

Uitbreiding strafbaarstelling spionage

'Verdediging van de Nederlandse soevereiniteit versterkt'



December 2020
Jeroen van Wijngaarden

De huidige strafbaarstelling van buitenlandse spionage schiet tekort

Spionage is schadelijk voor onze veiligheid, onze economie en ondermijnt onze vrije samenleving. Daarom hebben we de afgelopen jaren flink geïnvesteerd in onze veiligheidsdiensten, waaronder miljoenen in cybersecurity en het weerbaar maken van bedrijven. Maar we zijn er nog niet. Onze inlichtingendiensten waarschuwen dat we niet naïef moeten zijn over de gevaren van buitenlandse spionage. Een kwetsbaarheid is ook dat een Nederlander die heimelijk samenwerkt met een buitenlandse inlichtingendienst niet strafbaar is.

Een Nederlander die in opdracht van een buitenlandse inlichtingendienst in de gaten houdt welke wetenschappers, ambtenaren of medewerkers van bedrijven mogelijk open zouden staan (bijvoorbeeld vanwege financiële privéproblemen) om tegen betaling vertrouwelijke informatie te verkopen zou bijvoorbeeld lastig te vervolgen zijn. Hetzelfde geldt voor iemand die in opdracht van een buitenlandse inlichtingendienst gevluchte politieke tegenstanders in Nederland in de gaten houdt en over hen rapporteert. Ook iemand die in samenwerking met de Russische inlichtingendienst bewust en opzettelijk onwaarheden verspreidt aan de hand van, door diezelfde inlichtingendienst via hacken bemachtigde documenten rondom de ramp met vlucht MH17, zou bijvoorbeeld lastig te vervolgen zijn.

De VVD wil dat heimelijke samenwerking met een buitenlandse geheime dienst strafbaar wordt met vier jaar gevangenisstraf en zal het kabinet vragen hiertoe een wetsvoorstel te maken. Strafbaarstelling van spionage biedt de mogelijkheid voor de inlichtingen- en veiligheidsdiensten om een ambtsbericht uit te brengen op basis waarvan het Openbaar Ministerie vervolging kan instellen. De diensten verrichten uitstekend werk, maar hun werk bestaat uit monitoren en waarschuwen. Om echt op te treden moeten politie en justitie uiteindelijk kunnen opsporen en vervolgen. Ons huidige Wetboek van Strafrecht biedt in zulke gevallen onvoldoende mogelijkheden om spionage adequaat te vervolgen.

De strafrechtelijke mogelijkheden om spionage tegen te gaan zijn nu te beperkt. Het schenden van staatsgeheimen, ambtsgeheimen en bedrijfsgeheimen is in Nederland strafbaar, evenals diverse vormen van corruptie. Pas wanneer iemand staatsgeheime informatie deelt, spionagesoftware installeert of een hack uitvoert kan het Openbaar Ministerie overgaan tot vervolging. Iemand die voor een buitenlandse inlichtingendienst werkt is dus pas strafbaar als hij of zij op heterdaad betrapt wordt. Wij willen de samenwerking zelf strafbaar stellen, zodat je ook zonder een betrapping op heterdaad kunt vervolgen. Dit is qua gedachte vergelijkbaar met hoe iemand vervolgd kan worden voor deelname aan een criminele organisatie, los van eventuele bewezen concrete daden zoals moord of het transporteren van drugs. Dit opent ook de mogelijkheid om mensen aan te pakken die operationeel aangestuurd worden door een buitenlandse inlichtingendienst met een ander doel dan dat zij zelf een staatsgeheim schenden, bijvoorbeeld door zoals eerder genoemd agenten te spotten en mogelijk te rekruteren.

