Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

32 637 Bedrijfslevenbeleid

Nr. 592

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 december 2023

Op 20 december 2022 heeft uw Kamer een motie van het lid Van Haga aangenomen.[1] Hierin wordt het kabinet verzocht om ondernemers te ondersteunen bij de bescherming van intellectueel eigendom omdat er een concrete dreiging is van diefstal van intellectueel eigendom door Rusland en China. Deze diefstal heeft een remmend effect op innovatie in Nederland. Met deze brief geef ik een reactie op deze motie.

Het belang van intellectuele eigendomsrechten (IE-rechten) voor de Nederlandse economie en de Nederlandse ondernemers is groot. Uit onderzoek is gebleken dat IE-intensieve sectoren, dat wil zeggen bedrijven die in vergelijking met andere bedrijven meer dan gemiddeld aan intellectuele eigendomsrechten hebben geregistreerd, een belangrijke bijdrage leveren aan de werking van de interne markt van de EU.[2] Zij zijn goed voor meer dan 75% van de handel binnen de EU en voor het grootste deel van de export van de EU naar de rest van de wereld. Nederland loopt, naast Duitsland, Frankrijk en Italië, voorop bij het creëren/registreren van nieuwe IE-rechten. IE-beleid en -wetgeving zorgen voor een gelijk speelveld en vergroten de concurrentiekracht van Nederlandse ondernemingen in de EU en daar buiten. De beschikbaarheid van een systeem van parallelle bescherming van IE-rechten op zowel Europees niveau (Europees/unitair octrooi, Gemeenschapsmodel-recht, Uniemerk, communautair kwekersrecht, geografische aanduidingen) als bescherming op nationaal/Benelux-niveau (onder andere merken, modellen, octrooien, kwekersrecht) zorgt ervoor dat er voor ieder soort onderneming passende bescherming is.

Tijdens het Tweeminutendebat Bedrijfslevenbeleid van 20 december 2022 vroeg de heer Van Haga mij of ik de zorgen deelde die hij had, dat China

[1] Kamerstuk 32 637, nr. 519

[2] Studie IER-intensieve sectoren en economische prestaties in de Europese Unie, EUIPO en EPO, 4e editie – oktober 2022

kst-32637-592
ISSN 0921 - 7371
's-Gravenhage 2023

en Rusland IE en bedrijfsgeheimen buitmaken.[3] Die zorgen deel ik uiteraard. Het kan niet zo zijn dat wij enerzijds onze bedrijven, maar ook kennisinstellingen en andere organisaties, in vele opzichten stimuleren om zich in te zetten voor een innovatieve, duurzame en welvarende economie, maar anderzijds bij (dreigingen van) diefstal van IE of bedrijfsgeheimen van deze bedrijven en organisaties de andere kant opkijken. Wij werken al jaren voor en samen met hen om dit tegen te gaan. Diefstal van IE en bedrijfsgeheimen is helaas van alle tijden. Een van de meeste spraakmakende uitspraken van de Hoge Raad gaat over bedrijfsspionage en is uit 1919.[4] Ook wordt diefstal van IE en bedrijfsgeheimen gepleegd door allerlei partijen: statelijke actoren, zoals Rusland en China, (cyber)criminelen, maar ook door bijvoorbeeld werknemers of afnemers. Met name door de snelle digitale ontwikkelingen is dit een probleem dat zich niet beperkt tot onze landsgrenzen en dat betekent dat wij ook in een steeds breder verband moeten samenwerken.

Bedrijven hebben ter voorkoming en handhaving van diefstal van hun IE en bedrijfsgeheimen een grote eigen verantwoordelijkheid. Ik realiseer mij dat terdege. Maar de ondernemer staat er niet alleen voor. Het gaat hier om een gedeelde verantwoordelijkheid en daarom wordt er aan alle kanten door de Nederlandse overheid, Europese Unie of wereldwijd informatie verschaft, hulp aangeboden en samengewerkt. Er is voor bedrijven echter geen *one size fits all*-oplossing. Dat kan ook niet anders want (cyber) dreiging en diefstal van IE en bedrijfsgeheimen door statelijke actoren en anderen kent geen grenzen en is complex. Door middel van de in **Bijlage I** gegeven (niet limitatieve) opsomming maak ik duidelijk dat het aanbod in alle opzichten heel divers is. De ondernemers kunnen daarbij zelf bepalen wat op hun situatie het beste van toepassing is en waar zij gebruik van willen maken. Dat betekent niet dat ik hiermee volsta. De overheid blijft bedrijven hierbij ondersteunen door te blijven zorgen voor goede randvoorwaarden, zoals passend IE-beleid en -wetgeving, en door het actualiseren, verbeteren en aanvullen van de hiervoor genoemde maatregelen.

