94%D7%92%D7%A0%D7%94-%D7%91%D7%A1%D7%91%D7%A8/. Accessed 30 January 2024

The Jerusalem Post. 2022. Three new F-35 fighter jets land in Israel. The Jerusalem Post. https://www.jpost.com/israel-news/article-722294. Accessed 30 January 2024

The Marker. 2021. Surprise: IAI won the Ministry of Defense tender for the development of the 'light tank' technology. The Marker. https://www.themarker.com/news/2021-10-10/ty-article/.premium/0000017f-f174-d497-a1ff-f3f486d00000. Accessed 30 January 2024

The State of Israel. n.d.-a. The national program for natural language processing. The State of Israel. https://www.gov.il/en/departments/news/digital-nlp. Accessed 30 January 2024

———. n.d.-b. About Israel National Cyber Directorate. The State of Israel. https://www.gov.il/en/departments/about/newabout. Accessed 30 January 2024

Tor-Paz, Asif. 2022. For the first time in the world: Israeli "Adir" (F-35i) planes intercepted Iranian drones. The Israel Air Force. https://www.iaf.org.il/9501-55171-he/IAF.aspx. Accessed 30 January 2024

Tortoise Media. n.d. The Global AI Index. Tortoise Media. https://www.tortoisemedia.com/intelligence/global-ai/. Accessed 30 January 2024

Tzafarir, Yoel. 2021. The cloud significantly helps to increase the operational effectiveness of the IDF. The Marker. https://www.themarker.com/labels/cloud/2021-08-31/ty-article-labels/0000017f-f88a-ddde-abff-fcef76800000. Accessed 30 January 2024

Uzi, Rubin. 2021. Israel's air defense in test during operation guardian of the walls. The Jerusalem Institute for Strategy and Security. https://jiss.org.il/he/rubin-israels-air-defense-tested-during-operation-wall-guard/. Accessed 30 January 2024

Zarchia, Zvi. 2021. For the first time after three years: the government approved the state budget; The decision will go to the Knesset. Calcalist. https://www.calcalist.co.il/local_news/article/r15sjoeyy. Accessed 30 January 2024

Ziv, Amitai. 2019. Where is the field of artificial intelligence progressing in Israel? A second government committee will review. The Marker. https://www.themarker.com/technation/2019-12-31/ty-article/.premium/0000017f-eef4-da6f-a77f-fefef54c0000. Accessed 30 January 2024

Ziv, Amiti. 2021. Israel picks Google, Amazon for Massive Official Cloud: 'Data will remain here'. HAARETZ. https://www.haaretz.com/israel-news/tech-news/2021-04-21/ty-article/israel-picks-google-amazon-for-official-state-cloud/0000017f-e896-dc91-a17f-fc9fd1ce0000. Accessed 10 January 2024

Heavy Thunder, No Rain: Defense AI in Iran

Mahmoud Javadi

The application of artificial intelligence (AI) in defense made its debut in Iranian discourse in 2005 through a research paper published by the War University, that explored the integration of AI-enabled autonomous weapons in naval operations (Mahmoodi 2005). The power of defense AI, however, became starkly evident in the Iranian media and political discourse almost 15 years later, in the aftermath of the assassination of Mohsen Fakhrizadeh on November 27, 2020, carried out by an autonomous weapon (Kirkpatrick et al. 2020). Shortly after the killing of Fakhrizadeh, the father of Iran's industrial nuclear program, who benefitted from a personal protection regime comparable to that of Iran's President, a senior commander of the Islamic Revolutionary Guard Corps (IRGC) openly acknowledged the use of AI in the assassination (Wintour 2020).

One year later, Iran's Supreme Leader, Ali Khamenei—the singular authority responsible for defining Iran's strategies and serving as the Commander-in-Chief of the Iranian Armed Forces—addressed the topic of AI for the first time in a public speech. Khamenei outlined a vision for Iran to position itself among the top 10 nations in the realm of AI (khamenei.ir 2021). Since then, defense AI has emerged as a central theme in the statements of senior military commanders and government defense authorities in Iran.

AI is primarily viewed as a capability multiplier, injecting fresh blood into the defense doctrine. Iran's doctrine predominantly centers on deterrence, employing cost-effective asymmetric tactics and passive defense to counter both kinetic and non-kinetic threats. The focus is on addressing challenges from Tehran's longstanding major state adversaries, namely the United States (U.S.) and Israel which are perceived as proponents of regime change in Iran.

M. Javadi (✉)
Erasmus School of Social and Behavioral Sciences, Erasmus University Rotterdam, Rotterdam, The Netherlands
e-mail: javadi@essb.eur.nl

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_19

Iran takes pride in its past efforts to minimize the risk of ground invasions by adversaries. Despite the persistent territorial challenges posed by insurgent and terrorist groups in its peripheries, Tehran's military leadership is currently wary of potential threats emanating from the sea and air, perceiving these domains as vulnerable to kinetic military operations. In response, the Iranian armed forces have strategically prioritized the development of niche capabilities as deterrent measures. To realize this priority, Tehran has shifted its focus towards harnessing AI to principally sustain the credibility of these measures considering the rapid technological advancements of its major adversaries and regional rivals.

Despite the consistent discourse from Iranian leaders and strategists about the critical need to incorporate AI into Iran's defense strategy and posture, there appears to be limited tangible progress, as indicated by scant publicly available evidence of active projects. This slow development could be attributed to Iran's constraints in financial resources and technological access. Nonetheless, Tehran remains resolute in pursuing this trajectory, opting to sanctify defense AI rather than vilify it.

1 Thinking About Defense AI

The 2019 US assessment of Iran's power noted, "although still technologically inferior to most of its competitors, the Iranian military has progressed substantially over the past few decades" (U.S. Defense Intelligence Agency 2019). Iran is currently in the early stages of developing and operating defense AI, a contrast to other nations elaborated in this edited volume. The purported advancements claimed by Iran since 2021 may encompass a blend of genuine progress and propaganda. However, the Islamic Republic is currently at an advanced stage of thinking about defense AI, prompted by undeniable evidence highlighting the imperative need and urgency to incorporate AI into its defense doctrine.

1.1 The Islamic Republic's Grand Strategy in Defense

The Islamic Republic, a consequential product of the 1979 Revolution, has grappled with a persistent status of loneliness (Tabatabai 2019). Its interests and priorities face constant challenges, often struggling for recognition. The leadership's foremost concern has been the ongoing protection of the nascent Islamic political regime against perceived threats from both state and non-state actors (Bahgat and Ehteshami 2021). Thus, the context within which these perceived threats operate and the corresponding measures to counter them are crafted to fortify the Islamic Republic's triad grand strategy: survival, security, stability (S3).

1.1.1 Threat Perceptions

The ever-changing nature of the Islamic Republic, coupled with the inherent volatility in its surrounding regions, underscores the fluidity of Tehran's threat perceptions. However, the country's threat perception has changed between 2020 and 2024.

Ties with Saudi Arabia are warming up whereas the South Caucasus, traditionally aligned with Iranian interests, has become a new source of instability given resurfacing hostilities between Armenia and Azerbaijan. In addition, the U.S. and, to a lesser extent, Israel are consistently viewed as the Islamic Republic's most enduring state threats (Martini et al. 2023). Both nations also wield formidable capabilities to mobilize non-state threat actors. Tehran believes that Washington and Tel Aviv profoundly seek to disrupt its S3. The U.S. invasions of Iraq and Afghanistan in the early 2000s, coupled with the securitization of Iran's nuclear program, heightened Tehran's fears of an eventual U.S.-led kinetic military intervention. Therefore, recognizing its inability to compete with the U.S. conventionally and aiming to alter Washington's military calculations, Tehran has prioritized the enhancement of defensive capabilities and installations (U.S. Defense Intelligence Agency 2019), emphasizing asymmetric tactics which are "difficult to deter and provide plausible deniability" (Martini et al. 2023: 161).

As Iran has successfully built up its asymmetric capabilities, it has concluded that ground warfare may be given less, if not zero, priority by its major adversaries (MEHR News Agency 2017). This conclusion is rooted in various factors, including Washington's failure to achieve its goals in the invasions of Afghanistan and Iraq, America's Pivot to Asia and its subsequent efforts to right-size military postures in the Middle East (Barnes-Dacey and Lovatt 2022) as well as the absence of a forward-deployed military posture by Israel in Iran's immediate neighborhood. These perceptions have shaped Tehran's overall understanding of the evolving nature of conflict and warfare, especially in situations where its major state adversaries, leveraging advanced technologies, can coordinate kinetic and non-kinetic operations against the country.

1.1.2 Future Conflicts Setting

In the context of kinetic warfare, the Iranian senior military strategists affirm that future military conflicts initiated by state adversaries against Iran are likely to encompass scenarios of sea-based and air-based combat (Mashregh News Agency 2023b). Besides, the outcomes of these scenarios depend significantly on the technological supremacy wielded by either Tehran or its adversaries. According to Iranian military strategists, this superiority empowers either side to swiftly and efficiently gather and analyze vast amounts of data and information within a condensed timeframe (Tasnim News Agency 2023b).

Iran's comprehension of the evolving conflicts orchestrated by its state adversaries extends beyond conventional military operations. Non-kinetic warfare also plays a role in shaping Iran's perceptions of threats and the conflict environment

(U.S. Defense Intelligence Agency 2019). Acknowledging the escalating threats of non-kinetic warfare infiltrating civilian domains, Iran always points to Israel and the U.S. as primary actors or supporters behind cyber-attacks on civilian critical infrastructure (Reuters 2021; France24 2023). The Islamic Republic is deeply apprehensive that, depending on the magnitude of these operations, they may eventually interrupt national administration, undermine domestic stability, and wear off internal order; thus, to the detriment of Iran's S3.

The dual nature of perceived threats faced by the Islamic Republic, encompassing both kinetic and non-kinetic warfare, has led to the formulation of fundamental national security priorities and the corresponding defense doctrine.

1.1.3 National Security Priorities

The Islamic Republic has identified the physical withdrawal of its two principal enemies, the U.S. and Israel, from its vicinity as a paramount national security objective (Martini et al. 2023). Although the Iranian leadership has consistently characterized America as the primary threat to Iran's S3, Supreme Leader Khamenei's assessment of the U.S.'s diminishing influence and isolation in the emerging world order (khamenei.ir 2022a) has intensified Tehran's advocacy for the U.S. retreat from Iran's immediate surroundings. A similar perspective, albeit expressed more assertively, is held regarding Israel. In 2015, Khamenei foresaw the collapse of Israel by 2040 (Brodsky 2023).

The second national security priority underscores the Islamic Republic's aspiration to achieve regional power status. In November 2003, the Supreme Leader outlined the country's strategic vision for 2025, envisioning Iran as a developed nation occupying the foremost position in the economy, science, and technology across Southwest Asia, encompassing Central Asia, the Caucasus, the Middle East, and neighboring countries, as defined in the document. The objective also includes serving as a source of inspiration and a model for the Muslim world (INSF 2003). The Iranian leadership desires the Islamic Republic to be recognized as an influential and responsible power in the Middle East and Asia at large. This ambitious vision may be rooted in the desire to revive a glorified past (Javadi 2021). However, the persistent sense of loneliness, despite having diplomatic relations with the neighboring states, and perceived threats to its S3 since the 1979 Revolution, have compelled the Iranian leadership to seek a regional power status (Raouf 2019).

This pursuit is closely tied to Tehran's comprehension of its strategic depth, defined by the Office of the Supreme Leader as "any factor considered advantageous for a specific nation but recognized as a potential threat by adversaries, capable of serving as a deterrent for the nation in possession" (khamenei.ir 2008). The correlation between the concept of strategic depth and the number of subregions outlined in the country's 2025 strategic vision has motivated the leadership to secure the Islamic Republic's S3 beyond the political borders of the nation. This strategy is apparently rooted in the collective historical memory of the Iranian leadership. "Historically, whenever Iran defined its national security within its political border,

its independence and national sovereignty were violated, and its territorial integrity threatened … Therefore, Iran cannot counter external threats absent a robust regional or even extra-regional presence" (Alfoneh 2020).

1.1.4 Defense Doctrine

The Iranian leadership's comprehension of the nation's threats, the context in which conflicts may arise, and the strategic depth of the Islamic Republic acknowledge the necessity of adopting a comprehensive 360-degree defense approach (Black et al. 2022: 20). It aims to address both external threats posed by Tehran's archenemies and internal threats, which, according to the Iranian leadership, are supported or orchestrated by the same adversaries.

In terms of deterring kinetic operations, Iran acknowledges its conventional military technologies disadvantage compared to the U.S. and Israel (Tasnim News Agency 2023b). Consequently, Iran has formulated a defense strategy centered around cost-effective asymmetric tactics and niche capabilities (U.S. Defense Intelligence Agency 2019). Focusing primarily on countering potential kinetic threats emanating from sea and air, and seeking to bolster its strategic depth, Tehran has prioritized the augmentation of missiles, proxy forces, UAVs, and naval power as the four critical deterrence capabilities:

- *Missiles*

A crucial element of Iran's defense strategy centers on the development of a formidable arsenal, encompassing both cruise and ballistic missiles. These missiles primarily enhance Tehran's asymmetric capabilities. The Islamic Republic openly celebrates the progress in missile technology, considering it a source of prestige (Satam 2023). The Iranian missile arsenal is predominantly deployed from bases in western Iran (NTI n.d.). These bases offer closeness to U.S. military forces in the region, proximity to Israel—in the event of an American or Israeli intervention—, and the insurgent and terrorist entities including the Kurdish armed groups and Islamic State of Iraq and Syria (ISIS).

- *Proxy Forces*

Iran's imperative to deter kinetic operations, assert regional power status and exploit its strategic depth drives Tehran to cultivate proxy forces, predominantly in proximity to Israel (Martini et al. 2023). These proxies provide Iran with plausible deniability. Their demonstrated capabilities and preparedness to confront Iran's adversaries serve as an additional deterrent.

- *Uncrewed Aerial Vehicles (UAVs)*

Iran uses advanced UAVs to address gaps in its aging aircraft and enhance deterrence (U.S. Defense Intelligence Agency 2019). Throughout the 2010s, Tehran developed sophisticated UAVs, mostly through reverse engineering American drones (Iran Press 2020) and leverages UAVs technology to bolster deterrence

against the U.S. and indirectly threaten Israel and, to a lesser extent, Saudi Arabia through proxy networks (Eisenstadt 2021).

- *Naval Power*

The Islamic Republic strengthens its deterrence and power status through robust naval capabilities in the Persian Gulf and the Sea of Oman. The nation's maritime defenses incorporate a diverse range of platforms and weapons strategically designed to counter the U.S. Navy, primarily based in the Arab Gulf states, and regularly patrolled in the Persian Gulf and the Sea of Oman (Black et al. 2022). Iran places a significant emphasis on asymmetric tactics, notably the deployment of uncrewed surface vessels (USVs) and UAVs, as a crucial element of its naval strategy (U.S. Defense Intelligence Agency 2019). This approach aims to overwhelm the defenses of opposing warships. Additionally, in its quest for regional power status and the bolstering of strategic depth, Iran has showcased its naval capabilities by conducting out-of-area operations aimed at patrolling Iranian commercial vessels, reaching increasingly greater distances from Iranian shores (Bailey 2022). A notable achievement was the first-ever circumnavigation of the globe by the 86th flotilla of the Iranian Navy, spanning from September 2022 to May 2023 (Akbari 2023). This accomplishment was lauded by the Supreme Leader as a significant milestone and a source of national pride (khamenei.ir 2023).

While these four niche capabilities embody the Islamic Republic's asymmetric tactics to deter kinetic operations, the Iranian military has also predominantly developed electronic warfare (EW) mostly for defensive purposes (Tabatabai et al. 2021). EW is crafted and employed to optimize the functionality of defense assets and infrastructure, such as radar systems, and enhance their stealth connectivity with command and control (C2) (Battlespace 2023). The integration of AI into defense systems would further bolster Iran's EW, aligning it with the four key deterrence capabilities. Moreover, Iran's EW endeavors to identify and thwart state adversaries' intrusions into Iranian territories. The primary objective of Iran's EW military exercise in August 2023, for instance, was to counter intruding UAVs and micro air vehicles (MAVs) (Tehran Times 2023a). This exercise held particular significance as one of the key defense facilities in southern Iran had been targeted by MAVs in January 2023, allegedly conducted by Israel (Chulov 2023).

In response to non-kinetic threats, the Islamic Republic also employs asymmetric tactics, emphasizing a blend of deterrence, defense, and retaliation. In addressing perceived threats to its military and strategic assets, Iran actively engages in deterrence strategies while adhering to a passive defense doctrine (Nadimi 2018). As a comprehensive nationwide program, passive defense encompasses a range of tactics aimed at hindering foreign intelligence gathering and ensuring the resilience and protection of critical infrastructure, such as military equipment and nuclear facilities. Key measures include the use of camouflage, concealment, force dispersal, underground facilities, and the strategic deployment of highly mobile units (U.S. Defense Intelligence Agency 2019). Notably, grounded in the central tenets of Iran's passive defense doctrine, underground facilities have been constructed to

bolster diverse facets of Iran's defense industries, crucial nuclear infrastructure, and military forces (Gambrell 2023). This includes support for naval sites, missile bases, and equipment storage.

Iran's passive defense doctrine extends to cyber defense strategies focused on safeguarding civilian critical infrastructure and networks from cyberattack, misuse and compromise (Nazarinejad and Pourshasb 2020). The National Passive Defense Organization (NPDO), operating under the General Staff of the Armed Forces, whose constitution was ratified by Parliament in 2023, has evolved into an agency with the authority to issue legally binding decisions, marking a significant transformation two decades after its foundation.

One of the primary responsibilities of the NPDO is to leverage both national cyber and non-cyber resources to deter, prevent, identify, and effectively counter any cyberattacks on Iran's national infrastructure (Tehran Times 2023b). The NPDO plays a role in safeguarding the integrity and security of Iran's critical assets, ensuring resilience and survivability against cyber threats.

In addition to deterrence and defense, Iran has openly acknowledged its cyber offensive capabilities with the sole intention of retaliating against those responsible for cyberattacks aimed at its critical infrastructure (Anderson and Sadjadpour 2018). Cyber capabilities also play a key role for domestic stability as the Islamic Republic is convinced that major state adversaries want to exploit the cyber domain, including social media and satellite TV, to conduct "cognitive warfare" (Mirzaei 2023) and stir domestic upheaval. This expands the role of AI into the cyber domain, as well be discussed below.

1.2 Defense AI

As argued, Iran's threat assessment prompts the country to follow a 360-degree defense strategy focused on deterrence and asymmetric responses to strategic challenges (Martini et al. 2023; McInnis 2017a). In this context, Commander-in-Chief Khamenei consistently underscores the imperative of integrating cutting-edge science and advanced technologies into the armed forces' arsenals and installations (khamenei.ir 2022b). The ongoing modernization of Iran's defense assets and infrastructure equips the country with enhanced capabilities to safeguard its national security. However, the Islamic Republic has grappled with enduring challenges, notably long-standing restrictions on accessing the military technology market due to U.S. embargoes (Ben Taleblu 2023). Consequently, the Iranian armed forces have been compelled to maintain technological momentum through strategies such as indigenous procurement, technology appropriation, illicit acquisition, and reverse engineering (Boffey 2023).

Given these contexts and challenges, Iranian leadership and strategists have arguably recognized AI as a groundbreaking technology, applicable not only in defense but also in various facets of life. Supreme Leader Khamenei emphasizes the significance of AI as a crucial factor in shaping future global governance

(khamenei.ir 2021). A consensus among Iranian thinkers and strategists regarding AI is articulated by a philosopher who is loyal to the Islamic Republic:

> Artificial intelligence revolutionizes the production and distribution of goods, leading to substantial cost reduction and significantly expanding accessibility. In the contemporary landscape, a society's inability to master this technology poses a threat to economic viability and political competitiveness (Mashregh News Agency 2023d).

This understanding aligns with the dominant view on AI discussed in other chapters of this volume. Thus, the Iranian defense and military leadership acknowledges the transformative potential of AI, considering it a key force multiplier that elevates the effectiveness of the Islamic Republic's defense doctrine and strengthens the resilience of defense capabilities (Mashregh News Agency 2023a). This is of paramount importance for Iran, given that strategic considerations, influenced partly by the nation's isolation and constrained access to the global market imposed by Tehran's major adversary, have consistently prioritized the goal of achieving self-sufficiency in developing indigenous defense capabilities (Tabatabai 2020) with a focus on technological comparative advantages. In 2012, the Supreme Leader issued a comprehensive decree that forbade the procurement of foreign goods and services for defense purposes. The objective was to mitigate reliance on external entities during actual conflicts, thereby ensuring a self-sufficient and secure defense supply (khamenei.ir 2012).

Iran is driven to invest in defense AI by a compelling factor: the continuous integration of advanced technology into the defense and military capabilities of its major adversaries, notably the U.S. and Israel, along with key regional rivals such as Turkey and Saudi Arabia. The technological advancements of these nations pose a potential threat to Iran's asymmetric defense doctrine if it neglects the adoption of technological upgrades. Ideally, Tehran aspires to secure a leading position in the high-stakes military technology race, recognizing the potential for enhanced power and prestige for the Islamic regime in Tehran (khamenei.ir 2019). However, numerous challenges such as insufficient financial and skilled human resources as well as limited access to the global high technology market have impeded the realization of this vision. Therefore, Tehran strategically emphasizes the crucial role of cutting-edge military technology, including AI, as a means to sustain the credibility of its deterrence stance.

Since the entry of defense AI into Iran's mainstream discourse, military leaders have consistently emphasized the pivotal role of AI in streamlining data collection and analysis processes (Mashregh News Agency 2023c). However, there is skepticism regarding whether Iranian leaders possess a thorough understanding of the appropriate level of AI involvement in decision-making during actual conflict scenarios. Despite this uncertainty, incidents stemming from human errors, exemplified by the downing of Ukraine International Airlines Flight 752 over Tehran by Russian-made anti-aircraft missiles in January 2020 (The New York Times 2020) may propel Iran towards the adoption of AI-enabled autonomy in defense capabilities and installations. This strategic shift is aimed at mitigating the impact of human errors and enhancing overall operational efficiency.

Despite the potential benefits and incentives for autonomy in defense AI, the Islamic Republic is likely to maintain a cautious stance. The defensive posture of Iran's armed forces requires a strategy to avoid inadvertently targeting adversary's assets and forces when humans are not fully in the loop of decision-making. Iran consistently demonstrates a reluctance to provoke escalation, maintaining this stance even when supporting its partners and proxies across the region or undertaking retaliatory actions. For example, reports from both Iraqi and American sources indicate that Tehran communicated its specific retaliatory measures to Washington following the killing of IRGC Major General Qasem Soleimani, key architect of Iran's defense doctrine, by American forces in January 2020 (Ayash and Davison 2020). With the integration of AI into its defense capabilities, the Islamic Republic faces the critical challenge of striking a calibrated balance between autonomy and strategic restraint.

2 Developing Defense AI

Iran's development of defense AI remains in its nascent phase, shrouded in strategic ambiguity yet occasionally characterized as loud weapons. Nevertheless, the incorporation of AI into defense capabilities is in line with Iran's defense doctrine, which revolves around three key objectives: deterring threats posed by state adversaries, ensuring the survivability and resilience of critical infrastructure and ensuring domestic stability.

2.1 State Deterrence

Based on its strategic assessment discussed above, Iran has dedicated time and resources to bolstering its asymmetric sea and air capabilities, concurrently expanding its proxy network to enhance its strategic depth. AI emerges as a new enabling factor in Tehran's enhanced deterrence strategy.

As of January 2024, Major General Safavi, the senior military aide to Khamenei and head of the Defense-Security Commission within Iran's Strategic Council on Foreign Relations—an advisory body to the Supreme Leader—stands as the sole senior strategist elucidating Iran's three-fold rationale for integrating AI into naval and air force operations: (1) enhancing agility, (2) accelerating decision-making processes, and (3) reducing reliance on human forces (Mashregh News Agency 2023b).

In November 2023, the IRGC organized its first-ever national conference on emerging opportunities and threats in the maritime domain. Rear Admiral (RADM) Alireza Tangsiri, the commander of the IRGC Navy, identified four areas in which Iran has incorporated AI into its military capabilities: USV, UAV, missile, and submersible. According to Tangsiri (Gerdab 2023a):

- Iranian USVs are autonomous speed boats with extended coverage capabilities, excelling in mission execution through AI-guided missiles for precise and effective target engagement, combining autonomy and strategic firepower.
- Iranian UAVs have advanced with improved AI-driven capabilities, extended range, heightened precision, and stealth technology. Increased flight time, enlarged warheads, and the ability to confront EW tactics enhance offensive capabilities, allowing engagement of moving and maritime targets in diverse military scenarios.
- Iranian missiles feature extended range, adaptive navigation, and multi-system launch capability, with dynamic evasion options. They provide strategic advantages with reduced preparation time, rotational shooting, and counteraction measures against adversaries' EW. AI-based sea-based missiles demonstrate remarkable precision, targeting objectives up to 2000 kilometers away.
- Iranian submersibles showcase versatility in AI-enabled autonomous navigation, executing missions, and contributing to Intelligence, Surveillance & Reconnaissance (ISR) operations. Whether for military or scientific purposes, they navigate challenging underwater environments, playing a pivotal role in advancing technological capabilities beneath the ocean's surface.

On a different front, Iran has incorporated AI into its border control operations. Brigadier General Alireza Sheikh, Deputy of Training and Education of the Army, reveals that AI-enabled portals are now responsible for analyzing and transmitting real-time images and data pertaining to border movements directly to the Army's headquarters in Tehran (Tasnim News Agency 2022). This marks a notable departure from the past, where data collection, up until at least 2020, predominantly relied on human resources (ICAO 2021).

In the realm of C2, senior military commanders underscore the significance of AI in both air and sea domains. The Commander of the IRGC Aerospace Force's Passive Air Defense, for instance, emphasized that "the integration of AI-driven C2 offers crucial decision support to effectively counter extensive and intricate threats. It plays a key role in guiding air defense personnel, enabling them to respond to threats swiftly and appropriately" (Tasnim News Agency 2021a).

In addition to defensive capabilities, Iran's network of proxies serves as a formidable asymmetric asset, not only countering potential kinetic operations but also functioning as a crucial enabler for Tehran to maintain its strategic depth. Publicly available data does not confirm Iran providing AI-driven capabilities to its proxies. Nonetheless, Iranian authorities have openly admitted Tehran's support to both state and non-state actors within the Axis of Resistance (Fars News Agency 2015a). This assistance primarily entails technology transfer more than direct procurement of military equipment (Tabatabai and Clarke 2019), particularly in situations where ongoing resupply poses significant challenges (U.S. Defense Intelligence Agency 2019).

In this context, proxies, especially those in proximity to Israel, may acquire knowledge and technology from Tehran to enhance their AI capabilities. This holds particular significance given Tel Aviv's utilization of AI for ISR and carrying out

strikes against Hamas in Gaza during the military conflict that began in October 2023 (Davies et al. 2023). The IRGC may consider supplying AI-based technologies primarily aimed at countering Israel's ISR capabilities, despite Tehran's own defense AI development being in its early stages.

2.2 Critical Infrastructure Protection

Critical infrastructure remains a prime target in non-kinetic operations. Iran's significant challenges with the Stuxnet virus in its nuclear facilities during the late 2000s (Modderkolk 2024) have prompted a reassessment and refinement of strategies aimed at securing military and civilian critical infrastructure.

Denial and deception (D&D) techniques are instrumental in reducing vulnerability and bolstering the resilience of Iran's strategic assets and installations (U.S. Defense Intelligence Agency 2019). Simultaneously, Iran employs a multilayered passive defense strategy to safeguard civilian critical infrastructure from cyberattacks and external intrusions (Lamrani 2020). This defensive approach has gained prominence, particularly in the face of the evolving landscape where AI has become a potent tool for offensive cyber operations. The integration of AI introduces heightened complexity and diminished traceability to cyberattacks.

With 35% of cyberattacks targeting Iranian civilian critical infrastructure in 2022 leveraging AI (Tasnim News Agency 2023a), the NPDO has strategically prioritized the infusion of AI across all indigenous systems entrusted with national cyber defense responsibilities from 2023 to 2024 (Tasnim News Agency 2023d). Due to Iran's limited access to the global technology market and apprehensions regarding the security of advanced firewall technologies originating from the West, amid concerns of potential exploitation by adversaries, the NPDO has embarked on collaborative efforts with Iranian academic institutions and technology start-ups. This collaboration aims to seamlessly integrate AI into Iran's cyber defense strategy, ensuring a robust and indigenous approach to safeguarding national security.

Adopting a proactive stance towards AI, the NPDO focuses on enhancing all defense capabilities, encompassing infrastructure, through the seamless integration of AI. The Organization has ambitiously outlined mid-2024 as the timeline to realize this goal. This strategic endeavor, complemented by a fusion of D&D techniques and deliberate ambiguity regarding Iran's military advancement, positions the nation to safeguard critical infrastructure in both civilian and military sectors against non-kinetic cyber threats instigated or supported by Tehran's major state adversaries (Martini et al. 2023). Notwithstanding these concerted efforts, the Islamic Republic's technological lag may persist, rendering critical infrastructure vulnerable to cyberattacks as AI and other emerging technologies continue to advance.

NPDO asserts that Iran's cyber defense capabilities encompass an offensive component specifically crafted for retaliatory purposes. The focal points of Iran's cyber offensive endeavors primarily involve the infrastructure of the U.S. and Israel (Maloney 2023). Nevertheless, states perceived as threats to the regime's S3, such

as Albania, due to harboring the Islamic Republic's most formidable dissident group, are not exempt from Tehran's cyber offensive actions (Oghanna 2023). According to the 2024 U.S. Annual Threat Assessment, "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied and partner networks and data" (Office of the Director of National Intelligence 2024). The expanding expertise of Iran may involve the incorporation of AI in its cyber offense capabilities.

2.3 Domestic Stability

Post-revolutionary Iran has been marked by persistent protests and social upheaval. Since September 2022, the Iranian regime has grappled with one of the most extensive and prolonged series of protests since the 1979 Revolution, further eroding the key components of the regime S3. In response, Iran has consistently strengthened its law enforcement, military, and security apparatuses. This persistent pattern aims to suppress dissent at home and abroad and includes censorship to advance ideological control over the nation and impose a coercive order within Iranian society (Daragahi 2023; Fitzpatrick 2023). In this context, solutions combining AI with biometric technologies like facial recognition, developed by Iranian startups or imported from China (Alimardani 2023), are growing in importance to target dissenting citizens. In view of ensuring domestic control, Iran and Russia seem willing to formalize a bilateral Grand Interstate Treaty to advance military-technological cooperation (Institute for the Study of War 2023), which could include cooperation on AI.

3 Organizing Defense AI

The Islamic Republic's General Staff of the Armed Forces (GSAF) serves as the highest defense and military authority in the country, responsible for coordinating and overseeing the activities of the Iranian Armed Forces including the IRGC, the Army and the Ministry of Defense (MoD). Led by the Chief of General Staff, appointed by the Supreme Leader, the GSAF is instrumental in formulating defense policies, operational planning, and ensuring the overall readiness of Iran's armed forces and defense agencies.

The Army and the IRGC have distinct roles outlined by the GSAF under the Supreme Leader's guidance. Specifically, the IRGC operates in the Persian Gulf, while the Army manages operations in the Caspian Sea and the Sea of Oman. Domestically, the Revolutionary Guard oversees internal security, while the Army exclusively handles air defense (Tabnak News Agency 2022). However, unlike the Army, the IRGC faces no constraints on involvement in domestic politics and financial activities. In addition, the IRGC consists of two additional forces: the Quds Force, responsible for unconventional warfare, intelligence, and special operations

beyond Iran's borders, and the Basij, a paramilitary volunteer force deployed for internal security and crowd control during public protests. The Quds Force and, to a lesser extent, Basij, have played a crucial role in advancing Iran's strategic depth and revolutionary ideologies globally (Bahgat and Ehteshami 2021). Thus, through its engagement in domestic affairs and external actions, the IRGC has steadily increased its influence over time, becoming a decisive force in safeguarding Tehran's S3.

The GSAF is dedicated to acquiring advanced conventional and specialized defense capabilities for both the Army and the IRGC. With a focus on achieving self-sufficiency and developing indigenous defense capabilities, three departments within the GSAF—namely, "Logistics, Support, and Industrial Research," "Research and Training," and "Science, Research, and Technology"—are directly involved in steering defense research and development (R&D). However, the IRGC, the Army and the MoD have their own R&D departments, dedicated to advancing military technologies.

The Research and Self-Sufficiency Jihad Organization (RSSJO) is an entity closely associated with the air, navy, and ground forces of both the IRGC and the Army in Iran. The primary roles of these six organizations revolve around overseeing and conducting specialized R&D activities tailored to the unique needs of each respective military force. These entities also collaborate with civilian universities and military research institutes. Notable examples include Imam Hossein University (IHU), Malek Ashtar University of Technology (MUT), and Imam Khamenei University of Marine University and Technology (IKUMUT), which are three IRGC-affiliated research universities. Additionally, the Army operates the War University and the Imam Khomeini Naval University of Noshahr. These academic institutions engage in direct collaboration with various RSSJOs for R&D in defense. With a specific focus on defense AI, the RSSJOs are believed to be involved in independent R&D efforts and joint initiatives with academic institutions.

The MoD is also involved in defense R&D, overseeing multiple entities dedicated to advancing military technology and providing military capabilities to both the IRGC and the Army. The MoD comprises 13 companies and two organizations, with each entity being allocated a specific budget from the country's annual public budget. The Aerospace Industries Organization (AIO) stands out as a pivotal entity within the MoD, overseeing the development and production of aerospace technologies for both civilian and military applications. Established in the early 1980s, the AIO plays a central role in advancing Iran's capabilities across various domains, including reconnaissance planes, UAVs, cruise and ballistic missiles, satellite launch programs, avionics, propulsion systems, and aerospace manufacturing (IFMAT n.d.). Subsidiaries, subordinates, and front companies affiliated with the AIO have been implicated in procuring equipment worth millions of euros for the development of Iran's missile program (U.S. Department of the Treasury 2006). AIO developed and unveiled the first AI cruise missile, Abu Mahdi, in July 2023 (Iran International 2023).

As the MoD and its affiliated entities are engaged in the development of advanced military technology, a senior authority within the MoD announced in December

2022 that the Ministry has signed partnership agreements with 80 universities and the majority of the 800 industrial towns nationwide (IRNA 2022). The connectivity between universities, industrial towns, and MoD entities is facilitated primarily through two research institutions: the Defensive Innovation and Research Organization (DIRO) and the Defense Industries Training and Research Institute (DITRI).

Formerly led by Mohsen Fakhrizadeh until 2020, DIRO functions as Iran's equivalent to the U.S.'s Defense Advanced Research Projects Agency (DARPA), focusing on the development of cutting-edge technologies for defense and military applications. Besides, DITRI serves as a crucial component of the MoD's support structure, providing high-level scientific and technological assistance for educational and research processes. It plays a principal role in fostering technology and innovation within the defense industries. DITRI functions as a hub for missile design and the manufacturing of crucial components essential to produce solid rocket fuel (Iran Watch 2019).

No publicly available data or evidence exists regarding the involvement of these institutions in defense AI. However, considering the MoD's tangible strides in developing AI-driven capabilities, as demonstrated by the Abu Mhadi missile, the prospect of the MoD's departments and agencies playing a role in defense AI is not merely speculative.

This assumption is reinforced by the actions of the Supreme Council of the Cultural Revolution (SCCR), which established a dedicated Commission for Defense AI within its Secretariat in September 2022 (SCCR 2022). The Commission comprises representatives from all branches of the armed forces, the SGAF, the Office of the Supreme Leader, the Ministry of Intelligence, and the Ministry of Higher Education. This composition underscores the paramount importance placed on cultivating synergy and collaboration among diverse stakeholders in the realm of defense AI.

In the domain of critical infrastructure protection, the primary duty of securing military critical infrastructure rests with the armed forces and the MoD. Furthermore, the NPDO is assigned the responsibility of ensuring the safety and resilience of civilian critical infrastructure. As per the NPDO's director, this undertaking is accomplished with the collaboration of Iranian start-ups. The NPDO has also entered into partnership agreements with several civilian technology universities to garner assistance and intellectual support for its missions (SSN 2022). A noteworthy aspect of these agreements is the commitment of the universities to establish academic programs dedicated to the NPDO's focal areas. The NPDO has pledged to incorporate AI into safeguarding critical infrastructure. In pursuit of this goal, collaboration with start-ups and universities is anticipated to encompass elements of defense AI.

4 Funding Defense AI

In 2022 and 2023, Iran allocated €6.2bn and @6.3bn, respectively, to its defense budget (Emirates Policy Center 2023). Aligned with Iran's 7th Five-Year Development Plan, which shapes the country's annual budgets and development strategies until 2028, a provision exists mandating the dedication of at least 5% of the public budget to enhance defense capabilities (Government of Iran 2023). However, obtaining precise figures for defense AI R&D proves challenging due to the complex network of stakeholders in this domain, characterized by opaque budgets and the partial allocation of efforts, if any, to defense AI within each entity (McInnis 2017b).

In accordance with the latest annual budget for the fiscal year 2023, commencing on March 21, 2023, the AIO has been allocated the highest research budget among all entities under the MoD. The designated budget for AIO's research is €59,000; however, it does not provide a clear breakdown indicating the specific amount earmarked for investment in defense AI. The total research budget for the 15 entities within the MoD is approximately €265,000 (Shenasname 2023).

In relation to passive defense, the annual budget for the fiscal year 2023 designates €6.6M exclusively for the NPDO (Shenasname 2023). Furthermore, each agency and ministry is mandated to allocate a one-percent budget commitment to support passive defense initiatives facilitated by the NPDO, resulting in a combined contribution of €1.6bn throughout the fiscal year 2022 (SNN 2023). Although the specific allocation of these funds for defense AI remains unclear, the NPDO's emphasis on the comprehensive integration of AI into the critical infrastructure protection implies that a substantial portion of the budgets is likely directed towards advancing defense AI capabilities.

5 Fielding and Operating Defense AI

Despite a growing recognition of the pivotal role played by AI in Iran's defense doctrine, the current state of deployment, as per publicly available data, does not definitively illustrate complete integration into the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). Financial constraints emerge as a crucial impediment to Iran's progress, given that the R&D and implementation of advanced AI technologies demand substantial resources. Moreover, the challenges are exacerbated by the clear technological advantage maintained by adversaries compared to Tehran's utilization of less sophisticated, if not outdated, gear.

The strategic choices made by Iran in this context indicate a nuanced approach aimed at navigating financial limitations, addressing technological disparities, and progressively constructing a more resilient defense infrastructure capable of tackling contemporary challenges (Martini et al. 2023). Within this framework, the

deployment of AI remains selective, primarily confined to a few niche defense capabilities, representing a pragmatic response to the existing hurdles.

As of January 2024, the Abu Mahdi precision-guided cruise missile, formally disclosed in July 2023, signifies Iran's first foray into modern defense capabilities, wherein AI integration has been engineered into its core architecture since inception. Positioned as the premier long-range anti-ship cruise missile, it boasts a range exceeding 1000 kilometers, advanced AI-enabled C2 systems, radar evasion, and real-time course adjustments. Designed for engaging warships, frigates, and destroyers, it features dual-band radar seekers for enhanced precision. The launch system enables swift preparation and deployment, with multi-missile launch capability for synchronized convergence onto a target. Developed by the Ministry of Defense, it's a cutting-edge addition to Iran's military capabilities, deployed to both the IRGC and the Army. The missile's inauguration was characterized by the Iranian Minister of Defense as "strategic" and "unprecedented" in sophistication and impact (Tasnim News Agency 2023c).

Two additional missiles have been unveiled by Iranian military officials, featuring AI capabilities. In contrast to the Abu Mahdi missile, both the ballistic missile Fath-360 and the Ghadir cruise missile represent military capabilities that have been augmented through the integration of AI. The Fath-360 missile is a short-range tactical ballistic missile guided by satellites. It has a range of 30 to 120 km and can carry a warhead weighing up to 150 kg. Developed by the MoD, it was initially deployed to the IRGC in 2020 and later to the Army in 2021. The Ghadir cruise missile, introduced in 2014, is an anti-ship cruise missile featuring a range of 330 km. This missile can be deployed from both coastal installations and naval vessels (Gerdab 2023b). These AI-augmented missiles made their debut during the IRGC war game in August 2023, reportedly as a response to Russia's move against Iran's territorial integrity. This followed Moscow's support for the United Arab Emirates' stance on disputed islands with Iran, expressed in the July 2023 joint statement of the sixth Russia-Gulf Cooperation Council Joint Ministerial Meeting for Strategic Dialogue (Reuters 2023).

Iran's UAVs have garnered significant attention, particularly for their use by Russian forces in Ukraine. According to the U.S. official assessment, Iran supply Russia with UAVs to bolster Moscow's capacity to target Ukraine, given the depletion of Russia's own precision-guided munitions (U.S. Defense Intelligence Agency 2023). Subsequently, Iran has delivered numerous one-way attack UAVs, the Shahed-131 and Shahed-136, to support Russia's military operations in Ukraine. The Shahed-181, which can be used for ISR and combat missions and can be equipped with two precision-guided missiles (D'Urso 2020), is the sole UAV reportedly equipped with AI technologies within its class. Reports covering the IRGC Aerospace Force's annual military exercise in 2021 speculated that AI might have been used to coordinate navigation and flight paths to enable a group of several UAVs to fly in synchronized formation (Tasnim News Agency 2021b).

In the realm of securing critical infrastructure, each Iranian province has unique passive defense strategies sanctioned by the NPDO. These strategies are specifically designed to align with the varied networks and capabilities inherent to each

province (PANA 2023). This decentralized approach ensures a targeted and flexible nationwide passive defense strategy. Moreover, the NPDO has established offices within public agencies and national industries, providing guidance and regulations to fortify the resilience of the infrastructure (Tasnim News Agency 2023a). Additionally, it conducts real-time monitoring to guarantee the continual safety and security of vital assets, safeguarding against cyberattacks and external intrusions. With the NPDO's renewed focus and commitment to AI, it becomes evident that a significant portion of these passive defense efforts is updated through the application of AI technologies.

In sum, RADM Tangsiri's remarks on the defense AI development discussed above recognize Iran's multiple endeavors in this field. Nevertheless, upon closer examination of instances and use cases, it becomes evident that the envisioned advancement of defense AI in the Islamic Republic is not materializing to the extent initially articulated.

6 Training for Defense AI

The IHU and MUT are public post-graduate universities specifically designed to cater to the research and operational needs of the Armed Forces and/or the MoD. For the academic year 2023-2024, both universities had a capacity to admit 29 students for the Master of Science in AI. Additionally, these institutions admitted 26 students for the Master of Science in EW and 56 students for the Master of Science in passive defense. Upon graduation, admitted students are obligated to work either at the Armed Forces or the MoD (Sanjesh Organization 2023a). Regarding the PhD programs, the MUT has accepted four researchers for AI, while the IHU has admitted four researchers for EW for the academic year 2023-2024. Upon completion of their studies, the researchers are required to contribute their expertise to the Armed Forces (Sanjesh Organization 2023b).

The War University welcomes post-graduate officers from "friendly and allied" foreign countries. As of 2021, the institution has provided training to officers from North Korea, India, Oman, Pakistan, and Iraq. The training encompasses both theoretical and operational courses (ISNA 2021). While specific details about the incorporation of defense AI into the curriculum are not publicly available, given the program's emphasis on information and intelligence planning, it is plausible that the utilization of military technology, including AI for ISR, forms an integral component of the program.

Considering the ever-evolving landscape of AI, continuous in-service education and training programs are imperative for research and military personnel engaged in defense AI within the Armed Forces and the MoD. As the Army, the IRGC, and the MoD each maintain their dedicated research institutes, these institutes serve the crucial function of collecting best practices and state-of-the-art capabilities from both leading nations and potential adversaries (Fars News Agency 2015b), with the goal of bolstering local efforts in the field of defense AI. In this regard, Iran has also

benefited from training with countries like North Korea. Furthermore, unverified reports have occasionally surfaced indicating Tehran's collaboration with authoritarian states such as Russia, China, and Belarus for technology transfer and military personnel training (Ben Taleblu 2023). Despite the Supreme Leader's ban on acquiring foreign goods and services for defense, with certain exceptions, including technology transfer, it is difficult to gauge to what extent these training and technology transfer initiatives also cover defense AI.

Iran's approach to support proxies encompasses the transfer of technology. This requires equipping proxies with knowledge and technology on the assembly and use of the military capabilities (Al-Alam 2024). There is currently no evidence suggesting that Iran's proxies employ defensive AI capabilities. Nevertheless, it is reasonable to conjecture that Iranian military scientists and commanders may have shared advanced aspects of EW with Tehran's proxies. As defense AI advances, there is a potential for these proxies to exploit the positive externalities of defense AI capabilities provided by the Islamic Republic. This is particularly significant given that Iran's adversaries, such as Israel, have been using defense AI to counter Hamas in the Gaza Strip since October 2023.

In the realm of passive defense, the NPDO adopts a strategic approach that prioritizes public awareness. Harnessing the power of mass media and platforms such as Friday Prayers, the Organization is committed to educating and enlightening the public on passive defense measures (U.S. Defense Intelligence Agency 2019). Moreover, with a dedicated presence in industries and public agencies the NPDO strives to provide training and information to employees and workers, emphasizing best practices crucial for civilian infrastructure protection and staff safety in digital spheres. On an annual basis, a dedicated week is devoted to showcasing the accomplishments in passive defense and highlighting the NPDO's initiatives, drawing nationwide attention and admiration (Cyberno 2023). This weeklong event serves as a catalyst for amplifying the Organization's outreach through mass media channels, thereby fostering heightened public awareness.

7 Conclusion

Defense technological innovations play a pivotal role in conferring a strategic advantage upon the Islamic Republic—an ideology deeply embedded in the leadership's convictions in Tehran. Iran perceives defense AI as the latest innovation that can be leveraged to safeguard the core tenets of its overarching strategy: the preservation of regime survival, security, and stability against significant state adversaries.

Strongly opposed to the existing world order and its centers of power, the Islamic Republic is unreserved in thinking about and developing defense AI as a means to rekindle its founding vision: a resilient model for the Muslim world and a precursor for all oppressed communities and nations globally. The genuine architects of the Islamic Republic view Iran not merely as a state but as an ideology, and they believe

that AI in defense and other domains holds the potential to actualize the visionary aspiration.

If this is indeed Iran's perception of defense AI as a once-in-a-lifetime opportunity to challenge its major adversaries and transform into an unassailable and inspired power, then the leadership is likely to leave no room for hesitation in capitalizing on defense AI. However, Iran acknowledges its technological inferiority, a consequence of its restricted access to the global technology market. Thus, Iran may seek to expand cooperation with authoritarian regimes to co-develop or import defense AI solutions. But—as happened in the past when Iran stepped up its industrial nuclear programs and worked with Moscow and Beijing behind the scenes (Katz 2021)—any move to advance its defense AI capabilities could pose a direct threat to Russia, indirectly endanger China's interests in the Middle East, and further sour relations with regional powers. Although the Iranian leadership is fully cognizant of these dangers, the deeply ingrained sense of strategic loneliness, that is ingrained in the country's strategic culture, may compel Tehran to prioritize the development of defense AI, leaving little room for alternative options.

References

Akbari, Alireza. 2023. The West felt annoyed by Iran Navy's 86th flotilla circumnavigation. Tehran Times. https://www.tehrantimes.com/news/487622/The-West-felt-annoyed-by-Iran-Navy-s-86th-flotilla-circumnavigation. Accessed 30 January 2024

Al-Alam. 2024. From General Soleimani's secret trip to Gaza to the transfer of modern weapons manufacturing technology to the Resistance. https://fa.alalam.ir/news/6782868/. Accessed 30 January 2024

Alfoneh, Ali. 2020. What Iran's military journals reveal about the goals of the Quds force. The Arab Gulf States Institute in Washington. https://agsiw.org/what-irans-military-journals-reveal-about-the-goals-of-the-quds-force/. Accessed 30 January 2024

Alimardani, Mahsa. 2023. Aggressive new digital repression in Iran in the era of the woman, life, freedom uprisings. Carnegie Endowment for International Peace. https://carnegieendowment.org/2023/11/29/aggressive-new-digital-repression-in-iran-in-era-of-woman-life-freedom-uprisings-pub-91025. Accessed 30 January 2024

Anderson, Collin, and Karim Sadjadpour. 2018. *Iran's cyber threat. Espionage, sabotage, and revenge*. Washington, DC: Carnegie Endowment for International Peace.

Ayash, Kamal, and John Davison. 2020. Hours of forewarning saved U.S., Iraqi lives from Iran's missile attack. Reuters. https://www.reuters.com/article/idUSKBN1ZC219/. Accessed 30 January 2024

Bahgat, Gawdat, and Anoushiravan Ehteshami. 2021. *Defending Iran; From revolutionary guards to ballistic missiles*. Cambridge: Cambridge University Press.

Bailey, Michelle R. 2022. The Iranian maritime challenge. Naval Postgraduate School. https://apps.dtic.mil/sti/citations/trecms/AD1200387. Accessed 30 January 2024

Barnes-Dacey, Julien, and Hugh Lovatt. 2022. Principled pragmatism: Europe's place in a multipolar Middle East. European Council on Foreign Relations. https://ecfr.eu/publication/principled-pragmatism-europes-place-in-a-multipolar-middle-east/. Accessed 30 January 2024

Battlespace. 2023. C2, tactical communications, Ai, cyber, 5G, EW, cloud computing and homeland security update. https://battle-updates.com/update/c2-tactical-communications-ai-cyber-5g-ew-cloud-computing-and-homeland-security-update-8/. Accessed 30 January 2024

Ben Taleblu, Behnam. 2023. *Arsenal; Assessing the Islamic Republic of Iran's Ballistic Missile Program*. Washington, DC: Foundation for Defense of Democracies.

