Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

3284

Vragen van de leden **Van den Berg** en **Amhaouch** (beiden CDA) aan de Ministers van Economische Zaken en Klimaat en van Justitie en Veiligheid over *het bericht «Chinese spionnen stelen kostbare bedrijfsgeheimen van ASML»* (ingezonden 12 april 2019).

Antwoord van Minister **Wiebes** (Economische Zaken en Klimaat), mede namens de Minister van Justitie en Veiligheid (ontvangen 3 juli 2019). Zie ook Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 2552.

Vraag 1
Bent u bekend met het bericht «Chinese spionnen stelen kostbare bedrijfsgeheimen van ASML»?[1]

Antwoord 1
Ja.

Vraag 2, 3 en 4
Wat is uw reactie op dit bericht?
Deelt u de mening dat hier geen sprake is van een incident, maar dat deze diefstal past in een patroon van toenemende Chinese invloed in de westerse wereld en in Nederland?
Deelt u de mening dat deze ontwikkeling zorgelijk en onwenselijk is?

Antwoord 2, 3 en 4
Uit de ons bekende informatie blijkt dat er sprake is van diefstal van bedrijfsvertrouwelijke informatie door ex-werknemers van de Amerikaanse vestiging van ASML. Deze diefstal van bedrijfsvertrouwelijke gegevens betreft een ernstig incident bij ASML. Ik heb geen aanwijzingen dat er in casu sprake is geweest van directe betrokkenheid van een buitenlandse overheid. Er zijn wel overeenkomsten te zien met bekende Chinese spionagedoelwitten en -werkwijzen.
In algemene zin zien wij een ontwikkeling dat staten op steeds assertievere wijze hun eigen belangen behartigen en bereid zijn om middelen in te zetten die onze welvaart, stabiliteit en openheid kunnen aantasten. Steeds meer landen richten zich hierbij op politieke en/of economische spionage.

[1] Financieele Dagblad, 11 april 2019, https://fd.nl/ondernemen/1296245/chinese-spionnen-stelen-kostbare-bedrijfsgeheimen-van-asml.

ah-tk-20182019-3284
ISSN 0921 - 7398
's-Gravenhage 2019

Op 18 april jl. is uw Kamer over de dreigingen vanuit staten en de aanpak hierop geïnformeerd. Ook de AIVD en MIVD geven in hun jaarverslagen aan dat de grootste dreiging op het gebied van economische spionage van China komt.[2] [3] Hierbij zet China een breed scala aan (heimelijke) middelen in die het verdienvermogen van Nederlandse bedrijven kunnen ondermijnen.

Vraag 5
Heeft de diefstal bij ASML in de Verenigde Staten Nederlandse belangen geschaad?

Antwoord 5
Met betrekking tot het bedrijfsbelang geeft ASML aan dat het bedrijf geen omzetverlies heeft geleden als gevolg van gemiste verkoop. Het gestolen materiaal is teruggevorderd en de ASML-klant die door XTAL was verleid om over te stappen is weer terug bij ASML. De definitieve vergoeding van 845 miljoen dollar die de Californische rechter aan ASML heeft toegekend is gebaseerd op ongerechtvaardigde verrijking in relatie tot de gestolen bedrijfsgeheimen.

Vraag 6
Kan deze diefstal gevolgen hebben voor onze nationale veiligheid?

Antwoord 6
De software is onderdeel van de portefeuille van ASML en wordt gebruikt voor de optimalisatie van het chipproductieproces bij de klanten van ASML. De diefstal van deze software heeft op zichzelf geen directe gevolgen voor de nationale veiligheid.

Vraag 7
Kunt u in kaart laten brengen hoe deze diefstal precies heeft kunnen plaatsvinden en hoe we op basis van die analyse met bedrijven de juiste maatregelen kunnen nemen?

Antwoord 7
Het betreft hier een geval van diefstal van bedrijfsvertrouwelijke gegevens door ex-werknemers die zich in 2015 heeft afgespeeld in de Amerikaanse vestiging van het bedrijf die aldus valt onder Amerikaans recht. Het is primair de verantwoordelijkheid van het betreffende bedrijf om maatregelen te treffen. Zo daartoe aanleiding bestaat, is het aan de Amerikaanse autoriteiten om in deze casus eventuele strafrechtelijke maatregelen te nemen. Technologiediefstal bij bedrijven via (oud)medewerkers is een breder fenomeen dat zich ook in Nederland voordoet. De rol van de overheid is gericht op bewustwording en weerbaarheidsverhoging. Hiermee wordt bijvoorbeeld gedoeld op het delen van dreigingsinformatie en beveiligingsadvies.

Vraag 8
Heeft u signalen dat China deze «modus operandi», namelijk spionage en diefstal via medewerkers die banden hebben met de Chinese overheid, vaker en op meer plekken toepast?