Ik vertrouw erop uw Kamer hiermee voldoende te hebben geïnformeerd.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens

[3] Verslag Tweeminutendebat Bedrijfslevenbeleid d.d. 20 december 2022 https://www.staten-generaal.nl/9370000/1/j4nvi0xeni9vr2l_j9vvkfvj6b325az/vm0nly25zbza
[4] HR 31 januari 1919, NJ 1919, p. 161, Lindenbaum/Cohen

Bescherming van IE en bedrijfsgeheimen

Voor wij ons gezamenlijk kunnen inzetten tegen diefstal van IE en bedrijfsgeheimen is het natuurlijk wel zaak dat de ondernemers eerst – waar vereist – hun IE-recht(en) hebben geregistreerd. Bijvoorbeeld een technische vinding door een octrooi. Daarbij moet ook goed bedacht worden in welke landen men bescherming wil. Een octrooi geldt altijd voor een bepaald land of een groep landen. In geval van bedrijfsgeheimen moeten ondernemers voldoen aan de drie voorwaarden genoemd in de Wet bescherming bedrijfsgeheimen (Wbb): het bedrijfsgeheim moet een echt geheim zijn, het bedrijfsgeheim moet handelswaarde hebben en er moeten maatregelen genomen zijn om het bedrijfsgeheim geheim te houden.

Dat bedrijven vooraf iets moeten doen om bescherming te krijgen van hun IE of bedrijfsgeheimen klinkt logisch en het gebeurt ook heel veel, maar het kan altijd beter. Uit de hiervoor genoemde studie naar IE-intensieve sectoren blijkt een aanzienlijk aantal Nederlandse startups die weg nog niet te kennen: 14% heeft maar een IE-recht aangevraagd. Startups en scale-ups zijn de vernieuwers van de economie en cruciaal voor ons toekomstig verdienvermogen en onze brede welvaart. Ik verwijs naar mijn brief aan uw Kamer van 26 mei jl.[5] IE is een belangrijke randvoorwaarde hiervoor dus dit onderzoeksgegeven is een belangrijk punt van aandacht voor ons.

Advies over bescherming en registratie van IE of bedrijfsgeheimen kunnen bedrijven krijgen bij onder andere de Rijksdienst voor Ondernemend Nederland (RVO). RVO informeert bedrijven over de bescherming van bedrijfsgeheimen en de bescherming van IE door middel van octrooien, merken en andere IE-rechten. Octrooicentrum Nederland (OCNL), onderdeel van RVO, is de octrooiverlenende instantie voor het Nederlands grondgebied. Daarnaast kunnen bedrijven voor informatie over IE buiten onze landsgrenzen ook terecht bij het Europees Octrooi Bureau (EPO) over Europese octrooien, het Bureau voor intellectuele eigendom van de Europese Unie (EUIPO) over Europese-merken, tekeningen en modellen. Ook bij de Wereldorganisatie voor intellectuele eigendom (WIPO) is ook veel informatie over IE en bedrijfsgeheimen te verkrijgen.

Handhaving van IE en bedrijfsgeheimen in Nederland

Als het IE-systeem een positieve bijdrage wil leveren aan de economische en sociale welvaart, is het ook van essentieel belang dat er instrumenten beschikbaar zijn om ervoor te zorgen dat deze rechten op een effectieve, tijdige en toegankelijke manier worden gerespecteerd, vanzelfsprekend naast de legitieme belangen van andere betrokkenen. Uitgangspunt in Nederland is dat bedrijven en andere rechthebbenden in beginsel zelf verantwoordelijk zijn voor de handhaving van hun IE-rechten of bedrijfsgeheimen, en deze zonodig civiel handhaven. De huidige Nederlandse wetgeving biedt bedrijven een uitgebreid en doeltreffend instrumentarium om op te kunnen treden tegen inbreukmakers op IE en bedrijfsgeheimen. Strafrechtelijke handhaving van IE-rechten geldt als uiterste middel en is mogelijk in geval van bedreiging van de volksgezondheid of veiligheid, grootschalige namaak en piraterij, aanwijzingen van betrokkenheid van criminele organisaties of recidive.