De huidige delictsomschrijvingen rond spionage zijn nu onvoldoende om dit fenomeen in de volle breedte aan te pakken. Hierdoor ontbreekt nu een duidelijke normstelling vanuit de overheid ten aanzien van inlichtingenactiviteiten, terwijl

deze een ernstige inbreuk vormen op de Nederlandse soevereiniteit en het veilig en vrij functioneren van de samenleving. Op dit moment blijft die inbreuk vrijwel altijd zonder strafrechtelijke gevolgen, waardoor Nederland een relatief aantrekkelijk land is voor andere mogendheden om spionageactiviteiten te ontplooiën. Ook in het jaarverslag 2018 van de AIVD zijn er steeds meer landen die inzetten op politieke en/of economische spionage. Hierbij geldt dat (digitale) spionageactiviteiten steeds complexer en brutaler worden. Ook constateert de AIVD in het jaarverslag 2018 dat buitenlandse mogendheden interesse hebben in Nederlandse bedrijven uit de sectoren hightech, energie, maritiem en life sciences & health. Nederland is een aantrekkelijk land, maar dat geldt helaas ook voor kwaadwillende inlichtingendiensten. Door onze open economie staan we open voor mensen en bedrijven uit het buitenland en is bij bedrijven en kennisinstellingen een hoogwaardige kennis aanwezig. Ook zijn veel internationale instellingen hier gevestigd.

Met een specifieke strafbaarstelling van spionage wordt het mogelijk om personen die heimelijk activiteiten verrichten voor en/of informatie verschaffen aan buitenlandse mogendheden, inlichtingendiensten in het bijzonder, in Nederland te vervolgen.

Met strafbaarstelling spreekt de overheid zich daarnaast principieel uit over spionage en zorgt zij voor een instrument om op te treden tegen aantasting van de nationale soevereiniteit.

Wij willen spionage strafbaar stellen, zodat een Nederlander die heimelijk samenwerkt met een buitenlandse inlichtingendienst kan worden vervolgd.

Daarnaast pleiten wij voor een verplichte registratie voor alle individuen, bedrijven, onderwijsinstellingen en andere organisaties die openlijk of achter de schermen belangen van andere landen behartigen. In de Verenigde Staten¹ en Australië² heeft men goede ervaringen met zulke registers. Een openbaar register waarin alle *foreign influence agents* zich verplicht moeten inschrijven op straffe van een gevangenisstraf draagt eraan bij dat het voor iedereen binnen de overheid en het bedrijfsleven duidelijk is wiens belangen worden vertegenwoordigd, waarbij we in het oog houden dat een dergelijk register complementair is aan een duidelijke strafbaarstelling voor spionage.

Bronnen:

- Brede Maatschappelijke Heroverweging 16: "Speelbal of spelverdeler?" p. 94-95.
- Concept-verkiezingsprogramma VVD 2021-2025 p. 48
- AIVD Publicatie: Spionage, hoe herken je het en wat kun je ertegen doen?
- Artikel "Nederlandse MH-17 activist blijkt schaakstuk voor Russische inlichtingendienst" <https://www.groene.nl/artikel/nederlandse-mh17-activist-blijkt-schaakstuk-voor-russische-inlichtingendienst>

¹ <https://www.justice.gov/nsd-fara>

² <https://www.ag.gov.au/integrity/foreign-influence-transparency-scheme>

- Artikel "The GRU's MH17 Disinformation Operations Part 1: The Bonanza Media Project" <https://www.bellingcat.com/news/uk-and-europe/2020/11/12/the-grus-mh17-disinformation-operations-part-1-the-bonanza-media-project/>



Algemene Inlichtingen- en
Veiligheidsdienst
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Spionage

Hoe herken je het en wat
kun je ertegen doen?



Spionage is iets van alle tijden en vormt een grote bedreiging voor Nederland. Tegelijkertijd is spionage haast onzichtbaar en zijn weinig mensen zich bewust van de gevaren. In Nederland wordt door allerlei landen gespioneerd. Niet alleen digitaal, maar ook op de klassieke manier: door mensen in te zetten. Waarom gebeurt dit en waarom is het schadelijk? Belangrijker nog: hoe herken je spionage en wat kun je ertegen doen?

Wat is spionage?

Het doorspelen van kennis over het Nederlandse buitenlandbeleid, het kopiëren en tegen betaling overhandigen van documenten van de Europese Commissie of het hacken van een hightech-bedrijf om bedrijfsgeheimen buit te maken. Het zijn allemaal voorbeelden van spionage. Maar wat is spionage? Spionage is het op heimelijke wijze verzamelen van inlichtingen (informatie) of objecten (bijvoorbeeld producten of machines). Het kan bijvoorbeeld gaan om gevoelige (persoons)informatie, technologie of staatsgeheimen.

Nederland is een aantrekkelijk doelwit voor spionage. Ons land is lid van de Noord-Atlantische Verdragsorganisatie (NAVO) en de Europese Unie (EU) en beschikt over interessante informatie. Daarnaast zijn we gastland van tal van internationale organisaties zoals de Organisatie voor het Verbod op Chemische Wapens (OPCW) en het Internationaal Strafhof (ICC). Ook beschikken de Nederlandse universiteiten en het bedrijfsleven over veel kennis en hoogwaardige technologie. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) heeft als taak spionage te onderkennen, te helpen beëindigen en de bewustwording ervan te vergroten.

Wie spioneren en waarom doen ze dit?

Allerlei landen spioneren in en tegen Nederland om informatie of objecten te bemachtigen waarmee zij hun voordeel kunnen doen. Er zijn verschillende redenen om te spioneren. Zo kan een land geëmigreerde landgenoten in het buitenland in de gaten houden om te controleren of ze een bedreiging voor het regime vormen. Of ze brengen de politieke situatie en het besluitvormingsproces in Nederland in kaart om daar invloed op uit te oefenen. Ook kunnen ze economische kennis stelen om de eigen economie te bevorderen.

Sommige landen spioneren op grote schaal en beschikken over professionele inlichtingendiensten om dit werk zo goed mogelijk uit te voeren. De AIVD doet onderzoek naar deze landen. Welke landen de grootste dreiging vormen, is sterk afhankelijk van de (inter)nationale situatie. Verhoudingen tussen landen kunnen snel veranderen waardoor nieuwe spelers op het toneel verschijnen op het gebied van spionage.

Hoe wordt er gespioneerd?

Buitenlandse inlichtingendiensten spioneren op verschillende manieren. Tegenwoordig wordt er veel digitaal gespioneerd: inlichtingendiensten hacken computers om informatie ongezien te stelen. Ministeries, onderzoekscentra en bedrijven

in de hightech-, chemie- en energiesector worden veelvuldig digitaal aangevallen.

Spionage gebeurt ook nog steeds op de klassieke manier, door het benaderen van personen om via hen toegang te krijgen tot informatie. Medewerkers van inlichtingendiensten zoeken naar interessante gesprekspartners (bronnen) zoals ambtenaren, wetenschappers, topfunctionarissen en journalisten. Ook mensen in ondersteunende functies kunnen interessant zijn voor inlichtingendiensten, omdat ook zij toegang kunnen hebben tot vertrouwelijke informatie.

Waarom is spionage schadelijk?

Spionage gebeurt buiten het oog van de samenleving. Voor veel mensen is het moeilijk voorstelbaar dat spionage schadelijk is voor de nationale veiligheid, maar deze heimelijke manier van informatiegaring kan wel degelijk een grote impact hebben. Als een ander land bijvoorbeeld toegang krijgt tot geheime informatie, dan kan dat land de informatie gebruiken om besluitvorming te beïnvloeden of andere maatregelen te nemen. Landen kunnen informatie over de eigen bevolking in het buitenland gebruiken om tegenstanders te intimideren of zelfs uit te schakelen.

Spionage kan ook economische schade veroorzaken. Zodra andere landen toegang hebben tot vertrouwelijke

bedrijfsinformatie, heeft dit impact op de financiële positie van die bedrijven. Als blauwdrukken en unieke apparatuur worden gekopieerd, hoeft het land dat spioneert de (veelal hoge) onderzoeks- en ontwikkelingskosten niet meer zelf te betalen. Dit kan ertoe leiden dat het Nederlandse bedrijf minder producten verkoopt of de concurrentiestrijd met het buitenlandse bedrijf niet aankan. Wetenschappelijke projecten waarvan de resultaten en methoden stiekem worden overgenomen voor gebruik in een ander land, kunnen ervoor zorgen dat de financiering niet meer rendabel is. Ook is er een risico dat kennis over atoomtechnologie in de verkeerde handen valt. Het is daarom belangrijk dat vertrouwelijke informatie of technologie niet zomaar kan worden weggesluisd naar andere landen.

Hoe herken je spionage?

Spionage is grotendeels mensenwerk. Stel, je hebt interessante informatie en je valt daarom op bij een inlichtingendienst. Dan proberen zij via een medewerker met jou in contact te komen. Deze persoon zal proberen een vertrouwensrelatie met jou op te bouwen. Hij of zij doet zich bijvoorbeeld voor als diplomaat, journalist of ondernemer om op een natuurlijke manier in contact te komen. Toch zijn er bepaalde signalen waardoor je kunt merken dat je met een medewerker van een inlichtingendienst te maken hebt.

Inlichtingendiensten doen vaak uitgebreid vooronderzoek naar personen die mogelijk interessant voor ze zijn. Op internet zoeken ze bijvoorbeeld naar mensen die toegang hebben tot gevoelige dossiers. Ook zoeken ze naar persoonlijke informatie, zoals hobby's of een lidmaatschap van een sportclub, om iemand beter te leren kennen. Deze informatie wordt gebruikt om 'spontaan' met jou in contact te komen.

Is het eerste contact geslaagd? Dan volgen vaak meer ontmoetingen. Je wordt mee uit eten genomen, krijgt cadeaus en denkt misschien een vriendschap op te bouwen. Afspraken vinden vooral buiten de deur plaats en de medewerker van de inlichtingendienst heeft buitengewoon veel belangstelling voor jouw privé-zaken. Maar hij of zij heeft al die tijd maar één doel: jou zover krijgen om te spioneren. Uiteindelijk zal de medewerker van de inlichtingendienst vragen om tegen betaling informatie te leveren. In het begin misschien onbenullige informatie, een test om te kijken hoe ver je bereid bent te gaan, maar later ook gevoelige documenten waar jij toegang toe hebt.

Wat kun je doen tegen spionage?

Het helpt al om je bewust te zijn van het feit dat spionage bestaat. Als je een vreemd gevoel krijgt bij een contact is het altijd verstandig om je terughoudend op te stellen en dit

te melden bij de afdeling veiligheid van je werkgever. Door signalen te herkennen kun je spionage voor zijn. Vermoed je spionage door een inlichtingendienst? Meld dit dan bij je werkgever en de AIVD: aivd.nl/contact

Realiseer je hoe waardevol informatie over jouw werk en netwerk kan zijn. Informatie waar jij makkelijk bij kunt, zoals onschuldig ogende dossiers of werkomstandigheden, kan voor een inlichtingendienst interessant zijn. Ook kan een inlichtingendienst interesse hebben in jouw relatie met belangrijke personen.

Vind een goede balans in wat je online deelt over jezelf en je werk. Zet bijvoorbeeld niet op LinkedIn of Facebook dat je aan gevoelige dossiers werkt. Wees je bewust van wat je deelt en vooral met wie.

Bescherm je apparatuur. Inlichtingendiensten kunnen geïnteresseerd zijn in de informatie die op je telefoon of laptop staat. Wees alert op phishing mails, installeer beveiligingssoftware en houd deze up-to-date. Ook is het verstandig om tijdens zakenreizen apparatuur waar waardevolle informatie op staat bij je te houden en niet in te checken bij je ruimbagage. Lees ook de AIVD-publicatie 'Op reis naar het buitenland – Veiligheidsrisico's onderweg'.

Natuurlijk heb je niet automatisch met een inlichtingendienst te maken als je in contact komt met iemand uit een ander land.

Het is wel goed om je bewust te zijn van de aard van de relatie. Zorg ervoor dat je niet afhankelijk wordt van de ander en wees je bewust van de achterliggende intentie van je contacten.