Antwoord 8
Er is in deze casus geen directe betrokkenheid van de Chinese overheid vastgesteld.
Zoals aangegeven in het antwoord op vragen 2, 3 en 4 proberen staten op steeds assertievere wijze hun eigen belangen te behartigen. In de jaarverslagen van de AIVD en MIVD staat dat China een breed scala aan (heimelijke) middelen inzet die het verdienmodel van Nederlandse bedrijven kunnen ondermijnen, waaronder (digitale) economische spionage.

---

[2] Zie AIVD jaarverslag: https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2018
[3] Zie MIVD jaarverslag: https://www.defensie.nl/downloads/jaarverslagen/2019/04/30/jaarverslag-mivd-2018

Vraag 9
Zijn Nederlandse bedrijven volgens u voldoende beschermd tegen spionage, diefstal van bedrijfsgeheimen en oneigenlijk gebruik van gegevens door China?

Antwoord 9
Bedrijven zijn zelf in eerste instantie zelf verantwoordelijk voor het beschermen van hun bedrijfsvertrouwelijke gegevens. De overheid stelt bedrijven daartoe in staat met behulp van wetgeving op het gebied van intellectueleeigendomsbescherming en bescherming van bedrijfsgeheimen. Op 23 oktober 2018 is de Wet bescherming bedrijfsgeheimen in werking getreden, waaraan ondernemers bescherming kunnen ontlenen als hun bedrijfsgeheim onrechtmatig is verkregen, gebruikt of openbaar gemaakt, ook als dit door een ex-werknemer is gebeurd. Daarnaast kan bescherming ook worden verkregen op basis van het arbeidsrecht of algemene contractenrecht als een ex-werknemer bijv. zijn geheimhoudingsbeding heeft geschonden, of op basis van het algemene onrechtmatigedaadsrecht. Er kan bovendien onder omstandigheden een beroep worden gedaan op bescherming tegen een inbreuk op een octrooirecht of op een chipsrecht op basis van de Wet bescherming oorspronkelijke topografieën van halfgeleiderproducten. Daarnaast heeft de overheid de verantwoordelijkheid voor het creëren van awareness voor risico's en het bieden van een handelingsperspectief.
Zie daarnaast het antwoord op vraag 11, waarin nader wordt ingegaan op de rollen van verschillende overheidsorganisaties waar het bedrijfsleven terecht kan in dit kader.
In de Kamerbrief «Tegengaan statelijke dreigingen» is gemeld dat het kabinet met betrekking tot digitaal financieel economische spionage een verkenning heeft uitgevoerd waarin het beeld ten aanzien van de dreiging is aangescherpt en is bezien welk instrumentarium, complementair aan de maatregelen uit zoals de Internationale Cyber Strategie en de Nederlandse Cyber Security Agenda, van toepassing is om deze dreiging te mitigeren. Aanvullend instrumentarium, zoals bijvoorbeeld vergroting van het bewustzijn van deze dreiging, wordt in de verschillende beleidsterreinen opgenomen, zo ook in de aanpak tegengaan statelijke dreigingen. Het gaat hier ook om het inzetten van internationale samenwerking en diplomatieke instrumenten (inclusief attributie) zoals die in het kader van de EU Cyber Diplomacy Toolbox en om het benutten van bestaande WTO procedures waar nodig.
Bedrijven die opdrachten uitvoeren voor het Ministerie van Defensie worden contractueel Algemene Beveiligingseisen Defensie Opdrachten (ABDO) opgelegd, waanneer die bedrijven van doen krijgen met zogenoemde Te Beschermen (defensie) Belangen (TBB). Defensie controleert de bedrijven op naleving van deze eisen, en de implementatie van beveiligingsmaatregelen.

Vraag 10
Waar zijn bedrijven kwetsbaar en zitten zwakke plekken?

Antwoord 10
De toenemende digitalisering en internationalisering van productieprocessen en arbeidsmarkten vergroten de (digitale) spionagemogelijkheden. In 2010 is uitgebreid onderzoek gedaan naar de spionagerisico's op het terrein van economisch welzijn & wetenschappelijk potentieel en openbaar bestuur & vitale infrastructuur.[4] De conclusies van toen, die overigens los staan van deze casus waarin sprake was van diefstal door oud-medewerkers, zijn ook nu nog actueel. De verschillende mogelijkheden om telecommunicatieverkeer te onderscheppen, zijn een eerste belangrijke geconstateerde kwetsbaarheid. Uit het onderzoek blijkt ook dat de toenemende verwevenheid en complexiteit van computersystemen alsmede het koppelen van dataopslagsystemen, de gevoelige gegevens in systemen kwetsbaar maakt voor spionage. Het uitbesteden van activiteiten als systeem- en serverbeheer, datawarehousing en gegevensverwerking brengt eveneens spionagerisico's met zich mee.