Black, James et al. 2022. Multi-domain integration in defense; Conceptual approaches and lessons from Russia, China, Iran and North Korea. RAND Europe. https://www.rand.org/pubs/research_reports/RRA528-1.html. Accessed 30 January 2024

Boffey, Daniel. 2023. Revealed: Europe's role in the making of Russia killer drones. The Guardian. https://www.theguardian.com/world/2023/sep/27/revealed-europes-role-in-the-making-of-russia-killer-drones. Accessed 30 January 2024

Brodsky, Jason M. 2023. Iran gleefully eyes the protests in Israel, looking for weaknesses to exploit. The Middle East Institute. https://www.mei.edu/publications/iran-gleefully-eyes-protests-israel-looking-weaknesses-exploit. Accessed 30 January 2024

Chulov, Martin. 2023. Drones target Iranian weapons factory in central city of Isfahan. The Guardian. https://www.theguardian.com/world/2023/jan/29/drone-attack-hits-iran-ammunition-factory-reports. Accessed 30 January 2024

Cyberno. 2023. The passive defense week of 1402 and the importance of cyber defense. https://cyberno.ir/page/posts/135/. Accessed 30 January 2024

D'Urso, Stefano. 2020. Iran showcases Shahed 181 and 191 drones during "Great Prophet 14" Exercise. The Aviationist. https://theaviationist.com/2020/08/02/iran-showcases-shahed-181-and-191-drones-during-great-prophet-14-exercise/#google_vignette. Accessed 30 January 2024

Daragahi, Borzou. 2023. Iran is using its cyber capabilities to kidnap its foes in the real world. Atlantic Council. https://www.atlanticcouncil.org/blogs/iransource/iran-cyber-warfare-kidnappings/. Accessed 30 January 2024

Davies, Harry, Bethan McKernan, and Dan Sabbagh. 2023. 'The Gospel': how Israel uses AI to select bombing targets in Gaza. The Guardian. https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets. Accessed 30 January 2024

Eisenstadt, Michael. 2021. Iran's gray zone strategy: Cornerstone of its asymmetric way of war. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/irans-gray-zone-strategy-cornerstone-its-asymmetric-way-war. Accessed 30 January 2024

Emirates Policy Center. 2023. Iran's New Year military budget and shifting priorities. https://epc.ae/en/details/featured/iran-s-new-year-military-budget-and-shifting-priorities. Accessed 30 January 2024

Fars News Agency. 2015a. Amir Abdollahian: we have no qualms about transferring rocket manufacturing technology to Palestine. https://www.farsnews.ir/news/13931118000694/. Accessed 30 January 2024

———. 2015b. Defense Industries Educational and Research Institute, an arm to monitor and communicate with the world's military industries. https://www.farsnews.ir/news/13940431000810/. Accessed 30 January 2024

Fitzpatrick, Kitaneh. 2023. The Soft War: Understanding Iran's domestic ideological crisis. Critical Threats. https://www.criticalthreats.org/analysis/the-soft-war-understanding-irans-domestic-ideological-crisis. Accessed 30 January 2024

France24. 2023. Iran fuel supplies cut by US, Israel 'cyber attack', oil minister says. https://www.france24.com/en/live-news/20231218-iran-fuel-supplies-cut-in-cyber-attack-minister. Accessed 30 January 2024

Gambrell, Jon. 2023. An Iranian nuclear facility is so deep underground that US airstrikes likely couldn't reach it. Associated Press. https://apnews.com/article/iran-nuclear-natanz-uranium-enrichment-underground-project-04dae673fc937af04e62b65dd78db2e0. Accessed 30 January 2024

Gerdab. 2023a. Rear Admiral Tangsiri: Our missiles are equipped with artificial intelligence. https://gerdab.ir/0009eT. Accessed 30 January 2024

———. 2023b. Unveiling of missiles equipped with artificial intelligence in the IRGC Navy. https://gerdab.ir/fa/news/36368/. Accessed 30 January 2024

Government of Iran. 2023. Allocation of at least 5% of public budget resources in the 7th plan to strengthen the country's defense infrastructure. https://dolat.ir/detail/425572. Accessed 30 January 2024
ICAO. 2021. Flight PS752 accident investigation; Final report. https://www.icao.int/safety/air-navigation/AIG/Documents/Safety%20Recommendations%20to%20ICAO/Final%20Reports/PS752Finrep.pdf. Accessed 30 January 2024
IFMAT. n.d. Aerospace Industries Organization (AIO). https://www.ifmat.org/12/27/aerospace-industries-organization/. Accessed 30 January 2024
INSF. 2003. Vision, mission, and strategy. https://insf.org/en/page/29/vision-mission-and-strategy. Accessed 30 January 2024
Institute for the Study of War. 2023. Russian offensive campaign assessment, January 15, 2024. https://understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-15-2024. Accessed 30 January 2024
Iran International. 2023. Iran boosts navy with acquisition of new long-range cruise missiles. https://www.iranintl.com/en/202307259607. Accessed 30 January 2024
Iran Press. 2020. Shahed drone, symbol of Iranian creativity in reverse engineering RQ-170 drone. https://iranpress.com/shahed-drone-symbol-of-iranian-creativity-in-reverse-engineering-rq-170-drone. Accessed 30 January 2024
Iran Watch. 2019. Organization of defensive innovation and research. https://www.iranwatch.org/iranian-entities/organization-defensive-innovation-and-research. Accessed 30 January 2024
IRNA. 2022. Deputy Minister of Defense: developing the relationship between the defense industry and the university is one of the strategic principles of the Ministry of Defense. https://www.irna.ir/news/84968285/. Accessed 30 January 2024
ISNA. 2021. Foreign students of the Army University graduated. https://www.isna.ir/news/1400060100670/. Accessed 30 January 2024
Javadi, Mahmoud. 2021. Iran's emerging new 'Second Europe' strategy may be doomed. Foreign Policy. https://foreignpolicy.com/2021/10/29/iran-europe-policy-raisi-niclear-deal-jcpoa/. Accessed 30 January 2024
Katz, Mark. 2021. Russia secretly feared the Iran nuclear deal. Here's why. Atlantic Council. https://www.atlanticcouncil.org/blogs/iransource/russia-secretly-feared-the-iran-nuclear-deal-heres-why/. Accessed 30 January 2024
khamenei.ir. 2008. The strategic depth of the Islamic Republic of Iran, looking at the 20-year perspective. https://khl.ink/f/9199. Accessed 30 January 2024
———. 2012. Communicating the general policies of the establishment on defense and security self-sufficiency. https://khl.ink/f/37922. Accessed 30 January 2024
———. 2019. It is disgraceful to remain a student of westerners forever. https://english.khamenei.ir/news/6405/It-is-disgraceful-to-remain-a-student-of-westerners-forever. Accessed 30 January 2024
———. 2021. We should move on the path to making Iran a source of science within 50 years. https://english.khamenei.ir/news/8767/We-should-move-on-the-path-to-making-Iran-a-source-of-science. Accessed 30 January 2024
———. 2022a. Current world order will be replaced by a new order where US is isolated, Asia powerful, Resistance Front expanded. https://english.khamenei.ir/news/9273/Current-world-order-will-be-replaced-by-a-new-order-where-US. Accessed 30 January 2024
———. 2022b. Role of Arrogant Powers' policies in recent bitter events in Iran is obvious. https://english.khamenei.ir/news/9189/Role-of-Arrogant-Powers-policies-in-recent-bitter-events-in. Accessed 30 January 2024
———. 2023. The 86th Flotilla's successful trip around the world proved high seas belong to everyone. https://english.khamenei.ir/news/10001/The-86th-Flotilla-s-successful-trip-around-the-world-proved-high. Accessed 30 January 2024
Kirkpatrick, David D., Farnaz Fassihi, and Ronen Bergman. 2020. Killer robot? Assassination of Iranian scientist feeds conflicting accounts. The New York Times. https://www.nytimes.

com/2020/12/02/world/middleeast/iran-assassination-nuclear-scientist.html. Accessed 30 January 2024
Lamrani, Omar. 2020. Iran's conventional military capabilities. New Lines Institute. https://newlinesinstitute.org/strategic-competition/irans-conventional-military-capabilities/. Accessed 30 January 2024
Mahmoodi, Mehrdad. 2005. Target automatic identification in marine operations. *Quarterly Journal of Military Science and Tactics* 2: 55–61.
Maloney, Suzanne. 2023. Addressing Iran's evolving threats to US interests. The Brookings. https://www.brookings.edu/articles/addressing-irans-evolving-threats-to-us-interests/. Accessed 30 January 2024
Martini, Jeffrey, et al. 2023. *Deterring Russia and Iran; Improving effectiveness and finding efficiencies*. Washington, DC: RAND Corporation.
Mashregh News Agency. 2023a. Commander of the IRGC Navy: Missiles equipped with artificial intelligence were installed on IRGC vessels. https://www.mashreghnews.ir/news/1557570/. Accessed 30 January 2024
———. 2023b. Major General Safavi: future threats against Iran are sea-based and air-based. https://www.mashreghnews.ir/news/1544324/. Accessed 30 January 2024
———. 2023c. The nightmare of death does not leave the hearts of the officials of the Zionist regime/ The sea is a place to adapt the concepts of tactics, operations and strategy. https://www.mashreghnews.ir/news/1544625/. Accessed 30 January 2024
———. 2023d. Why do western leaders consider artificial intelligence dangerous?. https://www.mashreghnews.ir/news/1534187/. Accessed 30 January 2024
McInnis, Matthew. 2017a. Iranian concepts of warfare: understanding Tehran's evolving military doctrines. American Enterprise Institute. https://www.aei.org/research-products/report/iranian-concepts-of-warfare-understanding-tehrans-evolving-military-doctrines/. Accessed 30 January 2024
———. 2017b. Understanding the Iranian military budget. American Enterprise Institute. https://www.jstor.org/stable/resrep03275.5. Accessed 30 January 2024
MEHR News Agency. 2017. Enemy's likely threats against Iran to be through air, sea. https://en.mehrnews.com/news/130403/Enemy-s-likely-threats-against-Iran-to-be-through-air-sea. Accessed 30 January 2024
Mirzaei, Pooya. 2023. The key for actively dealing with cognitive warfare. Nour News Agency. https://nournews.ir/En/News/145443/The-key-for-actively-dealing-with-cognitive-warfare. Accessed 30 January 2024
Modderkolk, Huib. 2024. Sabotage in Iran. de Volkskrant. https://www.volkskrant.nl/kijkverder/v/2024/sabotage-in-iran-een-missie-in-duisternis~v989743/. Accessed 30 January 2024
Nadimi, Farzin. 2018. Iran's Passive defense organization: another target for sanctions. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/irans-passive-defense-organization-another-target-sanctions. Accessed 30 January 2024
Nazarinejad, Ahamd Ali, and Abdol-Ali Pourshasb. 2020. Adopt passive defense strategies to protect the critical infrastructure of the Islamic Republic of Iran. *Quarterly Scholar Science Journal of Strategic Defense Studies* 18: 313–336.
NTI. n.d. Bakhtaran Missile Base. https://www.nti.org/education-center/facilities/bakhtaran-missile-base/. Accessed 30 January 2024
Office of the Director of National Intelligence. 2024. 2024 annual threat assessment of the U.S. Intelligence Community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf. Accessed 6 May 2024
Oghanna, Ayman. 2023. How Albania became a target for cyberattacks. Foreign Policy. https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/. Accessed 30 January 2024
PANA. 2023. The comprehensive passive defense plan for 31 provinces is on the agenda. http://www.pana.ir/news/1417575. Accessed 30 January 2024

Raouf, Huda. 2019. Iranian quest for regional hegemony: motivations, strategies and constrains. *Review of Economics and Political Science* 4: 242–256. https://doi.org/10.1108/REPS-02-2019-0017.

Reuters. 2021. Iran says Israel, U.S. likely behind cyberattack on gas stations. https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/. Accessed 30 January 2024

———. 2023. Iran summons Russian ambassador over statement on Gulf islands. https://www.reuters.com/world/iran-summons-russian-ambassador-over-statement-three-islands-state-media-2023-07-12/. Accessed 30 January 2024

Sanjesh Organization. 2023a. Master's degree entrance exam guidebook. https://media.imna.ir/d/2023/05/31/0/1875672.pdf?ts=1685533523000. Accessed 30 January 2024

———. 2023b. PhD entrance exam guidebook. https://phdtest.ir/wp-content/uploads/2023/04/PhD1402-entekhab-reshte-PhDTest_ir.pdf. Accessed 30 January 2024

Satam, Parth. 2023. After hypersonic, Iran says its new missile is A.I-enabled; Can change direction & angle to hit targets. The EurAsian Times. https://www.eurasiantimes.com/after-hypersonic-iran-says-its-new-missile-is-a-i-enabled/. Accessed 30 January 2024

SCCR. 2022. Bylaws of the strategic council for defense and security science, technology and innovation. https://sccr.ir/pro/3296/. Accessed 30 January 2024

Shenasname. 2023. The budget law of 1402. http://bit.ly/budgetlaw1402. Accessed 30 January 2024

SNN. 2023. General Jalali: zero credit in 1402 for passive defense is not good for the country. https://snn.ir/fa/news/1062928/. Accessed 30 January 2024

SSN. 2022. Signing of a joint cooperation agreement between Tabriz University and the country's non-operational defense organization. https://snn.ir/fa/news/1047645/. Accessed 30 January 2024

Tabatabai, Adnan. 2019. Iran in the Middle East: The Notion of "Strategic Loneliness". ISPI. https://www.ispionline.it/en/publication/iran-middle-east-notion-strategic-loneliness-22246. Accessed 30 January 2024

Tabatabai, Ariane M. 2020. *No conquest, no defeat; Iran's national security strategy*. Oxford: Oxford University Press.

Tabatabai, Ariane M., and Clarke Collin P. 2019. Iran's proxies are more powerful than ever. The RAND Corporation. https://www.rand.org/pubs/commentary/2019/10/irans-proxies-are-more-powerful-than-ever.html. Accessed 30 January 2024

Tabatabai, Ariane M., et al. 2021. *Iran's military interventions; Patterns, drivers, and signposts*. Washington, DC: RAND Corporation.

Tabnak News Agency. 2022. Why were Army and IRGC not merged?. https://www.tabnak.ir/fa/news/1114310. Accessed 30 January 2024

Tasnim News Agency. 2021a. General Shaban: for the first time, we used artificial intelligence technology in the exercise. https://www.tasnimnews.com/fa/news/1400/07/21/2589031/. Accessed 30 January 2024

———. 2021b. The army reached the edge of the global technology of AI suicide drones. https://www.tasnimnews.com/fa/news/1400/02/07/2492448/. Accessed 30 January 2024

———. 2022. The war in Ukraine is monitored daily/The focus on the drone was with a view to recent wars. Conversation with Brigadier General Sheikh. https://www.tasnimnews.com/fa/news/1401/07/02/2775676/. Accessed 30 January 2024

———. 2023a. General Jalali: cyber defense systems are being equipped with artificial intelligence. https://www.tasnimnews.com/fa/news/1402/08/22/2987992/. Accessed 30 January 2024

———. 2023b. Major General Safavi: We have to go to the moon in space and in the sea to the north and south poles. https://www.tasnimnews.com/fa/news/1402/07/26/2973815/. Accessed 30 January 2024

———. 2023c. Minister Ashtiani announced: the use of artificial intelligence in the Abu Mahdi long-range missile system. https://www.tasnimnews.com/fa/news/1402/05/03/2931047/. Accessed 30 January 2024

———. 2023d. Using artificial intelligence to prevent cyber attacks in the power industry. https://www.tasnimnews.com/fa/news/1402/08/06/2979607/. Accessed 30 January 2024
Tehran Times. 2023a. Iran Army launches electronic warfare drills. https://www.tehrantimes.com/news/488330/Iran-Army-launches-electronic-warfare-drills. Accessed 30 January 2024
———. 2023b. Iran thwarted 10 big cyberattacks in a year. https://www.tehrantimes.com/news/490483/Iran-thwarted-10-big-cyberattacks-in-a-year. Accessed 30 January 2024
The New York Times. 2020. Plane shot down because of human error, Iran says. https://www.nytimes.com/2020/01/11/world/middleeast/plane-crash.html. Accessed 30 January 2024
U.S. Defense Intelligence Agency. 2019. *Iran military power*. Washington, DC: U.S. Government Publishing Office.
——— 2023. 2023 Iranian UAVs in Ukraine. https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/UAV_Book.pdf. Accessed 30 January 2024
U.S. Department of the Treasury. 2006. Treasury adds two entities to the list of Iranian weapons proliferators. https://home.treasury.gov/news/press-releases/hp17. Accessed 30 January 2024
Wintour, Patrick. 2020. Iran says AI and 'satellite-controlled' gun used to kill nuclear scientist. The Guardian. https://www.theguardian.com/world/2020/dec/07/mohsen-fakhrizadeh-iran-says-ai-and-satellite-controlled-gun-used-to-kill-nuclear-scientist. Accessed 30 January 2024

Passive Ambitions, Active Limitations: Defence AI in India

Shimona Mohan

Right from its Independence in 1947, India recognized that to advance in a rapidly changing world and establish itself as a nation without relying on the crutches of its erstwhile colonizers, it would need to focus on the development of its technological infrastructure. This was also a clear policy priority, and the early years of India's nationhood involved planning and setting up what would be the first of many Indian Institutes of Technology (IITs) in Kharagpur (Council of Indian Institute of Technology n.d.). The decades following this saw a steady increase in India's international partnerships around science and technology.

Another policy priority that remained consistently high on the agenda since Independence, given the geopolitically turbulent neighbourhood India found itself in, was that of national security. Surrounded by contemporary nuclear powers—Pakistan to the west and China to the east of its northern borders, both of which India fought several limited wars and border conflicts with—India's drive for technological advancement also seeped into its security and military priorities (Weisman 1987). This is why, despite being a nascent nation at the time, India invested heavily in military technology, ultimately developing its own nuclear weapons in 1974 (Kristensen and Kile 2020) and its first guided missile system in 1983 (Rakshak 1998).

However, while India's stake in the arms race undoubtedly accelerated during the Cold War era, its adoption of liberalization, privatization, and globalization (collectively referred to as the LPG reforms, National Council of Educational Research and Training 2023) in the early 1990s led to a shift in its security policy. While border clashes continued—and still continue at a reduced scale—trade relations with China and Pakistan improved irregularly but steadily following the LPG

The views expressed in this article belong to the author alone and do not reflect the views of her organization and affiliations.

S. Mohan (✉)
United Nations Institute for Disarmament Research (UNIDIR), Geneva, Switzerland
e-mail: shimona.mohan@graduateinstitute.ch

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_20

reforms. As a result, policy priorities for India seemed to shift from a security-dominant narrative to a more economy-oriented one, reminiscent of Immanuel Kant's trade peace theory (Russett et al. 1998).

Over the next few decades, the race to securitize critical emerging technologies took a backseat for India in the face of renewed geo-economic aspirations, and investments in tech became primarily industry oriented. Simultaneously, the information technology (IT) boom hit India, and Bangalore became the Silicon Valley of India towards the beginning of the 2000s, taking India's civilian tech and software industry to new heights both in metrics and magnitude. With the increased interest around artificial intelligence (AI) in the past decade, and especially in the past few years with the advent of generative AI, India is adjusting accordingly and now aspires to become a global AI superpower (Raja 2023).

Recently, military AI has been explicitly mentioned as part of India's AI ambition (DDP MoD 2022). This ties into the larger trend of India beginning sporadic activity around military AI in the recent past, although not nearly enough to realize its ambitions. Several internal factors have acted as limitations, including the lack of a structured and organized national roadmap, sizable investments by the government, and the quality of AI talent.

This chapter explores these broad challenges by giving an overview of the defence AI ecosystem in India. It clarifies the ambitions and limitations that India is facing regarding its defence AI architecture, examines multiple aspects of its defence AI landscape as it currently stands, and concludes with a prospective analysis of new challenges and the future trajectory that India sees itself on. This chapter primarily uses open-source information unless explicitly specified.

1 Thinking About Defence AI

After being recognized as a key IT hub, India has repeatedly expressed interest in replicating a similar success in AI. In defence AI, it has a particular line of thinking which is congruent to both its primarily peaceful foreign policy of *vasudhaiva kutumbakam* ('the world is one family' in Sanskrit), and a pragmatic consideration of being competent enough to avoid being dominated by other States. The Defence Minister of India has occasionally stated that India has "no intention to rule the world, [but] we must develop the capability of our [defence] AI technology so that no country can even think of ruling us" (Press Information Bureau 2022d). However, the much higher prioritization of other general-purpose AI—with India exploring AI use (Deloitte 2022) in several industries, ranging from its signature digital public infrastructure (Singal 2023), public services (Elias 2023), healthcare (NASSCOM 2021), and education (India Today 2023), to finance (Menon 2023) and creative profession (Das 2023)—means that defence AI often gets pushed to the sidelines.

This is related to a market trend where India is known for its AI talent but not its AI innovation. India is now ranked amongst the top countries in the world for AI skill penetration and AI talent concentration (IndiaAI 2023) but comes up short

compared to several other countries in terms of AI patents (Inside BigData 2020) and innovation (Cesareo and White 2023). It remains to be seen whether this is a function of its educational, skill and job market environments that prioritize building systems over creating them, of a proportional representation based on its large population, or merely a matter of time for it to catch up on innovation.

However, one recurring factor is that India has seen numerous knee-jerk developments and concentrated efforts around AI, but still has a hazy conception of how to establish a well-oiled AI ecosystem. India's widely adopted 'Make in India' program for import substitution and manufacturing capability enhancement has led to several new startups around AI and software as a service (SaaS), and a sub-campaign to 'Make AI Work for India' has recently also gained support (D'Cruze 2023). Although the assumption is that most workstreams across the government will implicitly follow this campaign, there is no overarching governance system guiding this or explicitly linking this campaign to defence AI production.

The lack of institutionalization around AI poses specific limitations to how efficiently India's AI ambitions are being realized. While the government appetite for defence transformation is present, with the Indian Prime Minister explicitly prioritizing replacing legacy military systems with updated ones in 2021 (The Indian Express 2021a), the fragmentation of its approach causes avoidable hurdles. Moreover, while the defence system brushes up on existing security developments, it risks being blindsided by emerging geopolitical and technological challenges for which government institutions are not prepared, leading to a pile-up of governance oversight.

This context shapes the way India thinks about the use of emerging technology for national security and defence. It is well established that India's relations with its neighbours are rocky at best and hostile at worst. While this was a largely kinetic consideration mostly confined to India's disputed physical borders up until recently, the geopolitical tussles have also gradually seeped into the virtual space. In 2023, India was the most targeted country in the world for state-sponsored cyberattacks—ahead of other popular targets like the US—and facing 13.7% of all cyberattacks globally (Roy 2023). Despite this concerning fact, India has not yet come up with its own cybersecurity law or policy document, instead relying on a dated IT Act from 2000 occasionally amended for current challenges, and the newly minted 2023 Digital Personal Data Protection Act, which primarily serves end-user protection (Ministry of Electronics & Information Technology 2024).

While cyberattacks are notoriously hard to attribute, the prevalent assumption is that most of these attacks were conducted by China and its occasional allies Russia and North Korea (Roy 2023). Considering that Pakistan is also one of India's main geopolitical adversaries but is not included within the attack vector analysis signals that India's updated security policies need to reflect its current realities, and not just its inherent rivalries. India has previously been cognizant of this fact and had attempted to respond to its military clashes with China in Doklam in 2017 (Chengappa and Krishnan 2017) and the Galwan valley in 2020 with a diplomatic and economic standoff as well as a 'tech decoupling' (Kumar 2020).

The latter was an especially gripping public move by the Indian government, which banned about 250 Chinese apps including TikTok, Shein, Aliexpress, etc., in four spates between 2020 and 2022 on the basis of the national security implications of these apps (Bhati 2022). This tech decoupling had borne very limited results since trade with China revived the following year (although the apps remain banned). However, one thing became increasingly clear to defence circles in India—security had definitively taken on a technological characteristic both on and off the battlefield, especially when engaging with more technologically advanced rivals (Off-the-record conversation with an Indian defence policy expert December 2023).

However, in the absence of a dedicated document delineating the thinking of senior military decisionmakers in India around defence AI, it is difficult to clearly see where India intends to take its nascent defence AI ecosystem. Some notional clarity about this is spread across press releases and leader statements, often indicating how defence AI is seen as an important tool for achieving military superiority, especially vis-à-vis over India's adversaries. In parallel, AI is also seen as a substantive means to strengthen and modernize the country's defence forces (DDP MoD 2022).

Moreover, there is also much confusion around where India's responsible innovation and AI ethics priorities lie when it comes to defence AI. A prime example of this is India's two-pronged approach on AI ethics and responsible AI (RAI) in the civilian and military spaces. India attended the Responsible AI in the Military (REAIM) 2023 Conference hosted by the Netherlands, where about 80 governments were represented. About 60 of them signed a Call to Action to include RAI considerations in their military ecosystems. Curiously, India was not amongst them (Government of the Netherlands 2023), and did not give a reason for not signing the Call despite having a clear RAI focus in its civilian AI landscape (NITI Aayog 2021a, b). This was either a result of contrasting priorities, a fragmentation of diplomatic decision making, or an example of India not aligning its security policies with majoritarian alliances in favour of its own security considerations. Such was the case when India was one of four countries to not sign the Nuclear Non-Proliferation Treaty (NPT) (Pai 2020).

Whichever the reason (or combination of reasons), the lack of either a comprehensive military strategy with respect to AI, or an updated AI strategy that includes the defence sphere, is a hurdle for India's AI advancement. This is also set to be exacerbated by the advent of emerging AI technologies, like generative AI, and their new potential impact on defence, such as contextual threats of asymmetric conflict using AI like information warfare and deepfakes (Galston 2020). This has already been observed before—an Indian cybersecurity agency unveiled a wide disinformation network of bot accounts on Twitter running China and Pakistan-favourable material before and after the Galwan valley clash in May 2020 (Goyal and Priyadarshini 2020). This network comprised about 400-500 Twitter accounts that spread misinformation and released deepfake-videos of the clash in an attempt to implicate the Indian army (Goyal and Priyadarshini 2020).

Given this backdrop, India began thinking about civilian applications of AI in 2018 and released its national AI strategy the same year (NITI Aayog 2018). The

strategy came at an initial stage of AI conceptualization by India and refers to AI as "a constellation of technologies that enable machines to act with higher levels of intelligence and emulate the human capabilities of sense, comprehend and act," an understanding which has steadily become a lot more nuanced globally. While the area of robotics and AI was already established within India's defence establishment, with a Centre for Artificial Intelligence and Robotics (CAIR) created under the Defence Research & Development Organization (DRDO) back in 1986, it remained mostly dormant until 2018 (Centre for Artificial Intelligence & Robotics (CAIR) (n.d.)). The following years saw an uptick in India's defence technology developments, and an expansion of its slow AI revolution from the civilian space into the military one.

In 2020, the government organized the Responsible AI for Social Empowerment (RAISE) Conference (Press Information Bureau 2020b). NITI Aayog, the policy think-tank of the Indian government, also released a two-part report in 2021 on approaches toward operationalization of responsible AI principles for civilian AI. In a parallel process, defence AI achieved newfound prioritization in 2018—a multi-stakeholder taskforce on defence AI was created by the government under the chairmanship of renowned Indian industrialist Mr. N Chandrasekaran (Sarangi 2019). The taskforce submitted its recommendations in a report in June 2018 (Press Information Bureau 2018), on the basis of which a number of measures were undertaken to expand the scope of India's defence AI.

2 Developing Defence AI

One of the first institutional changes made in the aftermath of the defence AI taskforce's recommendations was the establishment of the Defence Artificial Intelligence Council (DAIC) under the Ministry of Defence (MoD), as well as a Defence AI Projects Agency (DAIPA) created under the Department of Defence Production (DDP) of the MoD (Press Information Bureau 2022c). In 2019, the MoD also created an AI roadmap for each Defence Public Sector Undertaking (DPSU), with about 70 initial defence-specific AI projects identified for development in the coming few years (Press Information Bureau 2022c).

The development of defence AI during the next few years gained momentum, as about 75 AI-based defence products and technologies, many of which were identified by the AI roadmap (Government of India 2022), were unveiled during the first "AI in Defence" (AIDef) symposium and exhibition organized by the MoD in July 2022 (Press Information Bureau 2022d). Later in the same year, the DDP published a full catalogue of their features, capabilities, applications, and advantages in the public domain, including forewords by key political entities and introductory facts and figures, titled "Artificial Intelligence in Defence: Presenting AI Preparedness of the Country in Defence" (DDP MoD 2022).

The catalogue mentions an array of frontier defence AI products that have already been developed and/or deployed—these include a few types of lethal autonomous

weapons systems (LAWS), 3D-printed sentry systems, rail-mounted robots, autonomous intercept boats, AI-based swarm and storm drones, cognitive radars, unmanned vehicles, motion and anomaly detectors, target identification systems, facial and gesture recognition technologies, instantaneous translators, and monitoring and predictive systems (DDP MoD 2022). These products are being employed both on and behind the frontlines, in combat as well as in logistical and administrative roles.

This focus on the indigenization of defence technology production is also part of the larger Atal Innovation Mission (AIM), which is a whole-of-government approach to promote a culture of innovation across industries (Government of India n.d.-a). The resulting efforts of AIM mean that instead of simply importing, India has started prioritizing international partnerships and agreements around several types of military objectives and new technology, including defence AI. This process has also showcased a trend of altered relations with existing security partners and a renewed effort to establish new avenues of collaborative development and transfer of technology (ToT). An analysis of how India is organizing its international defence AI procurement and partnerships has implications vis-à-vis its foreign policy as well.

In terms of great power politics, India remained principally neutral throughout the Cold War, even though it shared friendlier relations with Russia—including defence ties. The Russian position retains a continued interest in India's expanding defence AI sphere, as evidenced by articles on Russian state-owned media portals like Sputnik News which highlight the importance of India recognizing Russia as a potential academic and research partner for defence AI applications (Trivedi 2023). However, India has recently looked to diversify from Russian imports and collaborations on defence technology primarily due to the cascading effects of the Russia-Ukraine war (Waldwyn and Solanki 2023). While India and Russia have traditionally had close defence ties it is not clear that these ties impact all weapon systems at all times. India still relies on Russia for conventional weaponry and nuclear power (Sharma 2023) but seems to have diversified in terms of emerging military technology; within which the US, China, and their allies seem leagues ahead (Heikkilä 2022). Despite this shift, India and Russia continue to align politically on defence AI and were two of only five states that voted against a 2023 United Nations First Committee resolution expressing concern about the possible negative consequences of LAWS (United Nations 2023).

The lull in the India-Russia defence relationship has made space for other actors, especially Western powers, to forge closer alliances with India. The US, for instance, has convened and rekindled several strategic partnerships on defence technology with India over the past few years, including the Quad (US, India, Japan, Australia), I2U2 (India, Israel, US, UAE), a flagship U.S.-India AI initiative (USIAI), and the bilateral initiative on critical and emerging technologies (iCET). Both countries have also conversed several times (U.S. Department of Defense 2023; Ministry of External Affairs 2023) and pursued collaborations around defence AI, such as through critical technology working groups (Vergun 2023) and partnerships to counter common adversaries like China (Singh 2023). In 2023, the Indian MoD approved the procurement of 31 MQ-9 reaper unmanned aerial vehicles (UAV)

from US-based General Atomics, which will be assembled at a new planned General Atomics facility in India (Renshaw 2023).

Another notable partner country that has allied with India on defence AI is Israel. The Indian Defence Minister and his Israeli counterpart adopted the 'India-Israel Vision on Defence Cooperation' in 2022 to strengthen the existing framework of bilateral defence cooperation on futuristic defence tech, deepen military cooperation, and co-produce new-age weapon systems (Press Information Bureau 2022e). Later the same year, India held a Defence Expo (Press Information Bureau 2022b) where several countries were present at ministerial levels in addition to businesses, investors, and startups. Here, the Indian company Adani Defence and Aerospace, along with its partner Israel Weapon Industries (IWI), unveiled ARBEL, India's first AI-based small weapons-embedded Intelligent Fire Control System (IFCS) with motion sensors (ET Now 2022).

India is now also in talks with other potential defence tech collaborators at various levels. France and India concluded their fifth Annual Defence Dialogue in 2023 with a promise to work together in niche military domains such as space, cyber, and AI (Press Information Bureau 2023b). Australia and India explored the possibility of co-production and joint skilling in defence AI in their 2023 2 + 2 Ministerial Dialogue (Suman 2023). Preceding a similar 2 + 2 Dialogue in 2022, Japan and India also identified key areas of defence cooperation, including UAVs, anti-drone systems, robotics, and intelligence systems (Singh 2022).

India's interest in these conversations around defence AI is only expected to increase given the nascent status of its ecosystem. Currently, many of these defence tech conversations happen at ministerial levels or higher and may or may not trickle down to actual cooperation. And if they do, the former may not always be reported. For most such conversations, either the Ministry of External Affairs (MEA) or the MoD are the torch bearers. Since the AI roadmaps for DPSUs mentioned earlier are not publicly available, it cannot be said with certainty whether these conversations and potential implementation plans are all part of one constructive engagement policy around defence AI.

3 Organizing Defence AI

A distinct characteristic of India's defence AI organization is its mixed approach model which lacks a central decision-making body. Design, development, deployment, proliferation, and control of defence AI is largely spread across the central government through the MoD (and rarely, the Ministry of Electronics and Information Technology or MeitY), the 16 DPSUs that work on specific projects under the MoD, the DRDO and its sub-centres, and the three services (army, navy and air force) themselves. India has no private military contractors (PMCs), so any other inputs or action around development and regulation of defence AI is often supplemented by the established industry, start-ups, academia, and the civil society.

However, interplay between these external actors and the government is usually limited and largely unidirectional.

The services, while ultimately within the ambit of the MoD, are also individually forthcoming in their defence AI engagements and have established their own institutional mechanisms in the form of an AI Sub Committee and a Joint Working Group on AI for the Tri-Services (Press Information Bureau 2022f). To ensure that their foundational structures are AI-ready, especially considering the copious amounts of data that AI will require, they have also formulated a data policy, convened a Data Management Framework, and appointed Data Management Officers (Press Information Bureau 2022f).

While defence AI research is usually unilaterally undertaken by academia and civil society actors independent of government oversight, the MoD has recently showed more interest in collaborating with the industry. The Ministry has started commissioning defence AI projects from startups through a new AIM avenue called Innovations for Defence Excellence (iDEX, Government of India n.d.-b). Notable examples include AI-based ground and air-mounted systems developed for the Indian military by indigenous startup Skylark Labs (Gandharv 2022), and unmanned marine vehicles (UMVs) developed by Pune-based startup Sagar Defence Engineering (Nath 2023). iDEX has been established by the conjunction of two DPSUs (Hindustan Aeronautics Limited and Bharat Electronics Limited) and is guided by a new Defence Innovation Organization (DIO).

4 Funding Defence AI

While India's scale of engagements around defence AI both nationally and internationally has been substantial, the litmus test of its prioritization with respect to the larger defence and tech architectures in the country can be seen through its monetary evaluation by the government. In 2022, the MoD announced the earmarking of a specific 'AI budget' from the amount disbursed as part of the yearly defence budget, with a corpus of INR10bn (approx. USD120M) to be provided each year for the coming 5 years to support defence AI activities (Press Information Bureau 2022f).

While this may seem significant, it barely makes up a fraction of India's 2023 defence budget—India allocated INR5.94tn (approx. USD73bn) for defence in the 2023-24 financial year, which makes the AI budget amount to less than 0.002% of the overall defence budget (Press Information Bureau 2023a). This is in spite of the fact that about INR1.62tn (approx. USD20bn) of the total budget was allocated to capital outlays pertaining to modernization and infrastructure development, of which a record 75% of the defence capital procurement budget was earmarked for domestic production (Press Information Bureau 2023c). Additionally, INR23bn (approx. USD2.8bn) was allocated to defence R&D through DRDO, which makes up almost 4% of the total defence budget, but DRDO's spending on and outputs in terms of defence AI have not been significant.

While India's magnitude of spending on defence makes it the fourth largest spender globally after the US, China, and Russia (WiseVoter n.d.), some estimates have calculated that over 50% of its defence budget is actually spent on its 1.4 million active personnel and their pensions, limiting the scope and resources for defence procurement and modernization (McGerty et al. 2023). Moreover, contrasted with other digital initiatives by the Indian government in 2023, the defence AI budget is a paltry sum. For instance, there was massive government support for and spending on digital public infrastructure (DPI) in 2023, and INR15bn (approx. USD180M) was allocated for the promotion of digital payments alone (Aryan 2023).

5 Fielding and Operating Defence AI

Despite limited funding, AI has begun to be deployed by each of the three services in various battlefield, logistical and analytical functions. The army, driven by border concerns, has mostly experimented with fusing AI with legacy systems and conventional warfare capabilities. The navy and the air force, in comparison, have been more forthcoming in testing AI and related technologies for a number of more creative applications, many of which do not involve conventional warfare.

5.1 Army

The army has installed about 140 AI-based surveillance systems—including high-resolution cameras, sensors, UAVs, and radars—to get live feeds from the Pakistani and Chinese borders (IndiaAI 2022). These feeds are aggregated and help the army get a more comprehensive idea of potential border intrusion detection, target classification, and enhance the accuracy of defence operations. This system is supplemented on the Line of Control (on the India-Pakistan border) and the Line of Actual Control (on the India-China border) by a Proactive Real-time Intelligence and Surveillance Monitoring (PRISM) system, which also assists in threat identification by generating multiple real-time audio-visual feeds of disturbed areas and generating alerts for suspicious movements (Mishra 2022).

Another breakthrough by the DRDO which is now in use by the Indian Army is the evolution of the Seeker Monitoring and Analysis System, which is touted to be a self-contained system with facial recognition technology (FRT) in addition to a surveillance, monitoring, and analysis system (DDP MoD 2022). It uses a novel facial recognition system under disguise (FRSD) which can identify individual faces even in low resolution settings with the addition of different clothing articles and accessories (Verma 2022). Several other similar tools have been employed by the army to track vehicles (Project V-logger), identify intruders using intrusion detection systems (Sarvatra Pehchaan), as well as autonomously detect humans

using facial recognition rail-mounted robots (Silent Sentry) at the northern and western borders of India for real-time threat monitoring (Bommakanti et al. 2023).

The army has also developed its own swarm and storm drones with Beyond Visual Line of Sight (BVLOS) attack capabilities, as well as drone feed analysis systems which India may consider exporting (DDP MoD 2022). Additionally, to better understand and collect information from adversaries, the army has started to equip soldiers with Natural Language Processing (NLP)-based wearable language translation devices. These are light, convenient to wear, and have a high battery life, and have been used to bidirectionally translate from Mandarin to English and vice versa (DDP MoD 2022).

5.2 Navy

The navy has had plans to integrate big data and AI within its systems since 2018, with concrete plans to develop and deploy AI into its operations (The Hindu 2018). In the same year, it also began looking into acquiring several types of unmanned underwater vehicles (UUVs)—significant among these was the memorandum of understanding (MoU) signed by India-based Mahindra Defence and Israeli company Aeronautics Ltd. for the latter to offer a maritime version of the Orbiter 4 UAV for the Indian Navy (Naval Technology 2018). The Orbiter 4 is an advanced multi-mission platform with an ability to carry and operate two different payloads simultaneously. It will be shipborne by the Indian Navy to carry AI-based sensor payloads which can be launched and recovered from small warships that do not have a helicopter deck (IndiaAI n.d.).

The navy unveiled its indigenous flagship Autonomous Fast Intercept Boat (AFIB) in 2022, which can perform autonomous operations for special forces, search, and rescue, patrolling and surveillance, as well as interception of high-speed vessels, even in dense maritime traffic and shallow water (DDP MoD 2022). Other functions within which the navy has recently deployed AI-based systems includes maritime motion pattern recognition & anomaly detection, acoustic and magnetic signature analysis, and AI-enabled voice transcription software (DDP MoD 2022).

More recently, the navy launched its first UUV, called ‘Neerakshi’ (‘eyes in the water’ in Sanskrit), developed by state-owned Garden Reach Shipbuilders and Engineers (GRSE) and Aerospace Engineering Private Limited (AEPL), which is deployed to help with underwater surveys, and mine detection and disposal (Malin 2023). The navy is also currently testing its AI-powered Combat Management System (CMS) for naval ships, which enables rapid threat assessment and algorithmic decision-support tools and will be built into all warships commissioned from 2024 (Malin 2023).

5.3 Air Force

The Indian Air Force (IAF) has been employing AI in various domains and workstreams as well. On the battlefield, an Enemy Aircraft Activity Recognition & Classification system has been developed for air defence systems, which uses AI to help identify enemy aircraft and employs predictive analytics to chart their plan of action (DDP MoD 2022). The DRDO has also developed novel manned-unmanned teaming (MUM-T) capabilities for a yet-to-be-released Twin Engine Deck Based Fighter (TEDBF) program, which will replace Russian Mig-29 K fighter jets currently in use by the IAF (Indian Research Wing 2023). MUM-T capabilities are also being explored by the DPSU Hindustan Aeronautics Ltd. (HAL) for the IAF's 'Loyal Wingman' warrior drone, which will be tested in 2024 (Chopra 2023).

HAL has also helped to develop a Voice Activated Command System (VACS) for IAF pilots, which recognizes their voice commands and sends the codes to the mission computer for actions like radio tuning, mode selection, navigation, etc. (DDP MoD 2022). Also on the logistical end, the IAF has delved into employing predictive monitoring for the maintenance of weapons and aircrafts through a system called PRO-HM+, which can identify trends, patterns, and relationships of aircraft behaviour, equipment failure and other future events (DDP MoD 2022). It uses descriptive, predictive, prescriptive, and prognostic layers of data analytics and has been known to predict maintenance requirements of aircrafts with a high confidence level (DDP MoD 2022).

On the administrative front, the IAF created an AI-based Campaign Planning and Analysis System (CPAS), which is utilized to provide functionality and efficacy for campaign planning and debriefing solutions for all aircrafts under its ambit (Bordoloi 2022). The IAF has also deployed an application that integrates all electronic intelligence gathered by it and other intelligence agencies to create a comprehensive electronic order of battle (EOB) (Bordoloi 2022). MeitY has collaborated with IAF to develop an imagery intelligence analysis tool to identify assets and assess enemy targets by employing AI on the reconnaissance data (Bordoloi 2022). Creatively, the IAF has also experimented with using virtual reality (VR) for wargaming and cadet training at various air force stations (Raksha Anirveda 2023).

6 Training for Defence AI

Most of the Indian military personnel are still used to legacy systems, which is why training them for new technology like defence AI systems is an essential part of military transformation. This has been taken up by both the government as well as the three services, and new centres and programs are now being created to ensure optimum training. However, since the introduction of defence AI systems is recent, it is difficult to say how appropriate, effective and/or reliable the training will be– there has been limited, if any, monitoring, and evaluation of either the deployed AI

systems or their training modules (Off-the-record conversation with an Indian defence policy expert December 2023).

Since most defence AI systems run on massive amounts of data, which several sections of the commanders and operators have not had to directly deal with until recently, a focus on training administration personnel for data management and the establishment of data centres has been the first step towards institutionalizing defence AI training. On the recommendation of the defence AI taskforce from 2018, the government acknowledged a need to scale the existing capabilities of military data centres; establish a centrally facilitated network of test beds; create a framework to work with industry partners; and encouraging start-ups to help the services with developing AI systems to manage their intellectual property (Press Information Bureau 2022f). The services have implemented some recommendations from the taskforce as well. They launched a Data Management Framework in 2022 which included, inter alia, agreeing on a data policy, establishing a Data Management Office, and appointing officers to manage it (Press Information Bureau 2022f).

Active defence personnel are also being trained through universities and training centres set up by the three services. The Army established an AI Centre at the Military College of Telecommunication Engineering in 2021, with support from the National Security Council Secretariat (NSCS) (The Indian Express 2021b). The Navy set up an 'AI core group' and designated its training institution INS Valsura as an AI centre of excellence, within the ambit of which it holds regular webinars, training sessions and workshops around AI (Indian Navy 2022). The Air Force founded its own Centre of Excellence for AI under the aegis of UDAAN (Unit for Digitisation, Automation, Artificial Intelligence and Application Networking, the word 'udaan' also means 'flight' in Hindi) in 2022 (Press Information Bureau 2022a) and has also held workshops on the integration of AI and other frontier technologies (Press Information Bureau 2023d). Most of these centres train cadets on how to use existing AI systems, while some like the DRDO may also delve into conducting research to develop new ones. Sometimes, civilian experts and think tanks are brought in to discuss dual use tech and conduct short-term training for certain systems, but these are entirely dependent on the services taking the initiative.

The DRDO has also taken up training and combined it with innovation defence AI innovation. It announced in 2020 that it would create five new laboratories around AI and other frontier technologies, named the DRDO Young Scientist Laboratories (DYSL)—the labs would focus on AI at Bengaluru, quantum technologies at IIT Mumbai, cognitive technologies at IIT Chennai, asymmetric technologies at Kolkata, and smart materials at Hyderabad (Press Information Bureau 2020a). As per the norms laid out, everyone at these labs, including the directors, should be under 35 years of age (Shukla 2020). However, it has been observed that it is difficult to find capable talent to staff these laboratories, given that most young scientists and engineers from premier tech institutions end up in the private sector which has a variety of other benefits and pays much higher salaries than the DRDO (Off-the-record conversation with an Indian defence policy expert December 2023).

7 Recommendations for India's Future Defence AI Trajectory

India has made considerable advances in defence AI for a nation that did not have an institutionalized conception of the technology until a few years ago. While there is no institutionalised metric to measure how significant the advancement has been, the magnitude of advancements itself seems considerable when viewed in the context of the rise in AI-related developments over the past 5 years or so. Whether all these developments, most of which only have singular visibility on paper, have been successful or worked as expected is a different performance-based metric altogether. This underlines the limits of evaluation since we have no concrete monitoring and evaluation data.

Given this context, it is plain to see that several gaps still exist in India's defence AI ecosystem. It aspires to be a leader in defence AI, but the country's military leadership still devotes limited resources to its development. This also means that there is little incentivization for India's AI talent to join the defence AI architecture. There is also a lack of interoperability amongst different AI applications and subsystems across civilian and military spaces, especially since India's only national AI strategy from 2018 is now decidedly outdated, leading to contrasts in AI policy priorities and approaches.

Going forward, India needs to ensure that it looks at AI as the highly diversified technology it is, instead of the siloed approach it has adopted with respect to its development and policy so far. An initial recommendation is to adopt a hydra approach to its AI ecosystem—this would consist of amalgamating its core AI philosophy and roadmap into one apex body and creating an updated national AI policy; additionally retaining and producing separate sectoral guidelines, bodies, standards, and strategies to ensure effective policy synthesis and execution at various levels, including defence (Mohan 2023).

It will also be crucial for India to ensure that it can establish systems for the prioritization of its defence AI to be both robust and responsible, efficient, and ethical. This should ideally include more government investment in military transformation, better training and incentives to ensure that quality talent can innovate and operate new systems, and a well-functioning cycle of monitoring, performance measurement, and evaluation, especially since the current defence AI paradigm in the country noticeably lacks the latter. There should also be an optimum constructive interaction amongst technologists, military personnel and policy experts who understand this nexus of issues that defence AI will continue to present. Consistent and multi-faceted actions around responsible innovation in all major tech and military developments is on the way to becoming a requirement, at least at a policy level, to participate in global networks, and India will need to carefully consider which priorities it values as it builds upon its defence AI ambitions.

References

Aryan, Ashish. 2023. Budget 2023: Govt allocates Rs 16,549 crore to IT ministry, 40% higher on year. The Economic Times. https://economictimes.indiatimes.com/tech/technology/fy24-budget-allocates-rs-16549-crore-to-it-ministry-40-higher-on-year/articleshow/97525268.cms. Accessed 30 January 2024

Bhati, Divya. 2022. Full list of Chinese apps banned in India so far: PUBG Mobile, Garena Free Fire, TikTok and hundreds more. India Today. https://www.indiatoday.in/technology/news/story/bgmi-garena-free-fire-tiktok-and-more-banned-in-india-check-the-full-list-1990048-2022-08-19. Accessed 30 January 2024

Bommakanti, Kartik, Yogesh Joshi, Shimona Mohan, Karthik Nachiappan, and Antara Vats. 2023. Emerging technologies and India's defense preparedness. Observer Research Foundation. https://www.orfonline.org/wp-content/uploads/2023/04/ORF_SpecialReport_209_Tech-Defense.pdf. Accessed 30 January 2024

Bordoloi, Pritam. 2022. Using tech in warfare: How IAF employs AI to safeguard our airspace. Analytics India Mag. https://analyticsindiamag.com/using-tech-in-warfare-how-iaf-employs-ai-to-safeguard-our-airspace/. Accessed 30 January 2024

Centre for Artificial Intelligence & Robotics (CAIR). n.d. Defense Research and Development Organisation. https://www.drdo.gov.in/labs-and-establishments/centre-artificial-intelligence-robotics-cair. Accessed 30 January 2024

Cesareo, Serena, and Joseph White. The Global AI Index. 2023. Tortoise Media. https://www.tortoisemedia.com/intelligence/global-ai/. Accessed 30 January 2024

Chengappa, Raj, and Ananth Krishnan. 2017. India-China standoff: all you need to know about Doklam dispute. India Today. https://www.indiatoday.in/magazine/cover-story/story/20170717-india-china-bhutan-border-dispute-doklam-beijing-siliguri-corridor-1022690-2017-07-07. Accessed 30 January 2024

Chopra, Anil. 2023. Manned unmanned aircraft teaming India. DefStrat.. https://www.defstrat.com/magazine_articles/manned-unmanned-aircraft-teaming-india/. Accessed 14 January 2024

Council of Indian Institute of Technology. n.d. History. Council of Indian Institute of Technology. https://www.iitsystem.ac.in/history. Accessed 30 January 2024

D'Cruze, Danny. 2023. 'Make AI work for India': Union Budget 2023 introduces big plans for artificial intelligence. Business Today. https://www.businesstoday.in/union-budget/story/make-ai-work-for-india-union-budget-2023-introduces-big-plans-for-artificial-intelligence-368428-2023-02-01. Accessed 30 January 2024

Das, Mohua. 2023. How Indian artists are using AI, AR to let creativity soar. The Times of India. https://timesofindia.indiatimes.com/india/how-indian-artists-are-using-ai-ar-to-let-creativity-soar/articleshow/98644302.cms?from=mdr. Accessed 30 January 2024

Deloitte. 2022. State of AI in India: Second Edition. Deloitte. https://www2.deloitte.com/in/en/pages/about-deloitte/articles/State-of-AI-in-India.html. Accessed 30 January 2024

Elias, Jibu. 2023. AI for All: how India is carving its own path in the global AI race. OECD. https://oecd.ai/en/wonk/india. Accessed 30 January 2024

ET Now. 2022. Adani defense, Israel weapons industries unveil India's first AI-based futuristic firing system. TimesNow. https://www.timesnownews.com/business-economy/companies/adani-defense-israel-weapon-industries-unveil-indias-first-ai-based-futuristic-firing-system-article-95053254. Accessed 30 January 2024

Galston, William A. 2020. Is seeing still believing? The deepfake challenge to truth in politics. Brookings. www.brookings.edu/research/is-seeing-still-believing-the-deepfake-challenge-to-truth-in-politics/. Accessed 30 January 2024

Gandharv, Kumar. 2022. This startup is building AI-based defense tools to strengthen India's national security. IndiaAI. https://indiaai.gov.in/article/this-startup-is-building-ai-based-defense-tools-to-strengthen-india-s-national-security. Accessed 30 January 2024

Government of India. 2022. Artificial intelligence in defense: presenting AI preparedness of the country in defense. Department of Defense Production (DDP), Ministry of Defense (MoD).

Government of India. https://www.ddpmod.gov.in/sites/default/files/ai.pdf. Accessed 30 January 2024
———. n.d.-a. About AIM. https://aim.gov.in/. Accessed 30 January 2024
———. n.d.-b. ABOUT IDEX. Innovations for Defense Excellence. https://idex.gov.in/about-idex. Accessed 30 January 2024
Government of the Netherlands. 2023. REAIM 2023 endorsing countries and territories. Government of the Netherlands. https://www.government.nl/documents/publications/2023/02/16/reaim-2023-endorsing-countries. Accessed 30 January 2024
Goyal, Prateek, and Anna Priyadarshini. 2020. How a 'disinformation network' on Twitter added to the tension surrounding the Galwan Valley conflict. NewsLaundry. https://www.newslaundry.com/2020/07/18/how-a-disinformation-network-on-twitter-added-to-the-tension-surrounding-the-galwan-valley-conflict. Accessed 30 January 2024
Heikkilä, Melissa. 2022. AI: Decoded: Putin's high-tech war — Making sense of AI systems — Deepmind controls nuclear fusion reactor. Politico. https://www.politico.eu/newsletter/ai-decoded/putins-high-tech-war-making-sense-of-ai-systems-deepmind-controls-nuclear-fusion-reactor-2/. Accessed 30 January 2024
India Today. 2023. How AI is transforming Edtech and education system in India. India Today. https://www.indiatoday.in/education-today/featurephilia/story/how-ai-is-transforming-edtech-and-education-system-in-india-2389368-2023-06-06. Accessed 30 January 2024
IndiaAI. 2022. The Army deploys 140 AI-based surveillance systems to enhance border security. IndiaAI. https://indiaai.gov.in/news/the-army-deploys-140-ai-based-surveillance-systems-to-enhance-border-security. Accessed 30 January 2024
———. 2023. India among top 5 countries with fastest-growing AI talent: LinkedIn report. IndiaAI. https://indiaai.gov.in/news/india-among-top-5-countries-with-fastest-growing-ai-talent-linkedin-report. Accessed 30 January 2024
———. n.d. Ministry of Defense. IndiaAI. https://indiaai.gov.in/ministries/ministry-of-defense. Accessed 11 January 2024
Indian Defense Research Wing. 2023. DRDO unveils manned-unmanned teaming capabilities for upcoming TEDBF Fighter Jet. Indian Defense Research Wing (IDRW). https://idrw.org/drdo-unveils-manned-unmanned-teaming-capabilities-for-upcoming-tedbf-fighter-jet/. Accessed 30 January 2024
Indian Navy. 2022. Leveraging Artificial Intelligence (AI) for Indian Navy' workshop at INS Valsura. https://indiannavy.nic.in/content/%E2%80%98leveraging-artificial-intelligence-ai-indian-navy%E2%80%99-workshop-ins-valsura. Accessed 30 January 2024
Inside BigData. 2020. Infographic: AI innovators – the countries & companies leading in AI patents. Inside BigData. https://insidebigdata.com/2020/09/06/infographic-ai-innovators-the-countries-companies-leading-in-ai-patents/. Accessed 14 January 2024
Kristensen, Hans M., and Shannon N. Kile. 2020. World nuclear forces. SIPRI Yearbook 2020. https://www.sipri.org/yearbook/2020/10. Accessed 30 January 2024
Kumar, Deepa. 2020. India and China decoupling. S&P Global. https://www.spglobal.com/marketintelligence/en/mi/research-analysis/india-and-china-decoupling.html. Accessed 30 January 2024
Malin, Carrington. 2023. India's tech play for naval leadership. Armada International. https://www.armadainternational.com/2023/08/indias-tech-play-for-naval-leadership/. Accessed 30 January 2024
McGerty, Fenella, Viraj Solanki, and Karl Dewey. 2023. Personnel vs. capital: the Indian defense budget. International Institute for Strategic Studies. https://www.iiss.org/en/online-analysis/military-balance/2023/04/indian-defense-budget/. Accessed 30 January 2024
Menon, Anoop. 2023. Next big thing: the AI revolution in India's financial sector. Fi. https://fi.money/blogposts/next-big-thing-the-ai-revolution-in-indias-financial-sector. Accessed 30 January 2024
Ministry of Electronics & Information Technology. 2024. Cyber Laws. Government of India. https://www.meity.gov.in/content/cyber-laws. Accessed 30 January 2024

Ministry of External Affairs. 2023. Joint statement: fifth annual India-U.S. 2 + 2 ministerial dialogue. Government of India. https://www.mea.gov.in/bilateral-documents.htm?dtl/37252/Joint_Statement_Fifth_Annual_IndiaUS_22_Ministerial_Dialogue. Accessed 30 January 2024

Mishra, Abhinandan. 2022. Indian Army gets future ready with AI-based equipment. The Sunday Guardian. https://sundayguardianlive.com/news/indian-army-gets-future-ready-ai-based-equipment#google_vignette. Accessed 30 January 2024

Mohan, Shimona. 2023. Emerging technology, emerging power: India in the age of AI. Observer Research Foundation. https://orfonline.org/expert-speak/emerging-technology-emerging-power. Accessed 30 January 2024

NASSCOM. 2021. How AI is transforming the future of healthcare In India. NASSCOM. https://nasscom.in/knowledge-center/publications/how-ai-transforming-future-healthcare-india. Accessed 11 January 2024

Nath, Dipanita. 2023. A drone that can carry humans? Meet the Pune startup that is working wonders for Indian defense. Indian Express. https://indianexpress.com/article/cities/pune/drone-humans-meet-pune-startup-working-wonders-indian-defense-8648061/. Accessed 30 January 2024

National Council of Educational Research and Training. 2023. Liberalisation, privatisation and globalisation: an appraisal. National Council of Educational Research and Training (NCERT). https://ncert.nic.in/textbook/pdf/keec103.pdf. Accessed 30 January 2024

Naval Technology. 2018. Mahindra defense and aeronautics to offer orbiter 4 for Indian navy. Naval Technology. https://www.naval-technology.com/news/mahindra-defense-aeronautics-offer-orbiter-4-indian-navy/. Accessed 30 January 2024

NITI Aayog. 2018. National strategy for artificial intelligence. NITI Aayog. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf. Accessed 30 January 2024

———. 2021a. Responsible AI #AIforAll: approach document for India Part 1 – principles for responsible AI. NITI Aayog. https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf. Accessed 30 January 2024

———. 2021b. Responsible AI #AIforAll: approach document for India: Part 2 - operationalizing principles for responsible AI. NITI Aayog. https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf. Accessed 30 January 2024

Pai, Nitin. 2020. NPT turns 50. The first half it lived a lie, the second half it saw its own demise. The Print. https://theprint.in/opinion/npt-turns-50-first-half-lived-a-lie-second-half-saw-own-demise/374512/. Accessed 30 January 2024

Press Information Bureau. 2018. AI task force hands over Final Report to RM. Press Information Bureau. https://pib.gov.in/newsite/PrintRelease.aspx?relid=180322. Accessed 30 January 2024

———. 2020a. PM dedicates 5 DRDO Young Scientists Laboratories to the Nation. Press Information Bureau. https://pib.gov.in/newsite/PrintRelease.aspx?relid=197246. Accessed 30 January 2024

———. 2020b. Prime Minister inaugurates RAISE 2020 - a Mega Virtual Summit on Artificial Intelligence. Press Information Bureau. https://pib.gov.in/PressReleasePage.aspx?PRID=1661859. Accessed 30 January 2024

———. 2022a. Artificial Intelligence (AI) Centre of Excellence (Coe) launched by IAF. Press Information Bureau. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1840695. Accessed 30 January 2024

———. 2022b. DefExpo 2022 propels 'Aatmanirbharta' in defense to next level. Press Information Bureau. https://pib.gov.in/PressReleasePage.aspx?PRID=1870082. Accessed 30 January 2024

———. 2022c. Enhancement of Capabilities of AI Technology. Press Information Bureau. https://www.pib.gov.in/PressReleasePage.aspx?PRID=1846937. Accessed 30 January 2024

———. 2022d. Ministry of Defense. Raksha Mantri launches 75 Artificial Intelligence products/technologies during first-ever 'AI in Defense' symposium & exhibition in New Delhi; Terms AI as a revolutionary step in the development of humanity. Press Information Bureau. https://pib.gov.in/PressReleasePage.aspx?PRID=1840740. Accessed 30 January 2024

———. 2022e. Raksha Mantri Shri Rajnath Singh & his Israeli counterpart Mr Benjamin Gantz hold bilateral talks in New Delhi. Press Information Bureau. https://www.pib.gov.in/PressReleasePage.aspx?PRID=1830445. Accessed 30 January 2024

———. 2022f. Task force for implementation of AI. Press Information Bureau. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1810442. Accessed 30 January 2024

———. 2023a. Defense gets Rs 5.94 lakh crore in Budget 2023-24, a jump of 13% over previous year. Press Information Bureau. https://pib.gov.in/PressReleasePage.aspx?PRID=1895472. Accessed 30 January 2024

———. 2023b. Raksha Mantri & French Minister of Armed Forces hold 5th Annual Defense Dialogue in Paris; Focus on enhancing defense industrial cooperation; Potential collaboration in niche domains such as space, cyber & Artificial Intelligence also discussed. Press Information Bureau. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1966922. Accessed 30 January 2024

———. 2023c. Record 75 per cent of defense capital procurement budget earmarked for domestic industry in FY 2023-24, announces Raksha Mantri at 14th Aero India. Press Information Bureau. https://pib.gov.in/PressReleasePage.aspx?PRID=1899388. Accessed 30 January 2024

———. 2023d. Seminar on Emerging Disruptive and Futuristic Technologies. Press Information Bureau. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1907707. Accessed 30 January 2024

Raja, Anjali. 2023. Top AI initiatives by MeitY in 2023. IndiaAI. https://indiaai.gov.in/article/top-ai-initiatives-by-meity-in-2023. Accessed 30 January 2024

Raksha Anirveda. 2023. Indian Air Force Leverages AI for Smarter Mission Planning. Raksha Anirveda. https://raksha-anirveda.com/indian-air-force-leverages-ai-for-smarter-mission-planning/. Accessed 30 January 2024

Rakshak, Bharat. 1998. Prithvi SRBM. Internet Archive. https://web.archive.org/web/20071212063803/http://www.bharat-rakshak.com/MISSILES/Prithvi.html. Accessed 30 January 2024

Renshaw, Jarrett. 2023. Flurry of US-India deals on AI, defense as Biden, Modi meet. Reuters. https://www.reuters.com/world/biden-modi-meet-flurry-new-us-india-deals-2023-06-22/. Accessed 30 January 2024

Roy, Annapurna. 2023. State-sponsored cyberattacks against India up 278% in three years. The Economic Times. https://economictimes.indiatimes.com/tech/technology/india-most-targeted-country-by-cyber-attackers-report/articleshow/104989856.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. Accessed 30 January 2024

Russett, Bruce, John R. Oneal, and David R. Davis. 1998. The third leg of the Kantian tripod for peace: international organizations and militarized disputes, 1950-85. *International Organization* 52: 441–467.