[5] Kamerstuk 32 637, nr. 567

Met betrekking tot de handhaving van IE-rechten aan de buitengrenzen door de Douane, heeft het Ministerie van Economische Zaken en Klimaat (EZK) afspraken gemaakt met het Ministerie van Financiën.[6] Bij de controles van het grensoverschrijdend goederenverkeer dat van buiten de EU Nederland binnenkomt, handelt de douane overeenkomstig de EU-Verordening 608/2013 inzake de handhaving van intellectuele eigendomsrechten door de douane. Dit doet de Douane onder meer in vrachtzendingen, post, koeriers en in reizigersbagage op Schiphol of in de Rotterdamse haven. Bedrijven en andere IE-rechthebbenden, die vermoeden dat er inbreuken op hun IE-rechten worden gepleegd, kunnen de Douane door middel van het indienen van een formulier verzoeken (in Nederland of in de EU) om daartegen op te treden.[7] De Douane treedt ook ambtshalve op. Voor de risicoselectie van controles hanteert de Douane methodes deels op basis van risicoanalyse en deels steekproefsgewijs. De Nederlandse Douane doet dat succesvol. Uit de meeste recente rapportage van het aantal tegenhoudingen aan de EU-buitengrens blijkt dat zes EU-lidstaten verantwoordelijk zijn voor meer dan 95% van het totale aantal aanhoudingen op de interne markt in 2021. Ook Nederland maakt deel uit van deze top 6: in 2021 heeft de Douane ongeveer 11 miljoen goederen tegengehouden die mogelijk inbreuk maken op IE-rechten, met een vermoedelijke waarde van € 106 miljoen.[8]

De mogelijkheden voor bedrijven om hun octrooien te handhaven is per 1 juni jl. uitgebreid. Op die datum is er een nieuwe rechtbank voor octrooirechtszaken in 17 Europese landen. Het Unified Patent Court (UPC) beslist over inbreukzaken en nietigheidszaken bij Europese octrooien én unitaire octrooien.[9] Het kabinet heeft zich daarom altijd ingezet voor de realisatie van het UPC. Het UPC vereenvoudigt de gerechtelijke handhaving van octrooien in de EU. In plaats van afzonderlijke nationale procedures te moeten doorlopen met bijbehorende administratieve lasten, biedt het UPC de mogelijkheid om bij één instantie een uitspraak te verkrijgen in octrooigeschillen met directe werking in een groot deel van de EU.

Advies en handhaving van IE en bedrijfsgeheimen buiten Nederland

De bescherming en handhaving van IE-rechten houdt niet op bij de Nederlandse grens. Diefstal op IE-rechten en bedrijfsgeheimen vormen een wereldwijd probleem. Nederland ondersteunt bedrijven door ervoor te zorgen dat de wetgeving op orde is, door samen te werken met EU-lidstaten en andere landen aan de bestrijding hiervan en door ervoor te zorgen dat er informatie beschikbaar is hoe bedrijven hun IE-rechten en bedrijfsgeheimen het beste in andere landen kunnen beschermen en handhaven.

---

[6] Convenant inzake de samenwerking tussen het Ministerie van Economische Zaken en Klimaat en het Ministerie van Financiën bij de uitvoering van wettelijke taken op het beleidsterrein van het Ministerie van Economische Zaken en Klimaat door de Douane en Bijlage 2 – Intellectuele eigendomsrechten, https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant-douane-economische-zaken-klimaat

[7] https://download.belastingdienst.nl/douane/docs/informatieblad_intelectueel_eigendomsrecht_d09531z5fd.pdf

[8] EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2021, EUIPO December 2022, https://euipo.Europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_EU_enforcement_of_IPRs_2021/2022_EU_enforcement_of_IPRs_results_2021_FullR_en.pdf