[4] https://www.aivd.nl/documenten/publicaties/2010/04/01/kwetsbaarheidsanalyse-spionage

Met de Handleiding Kwetsbaarheidsanalyse Spionage (KWAS)[5] van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties kunnen instanties zelf een inventarisatie maken van de eigen cruciale belangen en de daarbij behorende kwetsbaarheden.

Vraag 11
Waar in Nederland kunnen bedrijven en andere organisaties terecht voor advies over hoe zich te beschermen tegen economische spionage en bedrijfsspionage?

Antwoord 11
De Rijksdienst voor Ondernemend Nederland (RVO) informeert bedrijven over de bescherming van bedrijfsvertrouwelijke gegevens en de bescherming van intellectueel eigendom middels octrooien, auteursrecht en andere rechten. Octrooicentrum Nederland (OCNL), onderdeel van de Rijksdienst voor Ondernemend Nederland, is de octrooiverlenende instantie voor het Nederlands grondgebied.[6] Ook adviseert RVO over andere wijzen waarop bedrijfsgeheimen actief moeten worden beschermd, zoals fysiek en digitaal.[7] Daarnaast is het Digital Trust Center (DTC) opgericht, dat niet-vitale ondernemers helpt met veilig digitaal ondernemen.[8]
Het Nationaal Cyber Security Centrum (NCSC) dat deel uitmaakt van het Ministerie van Justitie en Veiligheid is het centrale informatieknooppunt en expertisecentrum op het gebied van cybersecurity voor de rijksoverheid en organisaties binnen de vitale infrastructuur. Het NCSC informeert en adviseert genoemde organisaties over digitale dreigingen en kwetsbaarheden, verricht daartoe analyses, en verleent die organisaties bijstand bij het treffen van maatregelen bij dreigingen en incidenten.
De AIVD heeft verscheidene publicaties uitgebracht over spionage voor zowel instanties en individuen. Voorbeelden hiervan zijn: «Bent u zich bewust van de risico's van cyberspionage?», «Spionage in Nederland» en de hierboven genoemde «Handleiding Kwetsbaarhedenanalyse Spionage». Deze zijn te vinden op www.aivd.nl/onderwerpen/spionage. Daarnaast informeert en/of adviseert de AIVD (in specifieke gevallen) instanties die het doelwit vormen van inlichtingenactiviteiten, en adviseert hen over weerstandsverhogende maatregelen. Personen of instanties die het vermoeden hebben doelwit te zijn (geweest) van spionage, kunnen dit ook altijd rechtstreeks melden bij de AIVD, of MIVD wanneer het opdrachten voor het Ministerie van Defensie betreft.
Bedrijven die opdrachten uitvoeren voor het Ministerie van Defensie worden contractueel Algemene Beveiligingseisen Defensie Opdrachten (ABDO) opgelegd. Deze bedrijven kunnen zich wenden tot Defensie voor advies en assistentie, alsmede met vragen over beveiliging.

Vraag 12
Zijn er, van bedrijfs- of overheidswege, maatregelen genomen na een eerdere Chinese hack bij Brion Technologies (een dochterbedrijf van ASML) in 2015? Zo ja, welke?

Antwoord 12
Ja, hoewel ASML in 2015 de hack tijdig heeft kunnen afslaan en deze geen schade heeft berokkend, zijn er omvangrijke maatregelen genomen waarmee bedrijfsvertrouwelijke gegevens significant beter zijn beschermd. De omvang van de maatregelen die ASML heeft genomen betreft tientallen miljoenen euro's. Zoals aangegeven bij het antwoord op vraag 11 ondersteunt de overheid bedrijven met dreigingsinformatie en beveiligingsadviezen.

---

[5] https://www.aivd.nl/documenten/publicaties/2011/02/17/handleiding-kwetsbaarheidsonderzoek-spionage
[6] https://www.rvo.nl/onderwerpen/innovatief-ondernemen/octrooien-ofwel-patenten/over-octrooicentrum-nederland
[7] https://www.rvo.nl/onderwerpen/innovatief-ondernemen/octrooien-ofwel-patenten/octrooi-anders-beschermen/bedrijfsgeheim/bedrijfsgeheim-actief-beschermen
[8] https://www.digitaltrustcenter.nl/

Vraag 13
Is de capaciteit van de Nederlandse inlichtingendiensten uitgebreid naar aanleiding van de hack bij Brion Technologies in 2015?

Antwoord 13
In 2017 is in het Regeerakkoord extra budget toegekend voor cyber security, onder andere bestemd voor AIVD en MIVD. Met dat geld zetten de AIVD en MIVD sterk in op het werven van nieuwe medewerkers en technische experts voor de onderzoeken naar digitale dreigingen.

Vraag 14 en 15
Hoeveel rechtszaken over economische spionage en bedrijfsspionage door buitenlandse mogendheden zijn er in de afgelopen jaren in Nederland geweest? Uit welke hoek kwamen deze?
Hoeveel van deze rechtszaken hebben geleid tot veroordelingen en/of straffen en boetes?

Antwoord 14 en 15
Economische spionage en bedrijfsspionage zijn geen zelfstandige strafbare feiten, maar zullen uiting vinden in andere strafbare feiten waaronder computervredebreuk. In hoeverre hierbij buitenlandse mogendheden betrokken waren, wordt niet dusdanig geregistreerd.

Vraag 16
In het geval van ASML is het nu – voor zover bekend – de tweede keer dat China betrokken is bij economische spionage en bedrijfsspionage. Gaat de Minister van Buitenlandse Zaken de Chinese ambassadeur hierover aanspreken?

Antwoord 16
Zoals aangegeven bij de beantwoording van vraag 2, 3 en 4 zijn er in deze casus geen aanwijzingen voor een directe betrokkenheid van de Chinese overheid. Los van deze casus kaart het kabinet de zorgen die bestaan met betrekking tot economische en bedrijfsspionage in EU-verband aan. Zo is dit onderwerp bijvoorbeeld ter sprake gekomen tijdens de EU-Chinatop op 9 april jl. Het kabinet zet tevens in op het versterken van internationale samenwerking op dit thema. Hierbij kan gebruik gemaakt worden van diplomatieke instrumenten zoals die in het kader van de EU Cyber Diplomacy Toolbox. Naar aanleiding van de Europese Raad van 18 oktober 2018 wordt tevens een cybersanctieregime afgerond.

Vraag 17
Deelt u de mening dat behalve vitale sectoren, zoals waterleidingsystemen, landbouwgronden en ook telecommunicatie en het toekomstige 5G-netwerk, eveneens bedrijven – of onderdelen van bedrijven – die gevoelige technologie maken (zoals ASML en NXP) moeten worden beschermd vanuit het oogpunt van nationale veiligheid?

Antwoord 17
Bij sommige bedrijven die hoogwaardige en gevoelige technologie ontwikkelen, kan een risico ontstaan voor de nationale veiligheid. Deze risico's omvatten het risico op ongewenste afhankelijkheden van buitenlandse investeerders of statelijke actoren, op het weglekken van vertrouwelijke of gevoelige informatie of op rechtstreekse aantasting van vitale processen en het functioneren van de Nederlandse economie en democratische rechtsorde. Deze risico's kunnen onder omstandigheden ontstaan bij overnames van en investeringen in dergelijke bedrijven, maar ook bij de inkoop van cruciale diensten of producten, de werving van personeel etc.
Het is een constant proces om te bezien welke nationale veiligheidsbelangen beschermd moeten worden, wat de dreiging is vanuit statelijke actoren voor de nationale veiligheid en hoe de weerbaarheid vergroot kan worden. De openheid van onze samenleving en economie vraagt om een zorgvuldige weging van het benutten van kansen enerzijds en het beschermen van nationale (veiligheids)belangen anderzijds.

Vraag 18
Deelt u de mening dat wetgeving hiertoe snel naar de Kamer moet komen? Zo ja, welke wetten kunnen worden verwacht en wanneer?

Antwoord 18
In de bijlage van de Kamerbrief Tegengaan Statelijke Dreigingen worden verschillende maatregelen genoemd ten aanzien van economische veiligheid, waaronder een betere benutting en aanscherping van huidige wet- en regelgeving ter bescherming van nationale veiligheid. Een van andere de maatregelen die wordt genoemd is een uitwerking van een investeringstoets. Hierbij is het uitgangspunt dat een verbod in het kader van de investeringstoets alleen daar wordt ingezet indien er geen alternatieve effectieve beschermingsmaatregelen voor handen zijn. Inzet is om een dergelijk wetsvoorstel in 2019 in procedure te kunnen brengen als onderdeel van een breder palet aan maatregelen.

Vraag 19 en 20
Deelt u de mening dat deze en andere incidenten, zoals rondom het Chinese bedrijf Huawei, de handelsrelatie met China op gespannen voet zetten? Weegt u de diefstal bij ASML mee in de nieuwe China-strategie die het kabinet momenteel aan het ontwikkelen is?

Antwoord 19 en 20
Het kabinet publiceerde op 15 mei de Chinastrategie die ingaat op de bredere relatie met China. De Chinanotitie staat los van het 5G-vraagstuk waarover uw Kamer separaat wordt geïnformeerd.