Sarangi, Subhasish. 2019. National initiatives on artificial intelligence in defense. *United* Service Institution of India. https://www.usiofindia.org/strategic-perspective/national-initiatives-on-artificial-intelligence-in-defense.html#:~:text=%5B4%5D%20On%2002%20February%202018,Tata%20Sons%20Chairman%20 N%20Chandrasekaran. Accessed 30 January 2024

Sharma, Kiran. 2023. India and Russia inch closer to jointly producing weapons. Nikkei Asia. https://asia.nikkei.com/Politics/International-relations/India-and-Russia-inch-closer-to-jointly-producing-weapons. Accessed 30 January 2024

Shukla, Ajai. 2020. PM Modi inaugurates five high-tech DRDO labs where everyone is under 35. Business Standard. https://www.business-standard.com/article/current-affairs/pm-modi-inaugurates-five-high-tech-drdo-labs-where-everyone-is-under-35-120010201072_1.html. Accessed 30 January 2024

Singal, Nidhi. 2023. Here's how India's Digital Public Infrastructure is going global. Business Today. https://www.businesstoday.in/magazine/deep-dive/story/heres-how-indias-digital-public-infrastructure-is-going-global-405177-2023-11-09. Accessed 30 January 2024

Singh, Dalip. 2022. India, Japan identify key areas of defense co-operation ahead of 2 + 2 dialogue at Tokyo. Business Line. https://www.thehindubusinessline.com/news/india-japan-identify-key-areas-for-defense-co-operation-ahead-of-22-dialogue-at-tokyo/article65833058.ece. Accessed 30 January 2024

Singh, Anamica. 2023. US, India enter deal that aims to counter China on AI and military. WION News. https://www.wionews.com/india-news/us-india-enter-deal-that-aims-to-counter-china-on-ai-and-military-557726. Accessed 30 January 2024

Suman, Prachee. 2023. India, Australia bolster defense cooperation during 2 + 2 Ministerial Dialogue. DD News. https://ddnews.gov.in/international/india-australia-bolster-defense-cooperation-during-22-ministerial-dialogue. Accessed 30 January 2024

The Hindu. 2018. Navy to opt for Big Data, AI in operational functioning. The Hindu. https://www.thehindu.com/news/national/navy-to-opt-for-big-data-ai-in-operational-functioning/article23857225.ece. Accessed 30 January 2024

The Indian Express. 2021a. Get rid of legacy systems that have outlived utility: PM Modi. Indian Express. https://indianexpress.com/article/india/get-rid-of-legacy-systems-that-have-outlived-utility-pm-modi-7217571/. Accessed 30 January 2024

———. 2021b. Army sets up quantum computing lab, AI centre at engineering institute in Mhow. The Indian Express. https://indianexpress.com/article/education/army-sets-up-quantum-computing-lab-ai-centre-at-engineering-institute-in-mhow-7697802/. Accessed 30 January 2024

Trivedi, Rahul. 2023. India would benefit from partnering with Russia in AI research, says expert. Sputnik News. https://sputniknews.in/20231221/india-would-benefit-from-partnering-with-russia-in-ai-research-says-expert-5916081.html. Accessed 30 January 2024

U.S. Department of Defense. 2023. Readout of the inaugural U.S. – India advanced domains defense dialogue. U.S. Department of Defense. https://www.defense.gov/News/Releases/Release/Article/3408336/readout-of-the-inaugural-us-india-advanced-domains-defense-dialogue/. Accessed 30 January 2024

United Nations. 2023. First committee approves new resolution on lethal autonomous weapons, as speaker warns 'An algorithm must not be in full control of decisions involving killing.' United Nations. https://press.un.org/en/2023/gadis3731.doc.htm. Accessed 30 January 2024

Vergun, David. 2023. U.S., India rapidly expand their military cooperation. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3433245/us-india-rapidly-expand-their-military-cooperation/. Accessed 30 January 2024

Verma, Rahul. 2022. DRDO has developed a facial recognition system that claims to see through masks and disguise. Business Insider India. https://www.businessinsider.in/science/research/news/drdo-has-developed-a-facial-recognition-system-that-claims-to-see-through-masks-and-disguise/articleshow/93726351.cms. Accessed 30 January 2024

Waldwyn, Tom, and Viraj Solanki. 2023. India's defense plans fall victim to Putin's War. Foreign Policy. https://foreignpolicy.com/2023/04/03/india-modi-defense-military-russia-putin-war-weapons-procurement/. Accessed 30 January 2024

Weisman, Steven R. 1987. On India's border, a huge Mock War. The New York Times. https://www.nytimes.com/1987/03/06/world/on-india-s-border-a-huge-mock-war.html. Accessed 30 January 2024

WiseVoter. n.d. Military spending by country. WiseVoter. https://wisevoter.com/country-rankings/military-spending-by-country/. Accessed 30 January 2024

‘Overtaking on the Curve’? Defense AI in China

John Lee

China has a clear understanding of the importance of artificial intelligence (AI) to the future military balance, and a well-developed and resourced system for domestic development of AI technologies. By the judgment of seemingly most Chinese and many foreign analysts, the People’s Liberation Army (PLA) remains far from implementing revolutionary uses of defense AI and is still grappling with the institutional reforms and basic capability development needed to effectively use AI in current operations. But Chinese thinkers are working through the possibilities for AI to give the PLA both symmetric and asymmetric tools for high-end conflict with the US military and its allies, in the context of reasonably clear military strategic goals. Fear of Chinese potential was enough for the US in late 2022 to introduce severe export controls targeting China’s access to high-performance semiconductors, expressly justified by the imperative to constrain Chinese advances in defense AI.

China is ruled by a Party that follows a materialist conception of human development and wields unchallenged authority over all social institutions including the PLA, with a leader who appears entrenched for the coming decade. Official judgments about AI’s structural importance, and of the need to be equipped for long-term strategic competition with the US, are thus unlikely to change. To this end, China is leveraging its dynamic civilian economy to boost defense AI development, within the larger context of a national drive for the commanding heights of AI and other emerging technologies. Whether methods that have worked as part of an integrated global economy can still deliver results under growing “decoupling” pressures from the US remains to be seen. But China’s internal means for AI development are now sufficiently robust that analysts of military and strategic global affairs will find it imperative to watch this space, even as it becomes increasingly opaque.

J. Lee (✉)
Leiden Asia Centre, Leiden, The Netherlands

East West Futures Consulting, Berlin, Germany
e-mail: johnlee@eastwestfutures.com; https://eastwestfutures.com/

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_21

1 Thinking About Defense AI

1.1 Political Context

The PLA's subordination to the Communist Party of China (CPC) needs consideration when evaluating Chinese thinking about defense AI. The CPC exercises ideological control through the commissar system at various levels, and at the apex of the military hierarchy through the chairman of the Central Military Commission (CMC), who typically is General-Secretary of the CPC and China's head of state (currently Xi Jinping). This means that the PLA's development and use of AI is at least nominally governed by the CPC's political priorities and theoretical judgments, and by the views of China's top leader.

Under Xi Jinping, official rhetoric and policy has increasingly emphasized emerging technologies like AI. In his "work reports" to the last two CPC congresses, Xi highlighted the PLA's need to "accelerate development of military intelligentization" and "intelligent combat capabilities," giving top-level endorsement to a focus on defense AI. Armed conflict with the US is the PLA's main preoccupation driving Chinese efforts to both close the defense capability gap with the US symmetrically, and to search for asymmetrical means of circumventing US military advantage. Either way, exploiting emergent information-centric technologies like AI appears critical.

1.2 Towards "Intelligentized Warfare"

China's successive defense white papers (DWPs) show progression from conceiving warfare's 'form' (形态) from being predominantly characterized by "mechanization" towards "informatization," and since 2014 towards "intelligentization" (Fedasiuk et al. 2021: 305). This reflects the CPC's conception of wider society's development, in which "informatization"—the widespread application of digital information and communications technology (ICT)—is a comprehensive and transformational global trend (Lee 2022a). The PLA has paid close attention to the US "Third Offset Strategy" for evolving capability, organization and operations that emerged in the mid-2010s, with a focus on employing new technologies like AI and on China as a specific adversary.

China's 2019 DWP cited the trend of "informatization" as a key feature of the global context for China's defense policy, with new technologies like AI, cloud computing and big data "being applied to the military field at an accelerated pace." However, this document still characterized "intelligentized" warfare as an emergent phenomenon, which the PLA must account for even while it strives to complete mechanization and integrate mechanized capabilities with ICT (Ministry of National Defense 2019).

By late 2020, the official assessment was that the PLA should “accelerate the integrated development of a mechanized, informatized and intelligent military, with a view to taking the initiative” in global military development (Ministry of National Defense 2020). The current (2020) edition of the doctrinally informed Science of Military Strategy includes intelligentization as a capability development requirement across the PLA’ services, stressing that the international environment now features “rapid development of military intelligentization” (Wuthnow 2021). As put by the director of the CMC’s science and technology (S&T) commission, AI’s disruptive nature offers the prospect of “overtaking (more advanced militaries) on the curve.”

However, this optimistic judgment about AI’s potential is matched with pessimistic assessments of the PLA’s state of development with defense AI compared to the US military (Dahm 2020). As one example of this lag in “intelligentized” capabilities despite the PLA’s rapid inventory expansion, a 2018 Chinese assessment identified a deficit of AI-enabled tools to process the volume of information provided by the PLA’s then-already extensive ISR (intelligence, surveillance and reconnaissance) assets (Qiao et al. 2018). By one US expert’s judgment in 2019, PLA modernization was still at the stage of strengthening the separate services’ basic capabilities rather than of developing a sophisticated joint operations capability, let alone effectively integrating AI for “intelligentized” warfare (Fravel and Carson 2019).

This is unsurprising given the general assessment by Chinese commentators, including Xi Jinping himself, that the PLA still lacks the organizational and human capital to conduct system-centric warfare as described below. PLA modernization and reform has been a methodical rather than revolutionary process, with the official goals remaining “full modernization” by 2035 and becoming a “world class military”—by implication, on par with that of the US—by 2050.

In this context, Chinese thinking about AI’s potential for more advanced and radical military uses can be assumed to be still largely theoretical. Describing the “end state” for PLA organization, capability and doctrine that AI applications will fit into apparently remains a work in progress.

While this doctrinal and organizational evolution is playing out, the PLA is steadily deploying a range of increasingly capable semi-autonomous platforms (Lee 2022b). Discussion in China (as elsewhere) about defense AI is grappling with the gap between current capabilities and the implications of full machine autonomy (Fedasiuk 2020). One 2021 survey of Chinese state media outlets concluded that the PLA has yet to reach an official consensus on AI’s fundamental attributes, absent which operational doctrine cannot be developed (Pollpeter and Kerrigan 2021).

1.3 "System-Versus-System" Operations

Nonetheless, the PLA does seem to have established an orthodox view of current and future warfare as essentially a contest between operational systems, in which more effective employment of ICT will prevail (Cozad et al. 2023). In its description of "basic operational doctrine," China's 2015 DWP refers to "prevailing in system-versus-system operations" (Ministry of National Defense 2015). In this context, AI's information processing capacity was identified at least a decade ago by Chinese theorists as useful to achieve the "information dominance" needed to win wars under "informatized" conditions, the official description of the PLA's basic mission.

One aspect of information dominance is enhanced command and control (C2). One recent Chinese publication highlights AI's utility in providing strategic early warning; assisting operational decision-making; integrating operational command (within a unified information environment); and optimizing resource allocation and mission management (Zhou and Chen 2022). These capacities overlap with those attributed by Chinese defense media commentary to next-generation (6G) telecommunications, identified as an enabler for AI (Lee et al. 2022a). This combination of AI with other emerging technologies into an operationally and strategically superior "system of systems" is the key theme in published Chinese descriptions of "intelligentized" warfare.

The advantages of enhanced C2 are often expressed by Chinese writers in terms of the OODA Loop concept, enabling the PLA to get inside the adversary's decision-making cycle and so deploy resources faster and more effectively (Zhou and Chen 2022). In the context of "system-versus-system" operations, this would allow simultaneous rather than sequential attacks on an adversary system's elements, bringing rapid paralysis of the adversary's war making capacity. Long-range precision fires, as exhibited by the US military over the past three decades and increasingly accumulated in the PLA's inventories, remain central to this operational conception. But kinetic strikes on disaggregated and thereby vulnerable enemy force elements are just part of the objective to achieve cascading and compounding failure in the enemy's warfighting system (Dahm 2020).

With information acquisition and processing seen as the glue for a superior warfighting "system of systems", AI stands out as a technology enhancing the PLA's potential to realize this in practice. Warfare's emergent form is now "information-based with intelligent features," with the mechanism for victory consisting of information-enabled conjoined operations that achieve precise use of firepower and destruction of the enemy system. "Whoever has a strong ability to acquire, process, transmit, utilize and control information, and whoever has a high degree of integration of information and firepower, will win in war" (Li and Huo 2023).

1.4 Future Operational and Strategic Concepts

This core conception of AI’s utility in evolving “informatized” warfare follows, or at least responds to, the path set by the US as global military leader. The US quest for first-mover advantage in military applications of next-generation technologies like AI that Chinese attention on accelerated progression by the PLA towards “intelligentized warfare” as necessary to perform its missions.

However, Chinese conceptions of “intelligentized warfare” also envision new concepts of operations in response to a transformed battlespace. As one 2019 commentary put it, “The elements of warfare are changing from “information-led” to “machine-led”, with machine-led warfare reshaping the operational process” (Li 2019). The substitution of unmanned platforms for humans expands the scope for military operations to new physical domains (the deep sea and outer space), while the pervasiveness of digital networks means that future war will extensively involve cyberspace. The need to develop network-based “all-domain operational capabilities” was emphasized in Xi’s 2017 work report.

In recent years, the term “multi-domain precision warfare” (多域精确战, MDPW) has emerged in Chinese discourse (Wang and Deng 2022). This term was highlighted by the US Department of Defense (DoD) in its 2022 annual report on China’s military power, which described MDPW as a “new core operational concept” that aims to target vulnerabilities in the US military’s operational system through the PLA’s own “network information system-of-systems” (Department of Defense 2022).

Chinese writers also take interest in AI’s possibilities for manipulating human cognition to influence the adversary’s perceptions, situational awareness and will to fight (Huang et al. 2023). This could be achieved by real-time analysis of adversary behavior, data degradation and manipulation, influence over public opinion, and direct control of adversary systems (Takagi 2022). Some published Chinese work on this theme shows progression from theory to specific application and assessment (Chen 2023a). This aspect of Chinese thinking about AI was also highlighted in the US DoD’s 2022 report, which describes the PLA as developing AI-powered “cognitive domain operations” as psychological warfare’s next evolution, useful for deterrence and achieving effects against the adversary before armed conflict begins.

1.5 Strategic Stability, Human Control, Ethics and Standards

Among the main themes in Chinese writings on “intelligentized” warfare is hybrid human-machine teaming, with machine intelligence seen as augmenting rather than replacing human control (Pollpeter and Kerrigan 2021). China’s position paper on regulating military applications of AI submitted to the UN Convention on Certain Conventional Weapons in 2021 states that “weapon systems must be under human control,” requiring “necessary human-machine interaction across the entire life

cycle of weapons" (Permanent Mission of the People's Republic of China to the United Nations, 2021). It also called on nations to "refrain from seeking absolute military advantage, and prevent the deepening of strategic miscalculation" (Permanent Mission of the PRC to the UN 2021).

This concern with strategic stability stems from Chinese self-assessments of disadvantage vis-à-vis the US not just in AI and in cyberspace capabilities generally, but in the overall balance of conventional military power (Austin 2014). US officials describe the PLA's new MDPW concept as a response to the US Joint All-Domain Command and Control (JADC2) warfighting concept. Conversely, PLA authors recognize that the Third Offset itself responds to the PLA's development of means to target the US military's vulnerabilities.

Specific concerns raised by Chinese authors about how US advances in AI could undermine Chinese deterrence include the potential for new US capabilities to overwhelm PLA air defense, successfully attack Chinese C2 systems and reduce available response time (Fedasiuk 2020). Such concerns sit within a larger international debate about the escalatory potential of military AI, especially given the "black box" nature of current machine learning techniques and AI's potential to exhibit emergent behaviors. Conversely, the PLA's doctrinal emphasis on "active defense" may encourage it to pursue its own "offset" of disadvantageous asymmetries vis-a-vis the US by leveraging AI for an effective first strike.

Notwithstanding professed Chinese concerns about strategic stability, the PLA has reportedly refused to admit mutual risk reduction around military uses of AI as an agenda item for official talks with the US Department of Defense (Allen 2022). China is also the world's leading exporter of combat drones, which does not suggest an excessive concern about destabilizing effects outside the context of the US-China military balance, at least concerning semi-autonomous technologies. The US, however, remains the leading exporter of surveillance drones.

Human control and data security appear as the salient concerns in Chinese discussion of ethics and safeguards for AI (Toner 2023). While some defense commentaries discuss a necessary progression with increasing automation from "human in the loop" to "data in the loop" (Li and Zhao 2020), such a trend can be expected to remain confined to lower levels of decision-making and command authority. Xi Jinping personally emphasized the need for AI to be "safe, reliable and controllable" in a 2018 Politburo study session (Xinhua 2018).

China is developing a comprehensive system of technical standards for AI, within which ethics and security standards have overriding regulatory effect (Lee et al. 2022a, b). But it is unclear how China's civilian AI governance frameworks will apply to the PLA, which is known to sit outside China's general data regulatory regime.

2 Developing Defense AI

2.1 “Military-Civil Fusion” and the Leading Role of China’s Civilian Sector

AI development is led by the civilian sector, in China as elsewhere: one 2021 survey of China’s largest academic database (CNKI) found just one PLA institution among the top 20 publishers of AI-related articles (Fedasiuk and Weinstein 2023). China’s “military-civil fusion” (MCF) policy is often cited outside China to justify zero-risk approaches to engaging with Chinese companies outside the state-owned or defense sectors. Xi’s leadership has seen private firms subjected to an expanded presence and influence of CPC committees, legislation and regulation requiring cooperation with authorities in national security situations, and a political climate incentivizing demonstrations of loyalty to the state’s policy goals.

MCF under Xi has involved increased top-down control and ambition, aiming to push China’s long-isolated and fragmented defense industry sector towards a level of interaction with the civilian economy closer to that prevailing in developed nations, in particular the US. Focused on opening China’s defense industry and PLA procurement systems to civilian participation, MCF aims to promote synergistic relations between these two worlds, rather than simply subjecting the latter to PLA control. The essential idea is “synthesis of military and civilian elements to generate new hybrid outcomes” (Cheung 2022: 85–86).

MCF is complemented by the state’s movement away from a siloed, command-style approach to strategic technology development towards one that is cross-sectoral and open to market actors, officially endorsed in 2019 as a “new whole-of-nation system” (新型举国体制) for developing “key core technologies.” Seeking to combine China’s Maoist legacy of top-down mobilization with market-conforming techniques and market-sourced funding, this approach shapes the bureaucratic environment within which directives such as the 2017 New Generation AI Development Plan (‘2017 Plan’) operate.

Among the 2017 Plan’s “basic principles” is “two-way conversion for military and civilian scientific and technological achievements, and … sharing of military and civilian resources.” The 2017 Plan contains a section on MCF that calls for institutionalizing coordination among research institutes, universities, enterprises, and military industry units (Webster et al. 2017).

The 2017 Plan’s top-level guidance was followed by a “three-year action plan” concerned with more detailed implementation, issued, and supervised by China’s Ministry of Industry and Information Technology (MIIT) (Ministry of Industry and Information Technology 2017). While this document does not reference military applications, it directs a focus on developing “core foundational” technologies that include neural network chips and intelligent sensors, corresponding to the conceptual defense AI applications and fielded PLA capabilities discussed in this chapter. MIIT has a close working relationship with the “Seven Sons of National Defense” universities (discussed further below).

One typology of Chinese companies involved in AI development describes five categories, with firms linked to the PLA and security services constituting one: the others are diversified digital giants (for instance, Alibaba and Huawei), large private firms focused on AI technologies, smaller private firms involved in AI inputs and applications, and state-owned enterprises (SOEs) that provide funding, backbone infrastructure and leadership in implementing AI applications (Sutter and Arnold 2023: 20–21).

Under the 2017 Plan, the state designated individual private sector firms to lead development of AI subfields in an "open national innovation platform" model: as of mid-2019, this involved 15 firms focusing on different subfields that range from autonomous driving to cybersecurity and video sensing. This approach aims for more efficient delivery of state support by avoiding duplications of effort, following market signals as to which firms have already achieved economies of scale and technological leadership (Sutter and Arnold 2023: 24–25). The "open" aspect should, in theory, promote information sharing and other non-monopolistic behavior by these dominant firms, and so benefit the development of a wider Chinese ecosystem.

China's technology policy approach has been described as "grand steerage:" the state steers direction, while letting market forces operate to increase efficiencies and available resources. In doing so, it welcomes foreign expertise and capital: for instance, China's prominent AI chip design startups have received significant foreign investments (Lee and Kleinhans 2021). Chinese actors have also made significant AI-related investments abroad, being involved from 2015 to 2019 in an estimated USD7bn of disclosed investments in non-Chinese AI companies (Sutter and Arnold 2023: 29).

AI tops the list of seven technologies prioritized for development in China's current (14th) Five Year Plan. The rapid development of China's larger digital economy and S&T innovation system means that AI-oriented firms benefit from a surrounding ecosystem of interrelated technologies. Beijing for instance, where China's National Engineering Laboratory of Deep Learning Technology is located, has been ranked by the journal *Nature* as the world's leading science city for several years (Nature 2022).

Collaboration between different types of actors across the development cycle for emerging technologies like AI is promoted by a system of State Key Laboratories, a growing number of which are run by private companies, and National Defense Key Laboratories (Weinstein and Stoff 2023). PLA academic institutions engaged in AI research notably include the National Defense University's Academy of Intelligent Sciences, which is conducting research into intelligent robotics, bionic robotics and swarm intelligence, and the Academy of Military Sciences, which hosts an AI Research Center that concentrates on deep learning and human-machine integration (Kania 2021: 527–528). The Chinese Academy of Sciences (CAS) is involved in AI research with military applications: its Institute of Computing Technology was added to the US Entity List for targeted export controls in December 2022. CAS' Institute of Automation developed the Miaosuan wargaming platform and the AlphaWar AI agent discussed below.

China’s state-owned conglomerates are also involved in developing military-oriented AI applications. China Electronics Technology Group Corporation (CETC) for instance appears to be a leader in swarm intelligence (Kania 2017). A research institute affiliated with China’s state-owned shipbuilding sector claimed in 2023 to have used AI to complete in one day design work for a warship’s electrical layout that with human designers had required 300 times this time investment, with 100% accuracy (Chen 2023b).

Much R&D is carried out at civilian universities and research institutes, some of which are working on AI-related projects with direct military applications. For example, Harbin Engineering University (HEU) developed the HSU001 autonomous submersible, while another autonomous submersible (the Sea-Whale 2000) deployed in 2019 for the declared purpose of deep-sea surveying in the South China Sea was developed by the Chinese Academy of Sciences (Panda 2019). Northwest Polytechnic University (NPU) hosts one of China’s leading R&D centers (the No.365 Institute) for military-use unmanned aerial vehicles (UAVs) (Kania 2018). Judging from published research and patents, multiple civilian universities appear to be working on UAV swarming technology, as are China’s state-owned defense conglomerates (Kania 2017).

Most published Chinese academic research on AI-enabled cyberspace operations is produced by a small number of elite research universities, particularly the so-called “Seven Sons of National Defense” (including HEU and NPU). This is an alliance of seven S&T and engineering-oriented universities that work closely with MIIT and are openly engaged in military research, including programs for AI and intelligent weapons development. Several universities were among the leading vendors identified by one survey of AI-related public procurement contracts from PLA service branches over April–November 2020 (Konaev et al. 2023).

China has also adopted an open “innovation challenge” model from US practice, with state authorities sponsoring contests to demonstrate AI-related technologies. For instance, the 2022 “Xingzhi Cup” National AI Innovation and Application Competition ran competitions on themes of technology innovation, industry empowerment and development of the AI industrial ecosystem (Ministry of Industry and Information Technology 2022). While the official notice made no reference to military applications, its mention of “multi-modal technologies,” “network communication” and other potentially dual-use fields means that the activity could well benefit the PLA, if not through direct technology transfers than by identifying promising civilian firms and research teams or implementation techniques.

One vulnerability for China’s AI development is reliance on foreign-developed software and machine learning software frameworks, historically dominated by US companies (Allen 2019), although Chinese developed equivalents are gaining ground (Ding 2022). Such “open-source open platforms” are among the “core foundational” technologies prioritized by MIIT’s 2017 AI action plan. Open-source approaches generally are now much promoted in China’s ICT sectors as a means of mitigating upstream dominance of US firms and the supply chain chokepoints this provides the US government: much of China’s recent AI processor development has

utilized the open-source RISC-V architecture, which is less exposed to US export controls than proprietary architectures like ARM and X-86.

Chinese firms are also competing in development of large language model-based AI tools like ChatGPT, the publicity for which has also drawn attention from China's defense community. Several commentaries in PLA Daily in early 2023 discussed applications for ChatGPT, both from the PLA's viewpoint and under the US military's JADC2 concept, and its potential for enabling cognitive domain operations of the type that the US DoD projects onto PLA thinking (Mao 2023). It can be assumed that generative AI will be incorporated into Chinese defense theorizing going forwards, although again, evidence of real-world implementations remains to be seen.

2.2 Effects of US Export Controls Targeting Chinese AI Development

Semiconductors (specifically, logic and memory chips) are a basic enabler for AI. The dominance of US firms and intellectual property in upstream segments of this complex supply chain allow the US government to target Chinese AI development by restricting Chinese access to semiconductor technologies. This was done with extensive export controls introduced in October 2022, and amended in October 2023, justified as necessary to restrict China's capacity to develop AI-powered military and espionage capabilities.

These US controls threaten the "fast follower" strategy that China has pursued to date to develop its semiconductor industry, aided by this technology's well-defined roadmaps for future development (Lee and Kleinhans 2021). Many of the technologies concerned are complex to a degree that means China, despite massive import substitution efforts, will likely remain dependent for years to come on foreign suppliers.

The US controls are framed in ways that are designed to restrict Chinese access to the most advanced generations of logic processors and memory chips, and to the technologies required to manufacture them. The amendments promulgated in October 2023 aimed to close loopholes and to increase US regulators' visibility of products approaching the controlled specifications thresholds.

The structure of global semiconductor markets and the small size of chips creates significant problems for enforcing export controls, illustrated by Russia's ability to maintain large amounts of military equipment enabled by export-controlled, foreign manufactured semiconductors obtained through clandestine channels. Where licenses are granted for export of controlled products to China, monitoring compliance of these items once in-country presents further challenges. As of late 2023, Chinese firms seemed able to continue producing increasingly advanced chips at parameters that the US controls are designed to restrict. However, continued dependence on foreign suppliers may put temporary hard constraints on this progress in coming years.

2.3 Human Capital

Both Chinese and foreign assessments of China's AI talent pool emphasize problems regarding both quantity and quality. One 2020 Chinese government estimate projected that domestic production of skilled AI workers in 2022 would fall 480,000 persons short of the economy's demand (Weinstein and Stoff 2023). The deficit is especially acute for the highest grade of AI researchers: one assessment of three studies published over 2017–2018 suggests that China is second after the US in number of "AI practitioners" but far behind the US and several other countries in number of "AI experts," defined as the most innovative personnel who generate the most patents and publications (Ding 2019). One Chinese study published in January 2022 assessed that this situation had not fundamentally changed despite improvement in China's relative position, "especially (for) … top talents who can integrate AI technology development with the industrial system" (Center for Security and Emerging Technology 2022).

However, Chinese contributions to AI research publications have risen steadily, as has their quality judging from metrics such as citation rates and acceptance rates for papers presented to leading international conferences. One survey of global AI publications over 2010–20 found that if including CNKI—which accounts for an estimated two-thirds of Chinese AI papers—China accounted for half of AI publications globally (Chou 2022).

For several AI subfields, China-based authors have surpassed the US-based author share of the top 1% of cited publications. China's production of PhD graduates in STEM (science, technology, engineering, and mathematics) disciplines is far outstripping that of the US. Many leading Chinese institutions now provide world-class AI programs, with the highest-ranked universities now accounting for almost half of China's STEM PhD graduations (Zwetsloot et al. 2021).

Education and talent cultivation for AI are central concerns of the 2017 Plan, including vocational training. In 2017 China revised its high school curriculum requirements to include AI, and in 2018 an AI talent cultivation plan was promulgated for higher education institutions, including measures such as building innovation bases to promote collaboration between universities, research institutes and enterprises (Weinstein and Stoff 2023: 59–60). However, China has had difficulty attracting foreign AI workers, a major handicap in a global talent market. By one 2019 estimate, over 90% of China's AI talent was domestically sourced (Center for Security and Emerging Technology 2022).

Chinese returnees who completed advanced degrees and gained industry experience in the US have made an outsized contribution to Chinese industry's development in the AI sector. But political tensions have increasingly impacted such cross-border activity, and these are increasingly translating into legal barriers. Restrictions on "US persons" participating in China's semiconductor sector included in the US export controls discussed above have already had negative impacts on Chinese industry in semiconductors, a key enabling technology for AI.

The PLA has struggled to compete with China's civilian economy for talent. The military's human capital deficit appears to be particularly significant for AI development. To address these issues, by early 2019 the PLA had reportedly established talent recruitment stations at over 2500 colleges and universities nationwide, and internal reforms have aimed to raise benefits for PLA "civilian personnel" to levels comparable with those enjoyed by civil servants (Kania 2021: 536).

2.4 Transnational Collaborations

One survey found that in 2020, 22% of AI publications globally with Chinese-affiliated authors were international collaborations, with the US being the most significant partner country followed by the UK (Chou 2022). A 2023 study found this remained the case despite political tensions, with the EU collectively coming third, EU-China AI collaborations having increased continuously over 2017–2022. In the UK and EU, collaborations with Chinese actors are concentrated in a small group of universities, twelve institutions accounting for over a thousand co-authored papers each over the surveyed period (Arcesati et al. 2023).

The US digital technology sector been an attractive target for Chinese investors, with one 2021 study finding that the Chinese stake in top US AI-oriented start-ups was double that of other foreign investors combined (Chang and Hannas 2023: 42–43). Conversely, a 2020 study found that China hosted 10% of US multinationals' (MNCs) foreign AI labs, paired with Israel in second place after Europe (Heston and Zwetsloot 2020). However, US investment in China's AI sector is now constrained by "US persons" provisions in export controls and the forthcoming outbound investment regulation mandated by Presidential Executive Order in August 2023.

The dual-use nature of many AI applications imports risk that transnational collaborations may support Chinese defense AI efforts. As examples, NPU (mentioned above) ran a long-term collaboration with the Technische Universität Berlin in applying brain–computer interfaces to drone swarming and flight control (Arcesati 2022). In 2022, a researcher affiliated with the Bundeswehr University Munich co-authored a study with individuals from the PLA Information Engineering University on machine learning applications for data extraction from remote sensing images (Arcesati et al. 2023).

China's strategic partnership with Russia makes that country China's leading potential partner for direct collaboration on defense AI (Lee 2022a, b). While there is little public evidence of this, the number of known bilateral defense cooperation projects and Russian advances in relevant technologies, combined with Russia's increased dependence on China since its 2022 invasion of Ukraine, means that such exchanges cannot be ruled out. This would accelerate a trend towards increased AI research collaboration between the two countries apparent since 2016 (Konaev et al. 2021).

3 Organizing Defense AI

The PLA's structural reform of the mid-2010s included creating a "Strategic Support Force" (SSF), charged with integrating various "strategic" functions previously scattered across the PLA and given a "mandate to innovate." Established directly under the CMC rather than affiliated with other PLA command elements, the SSF consolidated outer space, intelligence, electromagnetic and cyber warfare capabilities, all fields in which information processing and data analysis is at a premium and which would therefore benefit from AI.

In April 2024, the SSF was abolished and its constituent departments were elevated to the status of independent 'Arms' in the PLA hierarchy, which report directly to the CMC despite having a status below that of the separate services, namely the Army, Navy, Air Force and Rocket Force. Among these new Arms, the Information Support Force (ISF) has been assigned a coordinating role in developing and applying the PLA's networked 'system of systems' (Ministry of National Defense, 2024).

However, the precise division of responsibilities between the ISF and its counterpart Arms (the Cyberspace Force, Aerospace Force and Joint Logistics Support Force) was not made clear. Different AI-enabled functions may be distributed between these organizations as deemed appropriate. One goal of this institutional restructuring is likely to be mirroring the US military's JADC2 concept and its attempted consolidation of networks to centralize operational command and control (Dahm 2024).

The direct subordination of these Arms to the CMC suggests that at least some of their functions may be regarded as "strategic" capabilities over which the CMC wants to exercise close control, as is the case with China's nuclear forces. Chinese media in 2016 reported the CMC's establishment of an Intelligent Unmanned Systems and Systems of Systems S&T Domain Expert Group, which is probably charged with setting strategic objectives and requirements and exploring productive links with civilian industry (Kania 2017).

China does not yet seem to have an equivalent to the US DoD's Chief Digital and Artificial Intelligence Office (CDAO), responsible for clearing large project proposals and providing a whole-of-defense support hub of AI expertise. However, in addition to being CMC Chairman, Xi Jinping also nominally heads other national steering bodies whose decisions may bear on development of defense AI, notably the Central Commission for Cybersecurity and Informatization (CCCI). Based on its composition when established in 2014, the CCCI's membership includes inter alia the head of MIIT, the chief of the PLA's Joint Staff Department, and one of the two CMC Vice-Chairmen (Xi's uniformed deputies in exercising top-level command of the PLA) (Lee 2022a: 21). From early 2023, Xi has also led a "Central Commission for Science and Technology" to oversee national S&T policy.

The PLA's reform process includes efforts to integrate doctrinal development with technical realities of emerging technologies like AI, although equipment procurement has remained a service responsibility. In 2017 the Academy of Military Sciences, which is the PLA's top institution for doctrinal theorizing and reports

directly to the CMC, integrated six technical research institutes that were previously subordinate to the pre-reform PLA general departments (Wuthnow 2019).

Research on the supplier profile for Chinese defense AI-related procurement reinforces the picture of a decentralized vendor network and the civilian economy's leading role. One study of defense AI-related contracts over April–November 2020 identified 273 unique (sole source) vendors who were the most common suppliers of AI-related equipment, typically private firms that focus on intelligent software or sensing technologies. Of the contracts surveyed, 61% were awarded to private enterprises, skewed towards companies founded since 2010 (Fedasiuk et al. 2021: 32–32). A further analysis of this dataset focusing on PLA service branch procurements found that among the 1983 procurement records examined, only 13 suppliers were awarded two or more contracts, with the two numerically leading vendors receiving only four and three contracts respectively (Konaev et al. 2023: 17–19).

China's defense SOEs are both buyers and sellers of AI-related equipment, suggesting that they may be specializing in certain AI subfields and so may avoid "crowding out" private sector investment. This corresponds to the apparent role of these state-owned conglomerates in related ICT "high technologies" such as semiconductors. One such conglomerate (China Aerospace Science and Technology Corporation, CASC, with subsidiaries) appeared by a large margin to dominate numerically the 2020 AI-related public procurement dataset mentioned above, with the SSF coming second (Fedasiuk et al. 2021: 29–30).

4 Funding Defense AI

The opacity of Chinese defense spending inhibits detailed assessments about the PLA's direct funding for AI. Based on evidence including the 2019 DWP's statement that 41% of China's 2017 defense budget went to equipment, one 2021 foreign assessment put the PLA's annual spending on AI as USD1.6bn-USD2.7bn, or in any case 'in the low billions of US dollars', roughly on par with the US military's spending on AI (Fedasiuk et al. 2021: 10–11). Based on declared Chinese numbers, the equipment share of the defense budget has generally grown since 2010, though China's 2020 report to the United Nations on its military spending showed a fall to 37.19% (Permanent Mission of the PRC to the UN 2022).

Allowance must also be made that some of the PLA's major defense acquisition programs are classified and not reflected in publicly available data. The concentration of much R&D work in China's universities, non-PLA affiliated research institutes and civilian enterprises limits the usefulness of official defense spending as a metric of total defense AI funding. By one foreign estimate, in 2019 China spent around USD25bn on research, development, evaluation and testing for military purposes outside the official defense budget (Tian and Su 2021: 18).

The much-reported "tech sector crackdown" by the Chinese state in recent years has been targeted at large commercial internet platform service providers and does not reflect a general persecution of private enterprise. Top-level policy continues to

emphasize the key role in strategic technology development of private enterprise and market forces, though the compatibility of this stance with Xi's reassertion of CPC-led centralized top-down direction remains to be seen. One market research estimate published in late 2022 projects Chinese investment in AI may reach USD26.69bn by 2026, accounting for about 8.9% of global AI investment (IDC 2022).

5 Fielding and Operating Defense AI

One survey of 58 Chinese defense-AI related papers published between 2016–2020 identified twelve discrete applications that spanned unmanned platforms; "intelligentization" of munitions, satellites and ISR); automation of offensive and defensive cyber operations and missile launch software; and cognitive electronic warfare (Fedasiuk 2020:7). A review of 343 AI-related defense equipment contracts published in China between April–November 2020 found the dominant application areas to be intelligent or autonomous vehicles (over a third of the surveyed contracts), ISR, information and electronic warfare, and predictive maintenance and logistics. Other contracts in this sample set relate to simulation and training, command and control, and automated target recognition (Fedasiuk et al. 2021).

For years the PLA has showcased a succession of increasingly capable maritime and aerial unmanned platforms, including a series of stealthy combat models. By 2018 all four PLA services (including the Rocket Force) fielded a variety of UAVs, including a growing number of multi-mission capable models (Kania 2018). By late 2022, the PLA was integrating a drone "carrier" catamaran into experimental naval task force exercises, with apparent variants of a civilian Chinese tandem-rotor drone on board, potentially to provide transport or ISR functions (Trevithick 2022). Foreign media in 2022 also identified what appeared to be new and larger unmanned underwater vehicles (UUV) at the PLA's Yalong naval base facing the South China Sea, approaching the size of the US Navy's developmental Orca autonomous UUV (Sutton 2022). Although deployed numbers appear limited, the PLA has a record of iteratively prototyping new equipment, eventually transitioning to rapid serial production once a given model is regarded as fit for purpose.

The current edition of Science of Military Strategy states that UAVs should be prioritized in unmanned systems development, although PLA theorists also stress that some "intelligentiziation" is necessary for sensing capabilities across all domains. A focus on UAVs is unsurprising given that China is the world leader in civilian drones and in military drone exports, and that the aerial environment presents a relatively simpler challenge for development of machine intelligence. Orientation towards UAVs and aerospace-focused SOEs is apparent in defense AI-related procurement tenders and contracts (Fedasiuk and Weinstein 2023: 176–180).

The nature of China's maritime sovereign disputes in the East and South China Sea Seas, which incentivizes persistent assertion of claimed rights over vast tracts

of maritime space, puts a premium on effective ISR and long-range high-endurance capabilities. The PLA has been using UAVs for this purpose since the early 2010s. UAVs and UUVs are also useful for monitoring Taiwanese defense assets and activity. Unmanned platforms provide a relatively low-cost and low risk means of collecting data on foreign military assets' electronic signatures, training, tactics and procedures (TTPs) and other information that would be useful in an armed conflict.

Development of sensing capabilities likely benefits from China's long-term and world-leading development of AI-powered sensor-based networks for civilian applications, notably "smart city" management and self-driving cars. Claimed Chinese research advances in hypersonic weapons over 2022 involve sophisticated sensing capabilities, potentially using AI (Lee 2022b). These indicate near-term potential for deep penetrating strikes to paralyze adversary operational systems, in line with the concepts discussed above.

Another AI application that the PLA seems to be deploying in practice is logistics optimization. The PLA is developing a "strategic delivery" system of integrated transport services and military bases to enable efficient force projection into zones of current operations, utilizing AI to enhance the speed of real-time requirements analysis and services delivery (Chieh and Yang 2021: 62).

6 Training for Defense AI

UAVs are leading the PLA's deployment of AI-related capabilities and so are supported by a system of specialized military education: one 2016 study identified at least eight PLA academic institutions with UAV-related programs for training specialists (Kania and Allen 2016). AI-enabled virtual and augmented reality systems are also used to train pilots of manned aircraft, with reports in 2021 of an AI agent developed by PLA institutes defeating a fighter pilot in a simulated dogfight.

UAVs have appeared in multi-service PLA training activities, while dedicated UAV-equipped units have progressively increased the sophistication of their training exercises (Kania 2018). The PLA may also be learning from use of Chinese-supplied military UAVs in foreign conflicts, notably in the Middle East and Africa. Reported use of Chinese civilian drones by Russian forces in Ukraine and for training operations potentially provides further intelligence collection and evaluation opportunities.

AI can be used to train for current operations and simulate the effects of future operational concepts and C2 approaches. This is an attractive option for the PLA to address its own negative assessments of its officers' decision-making capabilities, in the context of the whole institution's dearth of recent operational experience.

The PLA has been applying AI to wargaming since at least 2017, led by the National Defense University. Some of these activities have involved universities, research institutes and civilian firms, and pitted machine intelligence against machine intelligence as well as against humans, generating data to support further machine self-learning. One US analyst in 2019 characterized these Chinese

exercises as exceeding comparable US activities in scope and scale (Kania 2019). The PLA has awarded contracts to develop AI wargaming software for use in professional military education.

AI agents and wargaming platforms for testing them are being developed by both civilian and PLA institutions. For example, the Chinese Academy of Science’s Institute of Automation (CAS IoA) has developed the Miaosuan (庙算) wargaming platform and the AI gaming agent AlphaWar. AlphaWar is claimed to have passed the Turing test—exhibiting behavior indistinguishable from a human’s—in 2020, and to have confirmed this result in the 2021 iteration of the “Miaosuan Cup” tournament (Yin et al. 2022).

This competition, organized by the Chinese Society of Artificial Intelligence and the CAS IoA, pits human and AI players in adversarial and collaborative games on the Miaosuan platform, with human finalists required to guess whether anonymous opponents were human or AI. The competition’s 2021 iteration included four AI agents, two of which were developed by PLA institutions (Institute of Automation, Chinese Academy of Sciences 2021). The competition’s 2022 iteration was described as involving human-machine collaborative teaming and confrontation, and as geared towards the needs of manned and unmanned human-machine hybrid intelligence (Institute of Automation, Chinese Academy of Sciences 2022).

7 Conclusion

The main driver of Chinese military strategy is, by official explanation, S&T-driven evolution in patterns of warfare (Ministry of National Defense 2020). ‘Intelligentization’ of warfare through application of AI is the latest trend in this evolution. The PLA’s overall state of development suggests it is some way from becoming a global leader in “intelligentized” warfare. However, it is already deploying numerous and capable semi-autonomous military systems, while Chinese thinkers are covering the ground in applying AI’s potential to both current military operations and future operational concepts. China has a comprehensive and well-resourced national system for AI development in general, and a focus at the top of its political system on bending this “whole-of-nation system” to the service of defense AI applications.

China does not appear on the point of snatching a decisive lead over the US and its allies in military uses of AI. But Chinese authorities do have a clear view of AI’s structural importance, and reasonably clear military strategic goals that AI development can be directed towards. Foreign analysts tracking Chinese AI development face an increasingly tight information environment, as more data sources are progressively closed off. Yet assessing China’s progress with defense AI will be indispensable to judgments about the global military balance of power.

References

Allen, Gregory. 2019. Understanding China's AI strategy. Center for Naval Analyses. https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy. Accessed 30 January 2024

———. 2022. One key challenge for diplomacy on AI: China's military does not want to talk. Center for Strategic & International Studies. https://www.csis.org/analysis/one-key-challenge-diplomacy-ai-chinas-military-does-not-want-talk. Accessed 30 January 2024

Arcesati, Rebecca. 2022. Foreign collaboration continues in China's drive for technology self-reliance. The Strategist. https://www.aspistrategist.org.au/foreign-collaboration-continues-in-chinas-drive-for-technology-self-reliance/. Accessed 30 January 2024

Arcesati, Rebeca, Wendy Chang, Antonia Hmaidi, and Kai von Carnap. 2023. AI entanglements: Balancing risks and rewards of European-Chinese collaboration. MERICS. https://merics.org/en/report/ai-entanglements-balancing-risks-and-rewards-european-chinese-collaboration. Accessed 30 January 2024

Austin, Greg. 2014. Managing asymmetries in Chinese and American cyber power. *Georgetown Journal of International Affairs International Engagement on Cyber* IV: 141–151.

Center for Security and Emerging Technology. 2022. China artificial intelligence talent training report: translation. https://cset.georgetown.edu/publication/china-artificial-intelligence-talent-training-report/. Accessed 30 January 2024

Chang, Huey-Meei, and William C. Hannas. 2023. Foreign support, alliances, and technology transfer. In *Chinese power and artificial intelligence: perspectives and challenges*, ed. William C. Hannas and Huey-Meei Chang, 36–53. New York: Abingdon.

Chen, John. 2023a. Cyber and influence operations. In *Chinese power and artificial intelligence: perspectives and challenges*, ed. William C. Hannas and Huey-Meei Chang, 189–204. New York: Abingdon.

Chen, Stephen. 2023b. In China, AI warship designer did nearly a year's work in a day. South China Morning Post. https://www.scmp.com/news/china/science/article/3213056/china-ai-warship-designer-did-nearly-years-work-day. Accessed 30 January 2024

Cheung, Tai Ming. 2022. *Innovate to dominate: the rise of the Chinese techno-security state*. Ithaca/London: Cornell University Press.

Chieh, Chung, and Andrew N.D. Yang. 2021. Crossing the strait: recent trends in PLA 'strategic delivery' capabilities. 2021. In *The PLA beyond borders: Chinese military operations in regional and global context*, ed. Joel Wuthnow, Arthur S. Ding, Phillip C. Saunders, Andrew Scobell, and Andrew N.D. Yang, 151–179. Washington, DC: National Defense University Press.

Chou, Daniel. 2022. Counting AI research: exploring AI research output in English- and Chinese-language sources. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/counting-ai-research/. Accessed 30 January 2024

Cozad, Mark, Jeffrey Engstrom, Scott W. Harold, Timothy R. Heath, Sale Lilly, Edmund J. Burke, Julia Brackup, and Derek Grossman. 2023. *Gaining victory in systems warfare: China's perspective on the U.S.-China military balance*. Santa Monica: RAND.

Dahm, Michael. 2020. Chinese debates on the military utility of artificial intelligence. War on the Rocks. https://warontherocks.com/2020/06/chinese-debates-on-the-military-utility-of-artificial-intelligence/. Accessed 30 January 2024

Dahm, Michael. 2024. A Disturbance in the force: the reorganization of people's liberation army command and elimination of China's strategic support force. https://jamestown.org/program/a-disturbance-in-the-force-the-reorganization-of-peoplesliberation-army-command-and-elimination-of-chinas-strategic-support-force/. Accessed 10 May 2024.

Department of Defense. 2022. Report on military and security developments involving the People's Republic of China. https://www.defense.gov/News/Releases/Release/Article/3230516/2022-report-on-military-and-security-developments-involving-the-peoples-republi/. Accessed 30 January 2024

———. 2019. China’s current capabilities, policies and industrial ecosystem in AI. Testimony before the U.S.-China economic and security review commission. https://cset.georgetown.edu/publication/chinas-current-capabilities-policies-and-industrial-ecosystem-in-ai/. Accessed 30 January 2024

———. 2022. AI frameworks development in China. https://chinai.substack.com/p/chinai-175-ai-frameworks-development. Accessed 30 January 2024

Fedasiuk, Ryan. 2020. Chinese perspectives on AI and future military capabilities. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/chinese-perspectives-on-ai-and-future-military-capabilities/. Accessed 30 January 2024

Fedasiuk, Ryan, and Emily Weinstein. 2023. AI in the Chinese military. In *Chinese power and artificial intelligence: perspectives and challenges*, ed. William C. Hannas and Huey-Meei Chang, 175–188. New York: Abingdon.

Fedasiuk, Ryan, Jennifer Melot, and Ben Murphy. 2021. Harnessed lightning: how the Chinese military is adopting artificial intelligence. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/harnessed-lightning/. Accessed 30 January 2024

Fravel, Taylor, and Brad Carson. 2019. Jaw-Jaw: a look at the PLA’s history of planning for war with Taylor Travel. War on the Rocks. https://warontherocks.com/2019/06/jaw-jaw-a-look-at-the-plas-history-of-planning-for-war-with-taylor-fravel/. Accessed 30 January 2024

Heston, Roxanne, and Remco Zwetsloot. 2020. Mapping U.S. multinationals’ global AI R&D activity center for security and emerging technology. https://cset.georgetown.edu/publication/mapping-u-s-multinationals-global-ai-rd-activity/. Accessed 30 January 2024

Huang, Yanlong, Wu Qiong, and Jiang Rilie. 2023. Intelligent algorithms: a winning tool for cognitive domain warfare. People’s Liberation Army Daily. http://www.81.cn/jfjbmap/content/2023-03/21/content_335982.htm. Accessed 30 January 2024

IDC. 2022. AI spending will rise over $46 billion by 2026 in Asia/Pacific. https://www.idc.com/getdoc.jsp?containerId=prAP49721022. Accessed 30 January 2024

Institute of Automation, Chinese Academy of Sciences. 2021. The 2021 ‘Miaosuan Cup’ human-computer confrontational test competition was successfully held. http://www.ia.cas.cn/xwzx/kydt/202108/t20210809_6153415.html. Accessed 30 January 2024

———. 2022. 2022 Miaosuan Cup Human-Machine Hybrid confrontational competition is about to open. http://www.ia.cas.cn/xwzx/xshd/202209/t20220928_6518314.html. Accessed 30 January 2024

Kania, Elsa. 2017. Swarms at war: Chinese advances in swarm intelligence. *China Brief* 17 (9): 13–19.

———. 2018. The PLA’s unmanned aerial systems: new capabilities for a new era of Chinese military power. China Aerospace Studies Institute. https://apps.dtic.mil/sti/citations/AD1082743. Accessed 30 January 2024

———. 2019. Learning without fighting: new developments in PLA artificial intelligence wargaming. *China Brief* 19 (7).

———. 2021. Artificial intelligence in China’s revolution in military affairs. *J. Strateg. Stud.* 44: 515–554.

Kania, Elsa, and Kenneth Allen. 2016. The human and organizational dimensions of the PLA’s unmanned aerial vehicle systems. *China Brief* 16 (8): 10–17.

Konaev, Margarita, Andrew Imbrie, Ryan Fedasiuk, Emily S. Weinstein, Katerina Sedova, and James Dunham. 2021. Headline or trendline? Evaluating Chinese-Russian collaboration in AI. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/headline-or-trend-line/. Accessed 30 January 2024

Konaev, Margarita, Ryan Fedasiuk, Jack Corrigan, Ellen Lu, Alex Stephenson, Helen Toner, and Rebecca Gelles. 2023. U.S. and Chinese military AI purchases: an assessment of military procurement data between April and November 2020. https://cset.georgetown.edu/publication/u-s-and-chinese-military-ai-purchases/. Accessed 30 January 2024

Lee, John. 2022a. Cyberspace Governance in China: evolution, features and future trends. French Institute of International Relations (IFRI). https://www.ifri.org/en/publications/notes-de-lifri/asie-visions/cyberspace-governance-china-evolution-features-and-future. Accessed 30 January 2024

———. 2022b. China-Russia cooperation in advanced technologies: the future global balance of power and the limits of 'unlimited' partnership. Australian China Relations Institute, University of Technology Sydney. https://www.australiachinarelations.org/content/china-russia-cooperation-advanced-technologies-future-global-balance-power-and-limits. Accessed 30 January 2024

Lee, John, and Jan-Peter Kleinhans. 2021. Mapping China's semiconductor ecosystem in global context: strategic dimensions and conclusions. MERICS. https://merics.org/en/report/mapping-chinas-semiconductor-ecosystem-global-context-strategic-dimensions-and-conclusions. Accessed 30 January 2024

Lee, John, Meia Nouwens, and Kai Lin Tay. 2022a. Strategic settings for 6G: pathways for China and the US. International Institute for Strategic Studies. https://www.iiss.org/blogs/research-paper/2022/08/strategic-settings-for-6g-pathways-for-china-and-the-us. Accessed 30 January 2024

Lee, John, Eric Zhang, and Rogier Creemers. 2022b. China's standardisation system: trends, implications and case studies in emerging technologies. Leiden Asia Centre, University of Leiden. https://leidenasiacentre.nl/chinas-standardisation-system-trends-implications-and-case-studies-in-emerging-technologies/. Accessed 30 January 2024

Li, Minghai. 2019. Where are the changes in the mechanism for obtaining victory in intelligentized warfare. People's Liberation Army Daily. http://www.81.cn/jfjbmap/content/2019-01/15/content_225335.htm. Accessed 30 January 2024

Li, Binhai, and Huo, Yunchao. 2023. Change in operational guidance, from the viewpoint of an evolving mechanism for obtaining victory. People's Liberation Army Daily. http://www.mod.gov.cn/jmsd/2023-02/02/content_4931741.htm. Accessed 30 January 2024

Li, Wei, and Zhao, Zipeng. 2020. Building a future superior operational chain. People's Liberation Army Daily. https://www.81.cn/jfjbmap/content/2020-02/11/content_253748.htm. Accessed 30 January 2024

Mao, Weihao. 2023. Looking at military applications of artificial intelligence from the viewpoint of ChatGPT. People's Liberation Army Daily. http://www.81.cn/jfjbmap/content/2023-04/13/content_337523.htm. Accessed 30 January 2024

Ministry of Industry and Information Technology. 2017. Three year action plan to promote development of the new generation artificial intelligence industry. https://app.www.gov.cn/govdata/gov/201712/15/416663/article.html. Accessed 30 January 2024

———. 2022. Notice of two ministries on the 2022 inaugural 'Xingzhi Cup' National Artificial Intelligence Innovation and Application Competition, MIIT No. 170/2022. https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art_f5ccabd9350b4bb7ad49fe5baec60b25.html. Accessed 30 January 2024

Ministry of National Defense. 2015. China's Military Strategy 2015. http://eng.mod.gov.cn/publications/2021-06/23/content_4887928.htm. Accessed 30 January 2024

Ministry of National Defense. 2024. Defense ministry spokesperson's remarks on recent media queries concerning the pla information support force. http://eng.mod.gov.cn/xb/News_213114/NewsRelease/16302635.html. Accessed 10 May 2024.