Meer weten?

Wil je meer weten over spionage en de rol van de AIVD? Kijk dan op aivd.nl/spionage.



Colofon

Deze brochure is een uitgave van:

Algemene Inlichtingen- en Veiligheidsdienst

aivd.nl

Postbus 20010 | 2500 EA Den Haag

mei 2020

Optie 22 Strafbaarstelling spionage

Huidig beleid

Buitenlandse mogelijkheden kunnen op allerlei manieren op heimelijke wijze informatie verzamelen in en over Nederland waardoor Nederlandse belangen kunnen worden geschaad. Het kan gaan om klassieke vormen van spionage, zoals het verwerven van vertrouwelijke of staatsgeheime informatie en de beïnvloeding van de politiek-ambtelijke besluitvorming, maar bijvoorbeeld ook om (digitale) economische spionage. Deze vorm van spionage kan het verdienvermogen van Nederlandse bedrijven ondermijnen wat op termijn kan resulteren in economische en politieke afhankelijkheden. Vaak worden de spionageactiviteiten in Nederland uitgevoerd door buitenlandse inlichtingendiensten die daarbij gebruik maken van Nederlandse staatsburgers en ingezetenen.

De strafrechtelijke mogelijkheden om deze vorm van spionage tegen te gaan zijn beperkt. Dit heeft te maken met het ontbreken van specifieke wet- en regelgeving op het gebied van spionage. Het schenden van staatsgeheimen, ambtsgeheimen en bedrijfsgeheimen is strafbaar, evenals diverse vormen van corruptie. De delictsomschrijving is echter in veel gevallen van spionage niet passend en heimelijke samenwerking met een buitenlandse inlichtingendienst is op zichzelf niet strafbaar.

Het ontbreken van een specifieke strafbaarstelling heeft bovendien tot gevolg dat er geen duidelijke normstelling is vanuit de overheid ten aanzien van dergelijke inlichtingenactiviteiten, terwijl deze een ernstige inbreuk vormen op de Nederlandse soevereiniteit. Op dit moment blijft die inbreuk vrijwel altijd zonder strafrechtelijke gevolgen, waardoor Nederland een relatief aantrekkelijk land is voor andere mogelijkheden om spionageactiviteiten te ontplooiën.

Omschrijving beleidsoptie

Zoals geconstateerd in het jaarverslag 2018 van de AIVD zijn er steeds meer landen die inzetten op politieke en/of economische spionage. Hierbij geldt dat (digitale) spionageactiviteiten steeds complexer en brutaler worden. Ook constateert de AIVD in het jaarverslag 2018 dat buitenlandse mogelijkheden interesse hebben in Nederlandse bedrijven uit de sectoren hightech, energie, maritiem en life sciences & health.

Met een specifieke strafbaarstelling van spionage wordt het mogelijk om personen die heimelijk activiteiten verrichten voor en/of informatie verschaffen aan buitenlandse mogelijkheden, inlichtingendiensten in het bijzonder, in Nederland te vervolgen.

Met strafbaarstelling spreekt de overheid zich daarnaast principieel uit over spionage en zorgt zij voor een instrument om op te treden tegen aantasting van de nationale soevereiniteit.

Effecten, voor- en nadelen

- + Strafbaarstelling van spionage biedt de mogelijkheid voor de inlichtingen- en veiligheidsdiensten om een ambtsbericht uit te brengen.
- + Van dergelijke wetgeving gaat een preventieve werking uit.
- + Normstelling overheid ten aanzien van spionage en bescherming soevereiniteit.
- Vergt een wetwijziging (aanpassing van het Wetboek van Strafrecht).
- Strafbaar gedrag moet voldoende concreet omschreven worden.
- Bewijsbaarheid en handhaving is naar verwachting lastig.

Uitvoering

Niet van toepassing.

Niveau van overheidsoptreden

Nationaal.

Budgettaire gevolgen

Financiële gevolgen voor OM en politie zullen bij de uitwerking in worden kaart gebracht.