[9] https://www.rvo.nl/files/file/2022–05/Unified-Patent-Court-UPC.pdf

Als eerste kan hierbij het Innovatie Attaché Netwerk (IA-netwerk) worden genoemd. EZK ondersteunt met het IA-netwerk de Nederlandse topsectoren, ondernemers en kennisinstellingen in hun internationale R&D- en innovatie-ambities. Vanuit 14 landen werken in ambassades en consulaten innovatieattachés om de Nederlandse concurrentiekracht op de langere termijn te versterken. Het gaat om «economische diplomatie» in technologie en kennis, het signaleren van kansen voor onderzoeks- en ontwikkelingssamenwerking (R&D) en het gezamenlijk innoveren. Ook het signaleren van kansen en bedreigingen op het gebied van IE en bedrijfsgeheimen behoren tot het werk van de innovatieattachés en worden gedeeld met Nederlandse belanghebbenden.

De Europese Commissie is ook al jaren actief op het gebied van de bescherming en handhaving van IE-rechten en bedrijfsgeheimen. Daar kunnen Nederlandse ondernemers zeker ook van profiteren. Een concreet voorbeeld hiervan is de EU de China IE-helpdesk. Deze helpdesk biedt kleine en middelgrote ondernemingen gratis eerstelijnsinformatie, (vertrouwelijk) advies, training en online bronnen over het beschermen en handhaven van IE-rechten en aanverwante kwesties in China (en Hong Kong, Macao en Taiwan).[10] Er zijn overigens ook EU-IP Helpdesks voor Afrika, Europa, India, Latijns Amerika en Zuid-Oost Azië.[11]

Tweejaarlijks publiceert de Europese Commissie een rapport over de bescherming en handhaving van IE-rechten in derde landen.[12] Het betreffen hier zogenoemde «prioritaire landen» waarin de stand van zaken op het gebied van IE een bron van grote zorg is. Op basis van deze bevindingen richt de Commissie haar inspanningen en middelen op de specifieke aandachtsgebieden in deze landen, met als doel de bescherming en handhaving van IE wereldwijd te verbeteren. Zoals uit het laatste rapport van mei 2023 blijkt, blijft China het topprioriteitland voor de EU. Naast inspanningen die de Commissie naar aanleiding van dit rapport onderneemt, is dit rapport ook een goede informatiebron voor de Nederlandse overheid. En het stelt bedrijven, klein of groot, in staat om kennis te nemen van de potentiële risico's voor hun IE wanneer zij zakelijke activiteiten ontplooien in de prioriteitslanden.

Ook heeft de Europese Commissie in december 2022 – in samenwerking met het EUIPO – de derde versie van de Watch List voor namaak en piraterij gepubliceerd.[13] Hierin worden buiten de EU gevestigde online- en fysieke marktplaatsen benoemd waarvan wordt gemeld dat zij bij belangrijke IE-inbreuken, en met name piraterij en namaak, betrokken zijn of deze faciliteren. Deze activiteiten ondermijnen de IE-rechten van bedrijven en schaden de bedrijfsvoering en banen in de EU. De Watch List heeft tot doel deze diensten en marktplaatsen, en lokale handhavingsautoriteiten en overheden, aan te moedigen actie te ondernemen om inbreuken op IE te stoppen of te voorkomen. Het is ook bedoeld om het bewustzijn van EU-bedrijven te vergroten door hen te informeren over malafide handelwijzen van een groot aantal (online) marktplaatsen buiten de EU.

---

[10] https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/china-ip-sme-helpdesk_en

[11] https://intellectual-property-helpdesk.ec.europa.eu/index_en

[12] https://policy.trade.ec.europa.eu/news/commission-releases-its-report-intellectual-property-rights-third-countries-2023-05-17_en

[13] https://policy.trade.ec.Europa.eu/news/commission-publishes-latest-counterfeit-and-piracy-watch-list-2022-12-01_en