———. 2019. China's National Defense in the New Era. http://eng.mod.gov.cn/publications/2019-07/24/content_4846452.htm. Accessed 30 January 2024

———. 2020. Regular Press Conference, 26 November. http://eng.mod.gov.cn/news/2020-11/29/content_4874839.htm. Accessed 30 January 2024

Nature. 2022. Leading science cities by the numbers. https://doi.org/10.1038/d41586-022-02881-8. Accessed 30 January 2024

Panda, Ankit. 2019 A new Chinese autonomous underwater vehicle? The Diplomat. https://thediplomat.com/2019/11/a-new-chinese-autonomous-underwater-vehicle/. Accessed 30 January 2024

Permanent Mission of the People’s Republic of China to the United Nations. 2021. Position Paper of the People’s Republic of China on Regulating Military Applications of Artificial Intelligence (AI). http://geneva.china-mission.gov.cn/eng/dbdt/202112/t20211213_10467517.htm. Accessed 30 January 2024

———. 2022. Report on military expenditure in 2020. https://front.un-arm.org/wp-content/uploads/2022/03/20220211-note-verbale-from-china-mission.pdf. Accessed 30 January 2024

Pollpeter, Kevin, and Amanda Kerrigan, with contributions by Andrew Ilachinski. 2021. The PLA and intelligent warfare: a preliminary analysis. Center for Naval Analyses. https://www.cna.org/reports/2021/10/the-pla-and-intelligent-warfare-preliminary-analysis. Accessed 30 January 2024

Qiao, Hui, Su Yun, and An Jin. 2018. Research on maritime intelligence data analysis technologies for massive data. *Command Control and Simulation* 40 (2).

Sutter, Karen M., and Zachary Arnold. 2023. China’s AI companies: hybrid players. In *Chinese power and artificial intelligence: perspectives and challenges*, ed. William C. Hannas and Huey-Meei Chang, 19–35. New York: Abingdon.

Sutton, H. I. 2022. China’s new extra-large submarine drones revealed. Naval News. https://www.navalnews.com/naval-news/2022/09/chinas-secret-extra-large-submarine-drone-program-revealed/. Accessed 30 January 2024

Takagi, Koichiro. 2022. New tech, new concepts: China’s plans for AI and cognitive warfare. War on the Rocks. https://warontherocks.com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare/. Accessed 30 January 2024

Tian, Nan, and Fei, Su. 2021. A new estimate of China’s military expenditure. Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/sites/default/files/2021-01/2101_sipri_report_a_new_estimate_of_chinas_military_expenditure.pdf. Accessed 30 January 2024

Toner, Helen. 2023. AI safeguards: views inside and outside China. In *Chinese power and artificial intelligence: perspectives and challenges*, ed. William C. Hannas and Huey-Meei Chang, 244–259. New York: Abingdon.

Trevithick, Joseph. 2022. China’s naval mothership for aerial drones looks to be operational. The War Zone. https://www.thedrive.com/the-war-zone/chinas-drone-carrier-mothership-looks-to-be-in-service. Accessed 30 January 2024

Wang, Ronghui, and Deng, Shifeng. 2022. Dialectical understanding of single and multiple domains in joint operations. People’s Liberation Army Daily. http://www.81.cn/jfjbmap/content/2022-01/20/content_307852.htm. Accessed 30 January 2024

Webster, Graham, Rogier Creemers, Paul Triolo, and Elsa Kania. 2017. Full translation: China’s ‘New generation artificial intelligence development plan’. New America. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/. Accessed 30 January 2024

Weinstein, Emily, and Jeffrey Stoff. 2023. China’s quest for AI talent. In *Chinese power and artificial intelligence: perspectives and challenges*, ed. William C. Hannas and Huey-Meei Chang, 57–72. New York: Abingdon.

Wuthnow, Joel. 2019. China’s ‘new’ academy of military science: a revolution in theoretical affairs? *China Brief* 19 (2).

———. 2021. What I learned from the PLA’s latest strategy textbook. *China Brief* 21 (11): 6–12.

Xinhua. 2018. Xi Jinping: promote the healthy development of new generation artificial intelligence in China. http://www.xinhuanet.com/politics/2018-10/31/c_1123643321.htm. Accessed 30 January 2024

Yin, Qiyue, Zhao Meijing, Ni Wancheng, Zhang Junge, and Huang Kaiqi. 2022. Intelligent decision making techniques and challenges for wargaming. *Acta Automat. Sin.* 48 (9): 1–15.

Zhou, Wei, and Yaning Chen. 2022. Applications of AI technology in military command and control against the backdrop of intelligentized warfare. *Military Digest* 2022 (15): 27–30.

Zwetsloot, Remco, Jack Corrigan, Emily S. Weinstein, Dahlia Peterson, Diana Gehlhaus, and Ryan Fedasiuk. 2021. China is fast outpacing U.S. STEM PhD growth. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/china-is-fast-outpacing-u-s-stem-phd-growth/. Accessed 30 January 2024

Overcoming the Long Shadow of the Past: Defense AI in Japan

Motohiro Tsuchiya

Since the end of World War II, Japan has not had a full-fledged military, but only Self-Defense Forces (SDF) for the sole purpose of defensive defense. Hesitancy exists in society, especially in academia, to research and develop technologies that could be diverted to military use. This has created a long shadow of the past in which public opinion, strategic culture, and the academic-industrial ecosystem mutually reinforce each other not to directly address defense technologies. However, with the recent deterioration of the national security environment around Japan, such hesitance is weakening, and research and development of technologies that can be applied to defense purposes is now being conducted, also in cooperation with partners like the United States, the United Kingdom, and others.

Discussions about artificial intelligence for defense purposes began in earnest around 2022, with descriptions found in government and defense ministry documents, and budget appropriations beginning to be made. However, the budget size is miniscule and no special organization for defense artificial intelligence (AI) exists. In addition, there is no plan to use defense AI in earnest in defense operations, and it is merely positioned as one of the technologies that attract widespread attention. Attempts to deepen the knowledge of artificial intelligence among SDF personnel have only just begun.

M. Tsuchiya (✉)
Graduate School of Media and Governance, Keio University, Kanagawa, Japan

Keio University Global Research Institute (KGRI), Tokyo, Japan
e-mail: taiyo@keio.jp

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_22

1 Thinking About Defense AI

A search of the database of the Nihon Keizai Shimbun (Nikkei), one of the most widely read newspapers by Japanese businesspeople, shows that the first article in which the words "artificial intelligence" and "defense" appear simultaneously was on 12 May 2014 (Nihon Keizai Shimbun 2014). After that, there are some reports on AI use on defense equipment and cyber defense.

Contrary to these public reports, aeronautical and space science journals discussed the defense AI much earlier. In 1983, Tamotsu Sakamoto of the third Research Institute of the National Defense Agency's Technical Research Headquarters published a paper titled "On Navigation Using Artificial Intelligence Search Methods" (Sakamoto 1983). However, when this paper was written, deep learning was not yet in use.

A paper with a similar perspective was published in 1990. In their paper Akira Soga and Hideo Nakashima wrote, "artificial intelligence application systems, including expert systems, have been studied and developed overseas, especially in the United States, under the Strategic Computing Program (SCP) and other programs. In contrast, in Japan, research and development tends to be conducted mainly for industrial applications" (Soga and Nakashima 1990). The paper focused on systems for use on manned aircraft, and it does not examine the use of autonomous artificial intelligence to control current unmanned aircraft.

Japan's defense policy is called "exclusively defensive defense." The Japanese constitution after World War II does not allow Japan to have full-fledged military forces and the Japanese nation cling to peace-oriented diplomacy. The so-called Yoshida Doctrine, which was named after Prime Minister Shigeru Yoshida, was the basis of Japan's diplomacy, defense policy and economic policy. The doctrine guided the Japanese government to allocate more resources towards the economy while keeping defense spending low under the nuclear umbrella based on the Japan--U.S. Security Treaty. That combination of policies enabled Japan to recover quickly from the destruction of World War II. This situation has been changing step by step as threat perceptions are altered by external incidents. However, there is a strong long shadow of the past in the use of technologies for defense purposes.

After the end of World War II, a general understanding emerged to avoid research on military-related technologies. Consequently, Japan has been reluctant to discuss military applications of new technologies, including AI. The Science Council of Japan was established in 1949, soon after the end of World War II. The following year, in 1950, the Council issued a "Statement of Determination to Never Follow Scientific Research for the Purpose of War," and in 1967 it issued a "Statement of No Scientific Technology for Military Purposes." This post-World War II atmosphere was based on the reflection that the academic community, including universities, had been mobilized for war.

However, with the outbreak of the Korean War in 1950, the General Headquarters of the Allied Forces (GHQ) decided to change the policy of demilitarization of Japan, and in August 1950, paramilitary organizations called the Japan Police

Reserve Corps and the Coastal Safety Force were established by GHQ. The Police Reserve Corps was reorganized as the National Safety Forces in 1952 and reorganized as the Ground Self-Defense Force in 1954. At the same time, the Coastal Safety Force became the Maritime Self-Defense Force, and the Air Self-Defense Force was newly organized. The three Self-Defense Forces were not full military forces like those of other countries, but rather organizations based on the constitution with an exclusively defense purpose. It took 53 years for the Defense Agency, which oversaw the SDF, to become a ministry as the Ministry of Defense in 2007.

Defense spending, but not military spending, subsequently increased as Cold War tensions rose, and there were calls for more defense equipment. However, the response of the Science Council of Japan and universities was weak, and there was no atmosphere of active cooperation, even for the sake of exclusive defense.

When the Cold War ended with the Malta Summit, the fall of the Berlin Wall in 1989, and the dissolution of the Soviet Union in 1991, calls for an expansion of the defense industry weakened.

However, in 1998, when North Korea launched a Taepodong missile and it passed over Japanese territory, the North Korean military threat was rapidly recognized and came to be known as the "Taepodong Shock." Simultaneously, China's gradual military buildup began to be viewed as a cause for concern. By that time, voices denying the existence of the SDF had weakened in Japanese society; rather, the development of defense forces on an appropriate scale was considered essential. Nevertheless, there was a political consensus that defense spending should be limited to 1% of GDP, and this was maintained until recently.

However, when the second Shinzo Abe's administration was formed in 2012, threats by North Korea and China became more obvious and the Abe administration set up "proactive pacifism" as a matter of defense policy. In December 2013, the Abe administration approved the National Defense Program Guidelines (NDPG). The document states:

> From the aspect of security, it is necessary to utilize civilian technology effectively also in the field of security through regularly assessing the trend in science and technology including information related to technological development as well as consolidating the capabilities of the government, industry and academia. Under such recognition, the Ministry of Defense will strive to make effective use of civilian technology that can also be applied to defense (dual-use technologies), by enhancing partnerships with universities and research institutes, while strengthening technology control functions to prevent the outflow of advanced technologies (MoD 2013: 28).

However, the 2013 National Defense Program Guidelines contained no mention of artificial intelligence. Yet, while a shift towards defense technologies in government and academia is occurring, the debate over artificial intelligence gradually coincided. The first Defense Program Guidelines that mention AI were released in December 2018, also under the Abe administration, indicating that:

> Due to advances in military technologies, a variety of threats can now easily penetrate national borders. States endeavor to develop weapons that leverage cutting-edge, potentially game-changing technologies. They also engage in research of autonomous unmanned weapon systems equipped with artificial intelligence (AI) (MoD 2018: 3–4).

It also stated that one of the measures to strengthen the basis of human resources is to "make focused investments through selection and concentration in important technologies including artificial intelligence and other potentially game-changing technologies" (MoD 2018: 24).

In response to the 2018 National Defense Program Guidelines, the Ministry of Defense showed plans to introduce artificial intelligence to use it to automate cyber defense, translate military and defense-related data, and manage equipment (determine repair points and the need to replace parts) (Nihon Keizai Shimbun 2019).

The National Defense Program Guidelines were renamed the National Defense Strategy when it was released 4 years later in December 2022. There is a reference to AI in the following statement:

> Rapid advances in science and technology are fundamentally changing the paradigm of security. Countries are striving to develop cutting-edge technologies that could dramatically alter the character of warfare and thus prove to become 'game changers.' China in particular has been rapidly promoting accelerated technological innovation and its application for military purposes under the name of the 'military-civilian integration strategy:' China is notably accelerating military capability development premised on unmanned assets that leverage artificial intelligence (AI). These trends are resulting in fundamental changes to the way the military is organized as well as the way warfare is prosecuted (NSC of Japan 2022a: 5).

In the Defense Buildup Program announced with the 2022 National Defense Strategy, a more in-depth description of artificial intelligence can be found (NSC of Japan 2022b). First, as a response to information warfare, including in the cognitive domain, the Plan states,

> In addition, the following functions will be developed: automatic collection and analysis of open-source information using artificial intelligence (AI), which will enable continuous collection and analysis of information on trends in each country; automatic collection of information on social networking sites, etc., to determine the authenticity of information communicated by each country; and future forecasting functions for estimating the security situation (NSC of Japan 2022b: 15).

In relation to command, control, and information-related functions, the plan seeks to "accelerate decision-making through the use of Artificial Intelligence (AI), etc., while strengthening the resiliency of the network." In about 10 years, the report continues, Japan will "reinforce information gathering and analysis capabilities through the use of AI, etc., while enhancing the system for persistent information gathering and sharing" (NSC of Japan 2022b: 51).

Colonel Hiroshi Ito, who worked in cyber defense in the Japan Ground Self-Defense Force, notes that artificial intelligence will be used in all kinds of weapons in the future (Ito 2023: 68–70). AI will extend human intellectual capabilities as an aid to humans and will play the role of a calm responder on behalf of humans. He points out that at present AI has five advantages:

1. Can learn;
2. Able to handle a wide variety and large volume of data;
3. Has high processing speed;
4. Can share what it has learned with other AIs;

5. Has no human error.

The destination, he says, is the unmanned battlefield. However, there are concerns about autonomous weapons, and he appeals for an urgent debate on laws, ethics, and policies to shape the development of this technology.

The 2023 Defense White paper mentions AI nineteen times (including in the headlines). It is mentioned in the defense policy descriptions of AUKUS, Australia, China, India, the United States, and Russia. The section that mentions AI the most is Section 1 "Trends in Science and Technology Expanding to Information Warfare" in Chap. 4 "Trends in Space, Cyber, and Electromagnetic Fields, Information Warfare, and Other Issues for the International Community." It covers about half a page and describes the defense applications of AI in various countries and internationally. However, there is little explanation of Japan's own defense use of artificial intelligence. After reiterating the items presented in the Defense Buildup Program, the following statement is made in the "Efforts to Enhance Intelligence Analysis and Other Functions" section:

> In order to win battles in a situation in which the battle situation will become more rapid and complex in the future, it is necessary to establish a system that enables real-time information sharing by making maximum use of various means, including artificial intelligence (AI), and further strengthening capabilities such as information gathering and analysis, and to continuously and more accurately grasp the intentions and capabilities of countries surrounding our country (MoD 2023d).

On 25 August 2023, the Japanese government held the first meeting of the Council of Ministers Concerned with Research and Development and Public Infrastructure Development that Contribute to Strengthening the Comprehensive Defense Systems (Cabinet Secretariat 2023). Among R&D for civilian use, nine areas, including AI and cyberattack countermeasures, were designated as "key technology issues" that will contribute to strengthening the defense system, and the government confirmed its policy to work on them across ministries and agencies (Table 1). At the meeting, the chairman, Chief Cabinet Secretary Hirokazu Matsuno, emphasized the importance of "breaking down the stove-piping between ministries and agencies and strengthening the comprehensive defense system in order to efficiently utilize the resources and capabilities of our entire nation" (Cabinet Secretariat 2023).

2 Developing Defense AI

The Japanese government's defense policies are presented in three defense documents: the National Security Strategy, the National Defense Strategy, and the Defense Buildup Program (MoD 2022b). The Ministry of Defense is responsible for their implementation, but the Acquisition, Technology & Logistics Agency (ATLA) is responsible for the technical aspects. ATLA's Technology Strategy Department conducts the Short-term Demonstration Project for New Technology. It is a project to demonstrate the effectiveness of advanced technologies that are at the level of

Table 1 Japan's key technology issues

Field	Contents
Energy	New energy sources, high-performance energy storage, high-power energy projection, etc.
Sensing	Establishment of high-precision positioning, navigation, and time measurement methods; high-precision sensing of people, objects, and the environment; higher performance sensing than conventional methods (quantum sensing, biosensing, etc.), etc.
Computing	High-speed, high-efficiency new principal computing (quantum, optical, brain-type, etc.), high-efficiency arithmetic processing of huge amounts of data, etc.
Data processing	Highly accurate prediction of the future, advanced artificial intelligence, improvement, and enhancement of cognitive abilities (including medical care), etc.
Telecommunications	Establishment of high-speed, high-capacity, highly secure, and high-performance information and communication device technologies (e.g., communication devices that can be used in space, etc.)
Information security	Efficient and continuous detection, prevention, and response to cyber attacks, enhancement of cyber resilience, advanced cryptography (quantum cryptography, high-performance cryptography, etc.), etc.
Material	Creation of new materials (including medical materials), establishment of advanced manufacturing and processing methods, etc.
Unmanned and autonomous	Unmanned and autonomous machines, advanced human-machine interfaces, group control and distributed control among multiple, manned, and unmanned machines, etc.
Machine	Highly functional and high-performance mechanical structure, establishment of hypersonic flight technology, long-duration, and long-distance navigation, etc.

Source: Council of Ministers (2023)

practical use in civilian applications by bringing together civilian engineers and operators in order to promptly solve problems faced by units and to promote their practical use in a short period of about 3 years. The project also aims to "reduce defense product prices and maintenance costs by using the results of this project in civilian markets, etc." (ATLA 2023c). Table 2 provides an overview of the projects launched within this framework.

ATLA began the Security Technology Research Promotion System in FY2015, which recruits and funds research and development through an open application process (ATLA 2023b). The launch of this system caused a major stir. This is because the Japanese academic community had been reluctant to research and develop technologies that could be diverted to military use, but the Ministry of Defense and ATLA decided to break that trend and provide its own R&D funds for technologies that could lead to defense capabilities. In FY2017, 109 applications were received, of which 58 (53%) were from universities and other institutions, 22 (20%) from public research institutions, and 29 (27%) from companies (ATLA 2015).

However, because applications to the Security Technology Research Promotion System stirred controversial media coverage, the number of applications in FY2016

Table 2 AI Projects Launched by Acquisition, Technology & Logistics Agency

Focus	Year	Bidder	Contract Volume
Construction of a tool for analyzing automatic vessel identification devices using artificial intelligence	2018	Unknown	
Streamline system maintenance and management operations using artificial intelligence,	2019	unknown	
Automatic generation of training data for identification of satellite images by artificial intelligence	2020	IHI Jet Service	Less than JPY6M (around €38 k)
Fully automated aeronautical weather observation using artificial intelligence	2020	Hitachi	JPY44M (around €277 k)
Construction of a support system for creating exercise scenarios using artificial intelligence	2021	Hitachi	Around JYP10M (around €63 K)

Source: ATLA (2020a, b, 2021)

decreased to 44, with 23 (52%) from universities, 11 (25%) from public research institutions, and 10 (23%) from companies (ATLA 2016). In FY2017, however, the numbers returned, with 104 applications (ATLA 2017).

The first research on AI under this program appeared in FY2018. Natsuki Matsunami of Mitsubishi Heavy Industries, Ltd, one of Japan's largest defense contractors, was awarded the "Basic Research on Problem Coping by Collaboration of a Very Small Number of Humans and AI" (ATLA 2018). In FY2019, developing AI to understand human mental states was included in "Development of a Method for Estimating Latent Brain Dynamics and Elucidation and Control of Mental State Transitions," for which Eiji Uchibe of Advanced Telecommunications Research Institute International (ATR) was awarded the contract (ATLA 2019b). Since 2018, 11 defense AI studies have been launched.

Despite a marginal number of applications, ATLA has shown strong interest in AI-related research. 31 research themes were listed by ATLA for the FY2023 open call, including the following 12 that directly refer to AI in the title or description (ATLA 2023a):

- Fundamental research on sequential decision-making AI architectures that can build trust in unknown environments
- Basic research on AI to realize accurate predictions from all kinds of information
- Fundamental research on AI architecture with robustness in unknown environments
- Basic research on the improvement of cognitive and communicative functions through brain science
- Basic research on human cognitive support for multiple unmanned aircraft operation and control
- Basic research on cognitive security
- Basic research on security that automates protection against unknown attacks on wireless communications and cyber kill chain fragmentation
- Basic research on magnetic sensor technology

- Fundamental research on technologies for understanding materials and objects in the ground or on the seafloor
- Basic research to significantly improve the performance of unmanned underwater and surface vessels and underwater vehicles
- Basic research to significantly improve the performance of aircraft and unmanned aerial vehicles
- Basic research to significantly improve the performance of vehicles and unmanned vehicles

It is important to note that none of these calls and the respective projects are directly related to weapons. With a sense of aversion to military-related research still lingering, researchers remain reluctant to directly engage in military technology research. Against this backdrop, open calls are being made for technologies that are less military in nature but still applicable to defense.

In addition to this funding for external research, development is also taking place within ATLA. At the Agency's Technical Symposium 2019, AI was mentioned in three of the 16 oral sessions and 23 poster session summaries, thereby covering, among other things, the following topics:

- Taisuke Katayama, "R&D Vision: Achieving Multidimensional Integrated Defense Capability and Beyond"
- Masataka Okubo, "An Attempt to Introduce Artificial Intelligence (AI) into Ship Design (Demagnetizer Gear Design)"
- Toshiro Kamitani, Hiroka Sano, and Kenji Hamano, "Target Categorization from Synthetic Aperture Radar Images"

According to a report of the second topic, the work that had been done by skilled technicians was replaced by AI, and tens of millions of verifications can now be done in three to four hours, a significant time saving. A report of the third topic examined the possibility of using AI to classify radar images (ATLA 2019a). These reports are also being used within ATLA to meet actual defense needs.

Japanese defense companies are working on AI, although not necessarily for defense equipment. The demand for Japanese defense companies comes primarily from the civilian sector. AI is being developed for such civilian demand, and there is a high possibility that such technology and knowledge will be applied to defense equipment if necessary.

Moreover, Japan also looks at international cooperation to develop emerging technologies and AI. In August 2023, Craig Martell, Chief Digital and AI Officer of the Pentagon, visited Japan, Singapore, and South Korea to discuss opportunities to "deepen cooperation associated with data, analytics, and the responsible deployment of AI" (Vincent 2023). These talks mirror long-standing bilateral interests in jointly advancing dual-use technology cooperation (Tajima 2023). To this purpose both countries signed a "project arrangement" in late December 2023 to jointly develop AI for the use of Unmanned Aerial Vehicles (UAV) "that will be used in a 'loyal wingman' role alongside" the Global Combat Air Program (GCAP) (Kadidal and Kumar 2023). US-Japanese defense AI cooperation could become even more

relevant should Japan join trilateral cooperation with Australia and the UK in the AUKUS framework.

In parallel to technology cooperation with the US, Tokyo and London have been extending technology ties as well. In May 2023, both nations adopted the "Hiroshima Accord," which outlines a strategic technology partnership, and renewed a science and technology agreement to cooperate on innovation and new technologies (Prime Minister's Office 2023; Evenstad 2023). Expanding science and technology bonds are relevant given trilateral cooperation with Italy on the GCAP (Chuter 2022) and recent developments in Japan's strategic environment. In view of both aspects General Jim Hockenhull, Commander of the UK Strategic Command, recently underlined that by "using both the Japanese and the UK industrial base, (both nations) can generate even greater and even better capabilities, which play a part in any deterrence approach" (Kitado 2023).

In addition, Japan also engages with France on AI cooperation. According to ATLA, bilateral research cooperation includes mine-countermeasure technologies, with AI being used to "identify targets from images obtained by mine detectors" (Majumdar 2023: 25).

3 Organizing Defense AI

In 2016, at the direction of Prime Minister Shinzo Abe, the Japanese government created the Strategic Council for AI Technology, which brings together the wisdom of industry, academia, and government and eliminates organizational silos (Cabinet Office 2018). On 31 March 2017, the Council released the Artificial Intelligence Technology Strategy presenting a three-phased approach: First, data-driven AI utilization will progress in each domain by around 2020; second, general use of AI and data will progress beyond the boundaries of individual domains by around 2025; and third, each domain will be connected in a complex manner by around 2030, creating an ecosystem (SCAIT 2017).

Two years later, the Council released the "Strategic Action Plan for Artificial Intelligence Technology" (SCAIT 2018). The plan aimed at promoting AI involving a diverse set of ministries—Ministry of Internal Affairs and Communications, the Ministry of Education, Culture, Sports, Science and Technology, the Ministry of Economy, Trade and Industry, the Cabinet Office, the Ministry of Health, Labor and Welfare, the Ministry of Agriculture, Forestry and Fisheries, and the Ministry of Land, Infrastructure, Transport and Tourism – the action plan primarily targeted the industrial use of AI whereas AI for defense was not considered.

Based on this strategy, AI research was to be conducted at three national research institutes:

- First, in April 2017 the National Institute of Information and Communications Technology (NICT) established the AI Science Research and Development Promotion Center (Kidawara 2019). However, NICT is a research institute under

the Ministry of Internal Affairs and Communications (MIC) and does not conduct defense-related research, apart from cybersecurity.
- Second is the Artificial Intelligence Research Center (AIRC) of the National Institute of Advanced Industrial Science and Technology (AIST). The center studies the application of artificial intelligence to the manufacturing, service, medical and nursing care, and security sectors. However, there does not appear to be any research focused on defense or military applications. The applications mentioned for the security sector are automatic explanation functions for videos and evacuation guidance during disasters.
- Third is the Center for Advanced Intelligence Project (AIP) of the National Institute of Physical and Chemical Research (RIKEN). The Center has three research groups: the Generic Technology Research Group, the Goal-Oriented Technology Research Group, and the Artificial Intelligence in Society Research Group. However, these groups do not appear to be conducting research directly related to defense.

On 11 June 2019, the Japanese government, via the Integrated Innovation Strategy Promotion Council, released the AI Strategy 2019: AI for People, Industry, Region, and Government (IISPC 2019). The document focuses on education and industry; again defense applications were not considered. Two years later, in June 2021, the Japanese government published the AI Strategy 2021, but again, the Ministry of Defense's efforts were not explicitly mentioned. In response to this AI Strategy 2021, the AI Strategy Executive Council established the "New AI Strategy Study Council". The AI Strategy 2022 was the first capstone document to refer to AI in relation to security with the following statement:

> In view of the increasingly complex international situation and changes in socio- economic structures, various initiatives are being considered for important technologies including AI from the perspective of economic security. Therefore, it is necessary to coordinate related measures so that the government as a whole can effectively prioritize them (IISPC 2022a).

However, this refers to economic security (or geo-economics), not military security. The following statement was also included.

> Pursue fusion of AI and Japan's strengths to address challenges unique to Japan ([1] health, medical care, and nursing care; [2] agriculture; [3] infrastructure and disaster prevention; [4] transportation infrastructure and logistics; [5] regional revitalization; [6] manufacturing; and [7] security) (IISPC 2022a: 27).

Attached to the 2022 strategy was a "List of AI Strategy 2022 Initiatives," in which the Ministry of Defense included a section on "Promoting Research on the Application of AI Technology to Contribute to the Defense of Japan" (IISPC 2022b). This is the first documents that brings AI and defense together and underlines the Japanese government's growing awareness of addressing this issue.

According to the AI Strategy 2022 progress report published in April 2023, the Ministry of Defense is addressing defense AI by bringing in experts from the outside and stepping up training efforts. In addition, the Ministry also intends to

enhance the capabilities of equipment used by the SDF, including detection and identification (IISPC 2022c).

On 11 May 2023, the Japanese government held the first meeting of the AI Strategy Council of experts together with the relevant Ministers. Prime Minister Fumio Kishida attended the first meeting. About 2 weeks later, the Council met again, discussed several topics and issues, among others, the following statements:

> AI is also an important tool in global issues such as security, disaster management, and global warming countermeasures, and our country needs to work on technological innovation together with volunteer countries (AI Strategic Council 2023: 6).

> There is an argument that the use of AI is important in security-related matters as well, but it should be handled flexibly, for example by leaving it for discussion by specialized departments, depending on the need for information management (AI Strategic Council 2023: 16).

In general, Japan's AI focus rests with industrial applications and educational efforts. Research to advance defense AI has only just started in 2022. Although no dedicated institutions addressing AI within the defense establishment have yet been created, the 2022 National Security strategy indicates the willingness of the Ministry of Defense to "establish a mechanism to aggregate military information" and urges the intelligence and policymaking departments to "enhance information management analysis" (Majumdar 2023: 25).

4 Funding Defense AI

No summarized data has been released on the Japanese government's AI budget. According to the Nihon Keizai Shimbun (Nihon Keizai Shimbun 2023), the Japanese government has summarized its basic policy and budget for policies related to generative AI for the FY2024 budget estimates. The government will focus on the development of infrastructure for the development of AI, including supercomputers and high-quality data, and will create a foundation for research and development in Japan to reduce its dependence on foreign countries for AI development.

The government's overall AI-related budget was approximately JPY100bn (or €630M) in the initial budget for FY2023. The government is considering doubling the budget to JPY200bn (€1.26bn) in FY2024. The basic policy has three pillars to strengthen the research and development infrastructure for generative AI by developing of data centers with supercomputers, developing high-quality AI training data, and creating generative AI that can be used in scientific research.

In March 2023, the Ministry of Defense included a section on defense AI in its budget (MoD 2023b, c). The overall amount spent on defense AI is JPY6.58bn (€41.4M), or around 0.096% of the total FY2023 defense budget of JPY6.8219tn (€42.9M). The defense AI budget encompasses the following items:

- Development of functions for automatic collection and analysis of public information using AI: JPY2.2bn (€13.9M)
- Research on speeding up decision making using AI: JPY4.3bn (€27M)

- Utilization of external forces for AI implementation: JPY50M (€0.32M)
- Training of AI human resources by providing AI training courses: JPY30M (€0.19M)

In addition to this, part of the "Project for Establishment of Systems for Strengthening Production Base of Defense Equipment, etc." (JPY36.3bn or €226M) will be used to "implement efficiency improvement of defense equipment manufacturing process, etc. through introduction of advanced technologies such as 3D printer technology and AI technology." Thus, the exact size of the defense AI budget is not publicly known as spending on AI in other budgets, for example on cybersecurity, need to be considered as well.

5 Fielding and Operating Defense AI

In April 2022, the Ministry of Defense held a presentation entitled "AI Initiatives in the Ministry of Defense" (MoD 2023a). The document states, that:

> In the field of national defense, AI technology is expected to be utilized for faster and more efficient information processing, situational assessment, operational planning, and high-level search and rescue using unmanned aircraft, etc. Many countries including China and the United States are actively investing in R&D related to AI technology as it could change the future of warfare.

The Ministry of Defense also believes that AI technology can be a game changer and that it is necessary to make focused investments and realize its implementation in defense applications as soon as possible. In this regard, the document also illustrates two practical examples illustrating exemplary lines of effort that the SDF are interested in:

- The first example refers to research on AI-based radar image identification to study the technology to automate the identification of radar images using AI to efficiently conduct constant and continuous information gathering and warning monitoring activities. By automating the deciphering and identification of radar images, which requires skill, it is expected to reduce the burden on units and improve mission efficiency.
- The second example refers to a study of the components of an unmanned submersible monitoring machine. This will involve research on autonomous monitoring technology and sensor systems. The plan is to apply AI technology to decisions about the behavior of underwater vehicles used for long term surveillance.

In addition to these two examples, the Ministry's presentation also discusses additional initiatives summarized in Table 3.

Table 3 AI efforts of the Japanese Ministry of Defense

Specific target	Initiatives	Details of initiatives
Construct a digital twin that will be the basis to use AI	Promotion of digital transformation (DX) in research and development of equipment, etc.	To introduce a digital twin, a digital thread, and others to strengthen the necessary governance at each level of design, numerical analysis, and experiments in research and development of equipment
	Promotion of research and development to use the human digital twin for education, training, and diagnosis	To build a human digital twin based on behavioral and neurological data and neuroscientific findings and to promote research and development for applications in education, training, and diagnostic treatment
Reinforce the governance to promote the introduction of AI in government agencies and enhance and improve administrative functions	Support of consideration of AI use by AI advisors and contribution to activities of SDF	To hire external AI advisors to promote AI use at each agency, to get advice on AI use policy, governance for operation and verification, and operational plan, and to examine AI-related governance issues, aspects of human resource management, use of data
	Conduct a basic AI training course to promote the use of AI in activities of SDF	To offer basic training on IT literacy, AI, and data science, as well as practical training on AI image processing to the staff of each organization to promote AI use
Pursue of fusion of Japan's advantages and AI to deal with challenges unique to Japan	Promote research on the application of AI technology that contributes to Japan's defense	To conduct research on the use of AI technologies in command and control, detection and identification, automation, and logistical support to advance SDF capabilities and equipment

Source: MoD (2023a)

6 Training for Defense AI

We were unable to find any direct documentation of how the Ministry of Defense and the SDF are training for the advent of defense AI. However, the SDF does recruit publicly for senior positions and mentions AI in current job openings as the examples illustrated in Table 4 and published in August 2023 highlight.

A public notice issued by the Ministry of Defense in December 2022 indicated a competitive bid to implement basic training for AI related to human resources development (MoD 2022a). This initiative exemplifies the Ministry of Defense's effort to recruit instructors from the private sector to help train the Ministry of Defense and the SDF. In addition, the Department of Information Engineering at the National Defense Academy, which trains many of the Self-Defense Forces officers, offers AI as an elective compulsory subject (National Defense Academy 2024).

At a more general level, Air SDF LTC Kenshi Kamitakahara, who belongs to the Operational Theory Laboratory of the Aviation Research Center, a research institute

Table 4 Job openings related to AI at Japan's Self-Defense Forces

Force	Department	Section	Summary
Maritime Self-Defense Force	Aircraft	Aeronautical equipment (underwater acoustic/non-acoustic systems)/AI	Research and development of underwater acoustic systems/non-acoustic systems. AI, technical guidance, and supervision of companies, etc.
	Technical Information Analysis	Artificial Intelligence	Research and development related to AI, technical guidance, and supervision of companies, etc.
Air Self-Defense Force	Weather	R&D	Research and development of AI technology, weather forecasting technology using numerical simulation, etc., and supervision and guidance related to weather forecasting and weather policies, etc.

Source: MoD (2023e)

within the Air SDF, recently touched upon another aspect related to training: the lack of data. In view of using machine learning related to defense equipment he underlined the need to "collect as much data as possible and extract high quality data from it" (Kamitakahara 2021a). In another paper, he focused on AI and defense simulations and argued that "AI for defense simulations is considered to be the most technically challenging area, as decisions to be made based on the simulation results are extremely critical" (Kamitakahara 2021b).

7 Conclusion

Although Japan is often recognized as one of the most technologically advanced countries, there is still strong hesitance to the use of technology for defense purposes. Universities and other research institutions are not necessarily active in R&D for defense uses.

On the other hand, interest in AI is growing, as in other countries. However, this interest is skewed toward educational and industrial applications. The defense industry is working on AI across the board, but Japan's defense industry has a large proportion of civilian demand, and there are aspects of the industry that are not necessarily for defense use. If necessary, they will be applied to defense applications, but they are not actively promoted as AI for defense.

The Ministry of Defense is gradually beginning to show interest in AI, as highlighted by a growing number of public documents referring to AI published since December 2022. Although still small, dedicated defense spending on AI is ticking up.

In general, Japan is a latecomer on the growing international defense AI scene—with no major achievements yet to see. However, the security environment surrounding Japan is worsening, and China's military spending is increasing

remarkably. China has also pointed out that it will use and incorporate AI for military purposes. Thus, for Japan to respond to what is going on in its strategic neighborhood, next-generation technologies are indispensable to expand its defense capabilities. In this regard, AI and other technologies are of strategic importance.

In so doing, ATLA is Japan's core organization to develop defense AI. ATLA should promote defense AI initiatives that reflect the strategic thinking of the Prime Minister's Office and the Ministry of Defense. In response, the academic community, including national and private universities, and the private sector should deepen their cooperation. Japan's unique post-World War II political environment should not be ignored. As the path toward war should be avoided, stepping up research and development efforts to the benefit of new technologies is indispensable to deter current and future threats.

References

AI Strategic Council. 2023. Provisional argument of issues concerning AI. AI Strategic Council. https://www8.cao.go.jp/cstp/ai/ai_senryaku/2kai/ronten.pdf. Accessed 30 January 2024

ATLA. 2015. Security technology research promotion program overview of applications. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/funding/kadai/h27oubojyoukyou.pdf. Accessed 30 January 2024

———. 2016. Security technology research promotion program overview of applications. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/funding/kadai/h28oubojyoukyou.pdf. Accessed 30 January 2024

———. 2017. 2017 Security technology research promotion program overview of applications. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/funding/kadai/h29oubojyoukyou.pdf. Accessed 30 January 2024

———. 2018. Fiscal year 2018 newly adopted research projects. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/funding/kadai/h30kadai.pdf. Accessed 30 January 2024

———. 2019a. ATLA technology symposium 2019. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/research/ats2019/img/ats2019_summary.pdf. Accessed 30 January 2024

———. 2019b. FY2019 Security technology promotion system (Secondary recruitment) application/adoption overview. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/funding/kadai/r01kadai_2.pdf. Accessed 14 January 2024

———. 2020a. Information related to a bid result. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/data/info/ny_honbu/pdf/kouhyou/r02/kouhyou02-073.pdf. Accessed 30 January 2024

———. 2020b. Information related to a bid result. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/data/info/ny_honbu/pdf/kouhyou/r02/kouhyou02-074.pdf. Accessed 30 January 2024

———. 2021. Information related to a bid result. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/data/info/ny_honbu/pdf/kouhyou/r03/kouhyou03-060.pdf. Accessed 30 January 2024

———. 2023a. About research themes related to public offerings in 2023. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/funding/koubo/r05/r05koubo_bessi1.pdf. Accessed 30 January 2024

———. 2023b. Security technology research promotion system. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/funding/kadai.html. Accessed 30 January 2024
———. 2023c. Short-term demonstration project for new technology. Acquisition, Technology and Logistics Agency. https://www.mod.go.jp/atla/rapid.html. Accessed 30 January 2024
Cabinet Office. 2018. Strategic council for AI technology. Cabinet Office. https://www8.cao.go.jp/cstp/tyousakai/jinkochino/index.html. Accessed 30 January 2024
Cabinet Secretariat. 2023. The first meeting of the council of ministers concerned with research and development and public infrastructure development that contribute to strengthening the comprehensive defence systems. Cabinet Secretariat. https://www.cas.go.jp/jp/seisaku/koukyou_infra/dai1/gijisidai.html. Accessed 30 January 2024
Chuter, Andrew. 2022. Move over, tempest: Japan pact takes UK-Italy fighter plan 'Global'. Defense News. https://www.defensenews.com/global/europe/2022/12/09/move-over-tempest-japan-pact-takes-uk-italy-fighter-plan-global/. Accessed 30 January 2024
Council of Ministers. 2023. Regarding initiatives that contribute to strengthening the comprehensive defense system (Research and Development). Council of Ministers Concerned with Research and Development and Public Infrastructure Development that Contribute to Strengthening the Comprehensive Defense Systems. https://www.cas.go.jp/jp/seisaku/koukyou_infra/dai1/siryou1-1.pdf. Accessed 30 January 2024
Evenstad, Lis. 2023. UK renews tech and science deal with Japan. Computer Weekly. https://www.computerweekly.com/news/366537634/UK-renews-tech-and-science-deal-with-Japan. Accessed 30 January 2024
IISPC. 2019. AI strategy 2019: AI for people, industry, region, and government. Integrated Innovation Strategy Promotion Council. https://www8.cao.go.jp/cstp/ai/aistratagy2019.pdf. Accessed 30 January 2024
———. 2022a. AI strategy 2022. Integrated Innovation Strategy Promotion Council. https://www8.cao.go.jp/cstp/ai/senryaku/10kai/sanko2.pdf. Accessed 30 January 2024
———. 2022b. List of AI strategy 2022 initiatives. Integrated Innovation Strategy Promotion Council. https://www8.cao.go.jp/cstp/ai/senryaku/9kai/siryo2-2.pdf. Accessed 30 January 2024
———. 2022c. Progress of AI strategy 2022. Integrated Innovation Strategy Promotion Council. https://www8.cao.go.jp/cstp/ai/senryaku/11kai/siryo1.pdf. Accessed 30 January 2024
Ito, Hiroshi. 2023. New battle fields brought about by the latest weapons and their impact on international politics (最新兵器がもたらす新たな戦闘領域と国際政治に与える影響). In *Global shift and the new realm, of warfare*, ed. Horoyuki Fujimaki, 48–77. Tokyo: Tokai Kyoiku Kenkyujo.
Kadidal, Akhil and Nishant Kumar. 2023. Japan to develop AI with US for "Loyal Wingman" UAVs. Janes. https://www.janes.com/defence-news/news-detail/japan-to-develop-ai-with-us-for-loyal-wingman-uavs. Accessed 30 January 2024
Kamitakahara, Kenshi. 2021a. Challenges in applying artificial intelligence to defense equipment: especially machine learning (人工知能の防衛装備品への適用における課題—特に機械学習について—). *Air and Space Power Studies* 8: 3–14.
———. 2021b. Challenges in applying artificial intelligence to defense simulations: limitations of applying machine learning to strategic simulations (防衛用シミュレーションへの人工知能の適用に関する課題—戦略シミュレーションへの機械学習適用の限界—). *Air and Space Power Studies* 9: 3–14.
Kidawara, Yutaka. 2019. AI science research and development promotion center. National Institute of Information and Communications Technology https://www.nict.go.jp/en/data/report/NICTREPORT2019_ebook/book/pdf/28.pdf. Accessed 30 January 2024
Kitado, Akira. 2023. Cutting-edge tech key to Deter Taiwan conflict: UK Military Officer. Nikkei Asia. https://asia.nikkei.com/Politics/Defense/Cutting-edge-tech-key-to-deter-Taiwan-conflict-U.K.-military-officer#. Accessed 30 January 2024
Majumdar, Oishee. 2023. Smart forces. Japanese and South Korean AI advancements. *Janes Defence Weekly* 28: 20–25.

MoD. 2013. National defense program guidelines for FY 2014 and beyond. Ministry of Defense of Japan. https://japan.kantei.go.jp/96_abe/documents/2013/__icsFiles/afieldfile/2014/02/03/NDPG.pdf. Accessed 30 January 2024

———. 2018. National Defense Program Guidelines for FY 2019 and beyond. Ministry of Defense of Japan. https://www.cas.go.jp/jp/siryou/pdf/h31boueikeikaku.pdf. Accessed 30 January 2024

———. 2022a. Implementation of basic training for AI (Artificial Intelligence) Human Resource Development. Ministry of Defense of Japan. https://www.mod.go.jp/j/budget/chotatsu/naikyoku/nyuusatu/2022/1208b.pdf. Accessed 30 January 2024

———. 2022b. National security strategy; National defense strategy; and defense buildup program. Ministry of Defense of Japan. https://www.mod.go.jp/j/policy/agenda/guideline/index.html. Accessed 30 January 2024

———. 2023a. AI initiatives in the ministry of defense. Ministry of Defense of Japan. https://www8.cao.go.jp/cstp/ai/senryaku/9kai/siryo7.pdf. Accessed 30 January 2024

———. 2023b. Defense programs and budget of Japan (1). Ministry of Defense of Japan. https://www.mod.go.jp/j/budget/yosan_gaiyo/2023/yosan_20230328.pdf. Accessed 30 January 2024

———. 2023c. Defense programs and budget of Japan (2). Ministry of Defense of Japan. https://www.mod.go.jp/j/budget/yosan_gaiyo/2023/yosan_20230329.pdf. Accessed 30 January 2024

———. 2023d. Defense white paper 2023. Ministry of Defense of Japan. https://www.mod.go.jp/j/press/wp/wp2023/pdf/R05zenpen.pdf. Accessed 30 January 2024

———. 2023e. Recruitment requirements for maritime self-defense force officers and air self-defense force officers. Ministry of Defense of Japan. https://www.mod.go.jp/gsdf/jieikanbosyu/pdf/y/r5_koubokanbu.pdf. Accessed 30 January 2024

National Defense Academy. 2024. Department of Computer Science. https://www.mod.go.jp/nda/education/files/files/1675043604phppFKGUu/03-14.pdf. Accessed 30 January 2024

Nihon Keizai Shimbun. 2014. Robotic weapons, mixed speculations, international regulatory conference starts from 13th (ロボット兵器、思惑交錯 13日から国際規制会議). https://www.nikkei.com/article/DGXNASGM08032_S4A510C1EAF000/. Accessed 30 January 2024

———. 2019. Expanding AI deployment for cyber defense in equipment repair (サイバー防衛にAI導入拡大　装備品補修で). https://www.nikkei.com/article/DGXMZO46170500W9A610C1PE8000/. Accessed 30 January 2024

———. 2023. FY24 AI budget, focus on development infrastructure: 200 billion yen, doubled (24年度AI予算、開発インフラに重点 倍の2000億円視野). https://www.nikkei.com/article/DGXZQOUA0206D0S3A800C2000000/. Accessed 30 January 2024

NSC of Japan. 2022a. National defense strategy. National Security Council of Japan. https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf. Accessed 30 January 2024

———. 2022b. Defense buildup program. National Security Council of Japan.. https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf. Accessed 30 January 2024

Prime Minister's Office. 2023. The Hiroshima Accord. https://www.gov.uk/government/publications/the-hiroshima-accord/the-hiroshima-accord#interoperable-resilient-and-cross-domain-defence-and-security-cooperation. Accessed 30 January 2024

Sakamoto, Tamotsu. 1983. On navigation using artificial intelligence search methods (人工知能の探索手法を用いた航法について). *Journal of the Japan Society for Aeronautical and Space Sciences* 354: 384–393.

SCAIT. 2017. Artificial intelligence technology strategy. strategic council for AI technology. https://www.ai-japan.go.jp/menu/learn/ai-strategy-1/Artificial%20Intelligence%20Technology%20Strategy%28March%2C2017%29.pdf. Accessed 30 January 2024

———. 2018. Strategic action plan for artificial intelligence technology. Strategic Council for AI Technology. https://www8.cao.go.jp/cstp/tyousakai/jinkochino/keikaku.pdf. Accessed 30 January 2024

Soga, Akira, and Hideo Nakashima. 1990. Application of artificial intelligence to aircraft navigation devices and problems (航空機用航法機器への人工知能の応用と問題点). *Journal of the Japan Society for Aeronautical and Space Sciences* 433: 60–65.

Tajima, Hiroshi. 2023. Japan, US to promote cooperation on dual-use technologies. The Japan News. https://japannews.yomiuri.co.jp/politics/defense-security/20230111-83142/. Accessed 30 January 2024

Vincent, Brandi. 2023. Pentagon's digital and AI chief works to deepen US Tech ties in visits to Singapore, South Korea and Japan. DefenseScoop. https://defensescoop.com/2023/08/31/pentagons-digital-and-ai-chief-works-to-deepen-u-s-tech-ties-in-visits-to-singapore-south-korea-and-japan/. Accessed 30 January 2024

Will the One Ring Hold? Defense AI in South Korea

Youngwook Park

In South Korea, artificial intelligence (AI) stands as a pivotal instrument and a guiding philosophy within the national vision and strategy aimed at spurring economic revitalization and enhancing competitiveness. The nation's historical inclination towards robust state-led initiatives in science, technology, and industrial policies, coupled with a socio-cultural landscape underpinned by a sophisticated information infrastructure, has cultivated widespread public endorsement of AI and digitalization. This societal embrace significantly bolsters the pursuit of national AI policies.

Since the launch of the first national AI strategy in 2019, the government strives to transform the country into an "AI powerhouse," characterized by AI-driven digital services of the state and powerful digital companies. This strategic orientation considers AI as the "One Ring," from The Lord of the Rings saga, and symbolizes the government's endeavor to construct a state-led technological utopia. South Korean Ministry of National Defense (MND) and its armed forces follow through on this vision. Therefore, defense AI plays a pivotal role to prepare the armed forces for the future. Cultivating technologically advanced armed forces that integrate AI is among the government's key priorities for defense modernization. This drive by the government is strengthened by the public's general acceptance of defense AI without any doubts regarding its morality or ethics.

The Ministry's defense AI approach emphasizes a gradual approach that starts with recognition intelligence, followed by judgment intelligence to culminate with decision intelligence. In addition, the MND also aims at establishing a new National Defense AI Center in 2024 in parallel to strengthening ministry-wide governance to coordinate all relevant stakeholders and research and development (R&D)

Y. Park (✉)
The Korea Institute of Defence Technology, Seoul, South Korea

Myngii University, Youngin-Si, South Korea

Woosuk University, Wanju-gun, South Korea
e-mail: parkwy@kidet.or.kr

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_23

initiatives. Integral to this strategy is the fostering of a collaborative defense AI ecosystem meant to provide novel impulses to reinvigorate a sclerotic traditional defense industrial system that suffers from a bifurcated procurement apparatus, a traditional preference for hardware over software, and limited indigenous defense AI capacities. There is, however, growing consensus among the country's civil and military leadership, that this system needs to be broken up to seize the benefits of defense AI, leverage informatization and digitalization for the armed forces, and bring in top-tier civilian talents working on information and communications technology (ICT).

South Korea's government backs up its ambition with robust spending on AI development. The country's defense R&D budget stood at around KRW5.15tn (USD3.9bn) in 2023, with 56% devoted to technology development. From 2017 to 2021, the MND spent around KRW190bn (USD145M) on AI-related technology development. This amount is set to increase significantly with the MND expected to spend around KRW100bn (USD77M) alone in 2023. Given the fact that other ministries also co-fund defense AI development projects, the total amount is around KRW30bn (USD23M) per year higher than what the defense budget indicates.

Right now, the MND looks at gradually integrating defense AI into surveillance and reconnaissance systems, combat systems as well as command and control (C2) systems. These lines of effort are meant to lead to the development of complex-manned-unmanned combat system (MUM-CS) and creating a Joint All-Domain Command and Control System akin to current US initiatives. In addition, South Korea is exploring the use of defense AI for different tasks like facility perimeter security, coastal surveillance, the use of unmanned systems, as well as multi-source image fusion.

In parallel to technology development and insertion, south Korea is placing significant emphasis on education aimed at nurturing talent in defense AI and enhancing the digital proficiency of defense personnel. The MND is engaging in collaborative efforts with academic institutions to cultivate AI specialists and has initiated a range of AI and software education programs, tailored to various participant groups. To provide a sustainable framework to advance defense AI, the MND also cooperates with the Ministry of Science and ICT, which is keen in educating an AI literate South Korean military. Moreover, the military services have designated several military pilot units to advance human expertise in using defense AI.

1 Thinking About Defense AI

The foreign policy of President Yoon Seok-yeol, who came into office in 2022, deviates from his predecessor by underscoring the significance of a robust U.S.-Republic of Korea (ROK) alliance, positioning it as a cornerstone of the nation's foreign and security policy. Additionally, the Yoon administration has pivoted towards policies that emphasize nuclear energy and industrial rejuvenation, marking a departure

from the preceding government's focus on green energy initiatives, such as solar and wind power, and its commitment to de-nuclearization.

Despite these notable shifts on foreign policy, President Yoon continues pursuing two policy priorities established by previous governments. First, the Yoon administration continues to prioritize information and communication technology (ICT), including AI, as a central pillar of the nation's strategic vision. In addition, the overarching strategy of augmenting defense capabilities through AI-driven scientific and technological advancements largely aligns with the previous government's approach, despite minor differences in emphasis and specific implementation plans. This continuity in AI-oriented policies reflects a broader historical trend, where successive south Korean governments have consistently emphasized state-led science and technology (S&T) and industrial policies as integral components of their national vision.

While attributing South Korea's rapid economic growth solely to state-driven policies may be an oversimplification, it is evident that an active role of the government is considered important for the country's prosperity. This also explains why the country's government, unlike other nations discussed in this volume, puts more emphasis on actively engaging different ministries in advancing AI to implement the national vision of economic revitalization, national competitiveness, and technologically well-equipped armed forces.

1.1 South Korea's National AI Strategy and Policy

In the early 2000s, the South Korean government embarked on a strategic initiative to harness the potential of IT and digital technologies as catalysts for the nation's economic and industrial resurgence. This period marked a concerted effort by the state to capitalize on the rapid advancements in the digital domain. The conducive socio-cultural landscape, characterized by a relatively advanced information infrastructure, and a public attitude favoring the adoption of sophisticated ICT, including AI, facilitated the effective implementation of these state-led policies.

Shortly after assuming office, the Moon Jae-in administration, in November 2017, established the 4th Industrial Revolution Committee (4IRC), a body designed to report directly to the President. This committee, integrating ministers from the Ministry of Science and ICT (MSIT) and the Ministry of Trade, Industry and Energy, along with private sector experts, was envisioned as a symbolic yet pivotal strategic entity for steering the nation's S&T policy. The Moon administration identified the data-network-AI nexus as one of the three primary innovative industries and launched the country's first national AI strategy in 2019. Led by the MSIT, this strategy marked the government's inaugural top-level AI policy guideline and action plan (MSIT 2019).

Under the guiding vision of "Transitioning from an IT to an AI Powerhouse," the administration set ambitious targets. These included generating up to KRW455tn (USD346bn) in economic impact through AI by 2030 and elevating South Korea to rank among the top ten nations globally in terms of quality of life. This strategy also

encapsulated the government's understanding of AI as technology that replicates human intellectual capabilities in computers, encompassing the ability to recognize situations, make rational and logical judgments and actions, and execute emotional and creative functions. Furthermore, in a significant move towards implementing human-centered AI, the government unveiled ethical standards for AI.

The new Yoon government replaced the 4IRC with the new Digital Platform Government Committee to "synergize governmental data with the services of the private sector, thereby leveraging state-of-the art technologies in AI, cloud computing, information processing, and networking" (Office of the President ROK 2023). The Digital Platform Government serves as a "control tower," envisioned to foster collaboration among citizens, businesses, and the government to address societal challenges and create new value with the help of a unified digital platform. In April 2023, the government unveiled the Implementation Plan for the Digital Platform Government. This initiative, galvanized by the emergence of hyper-scale AI technologies such as ChatGPT, aims to digitize the national administrative system and foster industrial and economic growth by actively leveraging and applying AI technology, thereby making its benefits tangible for the population.

1.2 Defense AI Understanding and Strategy

In line with the government's One Ring imaginary, the defense establishment considers AI an indispensable asset in fortifying military capabilities and readiness for future conflicts. This positions AI as a central pillar in strategic planning and operational preparedness, underscoring its significance in shaping a resilient and responsive military force.

Defense AI plays a key role amid a complex threat picture consisting of the military challenges posed by North Korea, raising tensions between the United States and China, pressing geoeconomic concerns related to technological dependence and insecurity of supply as well as maritime instability that threatens the stability of the sea lanes of communication across Asia-Pacific that are vital for South Korea. Therefore, the MND is actively advocating for the integration of AI across all defense domains as a pivotal component of its national defense strategy. This strategic direction emphasizes a robust investment in AI-related technologies, identifying them as potential game changers in shaping the future battlegrounds. The Ministry is committed to building intelligent defense solutions to enable highly efficient military operations.

While these AI motives align with those of the United States and other leading global powers, South Korea's situation is distinct as the country's conscript forces grapple with a declining birth rate amid complex security dynamics. Thus, the country's military emphasizes the role of AI in advancing the technology savviness of its armed forces while at the same time compensating for shrinking personnel. As this dual approach is broadly accepted by South Korea's society, the country benefits from broad political and societal support in advancing defense AI.

In the most recent iteration of the National Defense Science and Technology Basic Plan (2023–2027), the MND has delineated its strategic framework for defense R&D investment. This comprehensive plan identifies thirty critical defense strategic technologies across ten key fields, including AI, human-computer interaction, cyber and network communications, quantum technologies, and space. These technologies have been prioritized based on criteria like strategic significance, potential for innovation, urgency, and the possibility of acquiring these technologies (Presidential Advisory Council on Science and Technology 2023: 31). The plan divides the main AI technologies into four areas:

- Intelligent battlefield situational awareness and understanding refers to AI technology based on models and analyses that fuses, learns, generates information, and makes interferences based on data and information collected from diverse battlefield assets.
- Intelligent unified command and control refers to technology that enables decision-driven warfare by suggesting optimal measures based on battlefield situation analysis and judgment results with AI for effective command decisions in tomorrow's complex battlefield environment.
- Logistical support for smart military power includes technology that is used to support scientific and efficient combat sustainment by intelligently processing vast amounts of data generated from various logistic support activities such as advanced weapon system operation, supplies, ammunition, transportation support, personnel, administration, and medical care through AI.
- Finally, there are technologies related to developing and preparing future defense AI solutions (e.g., data management, high-performance computing). These support technologies have been identified as a critical area of government investment.

The MND perceives defense AI as a dynamic and evolving concept and thus proposes to develop the respective capability in three stages (MND 2022b: 6). Cognitive intelligence constitutes the first stage with AI for surveillance, reconnaissance, and early warning systems. While these systems are considered "initially autonomous," AI solutions at the second stage advance to "partially autonomous" capabilities. At the third and final stage AI solutions transition to "judgmental intelligence," which entails the use of AI for complex manned-unmanned combat systems. Most mature technologies would pave the ground for "fully autonomous" systems that encapsulate perception, judgement, and decision intelligence. Right now, however, South Korea's defense AI capabilities and capacities are nascent and mainly focus on the first stage. While it is challenging to predict the time needed to reach and operationalize the final stage effectively, R&D investments are concurrently being channeled towards the development of both the second-stage judgmental intelligence systems and the third-stage decisional intelligence systems.

In advancing this ambitious three-stage agenda, the South Korean MND faces a particular challenge that stems from the country's regulatory framework for data and information security, that is excessively rigid for historical reasons. Consensus is growing that overzealous secrecy practices and regulatory measures by the military and government agencies are currently impeding the efficient management,

sharing, and use of military data. This, in turn, could potentially constrain the defense application and expansion of AI, which relies on data. The lack of a well-structured and integrated military data management system has been consistently highlighted, particularly in terms of data visibility and accessibility, which are critical for effective data utilization.

The MND has initiated projects to address current problems, yet challenges persist as responsibility for data management and data sharing remain scattered across the ministry. The absence of a responsible organization for this task and the underfunding of the respective projects have raised concerns and skepticism regarding the feasibility of establishing a robust data and AI infrastructure. A key step toward ameliorating the situation was taken in 2022 with the setup of the new Defense Data Management Committee aimed at forging consensus on the need for defining a future defense data policy and advancing data-driven defense innovation. To this purpose efforts are underway to establish a data collection, sharing, and management system, as well as data quality management, by appointing data officers for each agency (MND Blog Defense News 2023).

2 Developing Defense AI

2.1 Evolution of South Korea's Defense AI Strategy

Since 2019, the South Korean government has embarked on the formulation of a comprehensive national AI strategy, specifically focusing on its application in the defense sector. The strategy sets out the following goals (Joint Ministry 2019: 34–35):

- Enable efficient and reliable national security and defense by intelligentizing and advancing core defense mission and tasks based on AI and data.
- Build an intelligent platform to develop and support AI services common to the entire military services; rapidly analyze and process large-scale defense data; develop and support common services such as medical, military, and administrative enterprise.
- Establish an intelligent data center for the standardization, accumulation, and sharing of defense data and accelerate the development of intelligent technologies that support the command and control (C2) system with respect to collaboration and determination.

South Korea's defense AI strategy development process emerged bottom-up with the ROK Army as the main driver. In 2019, the ROK Army stood up the AI Research and Development Center within the Training and Doctrine Command to plan for the use of AI across C4I, intelligence, firepower, maneuver, protection, and operational sustainment (Gook 2019: 22). One year later the Army unveiled the 2022–2033 Army AI Development Promotion Strategy and established an AI governance system. In parallel, the ROK Army also introduced the Army TIGER 4.0 vision to

transform ground forces by using AI and digital technologies as well as pushing for experiments with a focus on manned-unmanned cooperation to create hyper-intelligent, hyper-connected, and hyper-converged ground forces (MND Blog M-Friends 2020; MND 2021c). Bold ambitions, however, were difficult to implement, among other things, because of frequent changes at the Army Chief of Staff that somewhat dampened the momentum. But despite these challenges, the Army has historically been at the forefront in leading major defense and military policies given the size of its personnel and the service's resource power.

In 2021, based on preliminary studies by the Korea Institute of Defense Technology (KIDET) (Park et al. 2020), the ROK Army's initial impulse was backed up by the first formalized AI strategy and plan of the MND. In anticipation of troop reductions and to revolutionize the future battlefield, the MND formulated a strategy for the systematic application of AI across the defense sector. This strategy embraces innovation, the sharing and collective use of data, and collaboration via a public-private ecosystem as its three core values and lists several implementation tasks (MND 2021a). With this strategy, the MND put a key emphasis on developing and operating a data platform to collect and share usable data, thereby overcoming barriers stemming from disjunct data management systems and regulations. To this purpose, the strategy foresaw a comprehensive revision of existing regulations to focus on the use of data, dismantling inter-agency silos, fostering a culture of data sharing, progressively establishing platforms including data portals, and enhancing the Defense Data Commission to establish defense data governance.

Since its inception in 2022, the current government has championed the goal of fostering robust armed forces with the help of Defense Innovation 4.0 and AI (MND 2022b: 6–7). To further expand the use of defense AI, the MND has presented a phased approach, which encompasses the step-by-step intelligentization of surveillance and reconnaissance systems, combat systems, and C2 systems, taking into consideration current levels of AI maturity. In this regard, the MND has formulated a comprehensive defense AI governance roadmap, which includes appointing a Chief Defense AI Officer to oversee and coordinate AI tasks across all services, the Defense Acquisition Program Administration (DAPA), and the respective defense research organizations. Furthermore, the MND wants to establish a National Defense AI Center by 2024 to facilitate a robust top-down defense AI development approach. At the same time, the MND also puts significant emphasis on fostering an open and collaborative public-private defense AI ecosystem to help address the defense ecosystem's most pressing shortfalls that will be discussed below.

In view of advancing South Korea's AI-enabled military forces, MUM-CS play a pivotal role. To build these systems, the three-stage process discussed above provides the general framework. In the first phase, the MND's roadmap proposes implementing a system centered on remote control, followed by demonstrating an autonomous system in the second phase, and expanding the deployment of systems with semi-autonomous capability, eventually transitioning to fully autonomous systems in the third phase. Moreover, the second phase aims at implementing perceptual intelligence capabilities involving the promotion of an unmanned surveillance system through pilot projects, creating an AI-enabled intelligent surveillance

perimeter system using drones and robots. In the final phase, the goal is to execute the Joint All-Domain Command and Control System (JADC2), based on mature judgmental intelligence. This includes establishing an AI-based C2 system that can optimally implement joint all-domain operations on the future battlefield, integral to the third phase of Defense Innovation 4.0. This approach shall be implemented via a step-by-step plan to operate pilot units for each military service, identify the needs of future target systems, and spread AI systems to all units through evaluation, supplementation, and verification.

In sum it can be said that the current government has significantly advanced its commitment to defense AI by translating abstract propositions into specific implementation goals and frameworks. The ambition is bold and more concrete than in the past. However, developing and deploying the envisioned MUM-CS will remain challenging given current levels of maturity of defense AI available in South Korea and the need to further refine adjacent technologies for unmanned operations, autonomy, robust communication network infrastructures, and more general advancements in comprehensive battlefield digitization.

2.2 South Korea's Defense AI Ethics Policy

In February 2023, the Ministry of Foreign Affairs of Korea (MFA), in collaboration with the Ministry of Foreign Affairs of the Netherlands, hosted the inaugural Responsible AI in the Military Domain Summit (REAIM) 2023 in The Hague. The Summit's final Call to Action (REAIM 2023) emphasized the need for responsible AI in the defense context but also raised concerns that undue emphasis on additional regulations might hinder technological progress and pose risks to advancing AI-enabled defense capabilities. This summit, initially proposed by the Netherlands during the 2022 South Korea-Netherlands Summit, marked the first international conference dedicated to the responsible use of AI in military operations and provided a platform for Park Jin, Korea's Minister of Foreign Affairs, to underline the country's ambition in shaping the international defense AI ethics agenda.

Despite South Korea's international engagement in defense AI ethics, the current government's domestic digital platform policy appears insufficient to address the ethical and regulatory challenges posed by AI. The implementation strategy largely focuses on regulatory technologies and services centered on privacy and personal data protection, seemingly neglecting the fundamental ethical questions raised by hyper-scale AI. This approach indicates a potential dilution of ethical considerations compared to the previous government's AI policy. Furthermore, South Korea's "Bill on Fostering the AI Industry and Creating a Foundation for Trust," which is poised for enactment (ROK National Assembly n.d.), adopts a permissive and post-regulatory approach rather than setting clear standards and robust oversight. This has failed to alleviate concerns among some progressive intellectuals and civil society organizations.

Inter-ministerial collaboration also presents challenges. While the MFA plays a central role in AI ethics, the lack of cohesive cooperation with the MSIT, responsible for AI technology and service promotion, and the MND, the principal defense AI entity, is apparent. Additionally, there seems to be a disconnect between academic and expert groups concerning the promotion, regulation, and ethics of AI, indicating weaknesses in South Korea's national governance concerning the accountability and regulation of defense AI.

3 Organizing Defense AI

3.1 ROK MND, Military Services, and Adjacent Agencies

3.1.1 ROK MND

Based on the MND's AI strategy, the ministry plays a key role in developing the implementation plans needed to synchronize the defense AI activities of the military services and other MND agencies. Within the Office of the Minister and its affiliated organizations, the Intelligent Information Policy Bureau, the Military Force Policy Bureau, and the recently established Advanced Forces Planning Bureau are engaged in defense AI activities, but a central organization responsible for defense AI is missing.

The MND's leadership acknowledges the shortfalls of the current governance structure, but the flexibility needed for reorganization is constrained by relevant laws. Nonetheless, the MND is preparing to establish a new National Defense AI Center (NDAIC) in 2024. Based on the suggestions of KIDET, a private think tank, the center would be modeled after the US Department of Defense's Chief Digital and Artificial Intelligence Office (CDAO) and the UK Defense AI Center (DAIC) (Park et al. 2023). Expected to streamline existing organizations and improving better coordination among different defense stakeholders, critical voices have put forward fundamental questions regarding the identity and organizational structure of the NDAIC and its roles and responsibilities.

3.1.2 ROK Army

As outlined above, the ROK Army has been the frontrunner on defense AI and presented its comprehensive AI Integration Roadmap 2022–2033 in 2021 (ROK Army 2021). The roadmap established incremental objectives for the Army's intelligence evolution, aligned AI concepts with the Joint Staff's long-term armament system evolution trajectory, delineated requirements for intelligence systems, and outlined a comprehensive plan for AI platforms, AI human resources, and data (KRIT 2021: 13–15; MND 2021c).

The establishment of the AI Research and Development Center within the Training & Doctrine Command in 2019 marked a pivotal moment for the Army. This center, which has been folded into the AI and Drone-bot Combat Development Center, was instrumental in identifying future AI-enabled system requirements, forging collaborative relationships with private industry and research institute, and establishing the AI Policy Division under the Policy Division to develop medium and long-term defense AI policies. Although the impact of these endeavors has not yet been objectively evaluated, it is evident that the ROK Army's strategic commitment to using AI as a key means for force transformation remains steadfast and unimpeded. As of the first half of 2023, the Army boasts a robust cadre of 50 specialized AI personnel working at the Headquarters and Training & Doctrine Command (Interview, 10 March 2023).

3.1.3 ROK Air Force

In parallel with the MND, the ROK Air Force has formulated its Air Force AI Development Plan for 2021. Two years earlier, the Air Force Innovation Promotion Plan laid the groundwork by envisioning the Smart Air Force Power concept (News Aerospace 2019) to leverage emerging technologies. The service's defense AI plan is geared towards creating a mission environment that aligns with the Air Force's vision of future warfare by identifying and implementing defense AI across all Air Force activities, comprehensively embracing the management of mission data as a robust AI foundation and providing guidelines for effective human recourses development in support of defense AI (Ko 2023).

In line with the MND's AI strategy, the ROK Air Force is mainly interested in using defense AI in combination with space-based surveillance and reconnaissance systems, big data-driven intelligent command, and decision support systems as well as unmanned aerial vehicles (UAVs) (ROK Air Force 2021; Park 2022). Given the fact that many of the ROK Air Force's flying platforms are procured from overseas, predictive maintenance of aerial assets constitutes an additional priority, which is, at least for the moment, more pronounced than integrating AI into developing aerospace platforms. Furthermore, the Air Force has historically managed data in the logistics domain with a high degree of systematization, leading to a more systematic and rapid adoption of AI in this area compared to other branches of the military.

While the Air Force's plans for defense AI seem clear, its organizational setup remains complex due to overlapping responsibilities among various departments. Most importantly, the Planning and Management General Staff plays a crucial role in pinpointing and scaling up applications for AI across the entire spectrum of the Air Force and steering the course for AI-focused human resource development and structural improvements. Right now, a staff of around thirty, mainly working at the headquarters, is engaged on AI-related tasks with a focus on software policy for technological applications. Looking ahead, the ROK Air Force envisions establishing the Air Force AI Center by 2025 to consolidate and enhance the Air Force's defense AI capabilities.

3.1.4 ROK Navy and Marine Corps

The Navy Vision 2045, published in 2021, presents a demanding vision for the intelligentization of the naval forces and the Marine Corps, which is part of the Navy (ROK Navy 2021). In line with the sister services, the strategy emphasizes the goal of a SMART Navy that leverages emerging technologies. The vision identified five core AI capabilities alongside plans to establish a foundational infrastructure for defense AI, including expert training and data management (Ahn 2019). SMART Navy underlines the ambition to enhance naval weapon systems, inter alia, by integrating manned-unmanned combat capabilities, using emerging technologies to operate under a shrinking number of seamen, and advancing the operation of a cost-effective naval force. The Navy envisions defense AI to play a key role across these three goals (Park 2020: 7–8).

On the way to become a SMART Navy, the service established the Future Innovation Research Center in 2020, dedicated to exploring the development and application of new technologies, including AI. In 2023, the Navy expanded its focus by establishing a specialized AI division within the Navy Headquarters' Intelligent Information Technology Department. Concurrently, the Marine Corps formed the Intelligence and Information Technology Division at its headquarters, tasked with developing AI policy and managing related operations. Among the military services, the Navy currently maintains the smallest AI workforce. Additionally, it is poised to establish a dedicated data organization to centralize and manage naval data, integrating existing software technology and data-related entities such as the Information System Management Corps and the Ship and Aircraft Software Support Center.

3.1.5 ROK Joint Chief of Staff

As of today, the Joint Chief of Staff (JCS) lacks a department exclusively dedicated to AI, but two departments deal with AI-related tasks. The High-Tech Power Division outlines future warfare requirements based on advanced technologies and thus also identifies future defense AI needs. The Advanced Technology Force Test and Evaluation Division tests and evaluates technologies relevant for intelligentization and thus also looks at defense AI. As outlined above, defense AI strategy development has traditionally followed a bottom-up logic in South Korea. This contrasts with a top-down methodology promoted by the MND or the JCS. This existing dynamic continues to pose challenges to the establishment of comprehensive defense AI governance and a centralized control tower system.

3.1.6 Defense Acquisition Program Administration (DAPA)

Under the overarching supervision of the MND, DAPA operates as an independent government ministry, as delineated by the Defense Acquisition Program Act. DAPA bears responsibility for the acquisition of weapons systems, R&D programming and budgeting, acquisition project management, and defense industrial policy. Consequently, the successful execution of the defense AI strategy is contingent upon DAPA's proactive engagement and commitment to developing AI-applied intelligentization systems within the defense R&D and acquisition process.

In 2021, DAPA unveiled its own AI strategy, designed to innovatively enhance intelligence capabilities by integrating AI technology into weapon systems (DAPA 2021a). Efforts are underway to prioritize budget allocation for AI technology development and the R&D of intelligent systems. DAPA's AI strategy is aligned with the MND AI policy direction.

Given DAPA's independence, the military services are not directly involved in weapon system acquisition programs, which poses a specific challenge for the MND's intelligentization ambition. Should DAPA not act swiftly on allocating budgets and ensuring an adequate project management framework for each weapon system, the MND's ambitious intelligentization plans and its defense AI agenda will remain elusive. In addition, the current division of responsibilities foresees DAPA overseeing development and acquisition and the MND, together with Defense Logistics, managing acquisition policy including commercial products relevant for intelligentization. This bifurcated system hinders the full adoption of AI, that blurs the lines between traditional hardware-centric weapon systems and new software-based modifications and upgrades. Consensus is growing that this split needs to be addressed, yet specific measures and roadmaps to alleviate the situation remain to be adopted.

3.1.7 Agency for Defense Development (ADD)

The ADD, a government-funded research entity operating under the aegis of DAPA, has historically managed R&D projects pertaining to weapon system development and technology. Although the ADD has demonstrated leadership in conventional military technology fields, its competitiveness in AI and ICT, predominantly developed in the private sector, has been perceived as relatively limited.

Noteworthy improvements have been undertaken since 2021 with the foundation of the AI Autonomy Center. The center's primary mission is to research AI core technologies essential for the development of intelligent weapon systems. This includes conducting R&D on core technologies integral to intelligent weapon systems, such as AI common architecture, situation recognition, judgment intelligence, collaborative intelligence, surveillance and reconnaissance intelligence, and the development of multi-source image fusion systems. In 2023, the scope of the center was broadened to include autonomy technology.

3.1.8 Research Institutes

In 2023, the Korea Institute for Defense Analysis (KIDA), a government-funded research institute under the auspices of the MND, inaugurated the Defense Data Analysis Center to advance defense data analysis and support. In addition, the center conducts policy research on defense data, data construction management support, data quality management, and utilization support.

Outside the MND several government-funded research institutes contribute to defense AI. For instance, the Electronics & Telecommunications Research Institute (ETRI), an ICT technology research entity, is engaged in AI technology development and utilization projects. Similarly, the National Information Society Agency (NIA), primarily responsible for digital and intelligentization projects in the public sector, is involved in AI development projects and infrastructure construction in the defense domain.

Despite playing an important role in South Korea's civil-military AI ecosystem, many civil research institutes lack a comprehensive understanding of the defense sector and the armed forces long-term needs. In addition, top-tier academic research institutes and experts that provide world-leading ICT expertise are reluctant to engage on defense. In their view, the defense market is unattractive because it is limited in size and intellectual property rights cannot be used freely. Overcoming these problems will be essential for civil research institutes to assume a broader role in future defense AI projects and policies.

3.2 Defense Industry

South Korean defense R&D predominantly operates within an insular framework, principally involving the ADD and select defense institutions. The current system is considered excessively insular, inefficient, and unappealing due to its low profitability. Consequently, there is growing consensus that the ecosystem needs to be adapted for the country's armed forces to acquire innovative technologies for future capabilities. This prompts the need to open the existing ecosystem towards fostering synergies with non-traditional partners in the private sector.

In South Korea, dominant AI technology and industry players like Naver, Kakao, Samsung, LG, and SK show limited interest in defense projects. This, coupled with the fact that new companies and startups are still maturing, results in a relatively small pool of private AI industry groups available for participation in defense projects. Moreover, the military and ADD's requirements for defense domain expertise and system integration capabilities further narrow the field of eligible private new technology companies, constraining extensive collaboration between defense and private sectors.

Despite these challenges and although defense companies generally prefer to manage projects involving AI and autonomous technologies in-house, the engagement of private actors is on the rise. Currently, projects involving AI integration in

South Korean weapons system are typically undertaken as Core Technology Development or Dual-Use Technology Development projects, rather than focusing on System Integration Development Steps. To participate in these projects, AI ventures, startups, and private new technology companies are primarily contributing as lower-tier suppliers or contract research organizations to development projects initiated by the ADD or defense system companies. For example,

- DeepX has recently been selected as the prime to design and prototype AI semiconductors intended for use in future battlefield surveillance drones.
- SELVAS AI is developing an AI-based military medical system.
- Human ICT and Davio focus on computer vision for surveillance and reconnaissance.
- CTI Lab is an important player in the cybersecurity sector.
- WiseNut offers solutions for decision-making support along with SaltLux, 42Maru, and Konan Technology, which engage in developing large language models (LLM) (Interview, 28 November 2023).

Although numerous defense R&D stakeholders hope for a significant transformation of South Korea's closed defense industrial ecosystem in favor of closer public-private cooperation and easier access to defense projects by innovative companies, change will hardly materialize soon. Nevertheless, the government's firm policy intention as well as the growing interest of innovative companies to engage on defense are signs of hope for gradual change in the medium to long-term.

4 Funding Defense AI

4.1 Korea's National R&D Budget for AI

As highlighted above, state-led science, technology, and industry policies play a key role in South Korea. The MSIT is responsible for policy formulation in S&T and plays a pivotal role in shaping and implementing the nation's comprehensive R&D budget. Moreover, the government's industrial strategies, orchestrated by the Ministry of Trade, Industry, and Energy, exert considerable influence on the market and the industry landscape. Consequently, it is not surprising that government-funded research institutes play a pivotal role in the national S&T system. This encompasses over forty state-funded research institutes in S&T and engineering fields, including entities such as ADD, in addition to thirty institutes focused on humanities and social sciences. These institutes operate predominantly on national R&D funding and fall under the oversight and supervision of relevant government ministries, chiefly the MSIT, in alignment with their respective research domains.

In 2023, the South Korean government invested a total of KRW30.7tn (USD23.5bn) in state-run research institutes and various science and technology fields (MSIT 2023a: 3). As part of this budget, around KRW1.43tn (USD1bn) has

been earmarked for R&D on ICT, with around 50% directed at AI initiatives. Furthermore, investments in cybersecurity (KRW165.3bn or USD126M) and other digital technologies such as AI-centric semiconductors, quantum technology, metaverse, 5G, and 6G are on par with the funding allocated to AI (MSIT 2023b: 5; Industrial Daily 2022). Defense R&D accounted for 16.6% of the KRW5.1tn (USD3.9bn) in total government R&D, ranking third after the MSIT and the Ministry of Trade, Industry & Energy.

Recently, the efficiency and competitiveness of these government-funded research institutes has been criticized. Thus, the government, for the first time, decided to bring down the 2024 R&D budget by 14% to KRW21.5tn (USD16.5bn). While the ICT budget will be cut by 21% to KRW1.1tn (USD844M), the budget on R&D for AI will be increased by 4.5% to KRW37.1bn (USD565M).

4.2 South Korea's Defense Budget and Budget Trends in Defense AI

After several years of continued growth, South Korea's defense spending culminated at KRW57.1tn (USD43.4bn) in 2023 (MND 2023a: 3). The MND spends around 40% of the budget on personnel, 30% on force maintenance, and 30% on force modernization (MND 2023a: 4). Last year, defense R&D accounted for 9.1% of the budget or KRW5.1tn (USD3.9bn). 56% were spend to defense technology development and 21% or KRW1.4tn (USD1bn) has been earmarked for weapon systems development.

South Korea's defense R&D budget delineates priority investments across ten domains, encompassing thirty defense strategic technologies, which include AI, MUM-CS, and space. Like many other nations, the MND does not disclose an aggregate defense AI budget as spending on defense AI is part of many different program and budget lines. Scrutinizing the defense R&D budget yields the following results:

- The MND allotted KRW734.7bn (USD558M) to the defense informatization budget in 2023. This also includes unspecified spending on data handling and cloud AI infrastructure (MND 2023a: 9).
- From 2017 to 2021 the MND has spent round KRW190bn (USD145M) on AI-related technology development (MND 2021b: 3). This budget was set to increase with spending in 2023 alone reaching KRW100bn (USD77M) (MND 2023a: 9).
- As of 2022, around KRW61bn (USD47M) was invested in ten strategic defense technologies including AI as part of the defense technology development program. Of this amount, amount, around KRW30bn (USD23M) was directed towards AI technology projects (Presidential Advisory Council on Science and Technology 2023: 50–51).
- In parallel the MND is committed to increase investments in AI and unmanned systems technology. To this purpose, the ministry has formulated a plan to

> increase the current level of R&D funding on these technologies to KRW350bn (USD268M) per year until 2025 and to KRW1tn (USD767M) per year until 2030, albeit without specifying the budget share of defense AI (DAPA 2021b: 12).

Overall, these sums seem modest given the defense AI ambitions discussed above. But caution is at place as other ministries, primarily the MSIT, support the MND in co-funding defense AI. To this purpose, both ministries signed a memorandum of understanding in 2021 and have since engaged in funding cooperation projects. Since 2020, MSIT has allocated around KRW200-300bn (USD154–230M) per year towards the Munition and Military Supplies Acquisition Program, which focuses on non-weapon systems, namely force support systems. In addition, MSIT has contributed KRW17bn (USD13M) in 2023 for the AI-enhanced Intelligent Coastal Surveillance System and a cumulative total of KRW33bn (USD26M) to develop AI for X-ray image analysis to support doctors in remote precision diagnosis (MSIT & MND 2022: 3–6). Given financial contributions by MSIT and other ministries, it can be assumed that the annual budget on defense AI is around KRW30bn (USD23M) higher than the amounts extracted from the defense budget.

5 Fielding and Operating Defense AI

South Korea's armed forces are using AI for enterprise functions like human resources management, security clearance services or logistics. Technical complexities of using AI in weapon systems, likely consequences of the failure of AI on the battlefield and ethical concerns have so far limited the core military use of defense AI.

Among the military services, the ROK Army has been frontrunner in fielding defense AI applications, thereby using small-scale tests and experiments to use AI in combination with manned and unmanned systems. The Army's plans for manned-unmanned teaming strive for synergies with the strategies of the Navy and the Air Force to intelligentize their primary platforms. Against this background, the MND's strategies foresees an evolutionary path to building up defense AI capabilities in three stages (MND 2022b: 6; MSIT & MND: 3–5):

- *Stage 1: Recognition Intelligence*

At this stage the focus is on developing surveillance and reconnaissance systems. With the Critical Facility Perimeter System, for example, the MND wants to develop intelligent access system for key military installations such as munition depots and airfields until 2026. As indicated, the MND and the MSIT joined forces in 2020 to develop the Intelligence Coastal Surveillance System to autonomously identifying ships and targets by leveraging data from military coastal surveillance apparatus. The Multi-Source Image Fusion System will work on the real-time integration of data from satellites and reconnaissance aircraft in real-time. The 3-year project started in 2019. Lastly, the Medical Image Diagnostic Reading System, which automatically analyzes chest X-ray images of soldiers to assist doctors in diagnostic processes.

- *Stage 2: Judgment Intelligence*

At this stage the MND strives for partial autonomy with projects including intelligent tanks, ships, and fighters, as well as MUM-CS, drone swarms and robots, and intelligent military logistics systems. Projects falling under this second phase are either in the preliminary stages or just starting.

- *Stage 3: Determined Intelligence*

The final phase signifies the maturity of technologies and systems capable of achieving full autonomy. This stage envisions the full deployment of AI military medical personnel and counselors, AI combat staff, intelligent command and control systems, and autonomous combat systems. Accomplishing these tasks will be a long-time endeavor.

To overcome existing gaps, the military services have embarked upon strategic commitments to foster new capabilities by designating military pilot units to advance human expertise in tandem with novel AI-enhanced solutions (MND 2022a:112, b: 9):

- The Army will designate the Army TIGER Brigade, 70th Brigade Combat Team, 25th Division, as the pilot unit. This unit will undertake trials to assess the offensive capabilities and survivability of an integrated control system encompassing unmanned combat vehicles, attack helicopters, and drones.
- The Navy will utilize the Fifth Fleet as its pilot unit, conducting experiments to evaluate the efficacy of combined manned-unmanned demining operations, which will integrate small naval vessels and autonomous mine detection systems.
- In parallel, the Air Force has selected the 20th Fighter Wing as its pilot unit. This wing will be responsible for verifying the practicality of manned and unmanned squadron operations, integrating fighter jets with low-pitched unmanned aerial vehicles.
- Lastly, the Marine Corps will engage the 1st Marine Division as its pilot unit to validate amphibious operations capabilities, focusing on the integration of amphibious assault vehicles and obstacle-clearing robots.

While the ROK military's ultimate objective is to implement AI into complex weapon systems, the services often fail to clearly articulate their requirements. Consequently, financial resources tend to be predominantly directed towards the Technology Development Program, which focuses on technology maturation, rather than the System Integration Program aimed at developing intelligent systems. A case in point is the ongoing Command Decision Support System project, categorized as an AI core technology development initiative rather than a weapon system procurement endeavor.

Within the next 4–5 years, the MND and the armed forces want to explore how to identify the AI-relevant requirements to intelligentize existing and future systems. To this purpose, the development of intelligentization systems is expected to

take shape via a newly initiated rapid acquisition process, diverging from the traditional, protracted weapon system procurement protocols. Overall, however, it remains difficult to assess if the public-private cooperation is effectively advancing the military use of AI. Despite the MND's continuous declarations advocating for the integration of civilian AI technology within the defense sector and the establishment of a comprehensive ecosystem, many experts posit that substantial reforms in force system acquisition and defense-related R&D are indispensable prerequisites for fostering and developing a defense AI ecosystem that delivers the defense AI capabilities South Korea is looking for.

6 Training for Defense AI

South Korea is placing significant emphasis on nurturing defense-specific AI expertise and bolstering the digital proficiency of its defense workforce. To foster a robust pool of experts and establish a sustainable foundation for defense AI advancement, the MND has unveiled initiatives to partner with universities to train 1000 AI professionals who will spearhead AI integration in the military over the next 5 years and roll out AI and software education programs across various military training platforms for soldiers and officers, that shall be gradually expanded. But the general difficulties hampering the local defense sector described above and the current lack of the South Korean armed forces to properly understand and convey their AI requirements make it difficult for the MND to satisfy the growing demand for AI expertise.

6.1 Defense AI Talent Training Program of the MND

Given South Korea's priorities to establish a digital platform government with AI at its core, numerous government ministries and public institutions are engaged in general AI initiatives. The MND and the MSIT jointly drive Korea's defense AI education and training. Recognizing that most soldiers enter service during their college years and often perceive this period as a disconnect from academic and social pursuits, AI education for military personnel is envisioned not just as a means to enhance military capabilities through digitization and intelligence, but also as an essential bridge facilitating soldiers' transitioning back to academia or professional careers after discharge.

Therefore, both ministries formalized cooperation with a memorandum of understanding in 2021. According to the MND's strategy, the aim is to develop 50,000 military AI and software personnel by 2026. Right now, commissioned education for officers and mid- to short-term military-specific AI education programs is in progress (Ministry of Science and Technology 2021). Overall, the MND acknowledges that transforming officers' perceptions of digital transformation is crucial and

a prerequisite for the broader adoption and implementation of defense AI. A significant initiative involves collaboration with a private AI graduate school, entailing an investment of KRW36bn (USD27M) over 5 years to train approximately 1000 specialists in AI and software and to enhance educational facilities (MND 2022a: 6; MSIT & MND: 6).

While it may be premature to assess the actual impact and efficacy of these AI education and talent development projects for the military, it is evident that policy emphasis and efforts in AI education will persist, complementing the dedication to implement the national defense AI policy. Despite criticisms that the military's AI curriculum may be overly focused on the utilization of AI technology, insufficiently incorporating AI ethics, and prioritizing quantitative achievements over the cultivation of qualitative human resources, there is broad consensus and minimal contention regarding the national initiative's direction. The prevailing view is that the success of defense AI critically hinges on the development and education of human resources.

6.2 Defense AI and Simulation-Based Training

Like other leading military nations, the ROK military has long incorporated wargames based on modelling and simulation (M&S) and combat experiments into its core operational conceptualization and training methodologies. With the advent and integration of technologies like Virtual Reality (VR) and Augmented Reality (AR), collectively known as Metabus, there is a shift towards developing more sophisticated simulation-based training systems.

In 2022, the MND created and allocated a new budget within it of KRW43bn (USD33M) for enhancing practical scientific training. This included KRW22.1bn (USD17M) for AR-VR equipment, such as VR setups for special forces parachute training, VR education and training centers, and VR simulated firing systems for reservists. Additionally, KRW13.3bn (USD10M) was designated for constructing four new practical scientific training centers capable of data-driven scientific training, supplementing the existing science training center at KCTC. Furthermore, KRW7.5bn (USD5.7 M) was directed towards a new management system for the scientific training of reservists and trainees (Kim 2022: 15; YTN Science 2021).

The South Korean military has been actively considering the development of a training system akin to the Synthetic Training Environment utilized by the U.S. military. The need for such a system in the South Korean forces has been increasingly recognized. However, to date, there has not been a specific instance of a simulation-based training system project incorporating AI, nor has there been a designated budget for such an initiative. This situation stems partly from a fundamental issue within the national acquisition system: training systems are categorized as Force Support System rather than Weapons System, complicating the allocation of R&D budgets typically reserved for weapons systems. Additionally, the lack of cloud

infrastructure, practical data-driven culture and AI-related foundation within the South Korean military also contributes to this challenge.

However, there has been recent development projects in South Korea focusing on incorporating AI into simulators for individual weapons system operational training. Examples include the K2 tank simulator, the Short Distance Surface to Air Missile, and the Air Force's fighter jet simulator development project. This trend is driven not only by the necessity of these projects themselves, but also by the fact that AI-based simulators are often classified as weapons system acquisition projects in the South Korean defense context. This classification facilitates the allocation of R&D budgets for these initiatives. The current state of training systems reflects the broader challenges and complexities associated with implementing and realizing full-scale AI in South Korea's defense sector.

7 Conclusion

South Korea's current government strives to establish a digital platform government, amalgamating government data with private sector services. This initiative is driven by the dual goals of fostering national unity and revitalizing a stagnant economy. AI is being leveraged as a key tool in this endeavor, akin to the metaphorical One Ring from The Lord of the Rings, symbolizing a crucial instrument for crafting a state-led technological utopia. Consequently, the MND and the armed forces consider AI instrumental in constructing a robust military, equipped to navigate the challenges of future warfare. Confronted with a demographic crisis marked by a precipitous decline in troop numbers and escalating regional security tensions, the South Korean military identifies AI as a critical catalyst for augmenting its military capabilities. Consequently, the government has prioritized the development of a "formidable, AI-enhanced military, strategically positioned to spearhead advancements on future battlefields" (Presidential Advisory Council on Science and Technology 2023: 3).

Despite a strong commitment, South Korea's journey towards integrating defense AI faces many challenges. These include fragmented defense AI governance inside the MND, the structural disconnect between DAPA's responsibility for weapon system acquisition and the MND's overall responsibility to acquire military force support systems, a predominantly hardware-centric defense industry, a yet underdeveloped defense-specific AI infrastructure, restrictive data sharing regimes, and an overall low appeal of the defense sector among top civilian talents.

Cognizant of the existing shortfalls, South Korea's military decision-makers are increasingly recognizing the pivotal role of clearly and effectively identifying and addressing challenges in AI deployment as a foundational step towards establishing an AI-enhanced military force. This growing awareness is fostering optimism about the potential acceleration in the adoption and proliferation of AI technologies within the military sphere. In addition, the public's broadly supportive stance towards the government's steadfast commitment to boosting AI and ICT investment, aligned

with the national objective of nurturing a robust AI-centric science and technology sector, adds to the positive dynamics favoring the successful implementation of defense AI initiatives.

References

Ahn, Seunghee. 2019. Implementation of 'Navy Vision 2045' and 'Defense Reform 2.0 Navy Promotion Plan': Standing tall as an 'Ocean Navy' in 2045, the 100th anniversary of its founding. National Defense Journal 547: 17–23. Defense Media Agency. https://kookbang.dema.mil.kr/newspaper/JournalMng/journalData/2019/07/BBSMSTR_000000010110.pdf. Accessed 30 January 2024

DAPA. 2021a. *Strategy for application of artificial intelligence in weapon systems*. Gwacheon: DAPA.

———. 2021b. Chung A Raam. DAPA Newsletter 109: 20. https://www.dapa.go.kr/ebook/dapajournal/readerBook/vol109/book.html. Accessed 30 January 2024

Gook, Kyungwan. 2019. Artificial intelligence technology and application cases by industry. Weekly Technology Trends. IITP 1888: 22. https://docviewer.nanet.go.kr/reader/viewer. Accessed 30 January 2024

Industrial Daily. 2022. Total investment of KRW1.429 trillion in ICT R&D in 2023. Industrial Daily. https://www.kidd.co.kr/news/229966. Accessed 30 January 2024

Joint Ministry. 2019. ROK National Strategy for Artificial Intelligence: 34–35. https://www.korea.kr/docViewer/skin/doc.html?fn=e1b3919a9faf3e30720e22eec1d2c81e&rs=/docViewer/result/2020.03/12/e1b3919a9faf3e30720e22eec1d2c81e. Accessed 30 January 2024

Kim, Saeyong. 2022. MND's defense metaverse utilization and development. Defense XR Convergence Conference. 13 October

Ko, Kwangbon. 2023. In an era where warfare cannot be conducted without space...we must secure our own reconnaissance and surveillance capabilities. Sedaily. https://www.sedaily.com/NewsView/29S0IJK2SG. Accessed 30 January 2024

KRIT. 2021. Future National Defense 2030 Technology Strategy AI (Summary). Korea Research Institute for Defense Technology Planning and Advancement. https://www.krit.re.kr/krit/bbs/gbby_pdf.do?bbsId=gbby&article_category=&nttId=4443&page=1&searchCnd=0&searchWrd=%EA%B8%B0%EC%88%A0%EC%A0%84%EB%9E%B5&startd=&endd=&menu_no=03090300. Accessed 30 January 2024

MND. 2021a. *Strategic plan for defense artificial intelligence*. Seoul: ROK MND.

———. 2021b. *Defense AI strategy report*. Seoul: ROK MND. Internal resources.

———. 2021c. Press Release. 'Army tiger', a ground combat system implementing advanced technology, roars as the future Army's '4th generation combat power'. Korea Policy Briefing. https://www.korea.kr/briefing/pressReleaseView.do?newsId=156447348. Accessed 30 January 2024

———. 2022a. Defense White Paper. ROK MND. https://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_202303070948276600.pdf. Accessed 30 January 2024

———. 2022b. MND Work Report: 6. ROK MND. https://www.korea.kr/docViewer/skin/doc.html?fn=196871822&rs=/docViewer/result/2022.07/22/196871822. Accessed 30 January 2024

———. 2023a. Overview of the fiscal year 2023 MND budget and funding plan: 3. ROK MND. https://www.mnd.go.kr/mbshome/mbs/mnd/download/2023_budget(1).pdf. Accessed 30 January 2024

———. 2023b. Realizing peace through strength. MND Major Work Plan 2023: 9. ROK MND. https://www.mnd.go.kr/mbshome/mbs/plan/download/2023_report.pdf. Accessed 30 January 2024

MND Blog Defense News. 2023. 1st Defense Data Management Committee held. Korean MND Blog. https://m.blog.naver.com/mnd9090/222980181954. Accessed 30 January 2024

MND Blog M-Friends. 2020. AI based Future Combat System Army Tiger 4.0. https://m.blog.naver.com/mnd9090/222005709209. Accessed 30 January 2024

MSIT. 2019. Press Release. Announcing the AI National Strategy. Korea Policy Briefing. https://korea.kr/briefing/pressReleaseView.do?newsId=156366736. Accessed 30 January 2024

———. 2023a. Key Features of the 2023 National R&D Budget. 2023 Korean Government R&D Program Joint Ministry Briefing. https://www.kistep.re.kr/flexer/view.jsp?FileDir=/mjbs/2023/&SystemFileName=202302211050379201.pdf&ftype=pdf&FileName=202302211050379201.pdf. Accessed 30 January 2024

———. 2023b. ICT R&D Program. 2023 Korean Government R&D Program Joint Ministry Briefing. https://www.kistep.re.kr/flexer/view.jsp?FileDir=/mjbs/2023/&SystemFileName=202301091050152441.pdf&ftype=pdf&FileName=202301091050152441.pdf. Accessed 30 January 2024

MSIT & MND. 2022. DNA based Smart Defense Strategy: 3–6. https://doc.msit.go.kr/SynapDocViewServer/viewer/doc.html?key=793f94bfa56b4cb5853e9b1676b1d45d&convType=html&convLocale=ko_KR&contextPath=/SynapDocViewServer/. Accessed 30 January 2024

News Aerospace. 2019. Air Force completes high-tech military with smart innovation in the 4th Industrial Revolution. News Aerospace. https://post.naver.com/viewer/postView.nhn?volumeNo=18291804&memberNo=44742705#. Accessed 30 January 2024

Office of the President ROK. 2023. Press Release. President Yoon "Korea will be a key partner in global sup-ply chain" in Special Address at the 2023World Economic Forum Annual Meeting. Korea Policy Briefing. Office of the President ROK. https://www.korea.kr/news/policyNewsView.do?newsId=148910795. Accessed 30 January 2024

Park, Dongsun. 2020. 'SMART Navy' grand voyage plan based on advanced technology of the fourth industrial revolution. Journal of the Korean Society of Shipbuilders 57-1: 7–10. https://koreascience.kr/article/JAKO202010163509993.pdf. Accessed 30 January 2024

Park, Daero. 2022. Air Force builds kill web combining AI, drones. Financial News. https://www.fnnews.com/news/202205270501246455. Accessed 30 January 2024

Park, Youngwook et al. 2020. Research on defense AI development plan. KIDET. ROK MND Policy Report. https://www.prism.go.kr/homepage/entire/researchDetail.do?researchId=1290000-202000076&menuNo=I0000002. Accessed 30 January 2024

———. 2023. Research on how to establish and operate a defense AI center. KIDET. MND Policy Report

Presidential Advisory Council on Science and Technology. 2023. National Defense Science and Technology Framework Plan 2023-2027: 31/50–51. ROK MND. https://online.fliphtml5.com/lukuo/myik/#p=65. Accessed 30 January 2024

REAIM. 2023. REAIM 2023 call to action. https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/publications/2023/02/16/reaim-2023-call-to-action. Accessed 30 January 2024

ROK Air Force. 2021. *Air force artificial intelligence development plan*. ROK Air Force.

ROK Army. 2021. *AI integration roadmap 2022-2033*. ROK Army.

ROK National Assembly. n.d. Bill on fostering the AI industry and creating a foundation for trust proposal date 1 July 2021. https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_Y2B1M0R6G2I2P1B0V2X9H4Z0X3M3J2. Accessed 30 January 2024

ROK Navy. 2021. *Direction for intelligentization of naval battlefield functions*. ROK Navy.

YTN Science 2021. Military actively utilizes metaverse. KRW42.9 billion to strengthen safety training. YTN Science. https://m.science.ytn.co.kr/program/view.php?mcd=0082&key=202111151144174692. Accessed 30 January 2024

Intelligent National Defense Amid Strategic Ambiguity? Defense AI in Taiwan

Kitsch Liao

Taiwan's approach to defense AI suffers from the same issue plaguing its overall defense establishment: A legacy from an authoritarian past, which disconnects the civilian government and defense establishment. This inhibits effective strategic alignment to array the country's operational and tactical approach toward the Chinese threat in an asymmetric manner agreed upon by the country's political establishment and its primary security guarantor, the United States.

Such a disconnect also prevents the defense establishment from effectively leveraging Taiwan's impressive civilian technology innovation sector. Existing defense-AI programs tend to be piecemeal and unfocused and mostly aimed at "doing things cheaper and faster" instead of exploring new ways of doing things.

Even the rare attempt by the Taiwan Air Force to advance the future concept of operations (CONOP) incorporating AI as the centerpiece proved to be technically ambitious, organizationally far-reaching, yet conceptually ill-formed.

However, there is no shortage of grassroots ideas, within and without Taiwan's defense establishment. If the country finds a way to funnel grassroots talent and solutions more effectively into an open defense innovation ecosystem, Taiwan stands to benefit significantly from the adaptation of defense AI in contending with China.

K. Liao (✉)
Atlantic Council Global China Hub, Washington, DC, USA
e-mail: kliao@atlanticcouncil.org

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_24

1 Thinking About Defense AI

1.1 Taiwan's Unique Security Situation

Since the Nationalist Kuomintang (KMT) government retreated to Taiwan, Taiwan's military has been, much like their Communist cousins on the mainland, loyal to the Party and its leader. Thus, instead of a dialectic process informing a national defense strategy, it was often decided within a relatively small circle surrounding the leadership. In turn, this created a situation where the armed forces were operationally and tactically competent yet lacked the capacity and culture to conduct strategic planning and foresight.

Today, Taiwan's defense still suffers mismatched strategic, operational, and tactical objectives for Taiwan's defense strategy from this authoritarian legacy. This further influences force structure, training, research, and development, and acquisition. And the advent of defense artificial intelligence (AI) as an issue of significance cannot escape this trend.

The situation is further exacerbated by Taiwan's lack of international support due to China's ongoing efforts to prevent all other countries from maintaining official relations with Taiwan, let alone arms sales. Thus, with few exceptions, the US has remained the sole source of defense systems acquisition for the island nation.

These arms sales, along with the Taiwan Relations Act, in which the U.S. promises to maintain its ability but not intent to intervene should China invade, constitute a rather shaky promise toward Taiwan's security from its largest security partner in the world.[1]

This means Taiwan is a country that does not get to decide its own future. Instead, the largest piece of its security strategy is in a constant state of flux, aptly termed "strategic ambiguity," where the US attempts to simultaneously deter China from invading Taiwan, and Taiwan from declaring independence. This creates a powerful sense of contradiction within Taiwan's defense establishment in both that Taiwan needs to independently fight against a Chinese invasion, and regardless of what Taiwan does, the fate of Taiwan might still be decided in Washington DC.

1.2 The Overall Defense Concept and Asymmetric Defense

Facing such uncertainty in allied support, along with decades of force reduction following Taiwan's democratization and a lull in Cross-Strait tension in the late 90 s, leads to a military plagued by low morale and low investment. This situation is further exacerbated by the increasing shift of military balance across the Taiwan Strait, with the People's Liberation Army launching its largest ever comprehen-

[1] Taiwan does have, for example, joint-military exercise with Singaporean military (Ani 2021), but most of these single-case exceptions are also nestled under the umbrella of a US-led alliance response to any potential Taiwan contingency.

sive reform in 2015. And as the operational approach against enemy forces enshrined within the country's biannual National Defense Review gradually shifted from destroying invading forces outside of Taiwan's borders to ensuring their destruction on the beach, the country gradually came to terms with the imbalance and attempted to exploit various strategic and operational asymmetries to its advantage, culminating in the Overall Defense Concept (ODC) (Lee et al. 2020). The document is aptly characterized with the slogan "a large number of small but lethal things."

Yet the disconnect between the civilian government and defense establishment still remains, with the directives issued by the political institutions often failing to translate into operational or tactical realities. Instead, the official capstone documents such as the National Defense Review (NDR) and the Quadrennial Defense Review (QDR) merely serve to pay lip service to the concept promulgated by the civilian government. An example of this can be gleaned from the 2023 QDR, where strategic goals were logically placed, with the preservation of the democratic system placed above the preservation of life and property. However, when it comes to operational level discussions concerning the Overall Defense Concept, traditional platforms from capital ships to fighter jets were somehow characterized as fulfilling the asymmetric mandate without much explanation.

The convergence of these factors creates powerful incentives to search for a miracle solution to solve Taiwan's defense woes. In this regard, the utilization of AI in defense is only the latest miracle, following autonomous drones and satellite communications. But the force reduction is only the symptom of another societal issue,[2] as Taiwan's birthrate gradually declined over the decade, reaching its nadir in 2023 as the country with the lowest projected birth rate in world at 1.09 children per woman (台灣全球倒數第一 無解的難題 2023, CIA F). And for many in the defense establishment, adaptation of defense AI also represents an opportunity to ameliorate some of the pressures brought upon the existing force structure by the low rate of birth (陳建源 2018).

1.3 Defense AI under the Taiwan Context: Do it Cheaper and Do it Faster

Perhaps the most prominent public-facing conceptualization of Taiwan's defense AI is nested within the larger context of the "Intelligent National Defense Program," which began in 2019. Then Deputy Chief of General Staff General Li Ting-sheng, a proponent of the approach, would later disclose that the 10-year program was divided into six sequential stages (賴品瑀 2023):

[2] Force reduction in recent decade, and even the trend toward ending conscription beginning in 2008, was sometimes justified by authorities in claiming that the force structure was unsustainable given Taiwan's low birthrate.

- Integration of various technologies with AI
- Integration of Internet of Things (IoT) and 5G technologies with Taiwan's unique strength in Information & communication technologies (ICT)
- Support the use of AI-integrated IoT with big data
- Battlefield situational awareness
- Intelligent decision making
- Cyberwarfare.

The National Chungshan Institute of Science and Technology (NCSIST), the top state-run defense research institution, also set up a parallel "Ten Year Intelligent Defense Plan" aimed at making the intelligent National Defense program a reality. Details of NCSIST's plan were never made public, however anecdotal evidence suggests that these developments match closely with the Ministry of National Defense' vision of a six-phased approach. Orchestrated by the information and communication research division, the plan includes a potential long range anti-submarine warfare (ASW) early warning and surveillance system that incorporates autonomous sensing, learning, identification, and intelligent remote guidance and control to enable autonomous unmanned aerial vehicles (UAV) and potentially unmanned teaming through the Artificial Intelligence of Things (AIoT) (涂鉅旻 2019). The essence of Intelligent National Defense, as then director of NCSIST's information and communication research center, Lin Gao-chau stated, is the collection, integration, fusion and comparison of data to predict future situations, assist commander's decision making (涂鉅旻 2019).

The program launch coincides with the Ministry of National Defense (MND) framing 2019 as the "Year Zero" for Taiwan's intelligent defense, mirroring the "AI Year Zero" on the civilian side by the then Ministry of Science and Technology (朱泓任 2017). This highlighted the MND's desire to take advantage of Taiwan's robust tech ecosystem.

Many of these described efforts demonstrate three things concerning the Ministry of National Defense's approach toward defense AI:

- a propensity to favor the kinetic over the digital;
- a conceptual origin mixed in the context of digitization and threats posed by such, e.g. the penetration of digitized network by PLA cyber actors;
- and as a consequence of the first two, a very limited conceptualization of AI applications, with most applications filed under ICT and Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) contexts.

It is worth noting that the development and standing up of Taiwan's Information Communication Electronic Force (ICEF), colloquially known as the Cyber Force, also suffers a similar identity crisis.

1.4 Regulating Defense AI

As of the end of 2023, no specific code of ethics governing the use of defense AI exists in Taiwan. The development of defense AI would have to observe the AI Technology R&D Guidelines issued by the Ministry of Science and Technology

(later National Science Technology Council, NSTC) in 2019 (科技部 2019). The Guidelines stems from three core values the ministry has identified as conforming to universal expectations on the use of AI in the global community:

- Human-centric Values
- Sustainable Development
- Diversity and Inclusion

These three core values are further expanded into eight guidelines concerning the research and development of AI:

- Common Good and Well-being
- Fairness and Non-discrimination
- Autonomy and Control
- Safety
- Privacy and Data Governance
- Transparency and Traceability
- Explainability
- Accountability and Communication

Ethics governing specific aspects of AI applications also exists, and even predates the R&D guideline discussed above; the 2018 Unmanned Vehicles Technology Innovative Experimentation Act (Ministry of Economic Affairs 2018), where elements such as the protection of privacy and personal information, ensuring the safety of human beings, and the transparency of AI, are all present in some form.

Taiwan's comprehensive answer to the question of ethics governing AI, the Artificial Intelligence Fundamental Act, is expected to be introduced sometime in 2024. The overall regulatory approach will be similar to that of the European Union, through amending specific regulations like, for example, the Personal Data Protection Act. The Fundamental Act itself will classify AI systems into various levels of risk and allow individual competent agencies to come up with specific regulations, e.g. the Financial Security Commission will regulate intelligence finance, and the Ministry of Transportation will draft detailed codes governing intelligent transportation (王儷華 2023).

1.5 Defense AI According to Taiwan's Defense Documents

While exact details of the 10-year AI plan have not been publicly disclosed, parts of the vision can be gleaned from other official documents published by the MND. Taiwan's primary external-facing capstone defense documents comprise the biannual National Defense Review (NDR), and the Quadrennial Defense Review (QDR). Under the general direction of building an asymmetric force largely following the ODC, 2021's releases represented the first prominent mention of defense AI as an integrated component of Taiwan's defense concept. The 2021 NDR identified several technologies that have implications for warfighting, as well as influencing the modalities of war. Chief among them AI, with specific mentions on the development of disruptive AI such as swarm and human-machine cooperative UAVs in the

context of the US Third Offset Strategy, as well as the PRC's current focus of AI application in unmanned systems.

Other disruptive technologies listed include precision strike, wargaming, modeling and simulation, and deepfakes (Ministry of National Defense 2021a, b). Judging that these would significantly improve the PLA's joint operational capability and pose a significant threat to the Taiwan Strait and surrounding areas, the 2021 QDR stresses the need to integrate these technological trends into the development of Taiwan's C4ISR. Specifically to integrate them into intelligent command and control (C2) systems in order to achieve two major objectives: first, improving situational awareness for the battlefield commander, and secondly, to provide battlefield assessment and decision-making aid (Ministry of National Defense 2021a, b). Additionally, the QDR also emphasized developing AI applications in prosecuting offensive and defensive computer network operations (CNO).

The following 2022 NDR, 2022 QDR, and the 2023 NDR all presented similar characterizations for the future direction of Taiwan's armed forces as a combination of the asymmetric approach with the implementation of defense AI: "Mobile, small, man-portable & AI integrated." This is further reflected in Taiwan's latest 5-Year Force Planning Document submitted for review to the parliament in 2023 (陳鈺馥 2023), which echoed the characterization by stating the aim of developing a military that conforms to the asymmetric approach to defense as outlined in the ODC. Therefore, force planning should be geared towards improving the military's capacity to take advantage of "Long range [fire], Precision [fire], Unmanned [systems], and AI [systems]."

Curiously, in the discussion for another major pillar of defense strategy as outlined in the 2021 QDR, that of establishing a self-sufficient defense industrial base (國防自主), AI was not identified as one of the major categories to be developed in accordance with the need for defensive combat operations, but was instead given only a cursory mention in the development of next-generation intelligent unmanned aerial and underwater vehicles (Ministry of National Defense 2021a, b). This stands in stark contrast to the positions taken by the government during the 2017 establishment of the then brand new ICEF, where one of the three major directives for the new branch issued by President Tsai was to pioneer the development of an academic and industrial base for Taiwan's cybersecurity scene (楊孟臻 2017).

1.6 Origin of the Defense AI Civil-Military Ecosystem

On the civilian side, the "the Taiwan AI Action Plan" launched by the Ministry of Science and Technology pushes for the establishment of a civilian AI development ecosystem that leverages Taiwan's unique position in the global semiconductor supply chain (行政院 2019). The origin of parallel civilian and defense technology development ecosystems can at least be traced back to the National Science and Technology Development Plan for 2013–2016 (行政院國家科學委員會 2013). Since then, one of the primary missions of the self-suffi-

cient defense industry has been to spearhead technology and industry development, acting as the driving force for industry. This was further cemented in 2020 during President Tsai's speech, in which the government centered the civil-military integration of defense industry as one of the country's six major core strategic industry goals (National Development Council 2021). The details of such plans are further laid out in the Defense Technology Development Blueprint and White Paper, which also encompasses the plans to set up defense research centers within university campuses (Ministry of Science and Technology 2020), and the creation of the Defense Advanced Technology Development Program (國防部軍備局 2023).

2 Organizing Defense AI

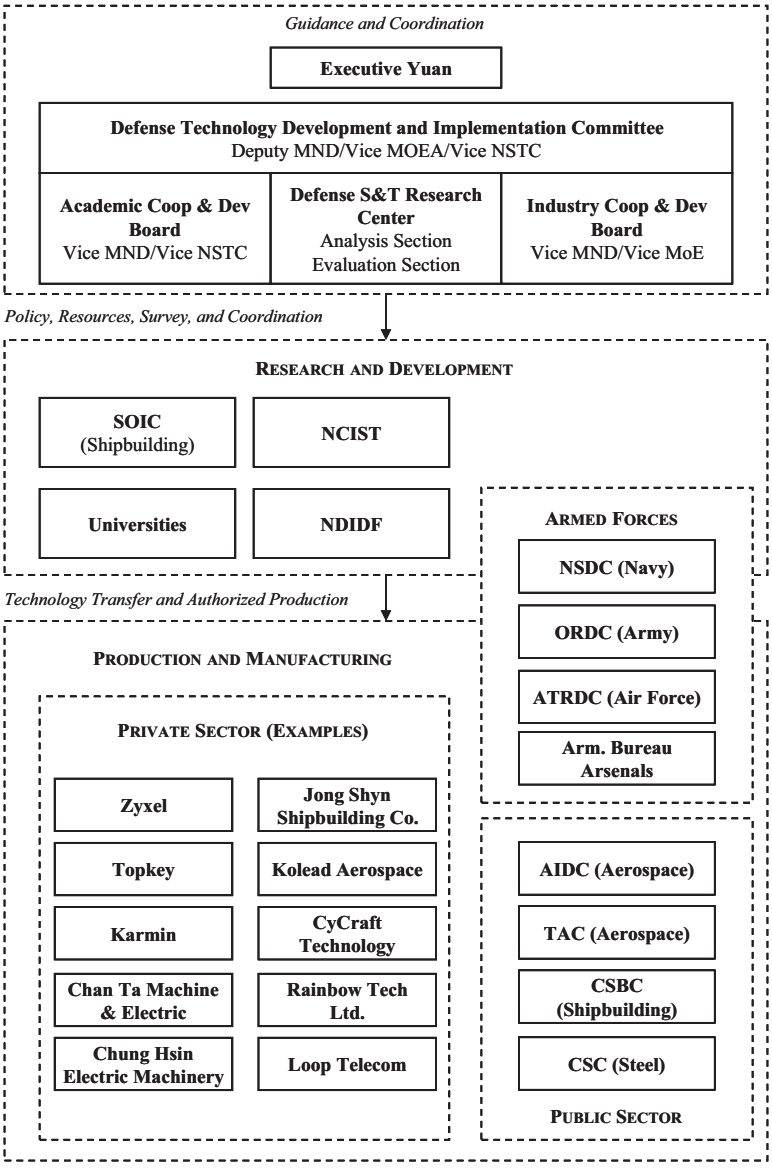
There is no dedicated defense AI organization, from policy to research to production and employment, within Taiwan's defense innovation ecosystem. Instead, various directives and experimental programs are nestled within different tiers of Taiwan's Defense Technology Development Mechanism (DTDM), with the majority of disclosed research programs belonging to the Defense S&T Research Center initiatives located in various universities.

2.1 The Defense Technology Development Mechanism

The DTDM can be roughly separated into three tiers (Fig. 1); policy guidance and coordination, research and development, and production and manufacture. At the top is the Defense Technology Development and Implementation Committee, chaired by the Deputy Minister of Defense, the Vice Minister of Economic Affairs, and the Vice Chair of the National Science and Technology Council. The committee coordinates myriad government organizations and provides policy guidance for the research and development tier of the system (林柏州 2019).

The research and development tier of the DTDM spans both public and private sectors. A series of armed forces organizations, including the Navy's Naval Ship Development Center (NSDC), the Army's Ordnance Readiness Development Center (ORDC), the Air Force's Aerospace Technology Research and Development Center (ATRDC), and the Armaments Bureau's various arsenals occupy both the R&D tier as well as the production and manufacturing tier, as they sometimes take part in limited production for more specialized projects, either due to sensitivity or lacking economy of scale for serial production.

Outside the armed forces, the National Chungshan Institute of Science and Technology (NCSIST) leads research and development on sensitive defense projects. The projects that require security clearance unavailable to civilian institutions are exclusively conducted within the confines of the defense industry development



Abbreviations
AIDC Aerospace Industry Development Cooperation; ATRDC Aerospace Technology Research and Development Center; CSBC China Shipbuilding Corporation; CSC China Steel Corporation; MND Ministry of National Defense; MOAE: Ministry of Economic Affairs; NCIST National Chungshan Institute of Science and Technology; NDIDF National Defense Industry Development Foundation; SOIC Ship and Ocean Industries R&D Center, TAC Taiwan Aerospace Corporation

Note: The Defense Technology Development and Implementation Committee has been defunct since 2020, the specific legislation indicated a successor should be set up to handle non-sensitive development of defense articles, however as of 2024 there has been no movement.

Fig. 1 Taiwan's defense technology development mechanism. Source: 林柏州 2019, partially updated by Author, 2020, "Defense Industry Development Act, Article 11," https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=F0110024

institutions (國防工業發展機構),[3] directly under the auspices of the MND. This means that most publicized research projects are equal or below technology readiness level (TRL) 5.[4]

The Ship and Ocean Industries R&D Center (SOIC) (Ship and Ocean Institutes R&D Center n.d.) and the National Defense Industry Development Foundation (NDIDF) (National Defense Industry Development Foundation n.d.) serve their respective niches as shipbuilding R&D centers and legacy funds for defense investment and tech transfers. Universities take center stage as the most vibrant defense AI element in the DTDM. The details and projects involved under the various universities' Defense Technology Research Centers will be further elaborated in the next section.

2.2 Defense S&T Research Center and Corresponding Universities

The most active and public portion of the DTDM concerns the "academic research center (學研中心)" initiative. A joint venture between the Ministry of Science and Technology and the Ministry of National Defense started in 2020, the NTD5bn (USD167M) initiative aims to establish an initial three to six research centers in various universities in order to foster systematic and continuous research on defense applications for various technologies. The initial focus of the project consists of seven major areas of research:

- Technology foresight research on sensing and precision manufacture
- Advanced materials and analytical mechanics
- Information, communication, electronics, and smart technologies
- Critical systems analysis and integration
- Cutting-edge power plants and aerial vehicles
- Advanced surface vessels and underwater vehicles
- Advanced systems engineering research

These research centers also serve as think tanks for defense technology development, advising on various topics including the defense application of artificial intelligence for the Ministry of National Defense (張玲玲 2023).

By 2023, there are at least seven defense S&T research centers located in various universities around Taiwan (科技部 2022), each specializing in one of the seven

[3] The term is used opposite of the "academic research institutions" that characterized the centers under various universities. However, the exact definition of which agencies are included as part of the national defense industry development institution were never explicitly stated in official documents. Nevertheless, the term has made multiple appearances in various policy documents, including a concept note by the MND's Department of Integrated Assessment describing research programs open for bids.

[4] Personal interviews with relevant personnel indicate that this is the cut-off point.

areas of focus (Table 1). These research centers are coordinated through the Defense S&T Research Center under the competence of the Defense Technology Development Implementation Committee (Fig. 1) located under the National Defense University's Chung Cheng Institute of Technology (CCIT).

2.3 Defense Technology Research Programs for Academia

There are two major defense technology research programs with three distinct horizons for maturity under Taiwan's defense innovation ecosystem; the Defense Technology Exploration Program (國防科技探索專案計畫, DTEP), which focuses on projects with a long maturity timeline (科技部 2022); and the Defense Advanced Technology Development Program (國防先進科技研究計畫, DATDP), which

Table 1 University Defense S&T Research Centers and Specializations in Taiwan

Universities	Specialization	Research Center
National Taiwan University (臺灣大學)	Technology foresight research on sensing and precision manufacture (前瞻感測與精密製造研究)	National Defense Technology Academic Research Center (國防科技學研中心)
National Tsinghua University(清華大學)	Advanced materials and analytical mechanics (先進材料與力學分析研究)	National Defense Technology Academic Research Center (國防科技學研中心)
National Yang Ming Chiao Tung University (陽明交通大學)	ICE & intelligent technologies (資電通訊與智慧化科技)	Technology foresight and systems academic research center (前瞻科技與系統學術研究中心)
National Chung Hsing University (中興大學)	Critical system analysis and integration (關鍵系統分析與整合)	National Defense Critical Systems Research and development center (國防關鍵系統研究發展中心)
National Cheng Kung University (成功大學)	Cutting-edge power plants and aerial vehicles (尖端動力系統與飛行載具)	Wang Tsoo systems engineering research center (王助系統工程研究中心)
National sun Yat-sen University (中山大學)	Advanced surface vessels and underwater vehicles (先進船艦及水下載具)	Academia Research Center of Underwater Vehicles (智慧操控水下載具學研中心)
National Defense University (國防大學)	Advanced systems engineering research (先進系統工程研究)	Advanced systems engineering research center (先進系統工程研究學研中心)

Sources: 國立台灣大學 2021; 清華大學 2021; 陽明交通大學 2021; 中興大學 2021; 成功大學 2022; 中山大學 2021; 中山新聞 2021; 蘇恩民 2023

fund projects with maturity horizons of either 3 years, or 5–8 years depending on the category (蘇思云 2020).

While these programs seemed to be tailor-made for defense S&T research centers coordinated through NDU CCIT's Defense S&T Research Center, application and participation in these research programs are not limited to the seven centers but are open to general academic institutions as well.

2.3.1 Defense Technology Exploration Program (DTEP)

DTEP, orchestrated by the Ministry of Science and Technology/NSTC,[5] is patterned after the Artificial Intelligence Exploration (AIE) and Microsystems Exploration (μE) programs conducted by the US Defense Advanced Research Projects Agency (DARPA). The DTEP aims to focus on dual-use technologies concerning small to medium unmanned vehicles in the air, ground, surface, and underwater terrains, as well as information, communication, electronics (ICE), and cybersecurity technologies (科技部 2022). The program invites submissions based on an envisioned scenario and uses a case in the 10–30-year horizon. Proposed projects will be evaluated first on the scenario set before technical evaluation. Successful pitches are given 18 months and a maximum of NTD8M (USD26,6700) per year to develop a proof of concept or a prototype, with the end results evaluated and rolled into consideration for approving future pitches by the same investigator (科技部工程司. 2022).

While DTEP has a stated goal of encouraging innovative thinking into future scenarios, the request for the proposal listed out extremely detailed guidelines taken directly from the year's NDR on Taiwan's current operational threat environment and current defense tactical needs. This somewhat defeats the purpose of an exploratory program with a long-term horizon, and to a certain extent, also explains the limited and scattered nature of the project requirements issued by different stakeholders within the defense innovation ecosystem.

2.3.2 Defense Advance Technology Research Program (DATRP)

DATRP orchestrated under the Ministry of National Defense covers a wide range of topics, where individual organizations under the ministry submit concept notes outlining interested projects and the timeframe of execution for academic institutions to apply. Generally, new projects are unveiled every year and can be divided into two categories: foundational research, with a max timeframe of 3 years, and breakthrough research, with a max timeframe of up to 8 years. The submitted projects follow the seven focus areas outlined for the academic research centers (Table 2).

[5] MoST reorganized as NSTC in 2022.

Table 2 Taiwan Technology Development Budget (in NTD100M)

	Government Technology Budget	Defense Technology Budget	National Chungshan Institute of Science and Technology Budget
2011	907	63	
2012	927	38	
2013	911	31	
2014	938	28	148
2015	983	30	230
2016	1021	65	291
2017	1044	80	293
2018	946	81	384
2019	969	130	422
2020	984	106	530
2021	942	104	574
2022	1015	138	852
2023	1383	131	1209
2024	1438	110	1109

Source: Total government technology budget and defense technology budget from Taiwan's Directorate-General of Budget, Accounting and Statistics (主計處 n.d.). NCSIST budget from NCSIST website financialdisclosure section (國家中山科學研究院 n.d.)

Submission agencies vary and include Navy HQ, Air Force HQ, ICEF HQ, and more. Some projects even originated from within DTDM's research and development tier, such as NCSIST and the Navy's. The number of projects submitted every year is also quite large. For 2023 alone, there were over 140 approved projects of varying sizes and length (國防部 2022a, b, c).

3 Developing Defense AI

This section will examine a selection of projects under the Defense Advance Technology Research Program (DATRP) from FY2022 and FY2023 involving the use of defense AI. Evaluation of technological maturity conforms to the technology readiness level (TRL) system first developed by NASA (國防部 2022a, b, c). Most projects were aimed at raising the underlying application's TRL to 4 or 5 for further development.

3.1 Developing Artificial Intelligence Applications for Close Quarter Air Combat

The Air Force has always been Taiwan's first line of defense against a Chinese invasion, and it has traditionally enjoyed political favoritism since the time of Chiang Kai-shek (許劍虹 2023). Thus, the attempt of the Air Force Technology Research

Development Center (ATRDC) to develop an AI-pilot within a simulated environment (國防部軍備局 2023) deserves special mention as this project is unique as it is technically ambitious, organizationally far-reaching, yet conceptually ill-formed.

Inspired by DARPA's Alpha Dogfight project, the goal of the 3-year project is threefold. First, to develop an intelligent platform capable of simulating operational scenarios involving AI pilots for tactics development and validation. Secondly, develop AI pilots that optimizes decision-making based on different scenarios, environments, and mission objectives. Thirdly, develop metrics for evaluating AI pilots' performance and feasibility for different missions.

Conceptually similar to many Taiwan armed forces projects, its stated origin is to follow the "trend set by major military powers," achieving a vision of "mosaic warfare" as set out by DARPA, where distributed shooters and sensors allowed the massing of firepower without having to mass forces (DAPRA 2018). Upon closer examination of the ATRDC's project proposal language however, it is uncertain whether the Air Force had sufficiently considered its adaption under Taiwan's operational context. In describing the future concept of operation, the proposal stated that the system should be able to achieve the following:

In a simulated environment, validate [the feasibility of] UAV wingman and manned lead aircraft can conduct missions together, that the human pilot can communicate and control the AI pilot to execute its assigned mission, with orders relayed through datalinks to the UAV wingman, where UAV wingman can achieve a high degree of autonomy through developed algorithm, and complete the mission assigned by the human lead, thus enhancing the Air Force's capability to conduct manned/unmanned operations (國防部 2022a, b, c).

This is almost an exact copy of the US Loyal Wingman project's conception of operation, aimed at operating against a near-peer power under a contested environment facing complex integrated air defense systems (IADS) (Losey 2022). However, the often-unstated assumption here is that this is used offensively during first days of a future war to conduct either deep penetration or suppression or destruction of enemy air defense (SEAD/DEAD) operations into enemy territory.

This is, however, far from the operational environment facing the Taiwan Air Force (TAF). The role of TAF is defensive, with contesting control of the air as its primary mission (中華民國空軍 2018). A mission Loyal Wingman would be ill-suited for this since it is principally developed, at least currently, for air-to-ground operations (Fish 2022). Furthermore, the extremely limited airspace above Taiwan is already heavily monitored, with the second highest density in radar stations and air defense missiles in the world (朱明 2021), controlled through four Regional Operation Control Centers (ROCCs), each capable of independently direct air defense of the entire island (徐葳倫 et al. 2021). The surveillance network is further augmented by airborne E-2 T AWACS. This comprehensive air defense network calls into question the utility of a loyal wingman-like platform to act as an independent sensor platform.

It is also interesting to examine the project's focus on within visual range (WVR) engagements, an understandable focus given the limited airspace above the Taiwan Strait and the relative proximity between Chinese and Taiwan airbases. Any beyond visual range (BVR) engagement would very quickly devolve into a dogfight, and

most engagements would offer little chance for coordinated and organized flow that a more offensively postured air force such as the US Air Force would be accustomed to.

Considering the defensive posture, and air-to-air mission focus of the force, another concept of operations (CONOPS) in the proposal entitled "maximizing UAV package recon/attack range" is even more puzzling:

In a simulated environment, when a UAV package is conducting recon/attack missions, it can utilize the minimum number of UAVs in achieving maximum effect. And although the goal is to minimize the number of UAVs engaged, redundancy should still be considered; beware of the tradeoff between reliability and UAV numbers to maximize operational range (國防部軍備局 2023).

It is hard to conceive that—under the current strategic guidance and operational doctrine –such an eventuality would manifest itself as a cost-effective measure for Taiwan's armed forces. It is perhaps worth further careful examination as to what asymmetric advantage such an unmanned, AI-agent-based UCAV could actually offer under Taiwan's strategic and operational context, especially considering the significant technical and organizational challenges to overcome.

A second category of issues stems from the ambition of the program in overcoming technical challenges in an impossibly short timeframe. Not only does the project attempt to replicate the results of Heron's winning bid for DAPRA's AlphaDogfight challenge (Tucker 2020), but it also further seeks to develop and implement human-machine teaming (HMT), which currently lacks any reliable framework for testing, evaluation, validation, and verification (TEV&V) (Motley 2022) within a yet to be developed simulated environment. The project further aims to involve not only academic research centers but also the defense industry development institutions, ATRDC, and active-duty pilots. All these efforts are to be accomplished, as defined by advancing development to TRL 5, within a mere 3 years.

Given the conceptual ambiguity and technical challenges facing such an effort, it is uncertain whether this particular effort represents an exploitation of Taiwan's asymmetric advantage in defense AI.

3.2 Additional Defense AI Projects

In addition to ATRDC's development efforts, Taiwan has also launched additional defense AI projects for support tasks, to advance predictive maintenance, for IT network management, and to assist space-based assets (機構系統開發 n.d.):

- *Optimizing Air Defense Launchers and Supporting Mechanisms with Artificial Intelligence (*運用 *AI* 智慧技術優化防空裝備發射暨支撐機構系統開發*)*

Issued by the Army's Missile and Electro-Optics Depot for FY2022–2023 (陸軍 2022), budgeted at USD1.5 M, the project aims to develop a series of autonomous stabilization and preventative maintenance systems using AI. Significant technical challenges are projected for creating the intelligent diagnostic system

for motors, bearings, and thread rods loads; the digitized monitoring system for the support struts motivator; and the intelligent monitoring system for the missile's box launcher motivator. All developments are judged to be a leap from TRL 1 to 4, as most of the prerequisite digitization to allow AI adaptations on machinery are non-existent.

- *Intelligent Balancing and Calibration of Vessel Propeller Shaft(*艦艇動力旋轉機構智動平衡校正之研究*)*

A project issued by Navy Headquarters for FY2022–2024 (國防部 2022a, b, c), budgeted at USD100,000 for the first year. The project seeks to utilize AI in the total life cycle management of a naval vessel's main screw(s), to facilitate preventative maintenance to increase mean time between repairs (MTTR) and estimate spare parts requirements. The project is divided into two major capstones: first, design a simulation of vessel propulsion system referencing MIL-STD-2189 (design methods for naval shipboard systems), validate with real-world data, and conduct dynamic analysis. Secondly, the project will develop a monitoring mechanism for the propulsion system's vibrations. This would allow real-time monitoring of the fatigue developed through normal wear and tear and enable automatic stabilization when unexpected vibrations occur.

- *AI Trained SDN Network Orchestration for Network Management and Security Detection (*以人工智慧導入*SDN*網路編排 管理與安全檢測之研究*)*

Issued by the ICEF Headquarters for FY2021–2023 (國防部 2022a, b, c), the project intends to utilize an AI algorithm to design a software-defined networking (SDN) architecture for Taiwan's armed forces and reorient the armed forces' various networked modules and platforms under this newly established architecture. The project is divided into 3 year-long phases with three respective capstones: establishing a network detection platform to analyze behaviors of individual packets and collecting information on SDN network and services for the first year, budgeted at USD60,000. The second year is spent on establishing an appropriate AI training and detection model to develop network orchestration techniques suitable for Taiwan's armed forces, budgeted at USD83,333. These efforts would culminate in the integration and evaluation of the Armed Forces' various platforms and modules subsumed under an SDN architecture in the final project year, with an additional budget of USD83,333.

- *AI-Assisted Next Generation Satellite Point Cloud Matching and Object-Oriented 3D Model Construction From Satellite Images (AI*輔助新世代衛星點雲密匹配及物件導向三維建模研究以衛星影像為例*)*

A follow-on to a previous project establishing AI-mapped terrain for a common operational picture (COP) issued by Arsenal 401 for FY 2022–2024 (國防部 2022a, b, c). Budgeted at USD66,666 for the first year, the project aims to construct ultra-high-resolution 3D object-oriented satellite images from vector models. Using clustering techniques and AI/ML algorithms on existing point clouds

produced from satellite remote sensing, a vector model can be identified as an object such as buildings. Sufficient mapping of these objects can then allow the detection and prediction of changing geological and terrain features, such as rivers and marine abnormalities.

3.3 Discussion

Additional defense AI research projects vary, from using AI to optimize UAV flight paths, to identify and map dangerous obstructions around airfields, to intelligent target identification for night-time urban warfare, and intelligent algorithms for tactical simulators. However, with the curious exception of the Air Force's AI dogfight project, most of these revolve around niche applications that endeavor to enhance, rather than revolutionize, the way business is done within the Taiwan Armed Forces. While there seemed to be some doctrinal attempts at narrowing down use-case and scenarios, the basic understanding of defense AI application does not exceed data-based optimization on "how to do things cheaper and faster."

4 Funding Defense AI

No dedicated budget categories for dedicated defense AI exist. Financial resources for projects reviewed above came from two sources: the academic research center initiative totaling NTD5bn (USD167M) over the course of 5 years, establishing seven defense research centers (蘇思云 2020), and the overall defense technology budget (Table 2).

Taiwan's defense technology budget has steadily increased over the past decade, consistent with the government's push to establish a self-sufficient defense industrial base through primarily public sector investment. In 2023, such expenditure accounted for around 3.16% of the total defense budget,[6] as compared to the United States, where research, development, test, and evaluation (RDT&E) accounted for about 17% of the total defense budget in the same year (Thomas 2023).

The annual budget for NCSIST, which conducts most application research once these development programs reach a certain level of maturity or sensitivity, has increased significantly over the past few years. While it is tempting to attribute these as pure R&D budget, it is important to note that NCSIST also conducts limited production of indigenous weapon systems. A non-trivial portion of its recent budget increase can be accounted for as part of the 5-year NTD240bn (USD8bn) contract NCSIST signed with the Ministry of National Defense on the indigenous production of eight major weapons systems (范正祥 2023).

[6] Taiwan's defense budget for 2023 was NTD415.1bn (USD13.2bn) (國防部 2022).

Taiwan's overall government technology budget as a percentage of GDP in 2023 to an impressive 4.5% (行政院主計總處 2023), whereas OECD countries average around 2.3–2.4% in this category (OECD 2023). After Taiwan's election on 13 January 2024, the incoming Lai administration indicated their focus on five major categories of industry, which included both AI and defense as two out of the five (呂雪彗 2023).

5 Fielding and Operating Defense AI

While there have been several research projects on defense AI over the past few years, public disclosure of the Armed Forces' operational defense AI applications has been relatively limited. A few scattered examples are outlined below to provide a feel of Taiwan's sensitivity in disclosing its defense AI applications. Notably, a few of these examples even predate the armed forces' focus on AI starting in 2019 (國防部 2017):

- *Intelligent ECG Analysis Platform*

An advisory panel on the development of intelligent military medicine was convened in 2019 consisting of members from the MND Medical Affairs Bureau, physicians, and industry representatives, to promote the development of AI application in medical affairs. In cooperation with Quanta computer, the armed forces established an AI Lab in 2020 (國防部 2021a, b). The effort seemed to bear some fruit in 2023 with the successful development and tech transfer to Quanta of the AI-based electrocardiogram (ECG) analysis platform, enabling advanced diagnoses of multiple cardiovascular disease, especially for remote areas with few experienced medical personnel present (范瑜 2023).

- *Constructive Mixed Reality CPR and AED Training System*

The Hualien Armed Forces General Hospital has developed a Mixed Reality training system for the instruction and training of cardiopulmonary resuscitation (CPR) techniques and the use of automated external defibrillator (AED). The system employs an AI-generated constructive simulation with a virtual patient and virtual AED, while allowing an on-site instructor and trainee to simultaneously interact with and be monitored by the simulation through linked cameras, receiving instantaneous feedback on accuracy of the technique and effects on the patient (國防部 2021a, b; 陳穎信 et al. 2020).

- *AI Performance Trend-based Engine Monitoring and Diagnostic System*

In 2018 the Air Force Institute of Technology demonstrated to the press corps a predictive engine monitoring and diagnostic system. Based on the digitization of past engine maintenance records and designs for Taiwan's next-generation jet engine for the Air Force's future fighter program, they were able to construct a digital simulation of the engine to predict failure trends. The system won a gold medal and the special contribution award in Poland's International Innovation Fair (徐振威 2018).

Perhaps the most damning testimony on the state of Taiwan armed forces' fielding of defense AI comes from the original proponent of the Intelligent National Defense program, General Li Ting-sheng. In an op-ed published in August 2023, General Li, now retired, remarked that the Armed Forces' application of AI to replace manpower in the spirit of asymmetric and innovative approach to defense has largely remained a matter of slogan, and rarely implemented (張延廷 2023).

6 Training for Defense AI

On top of establishing defense research centers, the NTD5bn academic research center initiative reviewed above also included provisions for training 150 graduate-level researchers for defense technology research. As early as 2016 defense AI training primarily focused on the employment of AI for computer network operations (CNO), setting up sections on information systems and network offense and defense under the department of information systems engineering of the National Defense University Chung Cheng Institute of Technology (國防大學理工學院 2023). Education on AI applications for defense logistics was introduced at Navy and Air Force Academies in 2019 largely through one man's effort, former Navy engineer Dr. Wang Zhi-zhong and his company Xwin Prognostics Technology, in collaboration with Microsoft and Axiomtek (李恬郁 2019).

Systematic training on the conceptual employment of AI in the defense realm seems to be lacking, other than the occasional conferences and workshops, predominantly focused on the intersection between digitization, cyber, and AI, targeting senior-level officers (周昇煒 2019), with occasional forays into issue areas such as the application of AI in AR and VR training (中華民國陸軍 2020). However, there does not appear to be an overall initiative aimed at providing the force with a comprehensive understanding for the role defense AI may play in future conflicts.

The incorporation of AI into civilian defense education seems to have received a better hearing on the civil defense education side following the outbreak of the Ukraine war, where middle-school activities on defense AI included simulations of battlefield operations involving autonomous UAVs and ground vehicles (方志賢 2022).

Incorporation of defense AI into training scenarios for the armed forces also proves promising, specifically in using AI to assist analysis of big data accumulated in training to improve future training modalities. The most prominent example lies in the medical realm, specifically at the National Defense Medical Center. The center has been incorporating augmented reality (AR), mixed reality (MR) and smart glasses in the training of simulated tactical combat casualty care (TCCC), simulated mass casualty events, simulated patient care on med-evac vehicles, and simulated assessment and emergency care for CBRN events. Data collected from these training events are incorporated with questionnaires filled by trainees post-event and analyzed through statistical software such as SPSS before feeding into the database for processing by AI algorithms to improve future training events (楊策淳 et al. 2020).

Other experimental examples of AI-assisted training methodologies include the National Defense University Management College's Military Human Factors Research Center, which began constructing databases of biometric data during the Marine Corps' long endurance exercise in 2019 and has recently been experimenting with collecting biometric data from soldiers engaged in VR simulations mounted on top of a 6-axis motion control platform for analysis on how to improve future training regimes (蕭佳宜 2023).

7 Conclusion

Much of Taiwan's approach to defense AI can be analogized as a microcosm of its approach to the defense of the nation, which can be summarized into three observations:

- *Observation 1: A propensity for "things done cheap" instead of "things done differently."*

A colloquial term often coined to describe Taiwan's current industrial approach is the "cost-down" approach (Liu et al. 2012). From many of the projects examined in this chapter, we can see that the approach was not a comprehensive rethinking on how business can be done differently, but how business can be done "cheaply."

- *Observation 2: A defense policy serving two masters—a government disconnected.*

The legacy of an authoritarian government created a rather disjointed approach to defense policy, where higher-level strategic considerations are disconnected with the operational and tactical realities executed by the defense establishment. The contradictory approach to the definition of asymmetric warfare to defend the country is just one example.

- *Observation 3: a bottlenecked civil-military defense innovation ecosystem.*

An obvious bottleneck, and potential explanation for Taiwan's lack of fielded examples of defense AI lies with the NCSIST. Any development into an operational application that is deemed even remotely sensitive would eventually have to pass through its doors. Yet this is an institution plagued with corruption scandals (楊國文 2022), ineffective auditing mechanisms that result in significant delays in the delivery of major weapons systems, and an inability to prevent revolving doors from taking place between the institute and the defense establishment (楊丞彧 et al. 2023).

Would a revised, more comprehensive, yet top-down approach on defense innovation, focusing on a select few applications and approaches, with more clear communications to stakeholders, be a more profitable approach?

The answer may lie in a more grass-roots and less restrictive approach to the development and adaptation of defense AI, especially from the civilian realm of applications. There is certainly no shortage of talents from the civilian side, with the

Minister of Digital Affairs Audrey Tang among TIME magazine's 100 most influential AI figures of the year (Serhan 2023), and innovators winning awards on AI applications all over the world (張淮壕 2023). The challenge seems to be setting up the appropriate infrastructure where Taiwan's defense establishment can properly benefit and harness from grassroots civilian efforts, without a preconceived notion of what the developmental pathway should be. To this end, a few policy recommendations may be beneficial in accelerating the process:

- *Stop leveraging defense innovation and industry for economic gains.*

The government should recognize the urgency and priority of Taiwan's defense needs and focus both the defense innovation system and defense industry at large on the overriding goal of ensuring Taiwan's security against the threat posed by China. This would mean a comprehensive assessment of what sort of defense industry Taiwan needs to maximize its resilience and self-sufficiency under various Chinese coercive scenarios, instead of attempting to devote government subsidies and issue policy directives based on an unobtainable win-win scenario where defense innovation and industry can enhance the economy while fulfilling defense needs. The relevant economic trade-offs of such an assessment should be made clear to the public before implementation. It also means that the government needs to proactively leverage civilian industries to fulfill defense needs by going out to the civilian industries and leveraging existing government bureaucracies outside of the defense establishment to do so.

- *Flatten defense RDTE organization and security considerations.*

The bottleneck represented by NCSIST and associated organizations within the defense industry development institutions must be alleviated. Consequently, a conscious, well-researched, well-informed trade-off between operational security and the ability of the defense establishment to benefit from civilian innovation must be made. Instead of a centralized and siloed approach based on clearance levels, and instead of issuing problems seeking solutions, a redesigned ecosystem should attempt to let the solutions be presented seeking potential applications from a democratized defense innovation ecosystem involving multiple operational stakeholders.

- *Establish an experimental unit for "roadshow."*

The previous two recommendations are really aimed at fostering an environment that would be more conducive to a bottom-up approach to defense innovation. But in order to spark such transformation, a small and nimble unit that can go around in a "roadshow" fashion, with both the authority and budget to experiment on solutions to various defense challenges and collect results for evaluation by both the defense and civilian establishment, would be crucial. The Ministry of National Defense Department of Integrate Assessment, a direct counterpart to the US Department of Defense's Office of Cost Assessment and Program Evaluation (CAPE) office, is ideally placed to take advantage of this approach, should the relevant budgetary authority be granted.

- *Emphasize potentially profitable approaches for Taiwan's defense AI.*

AI-enhanced real-time translation using large language models, capable of enhancing joint training and operation between US and Taiwanese forces, would also be an initiative that leverages the asymmetric advantage between the US and its allies against the solitary nature of Chinese forces. Additionally, applications that can leverage Taiwan's decades of consistent data collection of its surrounding operational environment, such as algorithmic optimization of decoys and smart sea mines, could also prove to be a profitable approach (Mitre et al. 2023).

References

台灣全球倒數第一　無解的難題. 2023.https://ec.ltn.com.tw/article/breakingnews/4507422. Accessed 30 Jan 2024

Ani. 2021. *Taiwan, Singapore resume military cooperation after long hiatus: Report*. https://www.business-standard.com/article/international/taiwan-singapore-resume-military-cooperation-after-long-hiatus-report-121121800093_1.html. Accessed 30 Jan 2024

DAPRA. 2018. DARPA tiles together a vision of mosaic warfare. *DAPRA*. https://www.darpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosiac-warfare. Accessed 30 Jan 2024

Fish, Tim. 2022. Uncrewed Ambitions of the Loyal Wingman. *Air Force Technology*. https://www.airforce-technology.com/features/uncrewed-ambitions-of-the-loyal-wingman/. Accessed 30 Jan 2024

Lee, His-min, et al. 2020. Taiwan's overall defense concept, explained. *The Diplomat*. https://thediplomat.com/2020/11/taiwans-overall-defense-concept-explained/. Accessed 30 Jan 2024

Liu, Da-Nien; Shih, Hui-Tzu. 2012. New Economic Development Opportunities for Taiwan in the Post-ECFA Era. *Center for Asian Studies, IFRI*. https://www.ifri.org/sites/default/files/atoms/files/av51complet.pdf. Accessed 30 Jan 2024

Losey, Stephen. 2022. How autonomous wingmen will help fighter pilots in the next war. *Defense News*. https://www.defensenews.com/air/2022/02/13/how-autonomous-wingmen-will-help-fighter-pilots-in-the-next-war/. Accessed 30 Jan 2024

Ministry of Economic Affairs. 2018. Unmanned vehicles technology innovative experimentation act. *Ministry of Economic Affairs*. https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0030147. Accessed 30 Jan 2024

Ministry of National Defense. 2021a. National Defense Review. *Ministry of National Defense*. https://www.mnd.gov.tw/NewUpload/%E6%AD%B7%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8%E7%B6%B2%E9%A0%81%E5%B0%88%E5%8D%80/%E6%AD%B7%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8%E5%B0%88%E5%8D%80.files/%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8-110/110%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8-%E8%8B%B1%E6%96%87%E7%89%88.pdf. Accessed 30 Jan 2024

———. 2021b. Quadrennial Defense Review. *Ministry of National Defense*. https://www.mnd.gov.tw/NewUpload/%e6%ad%b7%e5%b9%b4%e5%9c%8b%e9%98%b2%e5%a0%b1%e5%91%8a%e7%b8%bd%e6%aa%a2%e8%a8%8e(QDR)/%e6%ad%b7%e5%b9%b4%e5%9c%8b%e9%98%b2%e5%a0%b1%e5%91%8a%e7%b8%bd%e6%aa%a2%e8%a8%8e(QDR).files/%e6%ad%b7%e5%b9%b4%e5%9c%8b%e9%98%b2%e5%a0%b1%e5%91%8a%e7%b8%bd%e6%aa%a2%e8%a8%8e(QDR)-110/110%20QDR(%e8%8b%b1%e6%96%87%e6%ad%a3%e5%bc%8f%e7%89%88).pdf. Accessed 30 Jan 2024

Ministry of Science and Technology. 2020. 科技部徵求110年「學研中心」專案計畫，自即日起至109年12月15日止. *National Taipei University of Technology Office of Research and Development*. https://rnd.ntut.edu.tw/p/404-1042-104779.php?Lang=zh-tw. Accessed 30 Jan 2024

Mitre, Jim; Bajraktari, Ylber. 2023. These technologies could defeat China's missile barrage and defend Taiwan: Analysis. *The RAND Blog*. https://www.rand.org/pubs/commentary/2023/08/these-technologies-could-defeat-chinas-missile-barrage.html. Accessed 30 Jan 2024

Motley, Julie Obenauer. 2022. The testing and explainability challenge facing human-machine teaming. *Brookings*. https://www.brookings.edu/articles/the-testing-and-explainability-challenge-facing-human-machine-teaming/. Accessed 30 Jan 2024

National Defense Industry Development Foundation. n.d.. https://www.ndidf.org.tw/. Accessed 30 Jan 2024

National Development Council. 2021. 六大核心戰略產業推動方案. *National Development Council*. https://www.ndc.gov.tw/Content_List.aspx?n=9614A7C859796FFA. Accessed 30 Jan 2024

OECD. 2023. OECD Main science and technology indicators. *OECD*. https://www.oecd.org/sti/msti.htm. Accessed 30 Jan 2024

Serhan, Yasmeen. 2023. Audrey tang minister of digital affairs, Taiwan. *TIME Magazine*. https://time.com/collection/time100-ai/6308288/audrey-tang/. Accessed 30 Jan 2024

Ship and Ocean Institutes R&D Center. n.d.. https://www.soic.org.tw/. Accessed 30 Jan 2024

Thomas, William. 2023. FY23 Budget Outcomes: Department of Defense. *FYI Science Policy News*. https://ww2.aip.org/fyi/2023/fy23-budget-outcomes-department-defense#:~:text=The%20budget%20for%20the%20Department,over%20the%20past%20six%20years. Accessed 30 Jan 2024

Tucker, Patrick. 2020. An AI just beat a human F-16 pilot in a dogfight–Again. *Defense One*. https://www.defenseone.com/technology/2020/08/ai-just-beat-human-f-16-pilot-dogfight-again/167872/. Accessed 30 Jan 2024

中山大學. 2021. 智慧操控水下載具平台技術研發學研中心設置要點. 中山大學. https://ora.nsysu.edu.tw/static/file/45/1045/img/2721/845868214.pdf. Accessed 30 Jan 2024

中山新聞. 2021. 培育國防科技人才 中山大學成立「智慧操控水下載具學研中心」. 中山大學. https://news.nsysu.edu.tw/p/406-1120-267085,r2910.php?Lang=zh-tw. Accessed 30 Jan 2024

中興大學. 2021. 國防關鍵系統研究發展中心. 中興大學. https://secret.nchu.edu.tw/file-manager/02_admin/school_meet/94/94.pdf?_t=1626915054. Accessed 30 Jan 2024

中華民國空軍. 2018. 空軍任務. 中華民國空軍. https://air.mnd.gov.tw/TW/About/About_Detail.aspx?ID=3. Accessed 30 Jan 2024

中華民國陸軍. 2020. 人工智慧結合擴增實境的軍事應用專題講演. *Facebook*. https://www.facebook.com/ROC.armyhq/posts/3332539593460504/?paipv=0&eav=AfZGD7hSgkt8pMNxpWVZKr222J3i-pz3zFU7ZhnAz3uI5n3ujx62UyUa6xbW-D8iPAM&_rdr. Accessed 30 Jan 2024

主計處. n.d. 中央政府總預算及附屬單位預算. 主計處. https://www.dgbas.gov.tw/cp.aspx?n=3623&s=1208#Anchor_11333. Accessed 30 Jan 2024

呂雪彗. 2023. 因應地緣政治 賴清德主打五大信賴產業. 工商時報. https://tw.news.yahoo.com/%E5%9B%A0%E6%87%89%E5%9C%B0%E7%B7%A3%E6%94%BF%E6%B2%BB-%E8%B3%B4%E5%BE%B7%E4%B8%BB%E6%89%93%E4%BA%94%E5%A4%A7%E4%BF%A1%E8%B3%B4%E7%94%A2%E6%A5%AD-201000301.html. Accessed 30 Jan 2024

周昇煒. 2019. 國防部邀國網中心辦理AI發展講座 建構專業能量. 軍聞社. https://www.nchc.org.tw/Message/MessageView/3320?mid=46&page=1. Accessed 30 Jan 2024

國家中山科學研究院. n.d. 財務資. 中科院. https://www.ncsist.org.tw/csistdup/aboutus/page07.html. Accessed 30 Jan 2024

國立台灣大學. 2021. 國立臺灣大學國防科技學研中心設置要點. 國立台灣大學. https://ntuvp.ntu.edu.tw/centers/R50.pdf. Accessed 30 Jan 2024

國防大學理工學院. 2023. 歷史沿革. 國防大學理工學院. https://www.ccit.ndu.edu.tw/Unit/100023/24418. Accessed 30 Jan 2024

國防部. 2017. 106年國防報告書. 國防部. P. 165. https://www.mnd.gov.tw/PublishForReport.aspx?title=%E8%BB%8D%E4%BA%8B%E5%88%8A%E7%89%A9&Types=%E6%AD%B7%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8%E5%B0%88%E5%8D%80&SelectStyle=%E6%AD%B7%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8%E5%B0%88%E5%8D%80. Accessed 30 Jan 2024

———. 2021a. 110年國防報告書. 國防部. P. 129. https://www.mnd.gov.tw/PublishForReport.aspx?title=%E8%BB%8D%E4%BA%8B%E5%88%8A%E7%89%A9&Types=%E6%AD%B7%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8%E5%B0%88%E5%8D%80&SelectStyle=%E6%AD%B7%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8%E5%B0%88%E5%8D%80. Accessed 30 Jan 2024

———. 2021b. 110年國防報告書. 國防部. P. 178. https://www.mnd.gov.tw/PublishForReport.aspx?title=%E8%BB%8D%E4%BA%8B%E5%88%8A%E7%89%A9&Types=%E6%AD%B7%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8%E5%B0%88%E5%8D%80&SelectStyle=%E6%AD%B7%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8%E5%B0%88%E5%8D%80. Accessed 30 Jan 2024

———. 2022a. 國防部 112 年「國防先進科技研究計畫」評鑑實施計畫. 國防部. https://www2.nutn.edu.tw/randd/upload/120230619095859.pdf. Accessed 30 Jan 2024

———. 2022b. 國防部111年「國防先進科技研究計畫」申請書徵求主題一覽表(突破式國防科技研發計畫). 國防部. http://rdar.rdo.fju.edu.tw/sites/rdar.rdo.fju.edu.tw/files/%E5%BE%B5%E6%B1%82%E4%B8%BB%E9%A1%8C_0.pdf. Accessed 30 Jan 2024

———. 2022c. 國防部發布新聞稿說明行政院核列112年度國防部主管歲出預算. 國防部. https://www.mnd.gov.tw/Publish.aspx?p=80285&title=%E5%9C%8B%E9%98%B2%E6%B6%88%E6%81%AF&SelectStyle=%E6%96%B0%E8%81%9E%E7%A8%BF. Accessed 30 Jan 2024

國防部軍備局. 2023. 112年「國防先進科技研究計畫」構想書. *National Taiwan Normal University Office of Research and Development*. https://www.acad.ntnu.edu.tw/files/news/10962_ece636c6.pdf. Accessed 30 Jan 2024

張延廷. 2023. 國軍訓練 AI可代勞. 自由時報. https://www.chinatimes.com/opinion/20230805003387-262104?chdtv. Accessed 30 Jan 2024

張溎壕. 2023. 2023KIDE國際發明展 建國科大奪12獎!AI創新璀璨. 創新聞. https://n.yam.com/Article/20231213466388. Accessed 30 Jan 2024

張玲玲. 2023. 科技結合創新 建構智慧國防. *Youth Daily News*. https://www.ydn.com.tw/news/newsInsidePage?chapterID=1612391&type=forum. Accessed 30 Jan 2024

徐振威. 2018. 「故障預判」交給AI!導入航空發動機監控系統保飛安. 軍聞社. https://www.ettoday.net/news/20181031/1295089.htm. Accessed 30 Jan 2024

徐葳倫, 黃昭盛. 2021. 71年首次 空軍作戰指揮部"封洞"清消. 華視. https://news.cts.com.tw/cts/life/202106/202106142046050.html. Accessed 30 Jan 2024

成功大學. 2022. 國防關鍵系統研究發展中心. 成功大學. https://wtrc.web2.ncku.edu.tw/p/412-1177-25426.php?Lang=zh-tw. Accessed 30 Jan 2024

方志賢. 2022. 推動全民國防教育 AI無人機、無人車納入活動、模擬戰場實況. 自由時報. https://news.ltn.com.tw/news/life/breakingnews/3845885. Accessed 30 Jan 2024

朱明. 2021. 提升空軍防空飛彈攔截效能 「寰網」聯戰採以色列系統作為主要核心技術. *Up Media*. https://www.upmedia.mg/news_info.php?Type=1&SerialNo=132001. Accessed 30 Jan 2024

朱泓任. 2017. 臺灣AI元年 科技部5年160億打造AI新生. Newtalk新聞. https://newtalk.tw/news/view/2017-10-24/101480. Accessed 30 Jan 2024

李恬郁. 2019. 國軍後勤AI推手 原來是他!. *Youth Daily News*. https://tw.news.yahoo.com/%E9%9F%9C%E7%95%A5%E7%8B%80%E5%85%83-%E5%9C%8B%E8%BB%8D%E5%

BE%8C%E5%8B%A4ai%E6%8E%A8%E6%89%8B-%E5%8E%9F%E4%BE%86%E6%98%AF%E4%BB%96-160000438.html. Accessed 30 Jan 2024
林柏州. 2019.「智慧國防計畫」與國防科技機制發展. 國防安全雙週報. https://indsr.org.tw/respublicationcon?uid=12&resid=729&pid=2868. Accessed 30 Jan 2024
楊丞彧. 陳鈺馥. 2023. 中科院旋轉門疑慮 監院糾正國防部. 自由時報. https://news.ltn.com.tw/news/politics/paper/1606160. Accessed 30 Jan 2024
楊國文. 2022. 中科院爆集體貪污弊案 中校先收賄26萬才退伍. 自由時報. https://news.ltn.com.tw/news/society/breakingnews/4153805. Accessed 30 Jan 2024
楊孟臻. 2017. 資通電軍指揮部成立 蔡英文交付3項任務. *Up Media*. https://www.upmedia.mg/news_info.php?Type=24&SerialNo=19855. Accessed 30 Jan 2024
楊策淳. 劉律寬. 2020. 國軍戰術戰傷救護模擬訓練之成效分析與鏈結AI人工智慧發展. 陸軍後勤季刊109年第二輯. https://www.airitilibrary.com/Article/Detail/P20230131001-N202303040016-00002. Accessed 30 Jan 2024
機構系統開發. 陸軍飛彈光電基地勤務廠. n.d.. https://ord.nccu.edu.tw/download.php?filename=1471_1ade29f6.pdf&dir=rd_research&title=%E7%A0%94%E7%A9%B6%E8%A8%88%E7%95%AB%E6%A7%8B%E6%83%B3%E6%9B%B8. Accessed 30 Jan 2024
涂鉅旻. 2019. 中科院推智慧國防10年計畫. 自由時報. https://news.ltn.com.tw/news/politics/paper/1314948. Accessed 30 Jan 2024
清華大學. 2021. 清華大學國防科技學研中心. 清華大學. https://dod.site.nthu.edu.tw/. Accessed 30 Jan 2024
王儷華. 2023. 防止人類生存被威脅台灣將推AI基本法，會如何監管?. *Commonwealth Magazine*. https://www.cw.com.tw/article/5128521. Accessed 30 Jan 2024
科技部. 2019. 人工智慧科研發展指引. 科技部. https://www.nstc.gov.tw/nstc/attachments/53491881-eb0d-443f-9169-1f434f7d33c7. Accessed 30 Jan 2024
———. 2022. 111 年度科技部「國防科技探索專案計畫」徵求公告. 國科會. https://www.nstc.gov.tw/nstc/attachments/5a383553-47a2-481e-9194-f8ebd0573304. Accessed 30 Jan 2024
科技部工程司. 2022. 國防科技探索專案公告說明會. 科技部. http://www.etop.org.tw/index.php?d=epp&c=epp12911&m=download_attachment&post_id=1412&id=1209. Accessed 30 Jan 2024
范正祥. 2023. 落實國防自主政策 中科院預算連續兩年破千億. 中央社. https://www.cna.com.tw/news/aipl/202309160112.aspx. Accessed 30 Jan 2024
范瑜. 2023. 國醫、三總攜手廣達 打造心電圖AI判讀平臺. *Youth Daily News*. https://www.ydn.com.tw/news/newsInsidePage?chapterID=1604491. Accessed 30 Jan 2024
蕭佳宜. 2023. 管理學院科技教學 深化國軍訓練效能. *Youth Daily News*. https://www.ydn.com.tw/news/newsInsidePage?chapterID=1574154. Accessed 30 Jan 2024
蘇思云. 2020. 培育7大領域科研人才 科技部攜手國防部5年砸50億. 中央社. https://www.cna.com.tw/news/ait/202012160073.aspx. Accessed 30 Jan 2024
蘇恩民. 2023. 失控主持人1 國安危機!50億軍武科技研發保防破大洞?. 民視新聞網. https://tw.news.yahoo.com/%E7%8D%A8%E5%AE%B6-%E5%A4%B1%E6%8E%A7%E4%B8%BB%E6%8C%81%E4%BA%BA1-%E5%9C%8B%E5%AE%89%E5%8D%B1%E6%A9%9F-50%E5%84%84%E8%BB%8D%E6%AD%A6%E7%A7%91%E6%8A%80%E7%A0%94%E7%99%BC%E4%BF%9D%E9%98%B2%E7%A0%B4%E5%A4%A7%E6%B4%9E-192749192.html. Accessed 30 Jan 2024
行政院. 2019. 台灣AI行動計畫—掌握契機，全面啟動產業AI化. 行政院. https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/a8ec407c-6154-4c14-8f1e-d494ec2dbf23. Accessed 30 Jan 2024
行政院主計總處. 2023. 國民所得重要指標. 經濟統計數據分析統. https://dmz26.moea.gov.tw/GA/common/Common.aspx. Accessed 30 Jan 2024
行政院國家科學委員會. 2013. 國家科學技術發展計畫 (民國 102 年至 105 年). 行政院國家科學委員會. https://www.nstc.gov.tw/nstc/attachments/4b27e75d-7fa3-4ff9-879b-8329e06ff83f. Accessed 30 Jan 2024

許劍虹. 2023. 許劍虹觀點:重空軍而輕海軍的蔣中正. 風傳媒. https://www.storm.mg/article/4899570. Accessed 30 Jan 2024
賴品瑀. 2023. 整合科技研發與作戰運用 智慧國防十年計畫促臺灣成世界核心. 智慧國家. https://2030.tw/article/Digital-Strategy-for-Defence-033-Fiber-Li. Accessed 30 Jan 2024
陳建源. 2018. 「人工智慧AI」無人艦艇軍事倫理問題初探. 海軍學術雙月刊第五十二卷第四期. https://navy.mnd.gov.tw/Files/Paper/2-%E4%BA%BA%E5%B7%A5%E6%99%BA%E6%85%A7%EF%BC%A1%EF%BC%A9.pdf. Accessed 30 Jan 2024
陳穎信. 戴明正. 許秀珠. 程學儒. 2020. 建構MR心肺復甦術+AED教學系統. 財團法人生技醫療科技政策研究中心. https://innoaward.taiwan-healthcare.org/award_detail.php?REFDOCTYPID=0mge2rck644mcfl0&num=1&REFDOCID=0qls4a5ph377cqqq. Accessed 30 Jan 2024
陳鈺馥. 2023. 國軍運用AI 發展不對稱戰力. 自由時報. https://news.ltn.com.tw/news/politics/paper/1604187. Accessed 30 Jan 2024
陽明交通大學. 2021. 前瞻科技與系統學術研究中心. 陽明交通大學. https://fsc.nycu.edu.tw/. Accessed 30 Jan 2024

Reimagining Defense Innovation: Defense AI in Singapore

Michael Raska

This chapter provides brief contours of conceptual, organizational, and technological developments of AI intertwined within Singapore's defense and military innovation paths. It starts by outlining Singapore's evolving approach to AI and emerging technologies as a dynamic confluence of strategic, technological, ethical, and defense policy drivers in a much broader and comprehensive civil-military framework, which aims to balance AI-driven tech innovation, organizational agility, economic and defense capability development while adhering to responsible AI governance policies. As AI gradually permeates Singapore's multilayered 'Total Defense' strategy, including its Military Defense pillar, Singapore's thinking about defense AI is driven through broader technological innovation and defense management imperatives, not only in meeting the Singapore Armed Forces (SAF) operational requirements but, perhaps more importantly, sustainment of these technologies and capabilities in synergistic applications within Singapore's civil-military innovation ecosystem. Taken together, military AI development can be seen in Singapore's indicative desire to maintain its qualitative "strategic edge" or credible deterrence, defense capacity, and resilience amidts progressive complexity of security challenges of the twenty-first century and technological disruptions, while mitigating internal socio-economic constraints and resource limitations. In the process, the development of AI in defense is conditioned by defense policy imperatives for responsible innovation and AI governance—pursuing a multilateral, risk-based, and human-centric approach toward responsible, reliable, robust, and safe AI in defense innovation and military use.

The second part of the chapter then highlights Singapore's development approaches and methods to AI in defense. Specifically, its highlights the evolving 'Ops-Tech' model of defense innovation, which focuses on deep operational

M. Raska (✉)
S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Nanyang, Singapore
e-mail: ismraska@ntu.edu.sg

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_25

understanding, technological expertise, and collaborative connections among various actors in Singapore's defense ecosystem. Key drivers for Singapore's defense AI include organizational aspects such as collaborative defense networks involving the military, government agencies, and increasingly private tech companies and start-ups sharing data and best practices to tackle Singapore's complex security challenges and risks in innovative ways.

The final section of the chapter assesses Singapore's implementation of AI-oriented defense and military innovation. It delves into specific examples of SAF's digitization, robotization, and sensor revolution in the context of the SAF 2040 transformation, and the recent establishment of the Digital and Intelligence Service (DIS)—a fourth service of the SAF on par with the Army, Navy, and Air Force. The implementation of the AI-driven SAF 2040 effectively signifies a major military shift as it opens new strategic and operational frontiers for the SAF with concomitant opportunities, risks, and challenges. Ultimately, one could argue that diffusion of the AI wave in Singapore's security and defense is reaching a tipping point, in which emerging technologies are re-making Singapore's entire defense ecosystem.

Prior to the analysis, it's important to note a caveat. Except for Singapore's National Artificial Intelligence Strategy 2.0 (2023), which focuses on Singapore's AI development in civilian arenas, there hasn't been an official document to date providing a comprehensive and detailed view of Singapore's defense or military AI strategy, budgeting and resource allocation,[1] military-technological priorities, defense innovation ecosystem, military-tech governance, and private-sector partnerships. Indeed, much of the data on Singapore's AI defense programs, initiatives and trajectories, including funding details, remains classified. Despite the veil of secrecy, however, the trajectory of military AI in Singapore transcends purely military-technological and defense-organizational domains—it must be situated in the broader context of strategic nexus of Singapore's external foreign/defense and internal public policies that have shaped Singapore's technological and socio-economic development. Nevertheless, it is still possible to 'connect the dots' on Singapore's evolving strategic thinking, trajectory, and implementation of military AI using publicly available data such as statements, speeches, interviews, and press releases of the Ministry of Defense (MINDEF), SAF, Defense Science and Technology Agency (DSTA), and other government agencies as primary authoritative sources.

[1] This chapter does not discuss the funding dimension due to the lack of publicly available information.

1 Thinking About Defense AI

Singapore's strategic rationale for developing AI in defense and military innovation stems from a complex interplay of strategic considerations, driven by its unique circumstances and national security concerns. These begin with Singapore's perennial geostrategic constants: historical experience of vulnerability, lack of strategic depth, limited resources, and asymmetries in demography, which stipulate the need to keep Singapore's military as high-tech as possible—maintaining a qualitative 'strategic edge' to ensure credible deterrence, defense, and resilience (Raska 2016: 146). This enduring rationale is apparent when considering 'disruptive' convergence of contending geopolitics and military-technological arms competition in the Indo-Pacific over the past decade, as well as internal factors such as increasing demographic constraints, and socio-economic growth imperatives (Loo 2015). At the same time, however, the diffusion of Singapore's defense AI must be situated in a much broader and comprehensive civil-military framework, which balances AI-driven tech innovation, organizational agility, and operational security under evolving policies of responsible AI governance (Harjani et al. 2020). Therefore, thinking about defense AI in Singapore's strategic context must begin with its civilian 'AI strategy' roadmap, and recently published National Artificial Intelligence Strategy (NAIS 2.0)—and then projecting its applicability into the defense and military domain, particularly the evolving 'Total Defense' (TD) strategic concept, and its military applications.

1.1 Singapore's Evolving AI Strategies

In December 2023, Singapore unveiled an updated version of its National Artificial Intelligence Strategy (NAIS 2.0)—reflecting Singapore's commitment to become a global leader in the responsible and innovative use of AI, while providing a whole-of-government roadmap to accelerate AI adoption to unlock its economic and social benefits (Smart Nation Singapore 2023). While the NAIS 2.0 does not focus on AI in defense per se, it demonstrates Singapore's strategic thought on AI—an adaptive approach to AI-driven technological innovation, balancing rapid advancements in technology with responsible implementation. The NAIS 2.0 is also product of a decade-long evolution of AI research, development, and collaborations between industry, academia, and government, driving progress in AI-related fields in Singapore (Chia 2023b). From the early foundations of the Smart Nation concept in 2014 (Lee 2014), to the first AI Strategy—A National Roadmap in 2019, Singapore has pursued a comprehensive approach to AI adoption across its civilian sectors, from healthcare to finance. In the process, the evolving strategic roadmap established active testbed platforms for National AI Projects, including the development of AI workforce and computational resources with over 150 research and development teams, and 900 startups established since 2019 (Chia 2023a).

With the technological acceleration and exponential advancements in AI capabilities over the past 5 years, Singapore updated the strategy in 2023. It aims to build a trusted and responsible AI ecosystem, driving innovation and growth through AI, and empowering people and business to understand and engage with AI. Specifically, the strategy seeks to attract more international companies and talent to transform Singapore into an AI research hub by increasing research funding and creating a regulatory environment conducive to innovation. With five actions across three system areas and ten enablers, the NAIS 2.0 represents a strategic maturation of AI-thought in Singapore regarding responsible innovation, AI ethics, trustworthiness, and inclusive benefits. Moreover, the strategy is dynamic—it anticipates continuous updates and refinements to keep pace with evolving AI technologies (Tham 2023).

Parallel with NAIS 2.0, Singapore has focused on developing a new governance framework for generative AI—the Model AI Governance Framework for Generative AI (MGF-GenAI), with an initial draft presented in January 2024 at the World Economic Forum in Davos, Switzerland (Table 1). The MGF-GenAI, developed by the AI Verify Foundation and Singapore's Infocomm Media Development Authority, seeks to develop a comprehensive and trusted AI ecosystem, and serve as a toolkit for addressing global risks associated with the use of generative AI—i.e. providing guidance on the safety evaluation and testing of GenAI models (IMDA 2024). By presenting the MGF-GenAI model, Singapore supports international engagement and cooperation in regulating and researching GenAI, in addition to other multilateral and avenues such as at the Global Partnership on Artificial Intelligence, and bilateral cooperation efforts such as alignment with the US' AI Risk Management Framework (Goh 2024). While neither the NAIS 2.0 nor MGF-GenAI have a dedicated section on military AI, both indirectly yet profoundly influence the future of defense AI in Singapore—through their principles and strategic directions.

1.2 Integrating AI in Singapore's 'Total Defense' Strategy

The overarching philosophy of AI governance embedded in the NAIS 2.0 and MGF-GenAI –ethical and responsible AI, explainability and transparency, collaboration and inclusivity, and human-centric-AI—has significant implications for the direction and character of AI strategic thought, particularly in the context of integrating AI into Singapore's TD strategy, organizational structures, technological capabilities.

The TD strategy (Table 2), introduced in 1984, aims to unite all sectors of society—government, business, and people—to sustain Singapore's resolve, unity, and defense capabilities (MINDEF 1995: 1). Initially consisting of five and now six interdependent defense pillars –military, civil, economic, social, psychological, and digital—TD has evolved over the past four decades and essentially became a symbol of Singapore's security identity, resilience, and adaptability. Indeed, Singapore's conceptions of defense reflect a continuity and change in adapting the TD strategy

Table 1 Model AI governance framework for generative AI (MGF-GenAI)

Pillar	Description	Key Focus Areas
Accountability	Putting in place the right incentive structure for different players in the AI system development life cycle to be responsible to end-users	Developer transparency—Deployer due diligence—Ethical user practices
Data responsibility	Ensuring data quality and addressing potentially contentious training data in a pragmatic way	Transparency about data sources—Bias recognition & mitigation—Data governance controls
Trusted Development & Deployment	Enhancing transparency around baseline safety and hygiene measures based on industry best practices	Model testing & validation—External audits & certification—Deployment safety
Incident reporting	Implementing an incident management system for timely notification, remediation, and improvement	Unified reporting channels—Data-driven improvement—Timely mitigation & notification
Testing & Assurance	Providing external validation and added trust through third-party testing and developing common AI testing standards	Standardized evaluation benchmarks -addressing the 'black box' challenge - Verification as an industry
Security	Addressing new threat vectors that arise through GenAI models	Safeguarding against adversarial inputs—Deepfake Detection & Countermeasures - Cybersecurity best practices
Content provenance	Transparency about where content comes from as useful signals for end-users	Digital watermarks—Metadata standards—Transparency of Provenance
Safety & Alignment (R&D focus)	Accelerating R&D through global cooperation among AI safety institutes to improve model alignment with human intention and values	Aligning values with model decisions—Explainability & Human Oversight—Bias minimization
AI for public good	Harnessing AI to benefit the public by democratizing access	Improving public sector adoption—Upskilling workers—Developing AI systems sustainably

Source: Author's overview based on the MGF-FenAI Framework, IMDA Press Release (2024)

to evolving geostrategic, political, economic, technological, and socio-economic challenges (Zachariah 2023). Accordingly, one could argue that the diffusion of AI coupled with disruptive impact of emerging technologies is revamping Singapore's approaches to TD, presenting both opportunities and challenges. In 2022, for example, MINDEF launched a TD review, including the 'Total Defense Sandbox' ground-up initiative aimed to test new ideas, projects, prototypes, and potential solutions for current and potential future challenges such as AI-enabled cyber threats (MINDEF 2022a, b, c).

The diffusion of AI-driven technological innovation is gradually permeating into each pillar of Singapore's evolving TD concepts, organizations, and capabilities. On

Table 2 Overview of Singapore's total defense strategy

Pillar	Description
Military defense	Deterring aggression and defending Singapore with a strong and modernized Singapore armed forces (SAF).
Civil defense	Ensuring that life can continue as normally as possible during crisis situations through civilian training and organization with entities like the Singapore civil defense force (SCDF).
Economic defense	Maintaining a robust and adaptable economy in the face of challenges to support all other defense efforts and keep the nation stable.
Social defense	Creating a united and resilient population where Singaporeans of all backgrounds feel committed to the defense and shared future of the nation.
Digital defense	Protecting Singapore's cybersecurity and countering threats within the digital domain against infrastructure, networks, and information.
Psychological defense	Building a strong national identity, shared values, and the will to stand firm against internal or external attempts to divide and destabilize the nation.

Source: Author's overview based on MINDEF (1995)

the one hand, AI promises to enhance Singapore's multi-faceted approach to security and defense, strategically strengthening the resilience of each pillar. Yet, at the same time, the development and integration of AI brings a range of risks, vulnerabilities, and uncertainties. Accordingly, thinking about AI in Singapore's defense context arguably reflects a continuous balancing between technological innovation, organizational agility, resource efficiency, and security of each TD pillar (Matthews and Fitriani 2023). Navigating this 'problematique' can be seen in Table 3, which outlines illustrative promises and perils of AI in TD.

1.3 AI in Military Defense

By charting the evolving AI impact on the broader TD concept, it is possible to understand the strategic rationale for pursuing AI in Singapore's 'Military Defense' pillar, namely through three mutually supporting functions: (1) AI as intelligence enabler, (2) technology disruptor and force multiplier, and (3) defense diplomacy anchor. In doing so, Singapore is pursuing AI in defense in conjunction with other emerging technologies as a way to mitigate adverse effects of external geopolitical, technological, and internal demographic disruptions of the 21st century.

1.4 AI as Intelligence Enabler

Each pillar in TD, including Military Defense, embraces the need for long-term strategic foresight and intelligence—a combination of long-term horizon scanning risk/net assessment methodologies –, which is now increasingly augmented by

Table 3 AI opportunities and risks in Singapore's total defense strategy

Pillar	AI Opportunities	AI Risks
Military defense	Enhanced intelligence gathering and analysis—improved battlefield decision-making—development of autonomous defense systems—more efficient resource allocation	Ethical dilemmas surrounding autonomous weapons—vulnerability to cyberattacks—risk of escalation due to rapid AI decision-making
Civil defense	Predictive analytics for disaster response—improved resource allocation in emergencies—enhanced surveillance systems for homeland security—automated threat detection and response	Privacy concerns related to AI-powered surveillance—bias in AI-based decision-making—vulnerability of critical infrastructure to AI attacks
Economic defense	Increased innovation and productivity—enhanced cybersecurity for critical infrastructure—development of new AI-powered products and services—improved competitiveness in the global AI race	Job displacement due to automation—global competition in AI development—disruption of supply chains
Social defense	Countering misinformation campaigns—promoting social cohesion and understanding—personalization of social services—improved public engagement and communication	Spread of deepfakes and disinformation—algorithmic bias and filter bubbles—impact on human interaction and social bonds
Digital defense	Enhanced cybersecurity capabilities—more efficient detection and response to cyber threats—improved data security and privacy—development of new cyber defense technologies	Sophisticated cyber threats—disinformation campaigns and social engineering—data privacy risks
Psychological defense	Strengthening national resilience—countering psychological manipulation—promoting mental health and Well-being—building trust and confidence in institutions	Fear and uncertainty about the future manipulation of individuals and communities—erosion of trust in institutions

Source: Author's overview

AI-enabled data collection, processing, and analysis. The aim is to identify and monitor potential threats or disruptions and deliver potential solutions and policy options in advance of need. For example, in military and economic defense, Singapore's national security is not threatened as much by a single country, but by a disruption of commerce (Huxley 2000).

The potential risks become apparent when noting Singapore's geostrategic disposition. Singapore is a small island city-state of 719 square km—the smallest state in Southeast Asia. Its geographic location at the southern end of the Straits of Malacca crosses some of the most important Sea Lines of Communication (SLOCs) in the world, linking the Indian Ocean and the Pacific Ocean, which carry a major portion of the world's trade. The Malacca and Singapore Straits carry more than 40% of the world's commerce, half of the world's oil and 80% of oil bound for China and Japan (Maritime Executive 2018). Strategically, Singapore's position

coupled with its deep natural harbor provides a hub for maritime trade in Southeast Asia, connecting trade routes between Asia, Europe, America, and the Middle East, significantly contributing to Singapore's socio-economic prosperity. Accordingly, Singapore's strategic location and absence of natural resources amplify its extreme dependency on the outside world, which requires the need for early warning, timely intelligence analysis, and persistent situational awareness of external environment.

Therefore, Singapore sees the integration of AI systems and machine-learning algorithms as an intelligence enabler for processing vast amounts of data—determining who needs what and when, in predictive analysis—identifying indicators to events rather than the events themselves (Chia 2018). Singapore's government has dedicated units for scenario planning, horizon scanning, and threat anticipation, which are integrating diverse functional expertise, including AI systems and machine learning models for data fusion and analysis – making sense of massive amounts of structured and unstructured data from diverse sources, and integrating multiple intelligence streams using AI-powered data fusion techniques, natural language processing algorithms, and AI orchestration tools. Indeed, nearly all strategically significant agencies, including MINDEF with its Security and Intelligence Division (SID), have dedicated foresight teams. For example, the Centre for Strategic Futures—a Strategy Group in the Prime Minister's Office, provides the highest levels of Singapore government with the ability to "navigate emerging strategic challenges and harness potential opportunities" in multiple ways: building capacity and providing strategic foresight and risk management by training public servants; doing strategic foresight work—gathering insights on emerging trends and identifying signals of change; and by communicating and disseminating insights to decision- and policymakers across all of government (CSF 2023).

1.5 AI as Force Multiplier

AI technologies in Singapore's military defense coupled with the development and integration of unmanned systems, are seen as robust force multipliers for the SAF (Koh 2021). By combining AI-systems, cloud, and data science, automating tasks, improving decision-making, and maximizing the effectiveness of its small but well-trained force, the SAF can be better equipped to carry out their multifaceted missions (Table 4). This becomes apparent when considering Singapore's geostrategic asymmetries and resource constraints, which amplify the principal challenge for Singapore's defense planners: how to translate Singapore's limited resources of a small island nation into an effective defense capability amid the progressive range and complexity of security challenges (Raska 2021).

Singapore's defense planning projections have been shifting over the past decade by the confluence of multiple 'disruptive' strategic challenges and uncertainties. There are at least three mutually integrated 'disruptive' vectors:

Table 4 AI as force multiplier for the SAF

Area of Application	Description
Enhanced Situational Awareness & Decision-Making	AI-powered tools analyze large amounts of data (sensor streams, intelligence reports) in real-time, aiding commanders in rapid and informed decision-making on the battlefield.
Logistics and supply chain optimization	AI algorithms predict equipment maintenance needs, optimize resource allocation, and streamline supply lines, ensuring operational efficiency.
Cybersecurity and defense	AI can play a crucial role in advanced threat detection, vulnerability analysis, and the development of countermeasures in the increasingly complex cyber domain.
Autonomous systems	While likely regulated with extra careful consideration, AI could enable autonomous or semi-autonomous systems for tasks like surveillance, reconnaissance, and potentially future combat support roles.
Simulation and training	AI can revolutionize military training by creating highly realistic simulated environments and personalized training programs to enhance the readiness of soldiers.

Source: Author's overview

- Changing geopolitics prompting the need to plan for attendant consequences of growing Sino-U.S. strategic competition in the Indo-Pacific.
- Regional disparities in addressing unresolved historical legacies and tensions surrounding critically important geopolitical hotspots such as Taiwan, Korean Peninsula, and the South China Sea.
- The diffusion of emerging technologies as power projection capabilities in the region and resulting changes in the character of warfare, including the rise of cyber-enabled information/hybrid conflicts.

As a result of the increasing convergence of 'old' and 'new' security threats, Singapore faces a competing strategic landscape and relative uncertainty about which types of adversaries and contingencies will be the most consequential. From terrorism to responding to Sino-U.S. strategic competition, the SAF faces competing operational requirements, which are likely to increase further. If so, Singapore's defense planners must answer anew how the SAF should build a force and doctrine capable of dealing simultaneously with current security threats while anticipating future challenges.

This includes internal demographic and population constraints, reflecting continuous low-level birthrates, an ageing population, and a smaller talent pool. In 2022, Singapore's birth rate reached a record low of 1.05 (Ng 2023). If this trend continues, the SAF's manpower supply for its National Service (NS)—mandatory conscription—is projected to decrease by one-third by 2030 (Kor 2017). Consequently, the SAF 2040, a strategic blueprint for SAF force transformation in the twenty-first century, entails comprehensive AI adoption and adaptation in nearly all aspects of defense planning and military operations as force multipliers to amplify existing defense capabilities, while generating novel capabilities (Cheng 2016; MINDEF 2023a).

1.6 AI Governance as Defense Diplomacy Anchor

The diffusion of AI in Singapore's military is not only primarily about technology and military capability to ensure its strategic edge for deterrence, but also about the need to pursue defense diplomacy focusing on the need for responsible development and use of AI in the military domain. In a 2009 lecture on the "Fundamentals of Singapore's Foreign Policy: Then & Now" at the Ministry of Foreign Affairs' Diplomatic Academy, Singapore's founding Prime Minister Lee Kuan Yew explained the rationale for Singapore's approach to diplomacy in general, which might also explain the importance of Singapore's defense diplomacy:

> (A) small country must seek a maximum number of friends while maintaining the freedom to be itself as a sovereign and independent nation. Both parts of the equation—a maximum number of friends and freedom to be ourselves—are equally important and inter-related. (To achieve this), we must make ourselves relevant so that other countries have an interest in our continued survival and prosperity as a sovereign and independent nation; we must be different from others in our neighborhood and have a competitive edge. Because we have been able to do so, Singapore has risen over our geographical and resource constraints, and has been accepted as a serious player in regional and international fora (Lee 2009).

Singapore's defense diplomacy portfolio is broad and involves close and friendly ties with many of the armed forces of Association of Southeast Asian Nations (ASEAN) countries, bilateral defense relations with countries in the wider Asia-Pacific region, including the U.S., China, Japan, South Korea, New Zealand, and India, and friendly ties with armed forces in Europe, Africa, and the Middle East (MINDEF 2021a). Historically, defense diplomacy has enabled the SAF to overcome the limitations of Singapore's land and airspace. Various units of the SAF, predominantly the Army and Air Force, have maintained long-term training detachments overseas in friendly countries, including Australia, Brunei, France, Germany, New Zealand, Thailand, Taiwan, the United States, and other states. SAF's overseas training exercises and presence provide various benefits—from acquiring diverse training experiences, operational readiness, and accelerated technological assimilation to benchmarking SAF's abilities against more capable militaries and building sustained defense diplomacy that supports Singapore's long-term strategic interests (MINDEF 2018a).

Similarly, regarding AI, Singapore approaches defense diplomacy through a multi-pronged strategy, recognizing the interconnected nature of technological progress, responsible adoption, and collaboration both regionally and globally. Specifically, the Defense Policy Group (DPG) under MINDEF, which includes Defense Policy Office (DPO) with the Strategy and Futures Group (SFG), actively engage in international forums and dialogues on AI in defense, such as those at the United Nations and ASEAN forums, including representation at the OECD Network of Experts on AI, Global Partnership on AI, AI Partnership for Defense, and REAIM (Responsible AI in Military domain) process. In the process, Singapore advocates for a collaborative, risk-based approach to ethical and responsible AI development and deployment in military domain.

In this context, Singapore has pursued collaborative partnerships with major AI powers, including the U.S., France, Australia, and others. For example, in 2023, SG MINDEF and France's Ministry of the Armed Forces (MOAF) signed an agreement to establish a Joint Research & Development Laboratory (Joint Lab) to develop AI capabilities. Similarly, as part of the 2023 "US-Singapore Critical and Emerging Technology Dialogue", Singapore's MINDEF and the US Department of Defense (DoD) Defense Innovation Unit (DIU) agreed to formalize a partnership to accelerate the use of commercial and dual-use technologies such as autonomy, digital technologies, and AI, and strengthen integration of both countries defense innovation ecosystems. By fostering strategic partnerships with key regional and global partners for AI, Singapore is able to contribute to the development of global norms on AI governance. In 2021, Singapore's MINDEF established Singapore's preliminary guiding principles for AI governance in defense innovation and military use as depicted in Table 5. While these principles inherently shape the direction and character for AI research and development (R&D) and deployment in Singapore's defense technology community, they also serve as an anchor for promoting Singapore's AI defense diplomacy and strategy - advocating for responsible, safe, reliable, and robust development and use of AI in security and defense.

Table 5 Singapore's preliminary guiding principles for defense AI (2021)

Principle	Description	Risk-mitigation Example
Responsible	AI technologies in the defense sector must have well-defined objectives, aligned with law and ethical principles.	AI in target selection must adhere to clear criteria, with decisions ultimately subject to human authorization.
Safe	Defense AI systems must be rigorously tested to ensure reliability while mitigating potential safety risks.	Predictive maintenance AI needs high performance benchmarks to prevent unexpected equipment failures.
Reliable	Strict regulations for AI in defense, clear lines of responsibility for actions, and a focus on human oversight in critical decisions.	Autonomous systems require well-documented decisions and approval processes by authorized personnel.
Robust	Defense AI systems should withstand attempts at manipulation, continue to function under pressure, and adapt to changing circumstances.	AI for cyber threat detection needs strong defenses against attempts to trick or disable it.

Source: Author's overview based on DSTA Singapore Defence Technology Summit Opening Speech by Minister for Defence Dr. Ng Eng Hen (MINDEF 2021b)

2 Developing Defense AI

The development of defense AI in Singapore's defense ecosystem proceeds along multiple paths simultaneously (Table 6)- including: (1) technological capability development - i.e. AI as intelligence enabler and force multiplier; (2) organizational changes – restructuring of services and units to enhance organizational agility and adaptability to absorb emerging technologies, including AI; (3) talent development – investing in training programs and talent acquisition strategies to equip SAF personnel with the necessary skills for future operations; and (4) international collaboration and defense diplomacy – engaging in technology partnerships with other nations. At the strategic level, Singapore's MINDEF employs a multi-year

Table 6 Conceptualizing Singapore's AI-driven defense innovation

Strategic Focus	Examples	Potential Implementation
Enhancing situational awareness	Real-time data analysis for threat assessment	Data fusion across multiple sensors (satellite imagery, radar, etc.), real-time monitoring of troop movements, predictive threat modelling
Command and control optimization	AI-assisted decision support tools	Recommendation systems and optimized resource allocation, intelligent risk assessment, and scenario analysis
Defense logistics	Predictive maintenance and supply chain management	Analysis of equipment logs and sensor data for failure prediction, AI-based demand forecasting, automated inventory management
Cybersecurity and Network defense	Vulnerability analysis and intrusion detection systems	AI-powered network activity monitoring, identification of anomalous patterns, dynamic cyber threat response
Public Communication & Engagement	AI-driven public sentiment analysis	Social media monitoring for understanding public concerns, proactive crisis communication management
Internal operations optimization	Automation of administrative tasks	Intelligent processing of paperwork and logistics requests, streamlining HR processes
Human resource development	Personalized training and development programs	AI-assisted performance assessments, individual skill gap identification, tailored learning programs and simulations
Intelligence analysis	Image and signals processing for target identification	Data-driven recommendations and situational awareness enhancement
Autonomous systems	Research on AI-enabled decision-making for drones and unmanned vehicles	Reinforcement learning, sensor fusion, path planning, decision-making AI
Simulation and training	AI-powered realistic training scenarios and adaptive instruction	Generative adversarial networks (GANs), reinforcement learning, computer vision, procedural generation

Source: Author's overview based on publicly available information on DSTA website and MINDEF(MINDEF 2021c, d, e, f, 2022b, 2023a)

capability planning framework for the SAF. This includes multi-year strategic plans that define the direction and character of the SAF's military modernization, such as the 'SAF 2040' roadmap and its capability requirements, technological acquisition priorities, and overall military modernization trajectories—including the development of AI systems and technologies. In parallel, the SAF develops specific operational concepts and master plans, which are classified (MINDEF 2023b). According to MINDEF, the design of operational concepts is mostly service driven, while the varying operational master plans and engineering master plans identify required system architectures and technologies for specific capability development such as AI.

The purpose of the master plans is to ensure that Singapore's defense capabilities not only meet future user requirements for the SAF but can also be sustained in the long term through 'cost-effective' defense management and 'adaptive' systems integration (DSTA 2016). While specific details remain confidential, MINDEF releases factsheets and provides occasional media briefings that offer a glimpse into its priorities, programs, and initiatives. Perhaps the most detailed authoritative source of SAF's military modernization are annual statements from the Singapore Parliament Committee of Supply Debates, which outline SAF's focus areas and resource allocation imperatives. For example, the integration of AI, cyber defense, and unmanned systems in the SAF; continued modernization of the SAF's Land, Sea, and Air Forces including the acquisition of F-35B fighter jets and Archer artillery systems; promoting interoperability through enhanced training and exercises to hone operational readiness; and ongoing collaboration with international partners and joint exercises to counter diverse security challenges (MINDEF 2023c).

Another core feature of Singapore's AI development in defense is a focus on indigenous defense innovation and its civil-military integration through a collaborative framework of 'Ops-Tech' approach—integrate operations (Ops) with technology (Tech) across all pillars of national security, including military defense (MINDEF 2023b).

The idea is to combine a deep operational understanding, technological expertise, and collaborative culture between the varying actors in Singapore's 'defense ecosystem'—the users (SAF), developers (MINDEF, DSTA, DSO dual-use R&D labs, defense research institutes like Temasek Labs, start-ups), and producers (local defense industries such as ST Engineering) as well as Singapore's select foreign strategic partners. The goal of the broader Defense Technology Community (DTC) is a spiral development of technological capabilities, including AI systems, and tailored solutions that would integrate select AI technologies into existing platforms and systems or newly acquired equipment (MINDEF 2023b). In turn, the SAF then provides feedback loops on their performance validation and verification, system safety, reliability and maintainability, logistic support, and other factors. In doing so, however, Ops-Tech development in the DTC is not only about a joint approach to technology innovation and meeting SAF-user requirements but also about the sustainment these technologies and capabilities—in creating synergistic applications for defense within the ecosystem (DSTA 2016). Recent examples of Singapore's AI-Ops-Tech development include (MINDEF 2022b):

- AI-enabled Command and Control Information System (CCIS), a high-tech command post that uses AI to process and analyze intelligence data in real-time, while providing automatic target detection and classification to provide commanders with a real-time, situation picture of deployed sensors, assets, and the disposition of adversary forces on the battlefield.
- ARTEMIS (Army Tactical Engagement and Information System) battle management system.
- Modification and integration of diverse drones for reconnaissance, surveillance, and target acquisition such as Veloce 15 mini-Unmanned Aerial Vehicles—the first locally developed hybrid Vertical Take Off and Landing (VTOL) Fixed-Wing system, for the Army to use for its Intelligence, Surveillance and Reconnaissance (ISR).
- DSTA Maritime Security Unmanned Surface Vessel (USV).
- DSO Autonomous underwater vehicle Meredith-400 for seabed surveillance.
- DSO AI tools to detect cyber threats and deepfakes.

3 Organizing Defense AI

Within the MINDEF, the control tower for the research and development (R&D) of advanced technologies, including AI capabilities, is the Defense Tech Group (DTG). Established in 1986, the DTG's key functions include facilitating cutting-edge research on areas such as AI, robotics, unmanned vehicles, cyber security, and advanced materials; collaborating with academia and industry—partnering with universities, research institutes and private companies, including start-ups to leverage expertise and accelerate technology development; supporting technology acquisition and integration—assisting the SAF in identifying, testing, and deploying new technologies within its operations; and nurturing talent and building expertise—attracting and training skilled personnel in various fields of technology relevant to national defense (DSO 2024).

Specifically, responsibilities for technological innovation are divided in MINDEF's four main tech-departments with distinct technology planning portfolios and policy planning responsibilities (MINDEF 2023b). These include:

- *Future Systems & Technology Directorate* (FSTD)

FSTD is responsible for master-planning and managing the research and technology requirements of MINDEF and SAF. FSTD is led by Future Systems & Technology Architect and its organization structure comprises functional entities to master plan the R&D investments to deliver on game-changing concepts to realize cutting edge capabilities for the SAF. The Systems & Concepts Groups (SCGs) serve as FSTD's master planning offices, responsible for concept generation, as well as master planning systems and technologies development, including AI, to fulfil the SAF's key mission needs. The SAF Centre for Military Experimentation (SCME) formulates long term force development strategies and new war-fighting concepts.

- *Technology Strategy & Policy Office* (TSPO)

TSPO's role encompasses technology policy development, capability development, long-term planning, collaboration with the private sector, resource optimization, and technology transfer. TSPO collaborates with the broader civilian and private ecosystem, including startups, research institutions, and technology companies, to leverage external expertise and resources. This partnership approach aims to deepen innovation, accelerate technology development cycles, and enhance the agility of defense capabilities.

- *Industry & Resources Policy Office* (IRPO)

IPRO oversees the local defense industry, land use, logistics, technology security, defense exports, and procurement. IRPO collaborates with local defense companies to enhance capabilities, support innovation, and facilitate partnerships with international firms for technology transfer and knowledge exchange. IRPO works closely with relevant agencies to optimize land use for defense purposes, including the development of military training areas, storage facilities, and infrastructure for defense operations. IRPO also oversees logistics planning and management to ensure timely and efficient deployment of military assets, personnel, and supplies during peacetime and in crisis situations.

- *Defense Technology Collaboration Office* (DTCO)

DTCO is responsible for conceptualizing and implementing policies and plans for defense technology-related engagements with local research institutions and international partners. Specifically, DTCO formulates strategic policies and frameworks for engaging with local research institutions, universities, and industry partners to harness their expertise and capabilities in defense-related R&D activities. In doing so, DTCO also facilitates international collaborations and partnerships with foreign defense agencies, research organizations, and industry players to access cutting-edge technologies, expertise, and best practices for mutual benefit and knowledge exchange. DTCO manages technology transfer initiatives, facilitating the transfer of defense-related technologies between public and private sectors, academia, and defense industries to enhance Singapore's defense capabilities.

MINDEF's Defense Tech Group is further supported by the broader layer of the DTC that integrates three technology research arms, which pursue the research, development, testing, and evaluation of emerging technologies, including AI-enabled defense systems:

- *Defense Science and Technology Agency* (DSTA)

DSTA is a critical organization responsible for driving Singapore's advancements in defense science and technology. It plays a pivotal role in implementing defense technology plans, procuring defense material, developing defense infrastructure, and fostering collaboration within the defense and technology sectors. Additionally, DSTA works to build a strong community of experts and researchers, including AI engineers and scientists, to innovate and enhance Singapore's defense capabilities.

- *Defense Science Organization Labs (DSO Labs)*

DSLO Labs is Singapore's largest defense research and development organization, tasked with both basic and applied defense-technology related research. Its responsibilities encompass a wide range of areas, including exploring fundamental scientific principles, developing innovative solutions, and advancing cutting-edge technologies to enhance Singapore's defense capabilities.

- *Centre for Strategic Infocomm Technologies* (CSIT)

CSIT is a technical agency under MINDEF that focuses on cybersecurity, data analytics, software engineering, and could infrastructure and services. It is tasked to safeguard military systems, networks, and data from cyber threats. This includes developing robust cybersecurity strategies, implementing defensive measures, and conducting cybersecurity assessments and audits. CSIT leverages AI and data analytics techniques to derive valuable insights from large volumes of data for decision-making, threat intelligence analysis, and optimizing defense operations. Furthermore, CSIT engages in software development and engineering projects to create secure and reliable applications and systems for defense purposes. This includes developing custom software solutions tailored to specific defense requirements. CSIT manages cloud infrastructure and services for MINDEF, ensuring secure and efficient utilization of cloud computing resources. This involves deploying cloud-based applications, data storage, and computing resources while maintaining high levels of security and compliance.

The varying interactions within the DTC system shape specific military-technological development and acquisition processes, systems development and integration, and capabilities, which are subsequently integrated into the SAF services. In turn, the SAF then provides feedback loops on their performance validation and verification, system safety, reliability and maintainability, logistic support, and other factors (MINDEF 2023b). The administrative backbone of the DTC and the entire SAF is the Defense Management Group (DMG) within MINDEF, which is responsible for manpower and human resource management, implementation of National Service, financial planning and analysis, procurement, and contracts, and developing information technology infrastructure, and legal and other professional services for MINDEF and the SAF (MINDEF 2018b). Ultimately, the Defense Policy Group (DPG) under MINDEF plays a central role in developing and shaping defense policies, including for AI and emerging technologies, that align with Singapore's national security interests and strategic objectives. In doing so, the DPG manages international defense relations and collaborations, including bilateral and multilateral engagements with foreign defense ministries, organizations, and partners. This includes participation in defense dialogues, joint exercises, and cooperation frameworks to enhance defense cooperation and interoperability. In short, the DPG oversees the implementation of defense policies, working closely with other MINDEF departments, the SAF, defense industry partners, and other stakeholders to ensure policy objectives are achieved effectively and efficiently.

4 Fielding and Operating Defense AI

In September 2023, the Singapore Armed Forces (SAF) conducted its biennial, large-scale training exercise 'Forging Sabre' at the Mountain Home Air Force Base in Idaho, U.S. The exercise series, dating back to 2005, serves as platform for testing and refining SAF's cutting-edge capabilities, operational readiness, and proof-of-concepts. Its latest iteration provided perhaps the most visible insights into how the SAF integrates AI technologies, concepts, and organizations into its operational conduct. In particular, the SAF tested its latest version of the AI-enabled Command Post (CP) with CCIS discussed above. The system uses weapons-to-target matching algorithms, makes sense of information gathered by the various sensors, and generates defensive options and offensive choices. Commanders then decide from the proposed options and deploy select strike assets, including unmanned systems, in what the SAF terms 'sense-and-strike' operations (MINDEF 2023d).

4.1 SAF 2040 Transformation

The 2023 SAF 'Forging Sabre' is a relevant example of the direction and character of Singapore's ongoing AI-driven defense transformation, conceptualized as the 'Next-Gen SAF' or SAF 2040 capability roadmap (MINDEF 2021f). This roadmap aims to the combined effect of advanced (1) digitalization - integrating AI-enabled digital technologies to collect, store, process, and analyze data for decision-making, (2) growing maturity of robotization - development and deployment of AI-enabled autonomous systems for various tasks, and (3) sensor revolution - development and integration of advanced sensors across platforms and domains (Table 7).

Historically, the SAF modernization trajectory focused on gradual conventional military capability development: the first-generation or 1G SAF (1960s–70s) aimed at basic capability-development of individual services and the implementation of a purely island-defensive "poisoned-shrimp" strategy, which envisioned high-intensity urban combat to impose unacceptable human and material costs to potential aggressors. In the 1980s and '90 s, the second-generation or 2G SAF, shifted toward combined-arms maneuver warfare, and the "porcupine" defense strategy that envisioned a limited-power projection in Singapore's near seas and potentially a pre-emptive posture to be able to transfer a conflict into enemy's territory, for example, if Singapore's water supplies would be cut off (Loo 2004; Huxley 2000). At the turn of the twenty-first century, the SAF progressed toward the third-generation or 3G SAF, a transition towards 'network-centric' warfare for the land, air, and sea domains as well as an emphasis on defense diplomacy, operations other than war, counterterrorism, and disaster relief in geographically more distant areas from Singapore (Raska 2016).

Implementing the AI-driven SAF 2040, however, arguably signifies much more ambitious military change that transcends traditional conventional military

Table 7 AI-Enabled digitization, robotization, and sensor-revolution in the SAF

Aspect	Description	Examples in the SAF	Potential Impact
Digitization	Integration of digital technologies to collect, store, process, and analyze data. Example: Command and control information system (CCIS)	Battlefield management systems (BMS): Real-time data on troop movements, logistics, targets. Digital twin technology: Modelling and simulating platforms, operations, and training scenarios.	Improved situational awareness—Enhanced communication and coordination—Faster decision-making—Optimized maintenance and logistics—Faster training cycles—Risk-free experimentation.
Robotization	Introduction of robots and autonomous systems for various tasks. Example: Maritime security unmanned surface vessel (USV)	Unmanned ground vehicles (UGVs): Surveillance, mine disposal, logistics support. Unmanned aerial vehicles (UAVs): Reconnaissance, border patrol, air-to-ground strikes.	Reduced risk to personnel—increased efficiency in dangerous or repetitive tasks—greater operational endurance -expanded combat and surveillance reach—rapid situational assessment—extended mission duration.
Sensor Revolution	Widespread deployment of advanced sensors across platforms and terrains. Example: Republic of Singapore air force (RSAF) island air defense system	Integrated battlefield sensor networks: Fused data from radar, sonar, cameras, etc. Wearable sensors for soldiers: Monitoring health, fatigue, and environmental conditions.	Real-time threat detection—enhanced target identification—more effective countermeasures—optimized soldier performance—reduced risk of injury—improved tactical decision support.

Source: Author's overview based on publicly available DSTA and MINDEF factsheets and press releases (MINDEF 2021c, g, 2022b, 2023d; DSTA 2023a, b)

modernization. In particular, the AI diffusion in the SAF 2040 can be defined along four mutually reinforcing areas:

- Comprehensive adoption and adaption of AI systems into all domains of military operations.
- Organizational changes from restructuring existing units to creation of new command structures such as the Digital and Intelligence Service (DIS) to enable greater organizational agility and adaptability.
- Talent development by investing in AI training programs and talent acquisition strategies to diversify SAF personnel and provide them with the necessary skills for future operations.
- Pursuing responsible AI-governance in defense diplomacy.

While details are scattered in a mosaic of brief press releases and public statements in speeches of MINDEF's senior military leadership, the SAF 2040 envisions that Singapore's military will operate in a strategically uncertain and operationally complex environment that combines high-technology with new forms of 'hybrid' warfare -increasingly blurring the lines between peacetime and wartime, civil and military arenas, and new domains such as space, near space, cyberspace, and underwater (Raska 2019). The resulting "high-low" intensity threat spectrum combines diverse and often opposing challenges simultaneously: On one hand, regional extremists or terrorist organizations could evolve by using novel technologies and sheer brute force—for example, by simultaneously using swarms of drones, social media information warfare, cyberattacks, indiscriminate shooting, and use of explosives to attack Singapore's centers of gravity. On the other, with the ongoing China-US strategic rivalries in the Indo-Pacific and potential conflict scenarios in the South China Sea, the Malacca Strait, Taiwan and East China Sea, Singapore's security is increasingly affected by the diffusion of advanced military-technological capabilities and strategic competition in the Indo-Pacific.

In the military context, therefore, the SAF aims to preserve its deterrence and defensive options and inherently also offensive choices (Bitzinger 2021). In 2023, for example, the acquisition list for the SAF included upgraded early warning systems such as coastal surveillance network and air defense systems; F-35 s and upgraded F-15SG fighter jets, Multi-Role Tanker Transport and G-550 Airborne Early Warning aircraft, Unmanned Aerial Vehicles (UAVs) including Orbiter 4 close-range UAVs; new classes of ships that include Joint Multi-Mission Ships and Multi-Role Combat Vessels (MRCVs); Type 218SG submarines based on upgraded German Type 214 design, and new types of Underwater Unmanned Vehicles (UUVs); and ultimately, military systems and platforms for more protected and mobile Army, such as the indigenous Hunter armored fighting vehicles, Terrex Infantry Carrier Vehicles, upgraded Leopard tanks, High Mobility Artillery Rocket System (HIMARs) and howitzers, and their supporting systems (Koh 2021). Together, these platforms have the potential to increase the SAF's freedom of action, make the SAF more survivable due to the increased use of stealth and active defenses, and improve its capabilities for battlefield knowledge, situational awareness, and command and control—including the integration of AI-enabled battle-management systems such as Artemis (Ng 2021; Teo 2021). In the context of AI-enabled intelligence and maritime domain awareness capabilities, for example, the Republic of Singapore Navy (RSN) uses AI- enabled command, control, and communication (C3) system with AI video analytics to detect, track, and classify vessels visually – the C3 system is able to identify and classify up to 20 vessels per second, which reduces the cognitive burden and workload of human operators.

At the same time, the SAF, together with Singapore's security and intelligence agencies, must grapple with a new era of permanent low-level conflicts in and around the Indo-Pacific that utilize grey-zone strategies—using ambiguity or deniability in everything from disinformation and espionage, hostile influence campaigns, crime and subversion, and cyber means to gain political advantage by projecting instability within countries and a legitimacy crisis on the global stage.

While grey zone conflicts do not include the use of violent force, hybrid warfare does. Evolving hybrid warfare strategies often combine timeless 'unconventional methods' with novel technologies to create political, economic, and psychological effects. Like grey zones, hybrid warfare strategies are initially masked in non-military arenas, utilizing diplomatic deception, cyber and social media disinformation to influence public opinion. The aim is to maximize non-military forms of influence, political coercion, while seeding chaos and deception to undermine societal resiliency and military resolve. In theory, this creates a psychological advantage for sweeping military actions and undermines the resilience of multicultural societies such as Singapore. Therefore, the SAF must adapt its concepts, organizational structures, and technological capabilities to counter 'hybrid' threats in the information and cyber domains; expanding counter-terrorism capabilities, particularly by strengthening Island Defense and Special Forces; and leveraging advanced emerging technologies such as AI, data analytics, and robotics in nearly all aspects of defense planning and military operations (Raska 2021). In this context, for example, the DSTA has developed the Cyber Security Operations Centre (Cyber SOC) 2.0 that aims to enhance MINDEF and the SAF's ability to monitor, detect, analyse and respond to cyber threats. The Cyber SOC integrates AI and machine learning techniques to learn and adapt constantly, prioritise alerts on cyber incidents, and enhance detection capabilities. In 2020, the team behind the Cyber SOC received the Defence Technology Prize – MINDEF's most prestigious award for outstanding contributions in defence science and technology.

4.2 Digital and Intelligence Service

As part of the SAF 2040 major organizational change, the SAF established the Digital and Intelligence Service (DIS) in October 2022, as the fourth branch of the SAF, on par with the Army, Navy, and Air Force. The idea behind the DIS is to consolidate previously compartmentalized Command, Control, Communications, Computers, and Intelligence (C4I), cyber, military intelligence, and supporting units and capabilities. At its onset, the DIS as a Service headquarter (HQ) currently includes four Commands, each responsible for a specific domain: Intelligence, C4 and Cyber, Digital Defense, and Training. It also established the Joint Digital and C4 Department (JDCD) to scale up digitization within the SAF in collaboration with Singapore's DTC and the Digital Ops-Tech Centre (DOTC) that aims to serve as the SAF's center of excellence to integrate AI, data science, and emerging technologies into SAF's operational conduct (MINDEF 2022c).

Through the DIS, the SAF's evolving military-technological advances are combined with relevant organizational force structures and increasingly push for more transformative capabilities and conduct of operations, including AI. This means that current and future DIS units will increasingly utilize AI-enabled systems to provide situational awareness, intelligence of the operational environment, and cyber support for SAF's joint operations while defending Singapore's military networks,

electronic communications, and information environment (MINDEF 2023e). At the high end of warfare, DIS will also enable the so-called 'sense and strike' missions—a follow-up to the evolving 'sensor-to-shooter' concepts that have envisioned integrating diverse automated sensor networks, data sharing, and providing mission taskings to any weapons platforms or units. For example, an unmanned aerial vehicle or ground robot would be able to spot an enemy tank or ship, share the intelligence and data in real-time with relevant non-line-of-sight strike systems in the rear, which in turn would be able to use this automated target detection with the human-in-the-loop to launch precision strikes on the target (MINDEF 2021h, 2023d).

5 Training for Defense AI

Education and training are important for technology savvy SAF. This also mirrors the country's broader societal expectations as Singapore wants its armed forces to play on par with civilian and commercial technology developments. Consequently, the SAF considers AI an important tool to advance realistic digital environments for simulation-based training and to personalize training programs. In this context, recent AI-Ops-Tech developments also include an immersive training system utilizing Virtual Reality (VR) for soldiers to practice combat scenarios in realistic environments (MINDEF 2022b). The latest 'Forging Sabre' exercise, as illustrated above, also underlined that the SAF consider an increasingly complex battlefield environment in which information density is rising and human operators will more intensively interact with unmanned systems. While the SAF see a role for AI in dealing with the respective burden, that comes with these types of operations, human operators need to trust AI to accomplish its mission (Hamzah 2023). That's why the training curriculum is beginning to cover these aspects, to gradually nourish soldier's confidence in AI. In this regard, Singapore is also stepping up efforts to integrate AI-enhanced technology and AI-augmented concepts of operations into bilateral training efforts with key strategic partners like the United States, for example.

6 Conclusion

Amid external geostrategic and technological disruptions coupled with internal demographic challenges, Singapore has increasingly turned to emerging technologies such as AI systems, augmented reality, and data-driven decision-making methods, which are redefining traditional defense planning approaches and operational conduct of the SAF. Singapore's AI systems and machine-learning algorithms are helping to sort through vast amounts of data across various government and military applications, including predictive maintenance taskings, predictive analysis, and in cyber-defenses (Chia 2018; MINDEF 2021e).

At the same time, however, technology can't solve complex strategic and operational challenges alone. Therefore, Singapore's defense planning, including AI, is focusing on institutional agility through collaborative security, intelligence, and defense networks, in which traditional organizational boundaries are being erased. Collaborative defense planning relies on diverse networks that can be linked in novel ways—military, cross-agency government collaboration, and increasingly private companies can share data, experiences, and best practices to tackle complex security challenges (MINDEF 2021d). Over the past decade, strengthening a nodal resilience between the government, society, and technology has shaped the organizational agility in Singapore's defense planning approaches. The key enabler holding the various horizontal and vertical collaboration networks has depended on ramping up and maintaining internal trust and cohesion between Singapore's government agencies and society, and externally with international partners such as tech companies.

With the SAF 2040 transformation, Singapore's defense planners have continuously pointed toward the disruptive nature of emerging technologies and digital revolution as both strategic challenge and opportunity—turning to advanced technologies as an intelligence enabler, force multiplier, and defense diplomacy anchor that can strengthen its deterrence, defense, and resilience capabilities, while mitigating the effects of internal demographic changes and vulnerabilities. Therefore, the contours of the SAF 2040 defense planning effectively signify a major military change for the SAF.

Integrating AI into multidomain operations requires a new strategy, units, and doctrinal revision to include new missions and career paths, changing the curriculum of SAF's professional military education institutions, and revising training and experimentation. Technology is and will remain SAF's critical enabler in the process, especially as Singapore lacks strategic depth and a limited (and declining) manpower base. It must strive to keep its military as high-tech as possible, including its manpower. At the same time, Singapore must continue to leverage its relatively high level of education and technical training to craft a smaller but more technologically savvy military.

Ultimately, the SAF's irreducible priorities are still to protect the Singaporean homeland and to safeguard Singapore's security by working to maintain peace, stability, and reduced tensions throughout Southeast Asia. Deterrence, defense, diplomacy, and resilience are still the key watchwords of the SAF, but how these might be achieved in the twenty-first century is probably changing and may change further with intertwined geostrategic and technological challenges, uncertainties, as well as strategic opportunities—brought by the next wave of AI-driven revolution in military affairs.

References

Bitzinger, Richard. 2021. Military-technological innovation in small states: The cases of Israel and Singapore. *Journal of Strategic Studies* 44 (6): 873–900.

Centre for Strategic Futures (Strategy Group, Singapore Prime Minister's Office). 2023. *Who we are–Our Approach*. https://www.csf.gov.sg/our-work/our-approach/. Accessed 30 Jan 2024

Cheng, Kenneth. 2016. SAF looks to artificial intelligence to gain punch. *Today Online*. https://www.todayonline.com/singapore/saf-looks-artificial-intelligence-gain-punch. Accessed 30 Jan 2024

Chia, Osmond. 2023a. Singapore to triple AI talent Pool to 15,000 as part of National Strategy Update: DPM Wong. *The Straits Times*. https://www.straitstimes.com/singapore/singapore-updates-strategy-to-tackle-new-risks-of-generative-ai-implications-for-humanity. Accessed 30 Jan 2024

———. 2023b. National AI strategy 2.0 follows years of planning, growth in AI Sectro 'not by chance': DPM Wong. *The Straits Times*. https://www.straitstimes.com/singapore/national-ai-strategy-20-follows-years-of-planning-growth-in-ai-sector-not-by-chance-dpm-wong. Accessed 30 Jan 2024

Chia, Jie Lin. 2018. Singapore's new 'soldiers': AI, augmented reality, and data analytics. *GovInsider*. https://govinsider.asia/intl-en/article/singapore-defence-dsta-mindef-ai-ar-data-analytics. Accessed 30 Jan 2024

DSTA. 2016. *The DSTA Story 2000–2015*. Singapore: Defence Science and Technology Agency.

———. 2023a. *Transforming Air Defense*. https://www.dsta.gov.sg/what-we-do/detail?title=transforming-air-defence&category=e. Accessed 30 Jan 2024

———. 2023b. *Creating Dynamic Strikes*. https://www.dsta.gov.sg/what-we-do/detail?title=creating-dynamic-strikes&category=d. Accessed 30 Jan 2024

DSO National Laboratories. 2024. *Our History*. https://www.dso.org.sg/about/history. Accessed 30 Jan 2024

Hamzah, Aqil. 2023. AI, data analytics improve decision-making process, but human touch still key at SAF exercise. *The Straits Times*. https://www.straitstimes.com/singapore/ai-data-analytics-improve-decision-making-process-but-human-touch-still-key-at-saf-exercise. Accessed 30 Jan 2024

Harjani, Manoj, Dymples Leong, Teo Yi-Ling. 2020. *Artificial Intelligence: Sustaining Singapore's AI Ambitions. S. Rajaratnam School of International Studies Commentary*. https://www.rsis.edu.sg/rsis-publication/cens/artificial-intelligence-sustaining-singapores-ai-ambitions/. Accessed 30 Jan 2024

Huxley, Tim. 2000. *Defending the Lion City: The Armed Forces of Singapore*. St Leonards: Allen & Unwin.

Goh, Yan Han. 2024. Singapore seeks international feedback on new governance framework for generative AI. *The Straits Times*. https://www.straitstimes.com/singapore/s-pore-seeks-international-feedback-on-new-governance-framework-for-generative-ai. Accessed 30 Jan 2024

Infocomm Media Development Authority (IMDA). 2024. Singapore proposes framework to Foster trusted generative AI development. *IMDA*. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/public-consult-model-ai-governance-framework-genai. Accessed 30 Jan 2024

Koh, Fabian. 2021. Budget debate: Transformation to next-gen SAF on track despite Covid-19, says Ng Eng hen. *The Straits Times*. https://www.straitstimes.com/singapore/budget-debate-transformation-to-next-gen-saf-on-track-despite-covid-19-says-ng-eng-hen. Accessed 30 Jan 2024

Kor, Kian Beng. 2017. SAF confident of coping with tighter manpower resources. *The Straits Times*. https://www.straitstimes.com/singapore/saf-confident-of-coping-with-tighter-manpower-resources-thanks-to-increased-automation-and. Accessed 30 Jan 2024

Lee, Hsien Loong. 2014. Speech by PM Lee Hsien Loong at the Smart Nation Launch on 24 November 2014. *Prime Minister's Office Singapore*. https://www.pmo.gov.sg/Newsroom/transcript-prime-minister-lee-hsien-loongs-speech-smart-nation-launch-24-november. Accessed 30 Jan 2024

Lee, Kuan Yew. 2009. *The fundamentals of Singapore's foreign policy: Then & now. S. Rajaratnam Lecture at the Ministry of Foreign Affairs Diplomatic Academy*.

Loo, Bernard Fook Weng. 2015. The Management of Military Change: The case of the Singapore armed forces. In *Security, Strategy and Military Change in the 21st Century: Cross-Regional Perspectives*, ed. J.I. Bekkevold, Ian Bowers, and Michael Raska, 70–88. London: Routledge.

———. 2004. Explaining changes in Singapore's military doctrine: Material and ideational perspectives. In *Asia in the New Millennium*, ed. Amitav Acharya and Lee Lai To, 352–374. Singapore: Marshall Cavendish Academic.

Maritime Executive. 2018. *Strait of Malacca Key Chokepoint for Oil Trade*. https://maritime--executive.com/article/strait-of-malacca-key-chokepoint-for-oil-trade. Accessed 30 Jan 2024

Matthews, Ron and Fitriani Bintang Timur. 2023. Singapore's Total Defence strategy. Defence and Peace Economics. doi: https://doi.org/10.1080/10242694.2023.2187924. Accessed 30 Jan 2024

MINDEF. 1995. *Defense of Singapore 1994–95*. Singapore: Ministry of Defense.

———. 2023a. *Infographic: Towards SAF 2040*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2023/February/24feb23_infographic. Accessed 30 Jan 2024

———. 2023b. *Defense Science and Technology*. https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/defence-science-and-technology. Accessed 30 Jan 2024

———. 2023c. *Committee of Supply Debate 2023*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2023/cos2023. Accessed 30 Jan 2024

———. 2023d. *Factsheet: Ex Forging Sabre 2023—Multi-Domain Smart Warfighting*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2023/September/21sep23_fs. Accessed 30 Jan 2024

———. 2023e. *Factsheet: Update on the Digital and Intelligence Service (DIS) Capability Development Efforts*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2023/February/24feb23_fs. Accessed 30 Jan 2024

———. 2022a. *Factsheet: Total Defence Sandbox*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/february/12feb22_fs. Accessed 30 Jan 2024

———. 2022b. *Factsheet: Enhancing the SAF's Operational-Readiness and Servicemen's NS Experience through Digitalisation and Innovation*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/June/30jun22_fs. Accessed 30 Jan 2024

———. 2022c. *Factsheet: Digital and Intelligence Service*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/October/28oct22_fs. Accessed 30 Jan 2024

———. 2021a. *Defence Policy and Diplomacy*. https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/defence-policy-and-diplomacy. Accessed 30 Jan 2024

———. 2021b. *Welcome Address by Minister for Defence Dr Ng Eng Hen at the 3rd Singapore Defence Technology Summit*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2021/October/12oct21_speech. Accessed 30 Jan 2024

———. 2021c. *Fact Sheet: SAF Harnesses Artificial Intelligence and Data Analytics to Sharpen Sense and Strike Capabilities with Command and Control Information System*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2021/september/23sep21_fs2/. Accessed 30 Jan 2024

———. 2021d. *Fact Sheet: Leveraging Technology and Innovation to Drive Digital Transformation*. https://www.MINDEF.gov.sg/web/portal/MINDEF/news-and-events/latest-releases/article-detail/2021/March/01mar21_fs4/. Accessed 30 Jan 2024

———. 2021e. *Fact Sheet: Strengthening MINDEF/SAF's Cyber Defence Capabilities*. https://www.MINDEF.gov.sg/web/portal/MINDEF/news-and-events/latest-releases/article-detail/2021/June/30jun21_fs7. Accessed 30 Jan 2024

———. 2021f. *Fact Sheet: Transformation of the Singapore Army*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2021/June/30jun21_fs. Accessed 30 Jan 2024

———. 2021g. *Fact Sheet: Unmanned Surface Vessels to Enhance Maritime Security*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2021/March/01mar21_fs5. Accessed 30 Jan 2024

———. 2021h. *Fact Sheet: Ex Forging Sabre 2021—"Sense More, Smarter, Strike as One"*. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2021/September/23sep21_fs. Accessed 30 Jan 2024

———. 2018a. *Fact Sheet: Exercises and Operations*. https://www.mindef.gov.sg/web/portal/mindef/defence-matters/exercises-and-operations. Accessed 30 Jan 2024

———. 2018b. *Defence Management Group*. https://www.mindef.gov.sg/web/portal/mindef/about-us/organisation/organisation-profile/defence-management-group. Accessed 30 Jan 2024

Ng, Abigail. 2023. Singapore's Total fertility rate drops to historic low of 1.05. *Channel News Asia*. https://www.channelnewsasia.com/singapore/singapore-total-fertility-rate-population-births-ageing-parents-children-3301846. Accessed 30 Jan 2024

Ng, Jr. 2021. Eyes in the sky. *Asian Military Review*. https://www.asianmilitaryreview.com/2021/03/eyes-in-the-sky/. Accessed 30 Jan 2024

Raska, Michael. 2021. Rethinking defense planning in an age of disruption. *The Straits Times*. https://www.straitstimes.com/opinion/rethinking-defence-planning-in-an-age-of-disruption. Accessed 30 Jan 2024

———. 2019. *The SAF after Next Incarnation. S. Rajaratnam School of International Studies Commentary*.. https://dr.ntu.edu.sg/bitstream/10356/106416/1/CO19041.pdf. Accessed 30 Jan 2024

———. 2016. A structure-phased evolution: The 3G force transformation of the Singapore armed forces. In *Military Innovation in Small States: Creating a Reverse Asymmetry*, ed. Michael Raska, 130–161. New York: Routledge.

Smart Nation Singapore. 2023. *Singapore National AI Strategy 2.0. Government of Singapore*. https://www.smartnation.gov.sg/nais/. Accessed 30 Jan 2024

Teo, Jing Ting. 2021. RSAF Trials AI and Robotics for Smart Airbase Transformation. *Pioneer*. https://www.mindef.gov.sg/web/portal/pioneer/article/cover-article-detail/technology/2021-Q2/30jun21_news2. Accessed 30 Jan 2024

Tham, Davina. 2023. Singapore to triple AI talent Pool, build 'iconic' AI site as part of updated National Strategy. *Channel News Asia*. https://www.channelnewsasia.com/singapore/national-ai-strategy-artificial-intelligence-talent-iconic-site-3963971. Accessed 30 Jan 2024

Zachariah, Natasha Ann. 2023. Total Defence 'vital and needed' amid changing external security environment: Ng Eng hen. *The Straits Times*. https://www.straitstimes.com/singapore/total-defence-vital-and-needed-amid-changing-external-security-environment-dr-ng-eng-hen. Accessed 30 Jan 2024

Evolution Not Revolution: Defence AI in Australia

Peter Layton

Artificial Intelligence (AI) has become pervasive across global society over the last 15 years. This is principally because contemporary AI is overwhelmingly a commercial product, predominantly developed in the civil domain, and frequently designed to meet consumer market demands.

AI is now starting to be used for defence purposes, but the military comes late to the game. Defence AI is a case of technology push not technology pull. The result is that defence forces globally, and including Australia, are fundamentally uncertain about AI's place in warfighting. Accordingly, they are now deeply involved in numerous AI experimentation programs. Operational concepts will then be derived from these experiments with the concepts going on to drive future equipment acquisition programs.

While today's AI technology may not be optimized for defence purposes, there are definite upsides. Given mass civilian production, the technology is lower cost than defence-only technology traditionally is. Moreover, much of the personnel, training, logistics, industrial base and service support foundation such technology requires are already available and spread widely across society. Middle-power Australia fits within this paradigm. The Australian Department of Defence [hereafter abbreviated as Defence] use of AI fits within a broader national picture; it is effectively a subset although adjusted to meet specific defence needs, context, capabilities, and capacities.

This chapter initially discusses how Defence thinks about AI from a definitional and doctrinal perspective. The second section describes the recently revised innovation ecosystem that Defence uses to develop AI for military purposes, with the third detailing some important Australian defence AI projects currently in development, and the fourth assessing the ecosystem approach being taken. The fifth section looks at the forthcoming major projects that will provide funding for AI technology

P. Layton (✉)
Visiting Fellow, Griffith Asia Institute, Brisbane, QLD, Australia
e-mail: p.layton@griffith.edu.au

H. Borchert et al. (eds.), *The Very Long Game*, Contributions to Security and Defence Studies, https://doi.org/10.1007/978-3-031-58649-1_26

developments in the near-medium future. The sixth and seventh sections examine the single-service organisations currently involved in trialling AI and the single-service plans for training their future personnel in AI matters. The conclusion briefly assesses the Australian military's overall AI progress and intent.

1 Thinking About Defence AI

Military organizations traditionally desire to carefully define matters to ensure personnel across their large organizations have both a clear understanding and a shared one. However, with AI, as in the wider society, there are some definitional variations about what AI is. In early 2022, the Navy defined AI as "a collection of interrelated technologies used to solve problems and perform tasks that, when humans do them, requires thinking" (RAS-AI Campaign Plan 2022: 64). In August 2022, Army opted for a similar but subtly different definition: "A collection of techniques and technologies that demonstrate behaviour and automate functions that are typically associated with, or exceed the capacity of, human intelligence" (Robotic & Autonomous Systems Strategy 2022: 4).

Definitional precision is at least partly necessary as within Defence over the last five years there has been a conflation of AI and autonomy. Matters concerning AI are then often discussed in terms of autonomy, in some respects confusing a technology with a quality and inadvertently creating conceptual difficulties when the two do not overlap. The Army Robotic and Autonomous Systems (RAS) v2.0 strategy observes:

> AI underpins the realisation of true autonomy of RAS. Without it, RAS will reach autonomy limits quickly, remaining remote controlled and automatic at best. Extending AI to facilitate truly intelligent and adaptable machines and capable human-machine and machine-machine teams will be critical to future RAS capabilities. AI tools will also be foundational in decision support, providing RAS with the ability to rapidly analyse significant volumes of data, see patterns and make observations and recommendations (Robotic & Autonomous Systems Strategy 2022: 20).

A second aspect of Defence's conceptualization of AI is noteworthy, although within mainstream thinking: the clear recognition of the centrality of data in supporting AI development. The 2021 Defence Data Strategy argues that maintaining "a capable, agile and potent" Australian Defence Force (ADF) will increasingly rely on AI technologies, and this means that Defence's data holdings must be managed and discoverable in a way that can support AI development (Defence 2021: 35). The strategy sets out the vision, pillars, practical initiatives, and priority data areas to elevate Defence's data maturity and become a more data-informed organization.

1.1 Joint and Single Service Thinking

Given the conflation with autonomy noted earlier, the joint-service Concept for Robotic and Autonomous Systems published in late 2020 is effectively the ADF's capstone publication informing its adoption of AI technology. In terms of AI, the concept aims to address how Australia's future defence force can best exploit AI to gain advantages across the conflict spectrum and, rather innovatively, how Australia can counter threats posed to the future defence force by AI (Australian Defence Force 2020: 22).

The key exploitation judgements are to use AI in human commanded teams to improve efficiency, increase mass and achieve decision superiority while decreasing risk to personnel. Efficiency involves using AI to perform certain tasks faster and more reliably than human operators, thereby increasing force capacity. In terms of mass, defence force structures can now move away from being a small number of exquisite platforms to instead featuring many, small, lower-cost, AI-enabled systems. In so doing, military forces will have many more battlefield ways possible to generate an advantageous concentration of combat power, disperse the force to enhance survival, and generate deception (Australian Defence Force 2020: 36–37).

AI use for decision superiority involves assisting making and implementing better and more accurate decisions, while using tempo and leverage to best effect. An important part of this is improving the situational understanding of human or machine decision-makers by improving their awareness, analysis, and comprehension. Lastly, systems employing AI can operate in ways that decreases the risks to defence force personnel during operations; AI systems can be programmed to be as fearless as the decision-makers wish (Australian Defence Force 2020: 40–42).

The joint service document was shaped by earlier single-service thinking. Equally, more recent single-service thinking is now building on the joint service document, providing additional depth and insights.

The Australian Army provided the initial impetus for the ADF formally thinking about AI with its 2018 Robotic and Autonomous Systems Strategy; this has recently been revised and republished as the 2022 Robotic and Autonomous Systems Strategy v2.0 document. This asserts such technology can maximize each soldier's performance, improve decision-making, generate mass and scalable effects, enhance force protection, and improve efficiency. These attributes have some subtle differences to those which the joint service document sets out.

Soldier performance would be maximized by reducing individuals' cognitive burdens through collecting, processing and presenting information in a useful and intuitive manner. In terms of decision-making, the complicated battlespace of the future is seen as requiring AI processing of vast data troves of information on friendly and adversary forces to adequately support commanders at the operational and tactical levels. Moreover, AI through human-machine teaming could also potentially give a modestly sized army significantly increased combat power and mass through deploying large numbers of AI-enabled systems without the need to expand the human workforce. Likewise, humans might be better protected by transferring

many current dangerous battlefield tasks, such as reconnaissance and intelligence collection, to AI systems. Lastly, AI could noticeably enhance efficiency, particularly in the logistics chain. AI systems can bring "aware logistics," creating a "sense and respond" logistic structure that moves from a "just in case" to "as needed" as operations evolve (Robotic & Autonomous Systems Strategy 2022: 8–18).

In a similar vein, the Royal Australian Navy's (RAN) RAS-AI Strategy 2040 describes what the "five very fundamental effects" such systems will deliver:

- Force Protection involves shielding people by increasing their situational awareness and providing innovative alternatives to traditional maritime combat approaches so helping keep sailors out of harm's way.
- Force Projection sees AI allowing the RAN to generate mass and tempo on a scale otherwise unachievable while enabling a presence in Australia's maritime reaches that crewed platforms could not, on their own, achieve.
- Force Partnerships envisages Navy's AI systems being integrated by design with the overall ADF, and priority being given to interoperability with Australia's strategic partners.
- Force Potential involves human-machine teaming maximizing human potential by allowing novel ways to conduct and sustain operations, reducing cognitive loads on commanders and enhancing training, simulation, and force level planning.
- Sovereign Control encompasses two different aspects. Firstly, having a system of control that protects its data and secondly, the navy being able to rapidly task-organize multiple AI assets across air, land, sea, space, and electromagnetic domains (RAS-AI Strategy 2020: 14).

The Royal Australian Air Force (RAAF) has not yet published a formal document related to its AI intent although a recent Chief of Air Force argued that "artificial intelligence and human-machine teaming will play a pivotal role in air and space power into the future." The role envisaged is mainly increasing personnel productivity through using AI to undertake tasks that are predictable, repetitive and which do not require imagination and innovation. AI is not about replacing people but instead allowing employing this "scarce resource" better. The Chief's vision is that the RAAF "will be AI-enabled using robotics to augment roles, and humans working with machines, so they get the best out of both. The days of boring menial tasks will be gone. Our most scarce resource, our people, will focus on higher value and the creative tasks that we need" (Laird 2021).

1.2 Key Emerging Concern

The joint service document noted frets about countering hostile states and non-state actors using AI and envisages responding to this challenge by using:

- Perception Attacks that disrupt the ability of the AI to properly perceive its environment, possibly by inducing a false understanding of the situation.
- Control Attacks that are assume future AI systems will still need some human input or direction and so this connection may be purposefully obstructed.
- Information Warfare to degrade the quality of the data that the AI system is using, whether when devising its operating algorithms or when using them.
- Platform Destruction simply aims to physically destroy the AI system although this is becoming more difficult as such systems may be small and used in mass swarm attacks.

As an important enabling effort to countering hostile AI, Defence is developing the ability to collect technical intelligence on the algorithms and data utilized by adversary AI (Australian Defence Force 2020: 44–50). This will allow optimized counters to specific AI systems to be devised. Even so, generic counters will still be necessary given threat intelligence may have some gaps and shortcomings.

2 Developing Defence AI

2.1 National Framework

Defence AI development is nested within the overarching national AI Action Plan which itself is a key artifact of the Australian Government's Digital Economy Strategy. Australia's AI Action Plan sets out the Australian Government's vision for Australia to be a global leader in developing and adopting trusted, secure, and responsible AI. The plan will be implemented under four primary focus areas, all of which can be imagined within a defence perspective.

Focus One is supporting businesses to adopt AI technologies that increase productivity and competitiveness. Focus Two is creating an environment to grow and attract world's best AI talent. Focus Three is using cutting edge AI technologies to solve national challenges; in the defence domain these are identified as developing applications for intelligence mission data together with virtual reality and graphics applications. Focus Four stresses AI usage should reflect Australian values and that ethics are incorporated as the technology develops (Department of Industry, Science and Resources 2021).

The national AI Action Plan invests €63.33 M over 4 years to establish a National AI Centre and four subordinate AI Digital Capability Centres (DCC). It is envisaged that this initiative will help drive collaboration between research organizations, businesses and industry and generate a thriving AI ecosystem.

The National AI Centre is intended to drive business adoption of AI technologies by coordinating Australia's AI activity, expertise and capabilities in a manner that improves national productivity and competitiveness. The center focuses on key central themes including responsible AI, AI for diversity and inclusion, and AI at scale while becoming a focal point for international partnerships. The National AI Centre

is organizationally located within Data 61, the data and digital specialist arm of Australia's national science agency, the Commonwealth Scientific and Industrial Research Organization (CSIRO 2023).

The four, lower-level DCCs each focus on a specific application of AI, such as robotics or AI-assisted manufacturing. The centres are principally aimed at supporting the commercialization of Australia's AI expertise and capabilities which often resides at the small and medium enterprise level (CSIRO 2023).

2.2 Internal Defence AI Ecosystem

In the defence domain, an AI development ecosystem is also steadily being established. The Australian Department of Defence has two main parts: one commanded by the Chief of the Defence Force (CDF) and the other managed by the Secretary of the Department of Defence. Each is responsible for different parts of the overall defence AI ecosystem.

In some respects, the military part commanded by CDF has moved backward. The Joint Capabilities Group had earlier set up the Defence Artificial Intelligence Centre (DAIC) to build the capability foundations and accelerate the understanding and implementation of AI across Defence (Defence 2021: 35). However, the DAIC has now been discontinued with AI development activities in the military part of Defence now shifting solely to single service organizations (discussed later) rather than taking a joint force perspective.

The largest portion of the Defence AI ecosystem is within the civilian part of Defence and under the control of the Innovation, Science & Technology Capability Manager. A major reorganization has seen the Next Generation Technologies Fund, the Defence Innovation Hub and the Science, Technology and Research Shots (STaRShots) ended and the setting up of the new Advanced Strategic Capabilities Accelerator (ASCA). The development of AI for defence purposes will now be actioned under the ASCA process.

ASCA has been designed to address shortcomings in the earlier innovation pathway within Defence, in particular by integrating the diverse parts of the innovation process and in accelerating the transition of innovative technology into in-service military capabilities. ASCA comprises three distinct programs: the Emerging and Disruptive Technologies (EDT) program funds early research into promising new technologies; the Innovation Incubation program funds the acquisition of new commercial technology modified to meet military priorities; while the Missions program funds rapidly pulling through into military service those disruptive technologies that meet pressing defence needs (ASCA 2023).

ASCA has some €2.06bn of funding allocated to it over the next decade. Deliberations on funding allocations involve the Chief Defence Scientist at the Defence Science and Technology Group (DSTG), the Vice Chief of the Defence Force (a three-star military officer), and the Deputy Secretary Capability Acquisition and Sustainment Group. In this manner, ASCA encompasses defining the military

need, developing the new technologies to meet this need, the transition into equipment acquisition and the introduction into service (Hilder and Monroe 2023). ASCA began in July 2023 with initial starts including EDT program research into countering the effects of AI-powered technologies used for spreading disinformation, and the Mission program seeking improvements to the processing and synthesis of mass intelligence data (ASCA 2023).

DSTG is involved in other activities as well as ASCA. DSTG's latest strategic plan sees DSTG doing less research itself and instead playing a stronger role in coordinating support to Defence from the national S&T enterprise that encompasses other publicly funded research agencies, universities, and commercial enterprises (Defence 2020b: 2).

In terms of AI, a major entity within DSTG is the Trusted Autonomous Systems (TAS) defence cooperative research center. TAS facilitates emerging defence technology projects through coordinating, and at times collaborating with, other interested government, commercial and academic entities. Recent projects include involvement in developing an autonomous underwater vehicle, a prototype cooperative robotic system suited to high-tempo land operations called Hyper Teaming and a proof-of-concept demonstration using a patrol boat modified for autonomous operations. Most of the projects are industry-led but TAS is also undertaking two common-good activities: Ethics and Law of Autonomous Systems, and Assurance of Autonomy (Trusted Autonomous Systems 2022).

DSTG also works closely with universities including setting up the Defence AI Research Network. This aims to establish and sustain a community of AI researchers who work together in an environment that stimulates new ideas and knowledge and which supports AI system evaluation, testing, and integration. An example of the network's activities is the recent funding provided to the University of South Australia and Deakin University for two AI projects involving processing noisy and dynamic data into information useful for military decision makers (Defence 2023b).

There is also the more general Australian Defence Science and Universities Network that connects DSTG into state-based research and innovation networks. DSTG has a senior Defence scientist, an Associate Director, embedded in each of the state-based networks to promote cooperation useful to Defence (Defence Science and Technology Group 2022a). Beyond national defence, DSTG also manages the National Security Science and Technology Centre (NSSTC) concerned with domestic and transnational security matters. The Centre is involved in advancing relevant AI, machine learning and data science capabilities (Defence Science and Technology Group 2022b).

2.3 External Industry-Academia Defence AI Ecosystem

Small and medium enterprises (SME), and including start-ups, comprise some 90% of the companies in Australia's defence industrial sector. Of the remaining 10%, there are a few medium-sized companies and several large foreign-owned

businesses. Of the later, BAE Systems Australia has been involved in AI developments for more than a decade. Boeing Australia has become active in AI over the last 5 years, while the Australian subsidiaries of Lockheed Martin and Northrup Grumman have recently also become interested in AI in command and control systems. Within this, BAE Systems has done considerable work in-house whereas the American companies have acquired relevant Australian SMEs or formed business relationships with them.

Australian SMEs are proving innovative in devising AI solutions. However, the SME dominance of the defence industry sector, combined with few adjacent relevant industries such as telecommunications and personal electronics, means there is a shortage of investment capital that limits SME growth possibilities. Given this, there are uncertainties over whether Australian SME AI innovations can transition to become a sustainable operational capability; for such a transition, larger sovereign Australian enterprises or consortia are considered necessary (Robotics Australia Group 2022: 144).

The issue gains additional importance as AI, seen as encompassing algorithms, machine learning and deep learning, has been designated as a Sovereign Industrial Capability Priority. Accordingly, Australia "must have" access to, or control over, the skills, technology, intellectual property, financial resources, and infrastructure necessary for long-term defence capability support (Defence 2022: 1, 4). Given these requirements, the investment capital issue needs addressing to allow constructing Australian sovereign supply chains resilient to shocks and outside interference.

There are proposals to overcome the capital shortfall problem through shaping existing Government investment to generate enduring sovereign infrastructure that fosters SME growth. Significant capital and schedule efficiencies might be achieved through cost reduction of business and technical processes by creating a 'scaffolding' for re-use and leveraging of existing investments. Embracing enterprise collaboration may avoid wasteful duplication of effort, provide substantial efficiencies, and enable capital pooling that delivers outcomes unrealizable by individual enterprises (Robotics Australia Group 2022: 144–145).

Supporting SMEs and the wider defence industry sector there is the recently established Trailblazer Universities Program, intended to drive the commercialization of academic and industry research. Under this, the Concept to Sovereign Capability (CSC) project that encompasses defence AI will involve the University of Adelaide and the University of New South Wales working with industry to rapidly secure capital for both collaborative research projects and the commercialization of defence and dual-use technology successes. Over 80% of industry commitments to the CSC are from Australia-based SMEs (Savage 2022).

2.4 International Cooperation

DSTG is involved in defense Al R&D collaboration within the Five Eyes community (Australia, New Zealand, Canada, UK, and US) through The Technical Cooperation Program, and in specific bilateral collaborations with the UK and US. There is also growing interest in further developing S&T partnerships with Japan, the Republic of Korea, Singapore, India, and other countries in the Indo-Pacific region (Defence 2020b: 9).

In 2021, the existing AI collaboration with the US and UK was expanded under Pillar II of the AUKUS enhanced trilateral security partnership with an initially focus on accelerating AI adoption and improving the resilience of autonomous and AI-enabled systems in contested environments (Department of Prime Minister 2022). By late 2023 this had led to incorporating AI into anti-submarine sonobuoy processing systems on P-8A Maritime Patrol Aircraft that all three nations use, and in trialing in the UK and Australia AI algorithms and machine learning for force protection, precision targeting, and intelligence, surveillance and reconnaissance purposes (Defence 2023c).

Outside of the formal governmental processes, there are other linkages directly between countries and Australian AI companies. For example, the US Air Force's (USAF) venture capital division, AFVentures, a part of the AFWerx technology development organization, has recently funded Australian AI company Curious Thing to reimagine the USAF recruitment process (Australian Trade 2022).

2.5 Important Defence AI Projects in Development

There are three important defence Al R&D research projects underway that each illustrates various aspects of the current Australian thinking about defence AI and R&D priorities.

2.5.1 'Loyal Wingman' Airpower Teaming System

Boeing Australia has developed an Airpower Teaming System of which the most visible component is a jet powered Uncrewed Air Vehicle (UAV) with fighter-like performance. Initially called Loyal Wingman and now designated the MQ-28A Ghost Bat, this UAV uses cognitive AI to allow teaming with crewed fighter aircraft for air combat, reconnaissance, and surveillance missions in contested environments. The RAAF Chief at the time observed:

> The true value [of the project] is…hidden inside the airframe of Loyal Wingman. And that is the development of the code and the algorithms which form the AI behaviors that will optimize its combat capability. The Loyal Wingman project is a pathfinder for the integration of autonomous systems and AI to create smart human-machine teams (Laird 2021).

The joint venture between the RAAF and Boeing started in 2017. A major step forward was a 2019–2020 experimentation project approved by TAS and run by Boeing Australia that embedded machine learning techniques on board four small test-bed UAVs allowing them to detect, decide, and act during missions. In the Ghost Bat the AI is embedded in the BAE Systems (BAES) Australia flight and mission control system.

The prototype flew in February 2021 with five more since built; a final assembly facility for production UAVs is being constructed at Wellcamp in Queensland. In May 2022 the government announced a further seven would be acquired for €278M to enter service with the RAAF in 2024–25 (Airforce Technology 2023).

The seeming high unit cost of each Ghost Bat is an issue. In early 2023, the RAAF Chief considered the cost of advanced combat drones needs to reduce before they become widely used by the air force: "the price point, and where it really looks interesting to us, is if we can get it to about a tenth of the cost of a manned fighter. So if we get to 10%, then I can start to build the mass and survivability of not just manned platforms, but the entire air combat system" (Packham 2023).

2.5.2 M113 Optionally Crewed Combat Vehicle

In 2019, BAES Australia converted two M113 AS4 Armoured Personnel Carriers into Optionally Crewed Combat Vehicles (OCCV). This project involved the TAS and used the now ceased Next Generation Technologies Fund. The vehicles were used to help the Australian Army's Robotic and Autonomous Systems Implementation and Coordination Office (RICO) better understand employing autonomy on the battlefield and the implementation of the 2018 Robotics and Autonomous Systems Strategy. Natalie Waldie, BAES Program Manager Technology Development observes: "The M113 [is] a convenient (…) experimental platform to demonstrate autonomy. Autonomy doesn't achieve what it needs to unless you can effectively integrate it into your overall battle space CONOPS, and that's really what we're exploring with Army" (Levick 2020).

In 2020, a further 16 M113 AS4 vehicles were converted to OCCVs in a €5M project that also funded additional testing. In 2021, four OCCVs participated in Exercise Koolendong, a live-fire warfighting exercise in the Northern Territory, which tested the vehicles' ability to operate in harsh combat environments. In mid-2023, some of the vehicles were fitted with remote controlled, tele-operated weapon station and tested during live fire exercises in southern Australia. Three of the vehicles can be remotely operated from a single control vehicle up to 5 km away (Ferguson 2023).

The M113s use the BAE Systems Vehicle Management System (VMS) developed over the last two decades at the company's Red Ochre LABS in Adelaide. The VMS incorporates AI and is derived from the company's' domain agnostic autonomy technologies that have been used on several other programs, including in the Ghost Bat.

2.5.3 Bluebottle Uncrewed Surface Vessel

The OCIUS Technology Bluebottle is an uncrewed, long-duration, autonomous, 5kt surface vessel that operates on solar, wave and wind power, and can carry a payload of some 300 kg including thin line sonar arrays, radar, 360-degree cameras, an automatic identification system and other sensors. Bluebottle incorporates AI neural networks, edge computing processing of sensor signals, low bandwidth communication links and a "team" based software architecture where peer vessels independently maneuver to achieve the group's assigned common goals, such as making an interception.

Initially funded in 2015, the prototype began tests at sea in 2017. Another four Bruce-class Bluebottle were built to allow trailing Bluebottle teams in southern Australian waters. This experimentation then led onto design improvements incorporated into five Beth-class Bluebottles acquired between 2020–2023 (Naval Technology 2023).

In 2021, four Bluebottles operated as an intelligent network patrolling Northern Australian Indian Ocean waters fitted with a payload able to detect unauthorized vessels, alert a shore-based command centre and then approach the intruder for detailed investigation. In 2023, at a major autonomous system exercise in southern Australian waters, Bluebottles fitted with thin-line towed array sonars worked with vessels of the US Navy's Unmanned Surface Division One to track and isolate an autonomous underwater vehicle simulating a crewed submarine. The Bluebottles than worked in collaboration with a C2 Robotics Speartooth (an Australian developed uncrewed underwater vehicle) to cue a Navy MH-60R Romeo helicopter to further prosecute the target (Felton 2023).

2.5.4 Assessment

The three projects are quite different in aims although in each, AI and human machine teaming is at the core of their capabilities. The Bluebottle is on the cusp of being operational as an Exclusive Economic Zone patrol system with the Ghost Bat intended to lead directly to a near-term operational air combat capability. In contrast the M113 OCCV is simply an experimental platform for technology and operational concept development purposes. However, the crewed M113 is obsolescent, and the Army still has some 480 available. If these were converted into OCCVs they would significantly enlarge Australia's armored capabilities. Being uncrewed, the OCCV could be used in combat operations in situations a crewed M113 would not be risked.

In terms of exports, Ghost Bat would require US government approval. Boeing is already pitching some of the Ghost Bat technology for inclusion in emerging USAF uncrewed air vehicle programs. Similarly, BAES Australia exports of its VMS used on Ghost Bat and the M113 OCCV would probably require UK government approval. While Blue Bottle seems a simple sailboat, its technical sophistication may mean some variants may also be subject to US approval.

3 Organizing Defence AI

Defence is deeply involved in numerous experimentation projects to better understand AI and the contribution it may make. Given the demise of a joint approach, this experimentation is not unreasonably organized around the three services.

Implied in this approach is that AI will not cause significant structural change within Defence but rather be simply absorbed as just another new technology. AI is conceived as being used to either enhance, augment, or replace existing capability, meaning the existing services will not be greatly impacted. Organizationally, Defence will apparently remain as it now is well into the future, at least in terms of AI. This replicates the approach being taken by Australia's major allies and importantly allows interoperability to be more readily maintained than if there were major structural changes (Australian Defence Force 2020: 54–55, 60).

As part of the initial organizational steps, it is considered the acquisition of data storage and access capabilities must commence immediately. Such capabilities will be the foundation of AI used by Defence in the future. Moreover, building human confidence in AI will also begin, with trust built on relatively simple systems in preparation for the introduction into service later of more complex systems (Australian Defence Force 2020: 56).

The focus on experimentation has also led to a significant reorganization of the existing innovation pathway to better ensure a "good idea" moves expeditiously to in-service use. The ASCA process is still being developed and implemented meaning its successes or shortcomings are unlikely to be evidenced for some years. However, some tentative observations have been made.

ASCA will principally facilitate the adoption of core technologies developed elsewhere. Its design means that the entity will generally tend to neglect innovations that do not have a clear near-term pathway to acquisition. This means that AI developments are likely to get some funding, but the actual quantum will be meagre. Given this constraint, the desire to develop a sovereign AI capability able to optimize defence AI for national uses may be at odds with ASCA's design and its focus on adopting other's core technologies. Toby Walsh at the University of New South Wales' AI institute warns that "adopters don't get the rewards that creators do, and (…) adopters don't get to choose what the technology does" (Walsh 2023).

ASCA relies heavily on exploiting commercial technology for defence purposes not on bringing some wholly new break-through technology into use and gaining a distinct strategic edge. But this approach may not produce, what Defence is looking for, as George Henneke recently argued:

> We can develop an edge in dual-use technology by designing an acquisition system that runs faster than an adversary's. But it will never be more than an edge. On the time horizon of most acquisition systems—months or years, not decades—that adversary can mimic and counter our capabilities. Excessive reliance on dual-use technology creates not a sustained strategic advantage, but an arms race. Over time, we will not outpace our competitors (Henneke 2023).

4 Funding Defence AI

Beyond the R&D monies discussed earlier, AI development funding will be provided by those major capital equipment acquisition projects that feature extensive use of AI and machine learning technologies. The latest force structure investment plan was issued in 2020 and had six relevant major projects: one Army, three Air Force, one information and cyber domain, and one Navy. Four projects are in this decade: Air Force Teaming Air Vehicles, Integrated Undersea Surveillance System, Joint Air Battle Management System, and the Distributed Ground Station Australia. A new plan is expected in mid-2024 and may adjust some aspects.

4.1 Army

Under the new Future Autonomous Vehicles project, a fleet of uncrewed systems and vehicles, sufficient for up to brigade operations in size, will be acquired to support land force operations. This project will build from the M113 experimentation program and aim to enhance the war-fighting capability of the ADF while also protecting Australian personnel. The acquisition phase of the project is scheduled to run 2033–2040 and has been allocated a budget for planning purposes of €5–€7.5bn (Defence 2020a: 72, 77).

4.2 Air Force

The Ghost Bat/Loyal Wingman R&D program is envisaged being bought into service through a major project titled 'Teaming Air Vehicles.' This project will involve the "acquisition of remotely piloted and/or autonomous combat aircraft, including teaming air vehicles, to complement existing aircraft and increase the capacity of the air combat fleet." The project's acquisition phase is scheduled to run between 2026–2040 with a currently allocated budget provision of €5–€7.4bn (Defence 2020a: 51, 57).

The Distributed Ground Station Australia acquisition project will run between 2024–2031 and cost an estimated, €0.8–€1.2bn. This processing, exploitation and dissemination facility will be responsible for the analysis of data collected from Air Force intelligence, surveillance, and reconnaissance aircraft. Staff will be able to access national and open-source intelligence resources and use AI to rapidly fuse collected information to provide decision-makers with greatly enhanced near-real time situational awareness of events (Defence 2020a: 57).

The Joint Air Battle Management System (JABMS) acquisition project running from 2023–2031 has a budget provision of €1.2–€1.9bn. JABMS will provide greater situational awareness to deployed ADF forces from advanced air and missile

threats and improve interoperability with allies (Defence 2020a: 57). The JABMS project recently selected Lockheed Martin Australia as the preferred tenderer.

Lockheed is working with Australian company Consilium Technology on examining modelling, simulation and AI technologies that can be rapidly combined into an open architecture framework. Consilium Technology is also exploring the use of machine learning to support future all-domain data transfer capabilities during contested warfighting environments (ADM 2022). Another company, Consunet, is also participating in the project using AI for developing spectrum awareness and management tools, and electromagnetic spectrum modelling (APDR 2022).

4.3 Information and Cyber Domain

Defence has responsibilities for some defensive and offensive cyber capabilities, and certain intelligence collection systems. The force structure plan states that "funding will be set aside to ensure Defence remains competitive in the future as emerging technologies, such as artificial intelligence, arise in this domain." A new major acquisition project titled Emerging Technologies has been penciled in for 2033–2040 with a budget provision of €1.14–€1.7bn (Defence 2020a: 27, 31).

4.4 Navy

The Integrated Undersea Surveillance System acquisition project runs between 2025–2040 and has a budget provision of €3.38–€5bn. The project will bring into service an integrated undersea surveillance system and in this examine the utility of optionally crewed vessels, uncrewed surface systems and uncrewed undersea systems (Defence 2020a: 39, 45).

5 Fielding and Operating Defence AI

There are more organizations involved in Australian defence AI than only those at the government department level, joint service, dedicated science agencies or universities. The individual services, Navy, Army, and Air Force, each have their own internal entities that consider and support emerging technologies that might enhance their discrete warfighting capabilities.

5.1 Navy

To guide its adoption of AI, the Navy has a three-part policy of engagement, design, and demonstration. First, Navy will engage widely across Defence, with defence industry and with allies. Second, Navy will use a concept-led design approach to architectures, mission management and common control systems. Third, Navy will generate opportunities to demonstrate emerging and developed AI capabilities to operational users. This will both help develop new AI systems and expedite the introduction of fit-for-purpose capabilities into naval service.

Within Navy, the Warfare Innovation Navy (WIN) branch established in 2018 is the AI focal point for Australia and internationally, including at the NATO Maritime Unmanned Systems Initiative meetings. WIN is located within Navy's operational level headquarters at the Fleet Base East in Sydney and is currently facilitating an experimentation program to support force structure options development and capability improvements.

In terms of demonstration, the Autonomous Warrior (AW) series regularly displays, evaluates, and trials emerging AI capabilities at various Technology Readiness Level (TRLs). AW provides an opportunity to increase mutual understanding between industry and the Navy in a realistic environment while fostering collaborative relationships. AW involves four events conducted annually with each event having a specified operational focus and undertaken at different exercise locations, depending on the nature of the activity and convenience for industry (RAS-AI Strategy 2020: 44).

5.2 Army

In 2020, the Australian Army set up an organization somewhat like WIN. A difference however is the Robotic and Autonomous Systems Implementation and Coordination Office (RICO) is within the Future Land Warfare Branch of Land Capability division at Army's strategic level headquarters in Canberra. RICO's role involves exploration, coordination, and concept development of disruptive technology, specifically including AI.

In September 2023, the government announced a significant restructure of the Army which included re-rolling the first Armoured Regiment into an innovation and experimentation unit to accelerate Army's adoption of new and emerging technology (Defence 2023a).

5.3 Air Force

In 2015, the Air Force set up Plan Jericho to begin building an ecosystem in which good ideas, whether from within Air Force or externally, could answer military problems by translating and accelerating leading-edge knowledge and thinking into new defence capability. The intent was for partnerships with industry, academia, and broader society to support, inform and enable the rapid exploration and realization of ideas of researchers, innovators, and entrepreneurs. Since then, the concept has been sharpened and re-oriented to provide the infrastructure and services to make it easier to build partnerships across organizations and access the expertise and resources necessary.

Jericho has three main teams. The Jericho Edge team initially engages with partners to identify and understand opportunities. The Edge team then brings in Jericho Labs to assemble communities of interest across large-organizations, start-ups, small companies, and universities to discover, test, and prototype the identified opportunities. The separate Jericho Analytics team then tests the new ideas using net assessment, wargaming and red teaming (Air Force 2021).

Jericho's present thrust is in augmented intelligence, a concept developed from ideas of human-machine teaming. It is seen as combining the creativity and flexibility of humans with the tempo, precision, and mass of machines. The intent is to generate human-inspired dilemmas at machine speeds to cognitively overwhelm adversaries.

6 Training for Defence AI

Within Defence, some organizations have begun thinking about the training issues that the widespread introduction of AI will bring. Such training is situated within the national approach. In Defence, the single Services are responsible for raising, training, and sustaining their assigned force elements. Navy is the furthest advanced in considering the impact of AI with Army having given training matters some initial thought. Air Force has not publicly released its thinking on training.

6.1 Joint Workforce Perspective

The relevant ADF joint concept publication only briefly mentions training. Importantly though, it notes that with the introduction of AI military training will involve not just humans but also the AI. AI systems will need to be trained in a manner like their human operators by exposing them to operationally realistic scenarios so that the AI can develop knowledge bases from the data collected during these events. This training will not just be at the individual AI system level but also at the

formation level where multiple AI systems will interact with multiple human-machine teams (Australian Defence Force 2020: 34). AI machine learning is where most attention is currently focused. However, in the future collective training involving both humans and AI will become increasingly important. Such events will also allow humans who are teamed with AI, or who work with AI systems, to gain confidence in their reliability and dependability.

6.2 Navy Workforce Perspective

Navy presently leverages expertise from industry and academia to deliver formal AI training and on-the-job upskilling. The later "learning by doing" approach is increasingly important in growing Navy's AI workforce. Navy plans to continue to build upon these industry and academic relationships but sees the need to start Navy-wide AI education and training in three streams: specialists, generalists, and integration with industry.

- *Specialists*

In the near-medium term, Navy considers it will need to rapidly develop new specialist skills through either instituting new employment categories or expanding and re-defining existing ones. The more important new specialist skills are Technician, Data Specialists, AI System Operators and Test & Evaluation.

- *Generalists*

Navy's total workforce will need to incorporate foundational AI technology literacy. All commanders, operators and decision-makers will need to have a foundational understanding of AI. This is likely to include basic skills in machine learning, as well as an understanding of teaming and social decision-making. Navy believes that introductory AI courses should be introduced into *ab initio* training as soon as possible.

- *Integration with Industry*

The speed of AI development will not allow Navy to maintain in-house all the necessary AI skills required. Industry will be required to house, maintain, and deliver AI systems and will also increasingly play a role in analysis and decision support to deployed forces. These elements of workforce transformation are not mutually exclusive. While by 2040 Navy's whole workforce will require foundational AI knowledge, the Navy will still require specialists with deep knowledge and training as well as the ongoing delivery of specialist training and education by industry and academia. For some categories, such as Combat Systems Operators, the change will be evolutionary. For other categories, the introduction of AI will be disruptive and require close collaboration between AI technologists, category managers and workforce planners (RAS-AI Strategy 2020: 19).

6.3 Army Workforce Perspectives

Army is taking a more philosophical approach than Navy. This partly reflects that the changes to Army education and training that AI bring may be far-reaching. Army personnel often perceive their service as being personnel not equipment oriented. An oft used saying declares that 'Army equips the man, but Navy and Air Force man the equipment.' This logic would suggest Navy and Air Force would find it easier to adjust their existing education and training approach as AI is simply another digital technology to absorb. There is an emerging belief that in the age of AI, Army may have to rethink the importance of technical training to be comparable to the other services.

Looking to the future, with AI already proliferated across the commercial domain, AI is similarly likely to proliferate across Army. It may be used in intelligence analysis, strategic decision support, operational planning, command and control, logistics, and weapon systems. To use AI however, organizations will need their personnel to be well informed to both shape the application of AI and provide quality assurance (Ryan 2018).

Armies will need more than just deep technical experts in the development of algorithms and the design of AI for military systems. Army's future workforce using AI should be a mix of those with a basic understanding, more informed users, and specialists with advanced skills. Over the coming years, at almost every rank level, Army personnel will require basic literacy in AI, including knowledge of its application, how to provide a level of assurance and quality control, and how to optimally combine it with human intelligence. The Army's military education and training system does not currently provide technological literacy for all their personnel. However, it is the coupling of technical experts with a heightened technological literacy across the entire force that will allow future military organizations to fully exploit the benefits of artificial intelligence.

6.4 Enhanced Training Using AI

AI may change the way militaries educate their personnel. AI tutoring systems can already provide one-on-one human tutoring and this concept could be further developed into having an AI lifelong-learning partner accompanying individuals from entry into the military and through their career. In a similar manner, military instructors may have their own teaching assistant able to communicate with their students' AI partners to interpret individual students' profiles and provide suggestions on tailored learning.

AI may also help develop the cognitive skills that underpin higher-level operational and strategic planning in teams. This could be done by offering more authentic environments for collaborative learning, large-scale wargame simulations, providing more intelligent adversary systems to challenge students, and using

purpose-designed algorithms and curriculum data to amalgamate lessons from previous activities (Ryan 2018).

Field training using AI has both benefits and warnings. Training will need to evolve to properly incorporate human-machine teams, but these teams should not become overly dependent, complacent, or uncritical in using the technology. Training scenarios must develop users who 'trust but verify', that is, have confidence in the AI without being uncritically accepting of it. In this regard, data powers AI machine learning. Capturing and managing the data generated in training environments will be important to refine machine learning and system improvement (RAS-AI Strategy 2020: 19).

7 Conclusion

The ADF's conception of AI's utility for defence purposes is fairly conventional. AI is mainly conceived as being used in human-machine teams to improve efficiency, increase mass, and achieve decision superiority while decreasing risk to personnel. Even so, middle power Australia is following a relatively active AI development program with a well-defined innovation pathway and numerous experimentation projects underway.

There is also a reasonable level of force structure ambition. The latest major equipment acquisition plan, covering the next 10–20 years, sets out six defence AI-relevant projects, one Navy, one Army, three Air Force and one information and cyber domain. Even in this decade, the AI associated projects are quite substantial and include Air Force Teaming Air Vehicles (est. cost €6.15bn), Integrated Undersea Surveillance System (est. €4.19bn), Joint Air Battle Management System (est. €1.55bn) and Distributed Ground Station Australia (est. €1.01bn).

Associated with this investment is a high expectation that there will be considerable involvement by Australian AI companies. Indeed, as of recently AI has been determined to be a Sovereign Industrial Capability Priority. The Australian defence AI sector though is mainly comprised of multiple SMEs that individually lack the scale necessary for major equipment projects and would need to partner with large prime contractors to achieve the requisite industrial heft. There are also wider national concerns about whether Australia will have a large enough AI workforce over the next decade to handle commercial demands, even without Defence drawing people away for its requirements. Both factors suggest Defence could end up buying its AI offshore and principally rely on long-term foreign support, as it does in many other major equipment projects.

An alternative to simple offshore purchases might be funding collaborative AI developments with the US military. A harbinger of this may be the Australian Navy's new experimentation program that involves a recently decommissioned patrol boat being fitted with Austal-developed autonomous vessel technology, featuring AI. Austal is also involved simultaneously in a much larger US Navy program fitting its system to one of the company's Expeditionary Fast Transport, the

USNS Apalachicola (Austal 2023). In this case, Austal is an Australian company with a large US footprint and so able to work collaboratively within both countries. There is a strong possibility though that the Australian Navy, simply because of economies of scale, is likely to adopt the US Navy variant of Austal's work rather than a uniquely Australian version.

The outlier in this option might be the Boeing Australia Ghost Bat program that may see AI-enabled, loyal wingman type, uncrewed air vehicles in limited operational service with the ADF in 2024, and thus before the US services. The US Air Force is running several experimentation programs aiming to develop suitable technologies, some of which also involve the Boeing parent company. There is a high likelihood of cross-fertilization between Australian and US programs. This raises the tantalizing possibility of a two-nation support system of a scale that would allow the Australian companies involved to grow to a size suitable for long term sustainment of the relevant ADF AI capabilities. This possibility might be a one-off however, as there seems to be no other significant Australian AI program.

Australia collaborating with the US on AI or buying US AI products can ensure interoperability. However, in seeking such an objective there is always a tension between being interoperable with either specific individual US forces or instead across the whole of the ADF. This tension is likely to remain as AI enters service, especially given its demands for compatible big data.

Interoperability and domestic industry support maters are important issues that to varying degrees have influenced Australian government decisions on major capital equipment acquisitions for many decades. These traditional concerns though may need to be counter-balanced by emerging geostrategic uncertainties and ADF capability considerations.

Australia is now becoming worried about the possibility of conflict in the Indo-Pacific region given rising Chinese assertiveness coupled with the example of Russia's invasion of Ukraine. To offset the numerically large military forces of the more belligerent Indo-Pacific states, some advocate developing a higher quality, technologically superior ADF able to help deter regional adventurism.

In being a general-purpose technology, AI can potentially provide a boost across the whole ADF, not just one or two elements within it. Such a vision though is not what is being pursued. Current AI plans will most likely lead to evolutionary improvements not revolutionary changes. AI is conceived as being used to either enhance, augment, or replace existing capability; this approach will mean the future ADF will do things better, but not necessarily be able to do better things.

A revolution in Australian military affairs seems unlikely under present schemes. For this, defence AI would need to be reconceptualized as a disruptive technology not a sustaining innovation. Embracing a disruptive approach would be intellectually demanding and in suggesting adopting unproven force structures could involve taking strategic risks. These are reasonable concerns that would need careful management.

Against such worries though, must be balanced the risk of China's People's Liberation Army successfully fielding disruptive AI and suddenly becoming qualitatively and quantitively superior to other Indo-Pacific militaries. The business of

making war inherently involves balancing risks. Given the stakes, it might be time for Australia to embrace disruptive AI, rather than playing safe with a sustaining innovation approach that simply replicates current force structure thinking. The strategically intelligent choice might be doubling down on artificial intelligence.

References

ADM. 2022. Consilium Technology designs and tests AI capability for air 6500. *ADM: Australian Defence Magazine*. https://www.australiandefence.com.au/defence/air/consilium-technology-designs-and-tests-ai-capability-for-air-6500. Accessed 30 Jan 2024

Air Force. 2021. Jericho: connected, integrated. *Air Force*. https://airpower.airforce.gov.au/sites/default/files/2021-03/AF14-Plan-Jericho.pdf. Accessed 30 Jan 2024

Airforce Technology. 2023. *MQ-28A Ghost Bat Unmanned Aircraft, Australia*. https://www.airforce-technology.com/projects/loyal-wingman-unmanned-aircraft/. Accessed 30 Jan 2024

APDR. 2022. Consunet Developing AI Technologies for AIR6500. APDR: Australian Pacific Defence Reporter. https://asiapacificdefencereporter.com/consunet-developing-ai-technologies-for-air6500/. Accessed 30 Jan 2024

Army. 2022. Robotic & autonomous systems strategy. *Australian Government*. https://research-centre.army.gov.au/sites/default/files/Robotic%20and%20Autonomous%20Systems%20Strategy%20V2.0.pdf. Accessed 30 January 2024

ASCA. 2023. https://www.asca.gov.au/. *ASCA: Advanced Strategic Capabilities*. Accessed 30 Jan 2024

Australian Defence Force. 2020. Concept for robotic and autonomous Systems. *Australian Government*. https://tasdcrc.com.au/wp-content/uploads/2020/12/ADF-Concept-Robotics.pdf. Accessed 30 Jan 2024

Austal. 2023 Accelerating A 'Smart' path to autonomous capability. *Austal*. https://www.austal.com/ships/autonomous-ships. Accessed 30 Jan. 2024

Australian Trade and Investment Commission. 2022. Sydney AI startup launches HR tech services in Silicon Valley. *Australian Trade and Investment Commission*. https://www.austrade.gov.au/landingpads/news/case-studies/sydney-ai-startup-launches-hr-tech-services-in-silicon-valley. Accessed 30 Jan 2024

CSIRO. 2023. National artificial intelligence Centre. *CSIRO*. https://www.csiro.au/en/work-with-us/industries/technology/national-ai-centre. Accessed 30 Jan 2024

Defence. 2020a. Force structure plan 2020. *Australian Government*. https://www.defence.gov.au/sites/default/files/2020-11/2020_Force_Structure_Plan.pdf. Accessed 30 Jan 2024

———. 2020b. More, together: Defence science and Technology strategy 2030. *Australian Government*. https://www.dst.defence.gov.au/sites/default/files/basic_pages/documents/Defence%20Science%20and%20Technology%20Strategy%202030.pdf. Accessed 30 Jan 2024

———. 2021. Defence data strategy 2021–2023. *Australian Government*. https://www.defence.gov.au/sites/default/files/2021-08/DataStrategy2_0.pdf. Accessed 30 Jan 2024

———. 2022. Sovereign industrial capability priorities. *Australian Government*. https://www.defence.gov.au/sites/default/files/2021-09/Sovereign-Industrial-Capability-Priorities-Factsheet.pdf. Accessed 30 Jan 2024

———. 2023a. Major changes to Army announced. https://www.defence.gov.au/news-events/news/2023-09-28/major-changes-army-announced. Accessed 30 Jan 2024

———. 2023b. *Defence Artificial intelligence research network contracts signed*. https://www.defence.gov.au/news-events/releases/2023-03-06/defence-artificial-intelligence-research-network-contracts-signed. Accessed 30 Jan 2024

———. 2023c. *AUKUS Defense Ministers Meeting Joint Statement*. https://www.defense.gov/News/Releases/Release/Article/3604511/aukus-defense-ministers-meeting-joint-statement/. Accessed 30 Jan 2024

Defence Science and Technology Group. 2022a. *Australian Defence Science and Universities Network ADSUN*. https://www.dst.defence.gov.au/partner-with-us/university/adsun. Accessed 30 Jan 2024

———. 2022b. National security science and technology Centre. *Defence Science and Technology Group*. https://www.dst.defence.gov.au/nsstc. Accessed 30 Jan 2024

Department of Industry, Science and Resources. 2021. Australia's Artificial Intelligence (AI) Action Plan. *Australian Government*. https://www.industry.gov.au/publications/australias-artificial-intelligence-action-plan. Accessed 30 Jan 2024

Department of Prime Minister and Cabinet. 2022. *FACT SHEET: Implementation of the Australia–United Kingdom–United States Partnership (AUKUS)*. https://pmtranscripts.pmc.gov.au/sites/default/files/AUKUS-factsheet.pdf. Accessed 30 Jan 2024

Felton, Ben. 2023. AUKUS partners to develop common control system for drones. *Naval News*. https://www.navalnews.com/event-news/indo-pacific-2023/2023/11/aukus-partners-to-develop-common-control-system-for-drones/. Accessed 30 Jan 2024

Ferguson, Gregor. 2023. *Army fires live weapons from autonomous vehicle*. EX2. https://www.ex2.com.au/news/army-fires-live-weapons-from-autonomous-vehicle/. Accessed 30 Jan 2024

Henneke, George. 2023. Defence innovation: A view from indo-Pacific 2023. *The Strategist*. https://www.aspistrategist.org.au/defence-innovation-a-view-from-indo-pacific-2023/. Accessed 30 Jan 2024

Hilder, Emily, and Monro, Tanya. 2023. *Accelerating Defence innovation: The strategic imperative for change*. InnovationAus.com. https://www.innovationaus.com/accelerating-defence-innovation-the-strategic-imperative-for-change/. Accessed 30 Jan 2024

Laird, Robbin. 2021. *The Australian Army, navy and air Force shape a way ahead for the inclusion of autonomous systems*. SLDinfo.com. https://sldinfo.com/2021/06/the-australian-army-navy-and-air-force-shape-a-way-ahead-for-the-inclusion-of-autonomous-systems/. Accessed 30 Jan 2024

Levick, Ewen. 2020. Keeping the M113 relevant as unmanned platforms. *ADM: Australian Defence Magazine*. https://www.australiandefence.com.au/partners/keeping-the-m113-relevant-as-unmanned-platforms. Accessed 30 Jan 2024

Naval Technology. 2023. Bluebottle Unmanned Surface Vessels (USV), Australia. *Naval Technology*. https://www.naval-technology.com/projects/bluebottle-unmanned-surface-vessels-usv-australia/?cf-view&cf-closed. Accessed 30 Jan 2024

Navy. 2020. RAS-AI Strategy 2040. *Australian Government*. https://www.navy.gov.au/sites/default/files/documents/RAN_WIN_RASAI_Strategy_2040f2_hi.pdf. Accessed 30 Jan 2024

———. 2022. RAS-AI Campaign Plan 2025. *Australian Government*. https://www.navy.gov.au/sites/default/files/documents/RAS-AI%20Campaign%20Plan%202025.pdf. Accessed 30 Jan 2024

Packham, Ben. 2023. Air Force names its price for drones. *The Australian*. https://www.theaustralian.com.au/nation/defence/air-force-names-its-price-for-drones/news-story/92dee8652759a9312e3442785b05d798. Accessed 30 Jan 2024

Robotics Australia Group. 2022. Robotics roadmap for Australia 2022. *Robotics Australia Group* https://roboausnet.com.au/wp-content/uploads/2021/11/Robotics-Roadmap-for-Australia-2022_compressed-1.pdf. Accessed 30 Jan 2024

Ryan, Mick. 2018. *Intellectual Preparation for Future War: How Artificial Intelligence Will Change Professional Military Education. War on the Rocks*. https://warontherocks.com/2018/07/intellectual-preparation-for-future-war-how-artificial-intelligence-will-change-professional-military-education/. Accessed 30 Jan 2024

Savage, Crispin. 2022. Universities blaze a trail to commercialise defence research. *Newsroom*. https://www.adelaide.edu.au/newsroom/news/list/2022/04/07/universities-blaze-a-trail-to-commercialise-defence-research. Accessed 30 Jan 2024

Trusted Autonomous Systems. 2022. About Trusted Autonomous Systems. *Defence CRC TAS Ltd*. https://tasdcrc.com.au/about-us/. Accessed 30 Jan 2024

Walsh, Toby. 2023. *Home-grown AI is a key building block for our future*. InovationAus.com. https://www.innovationaus.com/home-grown-ai-is-a-key-building-block-for-our-future/. Accessed 30 Jan 2024