De afgelopen decennia zijn er diverse Europese mededelingen en wetsvoorstellen (verordeningen en richtlijnen), op het gebied van IE en bedrijfsgeheimen gepubliceerd respectievelijk – na goedkeuring van het Europees Parlement en de Raad – in werking getreden (en indien nodig geïmplementeerd in onze nationale wetgeving), zoals de Richtlijn 2004/48 betreffende de handhaving van intellectuele-eigendomsrechten, de Richtlijn 2016/943 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan of de Mededeling 2020/760 – Het innovatiepotentieel van de EU optimaal benutten; een actieplan inzake intellectuele eigendom om het herstel en de veerkracht van de EU te ondersteunen. De volgende stap is de Mededeling Handhaving IE, die de Commissie naar eigen zeggen voor het einde van het jaar publiceert. Naar verluidt doet de Commissie hierin aanbevelingen over de strijd tegen namaak, over de rollen en verantwoordelijkheden van alle betrokken partijen, het verbeteren van de samenwerking en gegevensuitwisseling en het stimuleren van het gebruik van nieuwe technologieën. Daarnaast moet de IE-veerkracht van bedrijven, met name het mkb, worden vergroot en moet IE in het DNA van de belangrijkste spelers worden ingebed. De precieze inhoud is nog onbekend, maar de mededeling wordt vanzelfsprekend nauwkeurig bestudeerd en de Kamer zal door middel van een BNC-fiche hierover geïnformeerd worden.

Op het gebied van de bestrijding van zware en georganiseerde criminaliteit in Europa werken de rechtshandhavingsinstanties van de EU-lidstaten nauw samen binnen Empact, het multidisciplinaire platform tegen criminaliteitsdreiging. Een van de tien prioriteiten voor de periode 2022–2025 heeft ook betrekking op «misdaad op het gebied van het intellectuele eigendomsrecht».[14] In het kader hiervan is door het EUIPO een onderzoekshandboek voor handhavingsautoriteiten ontwikkeld waarin heersende criminele bedrijfsmodellen op het gebied van IE-misdaad, die zowel online als offline, wordt beschreven.

In internationaal verband is er de Overeenkomst inzake handelsaspecten van de intellectuele eigendom (TRIPS) bij het Verdrag van de Wereldhandelsorganisatie WTO. TRIPS was baanbrekend in het multilaterale recht door algemene beginselen vast te stellen voor de handhaving van IE-rechten. Het vereist van de WTO-leden – inmiddels meer dan 160 – dat zij effectieve, evenwichtige en eerlijke procedures ter beschikking stellen die in de noodzakelijke rechtsmiddelen voorzien en tegelijkertijd waken tegen misbruik ervan en het creëren van obstakels voor legitieme handel. De TRIPS-bepalingen zijn onderworpen aan het WTO-geschillenbeslechtingssysteem. De EU schroomt niet dit middel in te zetten. Eind 2022 heeft zij verzocht om de oprichting van een WTO-panel voor een lopend handelsgeschil met China, namelijk besluiten (bekend als «anti-suit injunctions») van Chinese rechtbanken die bedrijven met hightechoctrooien verhinderen hun technologieën effectief te beschermen bij niet-Chinese rechtbanken, waaronder EU-rechtbanken. Uit het systeem voor geschillensbeslechting van de WTO komen onafhankelijke en onpartijdige uitspraken voort die bindend zijn voor de partijen bij het geschil.

Veiligheid en bewustwording

Ten slotte wil ik hier nog in gaan op en aantal activiteiten/maatregelen op het gebied van veiligheid – dus breder dan diefstal van IE of bedrijfsgeheimen – om het handelingsperspectief en de weerbaarheid van Neder-

[14] https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact

landse bedrijven te vergroten. De meest in het oog springende maatregelen zijn: beschermingsmaatregelen bij overnames en investeringen; maatregelen ter bescherming van kennis, informatie en technologieën, en bewustwording van bedrijven en kennisinstellingen.

Om de nationale veiligheid te beschermen bij bedrijven en kennisinstellingen beschikt het kabinet over investeringstoetsen, bijvoorbeeld binnen de Gaswet, Elektriciteitswet en Telecommunicatiewet. Bij een investeringstoets worden overnames en investeringen in het bedrijfsleven vooraf door de overheid gecheckt. In een uiterst geval kan het kabinet de activiteit verbieden. Ter bescherming van ondernemingen met sensitieve technologie en de nationale veiligheid is op 1 juni jl. de Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo) van kracht geworden. Ondernemingen met sensitieve technologie beschikken over zodanige kennis of informatie over deze technologie dat het gevolgen kan hebben voor de nationale veiligheid als deze uitlekt. Bijvoorbeeld een kwaadwillende partij zou via een investering bijvoorbeeld zeggenschap kunnen krijgen in een Nederlandse onderneming die hoogwaardige technologie met militaire toepassingen ontwikkelt. Als een ongewenste partij zo'n onderneming overneemt kan die techniek in verkeerde handen komen en tegen Nederlandse veiligheidsbelangen worden ingezet. Zowel ondernemingen met sensitieve technologie als investeerders moeten zelf wijzingen van zeggenschap melden bij het Bureau Toetsing Investeringen.

Veel bedrijven werken samen met kennisinstellingen. Daarbij worden IE en bedrijfsgeheimen gedeeld of zelfs gecreëerd. Maar ook kennisinstellingen worden in toenemende mate geconfronteerd met dreigingen van statelijke actoren die kennis en innovatie inzetten als strategisch machtsmiddel naast of in combinatie met klassieke middelen, zoals spionage. Het kabinet werkt daarom al enige tijd aan een toetsingskader om ongewenste kennis- en technologieoverdracht tegen te gaan. Ook het veiligheidsbewustzijn wordt vergroot, zowel bij kennisinstellingen als bedrijven. Dit bevordert ook de veiligheid daar waar sprake is van publiek-private samenwerking. Onder de maatregelen ter bescherming van kennis, informatie en technologieën vallen onder andere de Nationale Leidraad Kennisveiligheid en het Loket Kennisveiligheid. Voorts wordt gewerkt aan een wetsvoorstel screening kennisveiligheid. Op EU-niveau is de inzet gezamenlijk te werken aan een gelijk speelveld, waaronder de inzet op meer coherentie in nationale kennisveiligheidsmaatregelen.

Nederlandse bedrijven en kennisinstellingen zijn regelmatig het doelwit van digitale aanvalscampagnes van staten om hoogwaardige technologie en kennis buit te maken. De overheid wil de weerbaarheid van hen verder verhogen door hen bewust te maken van de dreiging en de maatregelen die organisaties en overheid kunnen nemen. Advies op het gebied van cyberdreigingen, cybersecurity en bedrijfsspionage (en dus breder dan diefstal van IE of bedrijfsgeheimen) kunnen ondernemers krijgen bij het Digital Trust Center (DTC), het Nationaal Cyber Security Centrum (NCSC), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Het DTC is in 2018 opgericht om Nederlandse bedrijven weerbaarder te maken tegen toenemende cyberdreigingen. DTC helpt met behulp van een interactieve website en community, niet-vitale ondernemers met veilig digitaal ondernemen. Het NCSC 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 doet wat nodig is om te voorkomen dat staten, organisaties of personen onze rechtsstaat

tegenwerken, ondergraven of aanvallen. Een van de aandachtsgebieden van de AIVD is economische veiligheid en klassieke respectievelijk digitale spionage. Op de website biedt de AIVD veel informatie aan, bijvoorbeeld het rapport Dreigingsbeeld Statelijke Actoren of de uitgave Spionage-Hoe herken je het en wat kun je ertegen doen?[15] De MIVD ondersteunt de krijgsmacht en doet dat door inlichtingen te verzamelen, analyseren en verspreiden. Een van de hoofdopdrachten van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is Nederland digitaal veilig maken. De NCTV geeft informatie o.a. door de jaarlijkse publicatie van het Cybersecuritybeeld Nederland en waarschuwt organisaties om het onverwachte te verwachten en hun beveiliging daarop in te richten.[16]Bedrijven die het vermoeden hebben doelwit te zijn (geweest) van spionage, kunnen dit rechtstreeks melden bij de AIVD, of de MIVD wanneer het opdrachten voor het Ministerie van Defensie betreft.

[15] file:///R:/Dreigingsbeeld+Statelijke+Actoren+2%20(1).pdf resp. file:///R:/Spionage+-+hoe+herken+je+het+en+wat+kun+je+ertegen+doen%20(1).pdf

[16] https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland