Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

30 821 Nationale Veiligheid

Nr. 125 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 februari 2021

In april 2019 heeft het kabinet uw Kamer geïnformeerd over het tegengaan van statelijke dreigingen. De Nederlandse samenleving staat in het teken van vrijheid, democratie, rechtsstaat en een internationale oriëntatie. Door deze waarden en openheid profiteren Nederland en Nederlanders van de kansen en mogelijkheden die bijvoorbeeld digitalisering en globalisering bieden. Een open economie, een open wetenschappelijk klimaat en vrijhandel liggen sinds jaar en dag aan de basis van het Nederlandse verdienvermogen en onze sterke positie. Zij vormen een groot goed dat moet worden beschermd. Sinds het presenteren van de aanpak statelijke dreigingen zijn veel stappen gezet waarover ik u graag informeer middels deze brief[1]. Eén van die stappen is de ontwikkeling van een dreigingsbeeld statelijke actoren dat gelijktijdig aan uw Kamer wordt aangeboden[2]. Deze brief vormt tevens de kabinetsreactie daarop. In deze brief ga ik eerst in op belangrijke aandachtspunten uit het dreigingsbeeld, waarna ik u informeer over de voortgang van de aanpak statelijke dreigingen. Als onderdeel daarvan geef ik toelichting op de versterkte aanpak vitaal, waarmee ik invulling geef aan de moties van het lid Van den Berg c.s. en van het lid Moorlag over een versterkte aanpak van de bescherming van de vitale processen en diensten[3]. Ook geef ik met deze brief invulling aan de motie die is ingediend door de leden Buitenweg en Yesilgöz-Zegerius over het inzichtelijk maken van cyberafhankelijkheden in vitale processen[4]. Tot slot zal ik concluderen welke aanvullende acties in het licht van de dreiging onderzocht worden.

Dreigingsbeeld statelijke actoren

Economie, geopolitiek en veiligheid raken meer met elkaar verbonden. Digitalisering en verschuivende geopolitieke verhoudingen veranderen

[1] Kamerstuk 30 821, nr. 72.
[2] Kamerstuk 30 821, nr. 124.
[3] Kamerstuk 24 095, nrs. 487 en 504.
[4] Kamerstuk 35 570 VI, nr. 38.

kst-30821-125
ISSN 0921 - 7371
's-Gravenhage 2021

het klassieke veiligheidsdenken en activiteiten van statelijke actoren manifesteren zich op steeds meer verschillende terreinen. Doelwitten lopen uiteen van lokale verenigingen tot internationale veiligheidsorganisaties en van individuen tot hele gemeenschappen. Met het toenemende aantal doelwitten hebben ook meer partijen baat bij dreigingsinformatie. Om enerzijds in deze behoefte te voorzien en anderzijds de aanpak statelijke dreigingen nader inhoudelijk te onderbouwen, heeft het kabinet ervoor gekozen het dreigingsbeeld statelijke actoren op te laten stellen.

Managementssamenvatting dreigingsbeeld statelijke actoren

Deze analyse is in samenwerking tussen AIVD, MIVD en NCTV tot stand gekomen en biedt inzicht in welke nationale veiligheidsbelangen geschaad (kunnen) worden door statelijke actoren en op welke wijze dat gebeurt of kan gebeuren. Met dit inzicht wordt een inhoudelijke grondslag geboden op basis waarvan beleid gevoerd kan worden ten behoeve van de weerbaarheid van de samenleving tegen de dreiging door statelijke actoren.

In dit beeld is uitgegaan van de interdepartementale definitie van statelijke dreigingen: *dwingende, ondermijnende, misleidende of heimelijke activiteiten van of namens statelijke actoren, onder de drempel van gewapend conflict, die de nationale veiligheidsbelangen van Nederland kunnen schaden door een combinatie van nagestreefde doelen, gebruikte middelen en ressorterende effecten*. Statelijke dreigingen evolueren voortdurend, veranderen van karakter, worden diffuser of juist meer manifest. In dit dreigingsbeeld wordt niet alleen uitgegaan van actuele dreigingen, maar ook van potentiële dreigingen en nevenschade aan de nationale veiligheidsbelangen ontstaan door activiteiten van statelijke actoren.

De verschillende nationale veiligheidsbelangen zijn kwetsbaar en worden door statelijke actoren substantieel bedreigd en aangetast, maar niet in dezelfde mate. Deze kwetsbaarheid is niet alleen afhankelijk van de dreiging door statelijke actoren, maar ook van het effect van tegenmaatregelen in Nederland of in een internationale context. Op dit moment heeft geen van de statelijke actoren de benodigde combinatie van intentie en capaciteit om de nationale veiligheid op de korte termijn (tot twee jaar) te ontwrichten. Ontwikkelingen op middellange en lange termijn geven reden tot zorg.

Statelijke actoren beschikken over een breed palet aan middelen, al hebben niet alle actoren dezelfde capaciteiten. Beïnvloeding, inmenging, desinformatie en spionage zijn veelgebruikte middelen. Hier valt onderscheid te maken tussen statelijke actoren die deze activiteiten primair richten op specifieke groepen (zoals hun diaspora) en statelijke actoren die juist de Nederlandse samenleving in den brede willen beïnvloeden. Ook economische instrumenten worden ingezet om geopolitieke doelen te behalen. Bij de structurele en centraal aangestuurde inzet van economische instrumenten is het aantal actoren beperkt. Slechts enkele actoren verrichten voorbereidingshandelingen voor digitale verstoring of sabotage. Het aantal actoren zegt daarbij niets over de ernst van deze potentiële dreiging. De mogelijke doelwitten van statelijke actoren zijn divers: van lokale verenigingen tot internationale veiligheidsorganisaties en van individuen tot hele gemeenschappen. In totaal zijn vijftien doelwittypen geïdentificeerd en behandeld in deze analyse.

De territoriale veiligheid van het EU-grondgebied en het NAVO-bondgenootschap staan onder druk door de aanzienlijke toename

van het Russische conventionele en nucleaire militair vermogen. Ondanks een assertief en agressief Russisch buitenland- en veiligheidsbeleid wordt de fysieke territoriale veiligheid de komende twee jaar zeer waarschijnlijk niet direct bedreigd. Er gaat wel concrete dreiging uit van activiteiten door statelijke actoren in het digitale domein. Behalve digitale spionage gaat het hier ook om voorbereidingsactiviteiten vanuit onder meer Rusland en Iran voor digitale verstoring en sabotage. Nederland kan daarnaast geconfronteerd worden met nevenschade uit digitale aanvallen in andere landen. De sociale en politieke stabiliteit wordt geschaad door staten wiens doelstelling het is om de democratische rechtsorde in andere landen te ondermijnen, zoals Rusland, en door staten met een actieve diasporapolitiek, zoals Iran en Turkije. De economische veiligheid wordt geschaad door spionage van diverse landen, waaronder Rusland en China, en door bepaalde economische activiteiten van China. Economische spionageactiviteiten zijn met name gericht op Nederlandse topsectoren en kennisinstellingen. Economische activiteiten zoals investeringen in en samenwerking bij de ontwikkeling van sensitieve technologieën vormen een dreiging, omdat kennis- en technologieoverdracht die vanuit het oogpunt van nationale veiligheid ongewenst is kan plaatsvinden en omdat (ongewenste) strategische afhankelijkheid kan ontstaan. De internationale rechtsorde, hoeksteen voor onze veiligheid en welvaart, staat vanuit verschillende kanten onder druk. Rusland en China streven ernaar de internationale rechtsorde naar eigen inzicht om te vormen. Zij spelen hierin, gezien hun omvang, militaire en economische macht en hun positie als permanente leden van de VN-Veiligheidsraad, een grote rol.

Beleidsreactie dreigingsbeeld

Het dreigingsbeeld maakt dat integraliteit het sleutelwoord is om adequaat op de dreiging te reageren en bevestigt hiermee dat de aanpak van statelijke dreigingen zoals beschreven in de Kamerbrief van april 2019 nog altijd actueel is en met kracht dient te worden voortgezet. Staten hanteren elk hun eigen strategie en dreigingen overstijgen individuele domeinen. Dit benadrukt het belang van kennisopbouw en informatie-uitwisseling op nationaal en internationaal terrein en het zoveel mogelijk samenbrengen van (dreigings)informatie over activiteiten van staten. Het kabinet zet zich daarom verder in voor samenwerking, informatievoorziening en bewustwording binnen en buiten de overheid, in Nederland en daarbuiten.

Het beeld laat zien dat een integrale benadering nodig is om de dreiging in beeld te brengen, maar ook bij het formuleren van tegenmaatregelen op specifieke doelwitten en specifieke actoren. Waar dreigingen en risico's van oudsher voornamelijk in verband werden gebracht met de vitale infrastructuur worden nu veel breder doelwitten benoemd als mogelijk doelwit van statelijke actoren. Zoals doelwitten die werken met hoogwaardige technologie of kennis, zoals topsectoren en kennisinstellingen. Dit dreigingsbeeld vraagt dan ook om een herbeoordeling van wat we in het kader van de nationale veiligheid moeten beschermen en een benadering waarin we over de gehele linie kijken naar mogelijke doelwitten en de gehele (toeleveranciers)keten van de klassieke én toekomstige vitale infrastructuur.

Vanuit deze bredere blik worden de huidige maatregelen binnen de aanpak statelijke dreigingen onder de loep genomen en indien nodig versterkt.

Voortgang aanpak statelijke dreigingen

De afgelopen twee jaar is het inzicht in de dreiging met behulp van extra inzet van de AIVD en MIVD gegroeid en wordt dreigingsinformatie vanuit verschillende domeinen steeds beter samengebracht. Dit zien we bijvoorbeeld terug in de structurele samenwerking rondom telecomnetwerken. Alleen door informatie vanuit verschillende perspectieven bij elkaar te brengen is het mogelijk activiteiten te beoordelen, de gehele dreiging te overzien («connecting the dots») en tegenmaatregelen te formuleren.

Werkwijze

Met de introductie van de aanpak statelijke dreigingen in 2019 is een werkwijze ontstaan waarbij alle relevante partijen op een blijvende en continue basis bijdragen aan de weerbaarheid tegen statelijke actoren. De landenneutrale aanpak richt zich op de gehele maatschappij en werkt volgens een vaste systematiek van belangen-dreiging-weerbaarheid: welke veiligheidsbelangen moeten worden beschermd, wat is de dreiging vanuit statelijke actoren en hoe kan de weerbaarheid vergroot worden[5]. Het te beschermen belang staat hierin voorop om ervoor te zorgen dat alle benodigde maatregelen ingezet worden. Als het bijvoorbeeld gaat om het beschermen van bepaalde kennis wordt met behulp van dreigingsinformatie bepaald of bedrijfsovernames voorkomen moeten worden, er extra inzet op bewustwording nodig is of dat de digitale veiligheid verhoogd moet worden. In de meeste gevallen gaat het om een mix van maatregelen om de weerbaarheid te verhogen en worden er zowel maatregelen genomen tegen de fysieke als de digitale dreiging.

Tot slot vindt er bij het formuleren van tegenmaatregelen altijd een zorgvuldige weging plaats tussen het veiligheidsbelang en de mogelijke gevolgen voor onze open samenleving en open economie.

In lijn met belangrijke aandachtspunten uit het dreigingsbeeld wordt eerst ingegaan op de voortgang van een aantal generieke maatregelen en vervolgens zal de voortgang gerelateerd aan de sociale en politieke stabiliteit en de economische veiligheid worden toegelicht[6].

Generieke maatregelen ter verhoging van de weerbaarheid

Versterkte aanpak vitale infrastructuur

Integriteit van informatie, veilige toegang tot systemen en zeggenschap over vitale infrastructuur zijn belangrijk voor de nationale veiligheid. Dit is echter niet meer altijd vanzelfsprekend door de toenemende dreiging van statelijke actoren en cybercriminelen, de digitale verwevenheid en ketenafhankelijkheden. Het is niet langer een vast gegeven welke processen, bedrijven en organisaties we moeten beschermen en hoe we dit moeten doen. In de Nationale Veiligheids Strategie 2019 heeft het kabinet aangekondigd te werken aan de ontwikkeling van een versterkte aanpak voor de bescherming van de vitale infrastructuur, conform de motie van het lid Van den Berg[7]. De versterkte aanpak zet in op het versterken van het huidige Rijksbrede programma weerbare vitale infrastructuur, door het huidige instrumentarium en de governancestruc-

---

[5] Kamerstuk 30 821, nr. 72.

[6] De thema's ongewenste buitenlandse inmenging gericht op diaspora en beschermen democratische processen en instituties werden in de brief in 2019 apart benoemd, maar in de huidige aanpak samengevoegd onder sociale en politieke stabiliteit.

[7] Kamerstuk 30 821, nr. 81 en Kamerstuk 24 095, nr. 487.

turen te actualiseren en toekomstbestendig te maken. De combinatie van technologische ontwikkelingen en geopolitieke veranderingen maken dat met een andere blik gekeken moet worden naar wat we willen beschermen. Met een geactualiseerd instrumentarium worden onder andere technologische ontwikkelingen en geopolitieke veranderingen integraal meegewogen in het beoordelen van risico's en vervolgens bij het nemen van gepaste weerbaarheidsverhogende maatregelen. Hierbij wordt ingezet op een integrale aanpak waarin de digitale en fysieke weerbaarheid in zijn geheel wordt bezien. Hierbij worden ook ketenafhankelijkheden meegenomen, omdat vitale processen onderling sterk verweven zijn en ook afhankelijk zijn van toeleveranciers in ketens. Tot slot zal de borging en ontsluiting van kennis en kunde binnen de overheid sterker georganiseerd worden, om alle partijen in staat te stellen de juiste maatregelen te nemen. Met het opnemen van de digitale weerbaarheid in de integrale aanpak en het voorstel van de Europese Commissie tot herziening van de NIB-richtlijn wordt invulling gegeven aan de motie Moorlag[8].

In lijn met het nationaal beleid wordt ook op Europees niveau ingezet op de aanvullende bescherming van de vitale infrastructuur. Op 16 december 2020 heeft de Europese Commissie een voorstel gepubliceerd voor een Critical Entities Resilience Directive (CER-richtlijn), met aanvullende maatregelen voor de bescherming van vitale infrastructuur[9]. Daarnaast heeft de Commissie op 16 december ook een voorstel gepubliceerd voor de herziening van de NIB-richtlijn, inzake netwerk- en informatiebeveiliging[10].

Digitale veiligheid

Het Cybersecuritybeeld Nederland 2020 geeft aan dat spionage en (voorbereidingen tot) sabotage van statelijke actoren het grootste digitale risico vormen voor de nationale veiligheid[11]. Door digitalisering zijn wij steeds afhankelijker van digitale systemen en processen. De groei aan digitale systemen en processen zorgen ook voor een groei van het aanvalsoppervlak. De drempel om via de digitale weg te verstoren of te saboteren ligt lager dan de fysieke weg en het wordt gemakkelijker voor staten en andere actoren om doelwitten te bereiken, bijvoorbeeld via phishing-campagnes. Het kabinet werkt via de Nederlandse Cybersecurity Agenda (NCSA) met een brede aanpak aan het verhogen van de digitale weerbaarheid van Nederland, ook ten opzichte van de dreiging van statelijke actoren[12]. In dit kader heeft de AIVD in juni 2019 «Offensief cyberprogramma, een ideaal businessmodel voor staten» gepubliceerd[13]. Daarnaast is binnenkort een update voorzien van de brochure uit 2017 voor bestuurders en ICT-beveiligers om hen te informeren over cyberspionage en hoe cyberspionnen te werk gaan. Hiermee worden zij geactiveerd om hun digitale veiligheidssituatie te verbeteren. Organisaties, vitaal en niet-vitaal, zijn immers altijd zelf primair verantwoordelijk voor hun eigen weerbaarheid. In de Kamerbrief «Verkenning wettelijke taken en bevoegdheden digitale weerbaarheid en beleidsreacties WODC-rapporten», die gelijktijdig met deze brief aan uw Kamer is

---

[8] Kamerstuk 24 095, nr. 504.

[9] Voorstel CER-richtlijn, zie: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829&qid=1608544932364.

[10] Voorstel herziening NIB-richtlijn, zie: https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union.

[11] Kamerstuk 26 643, nr. 695.

[12] Kamerstuk 26 643, nr. 695.

[13] AIVD publicatie, «Offensief cyberprogramma, een ideaal businessmodel voor staten», zie: https://www.aivd.nl/documenten/publicaties/2019/06/27/offensief-cyberprogramma-een-ideaal-businessmodel-voor-staten.

verzonden, wordt dieper ingegaan op verschillende trajecten die gericht zijn op het verhogen van de digitale weerbaarheid[14].

Het grensoverschrijdende karakter van de digitale (statelijke) dreiging vereist ook robuuste internationale inzet. Drie sporen zijn richtinggevend voor de Nederlandse beleidsinzet in het internationale cyberdomein: het bestendigen van de internationale rechtsorde in het digitale domein, het formuleren van diplomatieke en politieke respons op inbreuken en ongewenste (statelijke) cyberoperaties en het versterken van de digitale weerbaarheid door andere landen te helpen met capaciteitsopbouw op het gebied van cybersecurity[15]. Zo is Nederland een van de drijvende krachten achter de EU Cyber Diplomacy Toolbox en het EU cybersanctie-regime. Daarnaast spant Nederland zich samen met Europese en internationale partners in om de weerbaarheid tegen cyberdreigingen te vergroten onder meer via de Europese samenwerkingsgroep en het CSIRT-netwerk in het kader van de NIB-richtlijn. Op 16 december hebben de Europese Commissie en de Hoge Vertegenwoordiger in een gezamenlijke mededeling aan de Raad en het Europees parlement een nieuwe EU Cyber Security strategie gepresenteerd met aanvullende maatregelen en regelgeving om te anticiperen op de toenemende digitale dreiging[16].

Samenbrengen responsopties

Om actieve handelingsperspectieven tegen statelijke dreigingen – onder de drempel van een gewapend conflict – voor besluitvormers binnen de rijksoverheid in kaart te brengen, wordt een domeinoverstijgend Rijksbreed Responskader (RBRK) statelijke dreigingen opgesteld. Hierin worden alle mogelijke responsopties binnen de rijksoverheid met een escalatieladder en afwegingskader bij elkaar gebracht en worden de bestaande responskaders binnen de verschillende domeinen, bijvoorbeeld binnen het economisch, financieel, diplomatiek en veiligheidsdomein, met behoud van hun rollen en procedures, op elkaar afgestemd. Oplevering van het RBRK is voorzien uiterlijk aankomende zomer.

Het belang van integraliteit en het voorkomen van «versnippering» zien we terug in de strategische communicatie van nationale en internationale partners. Een recent voorbeeld hiervan is dat bij aanvang van de COVID-19 crisis verschillende staten de eigen COVID-aanpak als superieur aanprezen, terwijl onder andere door desinformatie de samenwerking en de gemeenschappelijk aanpak van onder meer de EU en de NAVO werd ondergraven. De EU en de NAVO reageerden hierop door hun strategische communicatie hierover te versterken met als centrale boodschap, gestaafd met vele voorbeelden, dat beide organisaties elkaar wel weten te vinden in de strijd tegen COVID-19.

Bewustwording

De kennis op het thema statelijke dreigingen groeit ook buiten de overheid. Organisaties zijn in eerste instantie zelf verantwoordelijk voor hun weerbaarheid. Om organisaties hierin te ondersteunen werkt de rijksoverheid aan bewustwording onder verschillende doelgroepen. Door middel van (kleine) bijeenkomsten, voorlichting en de ontwikkeling van communicatiemateriaal, groeit de kennis op het thema statelijke dreigingen. Er wordt bijvoorbeeld actief ingezet op bewustwording van lokale partners. Begin 2020 organiseerde de NCTV in samenwerking met

---

[14] Kamerstuk 30 821, nr. 124.
[15] Kamerstuk 26 643, nr. 660.
[16] EU Cyber Security strategie, zie: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.

de gemeente Rotterdam een themadag voor gemeentes en zijn er vervolgens met een aantal gemeentes verdiepende gesprekken gevoerd. Doel hierbij is dat activiteiten die zich manifesteren op lokaal domein worden herkend, waar mogelijk decentraal wordt opgetreden en signalen ook bij de rijksoverheid terecht komen. Ook de AIVD zet zich in voor de bewustwording van de risico's van statelijke dreigingen zoals spionage en legt waar mogelijk uit aan bedrijven, overheden en kennisinstellingen hoe ze dit nu en in de toekomst kunnen voorkomen dan wel er mee om kunnen gaan. Met betrekking tot kennisinstellingen is het vergroten van de bewustwording bovendien een van de maatregelen die recent door het kabinet zijn aangekondigd om ongewenste overdracht van kennis en technologie tegen te gaan[17]. In dat kader is in september 2020 een intensieve ronde gesprekken met alle kennisinstellingen gestart. Alle universiteiten en ongeveer de helft van de onderzoeksinstituten (inclusief TO-2 instellingen voor toegepast onderzoek) zijn in het kader van deze «kennisveiligheidsdialoog» inmiddels bezocht. Binnenkort wordt gestart met de gesprekken met de hogescholen en wordt bezien hoe deze kennisveiligheidsdialoog na deze ronde kan worden voortgezet.

Onderzoek

Ter verbetering van het begrip van statelijke dreigingen en wat ertegen gedaan kan worden, draagt het kabinet nationaal en internationaal bij aan onderzoek. Sinds 2018 werkt het kabinet aan de ontwikkeling van een nationale kennisinfrastructuur op het terrein van (inter)nationale veiligheid. Deze infrastructuur berust op het interdisciplinaire Analistennetwerk Nationale Veiligheid (ANV), het gezamenlijke onderzoeksprogramma Progress van de Ministeries van Buitenlandse Zaken en Defensie en de gezamenlijke onderzoeksportefeuille naar de nexus tussen interne en externe veiligheid van de Ministeries van Buitenlands Zaken, Defensie en Justitie en Veiligheid. In het kader van Progress vinden bijvoorbeeld diverse onderzoeken naar strategische afhankelijkheden plaats. Ook in het kader van het China Kennisnetwerk vinden onderzoeken plaats die bijdragen aan een beter begrip van de statelijke dreigingen waarmee Nederland te maken heeft. Op het gebied van statelijke dreigingen is daarnaast door HCSS in samenwerking met internationale partners onderzoek uitgevoerd naar internationale normering in het hybride domein: *From Blurred Lines to Red Lines: How Countermeasures and Norms Shape Hybrid Conflict.* Daarnaast loopt er van 2019 tot 2023 een omvangrijk meerjarig onderzoek bij TNO naar het verhogen van de weerbaarheid tegen hybride dreigingen waarvan de resultaten interdepartementaal beschikbaar zijn en maakt Nederland deel uit van HYBNET, een onderzoeksnetwerk naar hybride dreigingen met 25 partners uit 14 Europese landen.

Civiel-Militaire samenwerking

In de *Defensievisie 2035*[18] wordt geconstateerd dat staten steeds openlijker kiezen voor competitie en daarbij gebruik maken van zowel civiele en militaire activiteiten. Om de meer permanente hybride dreigingen het hoofd te bieden, verdiept Defensie de geïntegreerde benadering van militaire en civiele middelen. De verwachting is dat er steeds vaker een beroep op het militair vermogen van Defensie zal worden gedaan en Defensie dient hierop voorbereid te zijn, zowel nationaal als internationaal. Hiervoor is het van belang om Europese defensiebudgetten te laten groeien naar de NAVO-norm, zodat Europa militair zelfstandiger wordt en de NAVO wordt versterkt. Doorlopende

[17] Kamerstuk 31 288, nr. 894.
[18] Kamerstuk 34 919, nr. 71.

inzet op civiel-militaire samenwerking is daarnaast van belang omdat Defensie zowel in normale als in buitengewone omstandigheden het civiele gezag kan ondersteunen en civiele partijen op hun beurt Defensie en onze bondgenoten steunen om militaire operaties mogelijk te maken. In juni 2020 is uw Kamer geïnformeerd over de doorontwikkeling van de civiel-militaire samenwerking met betrekking tot nationale veiligheid en crisisbeheersing[19].

Internationale samenwerking

Het is goed dat onderwerpen als ongewenste overdracht van kennis en technologie, bescherming vitale infrastructuur en ongewenste overnames hoog op de internationale agenda staan. De meeste landen om ons heen zijn bezig met de bescherming van dezelfde belangen en daarom kijkt het kabinet naar kansen om gezamenlijk op te trekken, bijvoorbeeld in EU, bilateraal of like-minded verband. Gezien deze ontwikkelingen wordt er in de aanpak statelijke dreigingen verder ingezet op het verbeteren van de informatiepositie en op het in kaart brengen van een internationaal netwerk. Door de uitwisseling van informatie krijgen we zicht op landen die een vergelijkbare problematiek kennen, kunnen we leren van hun ervaringen en de bewustwording op deze onderwerpen vergroten.

In internationaal verband wordt (het tegengaan van) statelijke dreigingen die zich manifesteren veelal hybride dreigingen of Countering Foreign Interference genoemd. Hierna volgt een overzicht van bestaande Europese en NAVO initiatieven op het gebied van hydride dreigingen die door Nederland aangemoedigd worden:

Op 24 juli 2020 heeft de Europese Commissie de Veiligheidsunie Strategie voor 2020–2025 gepubliceerd met o.a. aandacht voor de aanpak van hybride dreigingen[20]. Nederland steunt de brede geïntegreerde aanpak die de Europese Commissie nastreeft en onder andere gestalte krijgt door samenwerking tussen de EU-Lidstaten in de sinds juli 2019 in het leven geroepen «horizontale EU-Raadswerkgroep hybride dreigingen en tegengaan desinformatie», alsook via de EU Hybrid Fusion Cell. Op 15 december 2020 zijn EU raadsconclusies aangenomen over het versterken van de weerbaarheid van de EU en haar lidstaten en het bestrijden van hybride dreigingen, waaronder desinformatie, in de context van de Covid-19 pandemie[21]. Staatshoofden en regeringsleiders van NAVO-bondgenoten spraken tijdens de Leaders Meeting eind 2019 af om meer te doen tegen cyberaanvallen en hybride tactieken waarmee onze veiligheid en samenlevingen worden bedreigd[22]. Ook het recent gepubliceerde rapport «NATO 2030: United for a New Era» van de onafhankelijke reflectiegroep die aanbevelingen heeft gedaan aan de Secretaris-Generaal van de NAVO, onderkent het belang van een weerbare NAVO ten aanzien van huidige en toekomstige uitdagingen waaronder hybride dreigingen[23].

Nederland draagt actief bij aan het verhogen van de weerbaarheid tegen statelijke dreigingen in NAVO-verband onder andere door een actieve rol te spelen in de onderhandelingen over civiel-militaire weerbaarheidsmaatregelen en door het stimuleren van oefeningen in het kader van snellere

---

[19] Kamerstuk 34 919, nr. 68.

[20] Veiligheidsunie strategie over een breed scala aan onderwerpen: Zie: https://ec.europa.eu/info/strategy/priorities-2019–2024/promoting-our-european-way-life/european-security-union_nl.

[21] Persbericht over de raadsconclusies, 15 december 2020, zie: https://www.consilium.europa.eu/en/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation-in-the-context-of-the-covid-19-pandemic/.

[22] Kamerstuk 28 676 nr. 331.

[23] Reflection Group «Nato 2030: United for a New Era» Zie: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

herkenning en respons. Ook nam Nederland deel aan de eerste adviesmissie van de NAVO Counter Hybrid Support Teams in Montenegro. Nederland hecht aan een effectieve samenwerking tussen de EU en de NAVO. Het European Centre of Excellence to Counter Hybrid Threats speelt hierin een positieve rol. Dit centrum is in korte tijd uitgegroeid tot hét internationale kennisplatform rondom hybride dreigingen, waaraan 31 landen (EU/NAVO) verbonden zijn, waaronder Nederland.

Maatregelen ter verhoging van de weerbaarheid: sociale en politieke stabiliteit

Om ondermijning van de sociale en politieke stabiliteit tegen te gaan, worden uiteenlopende algemene, preventieve en repressieve maatregelen getroffen:

- Voor het tegengaan van ongewenste buitenlandse inmenging richting in Nederland wonende gemeenschappen met een migratieachtergrond is in 2018 een zogenoemde «OBI-aanpak» ontwikkeld, waarover is uw Kamer op 16 maart 2018 per brief geïnformeerd[24]. Voor een effectieve OBI-aanpak wordt onverminderd ingezet op het versterken van onze informatiepositie, onder andere door de inlichtingen- en veiligheidsdiensten. De vraag over welke actoren, dreigingen en kwetsbaarheden we het daarbij precies hebben, speelt een centrale rol.
- Internationaal zet Nederland in op samenwerking met een aantal internationale partners, met name binnen Europa: met EU-landen met vergelijkbare OBI-problematiek als Nederland wisselt Nederland kennis, ervaring- en handelingsperspectieven uit.
- Er wordt ingezet op het versterken van de weerbaarheid van de gemeenschappen waarop de ongewenste buitenlandse inmenging zich richt. Vanzelfsprekend wordt er doorlopend bekeken of deze aanpak volstaat en of aanvullende of andere instrumenten/maatregelen nodig zijn.
- Op 10 juni 2020 en op 23 november 2020 is uw Kamer schriftelijk geïnformeerd over -onder andere – de aanpak van ongewenste vormen van diasporapolitiek vanuit Turkije, die ervoor zorgt dat de overheid kan acteren bij vormen van ongewenste buitenlandse inmenging in het geval dat er sprake is van politieke sturing vanuit Turkije[25]. Ook gaat het kabinet verder inzetten op het ontwikkelen van beleid dat de weerbaarheid tegen onverdraagzame boodschappen in het kader van informele scholing vergroot[26].
- Om de verspreiding van desinformatie tegen te gaan, zet het kabinet sinds 2019 in op verschillende sporen[27]. Een van de uitgangspunten van het rijksbrede desinformatie beleid is dat statelijke actoren de capaciteit en middelen hebben om desinformatie te verspreiden, mede als onderdeel van hybride conflictvoering. Daarbij dient te worden opgemerkt dat het verspreiden van desinformatie zelf niet strafbaar is. Het beschermen van rechtsstatelijke waarden en grondrechten zoals de vrijheid van meningsuiting en pers staat voorop. In de aanpak van desinformatie zijn drie sporen benoemd: Het eerste spoor is preventie, acties die het doel hebben om te voorkomen dat desinformatie impact heeft en zich verspreidt, zoals het creëren van bewustwording bij alle betrokkenen (burgers, bedrijven, overheidsorganisaties, etc.) Het tweede spoor betreft het verstevigen van de informatiepositie, door o.a. betere informatiedeling is er tijdiger zicht op en duiding van de

[24] Kamerstuk 30 821, nr. 42.
[25] Kamerstuk 30 821, nr. 114 en Kamerstuk 35 228, nr. 33.
[26] Kamerstuk 29 614, nr. 153.
[27] Kamerstuk 30 821, nrs. 91 en 112.

(potentiële) dreigingen. Het derde spoor bestaat uit reactieve acties, en het vergroten van het handelingsperspectief bij desinformatie.
- Op EU-niveau wordt de verspreiding van desinformatie ook aangepakt. Het Europese Democratie Actieplan (EDAP) van 3 december 2020 vraagt o.a. sociale media platforms hun verantwoordelijkheid te nemen en gaat in op het beschermen van de verkiezingen en democratieën.
- Op 15 december 2020 is de *Digital Services Act* (DSA) gepresenteerd door de Europese Commissie. Hierin worden nieuwe richtlijnen gesteld voor sociale media platforms die het delen van illegale content tegengaan en meer transparantie geven over wat er op deze platforms gebeurt (welke data wordt er gedeeld, welke algoritmen liggen hieraan ten grondslag).
- Naast de generieke inzet tegen desinformatie rondom specifieke gebeurtenissen zoals het strafproces MH17, de coronacrisis of de Tweede Kamerverkiezingen 2021 houdt het kabinet samen met alle betrokken partijen de vinger aan de pols en neemt het waar nodig aanvullende stappen om te voorkomen dat de integriteit van de Nederlandse democratische rechtsorde en instituties worden ondermijnd.
- Wat betreft het tegengaan van ongewenste buitenlandse geldstromen werkt het kabinet, zoals aangegeven in de kabinetsreactie op het onderzoek door de parlementaire ondervragingscommissie naar ongewenste beïnvloeding uit onvrije landen (POCOB)[28], aan het vergroten van het zicht op de herkomst van buitenlandse geldstromen. Onlangs is aan uw Kamer het wetsvoorstel transparantie maatschappelijk organisaties gestuurd. Dit wetsvoorstel geeft het Openbaar Ministerie en burgemeesters de bevoegdheid om -indien er aanleiding toe is- inzicht te kunnen eisen bij maatschappelijke organisaties in Nederland naar financiële stromen vanuit het buitenland. Verder verkent het kabinet maatregelen om concrete ongewenste buitenlandse geldstromen tegen te gaan. Bij de verkenning wordt er gekeken naar de mogelijkheden om deze financiële stromen (tijdelijk) te kunnen stilleggen, bevriezen of verbeurd te verklaren.
- Om ongewenste belangenbehartiging van statelijke actoren te voorkomen zet het kabinet op dit moment vooral in op het verhogen van het bewustzijn bij personen en organisaties die hiervoor ingezet kunnen worden.

Maatregelen ter verhoging van de weerbaarheid: Economische veiligheid

In het dreigingsbeeld wordt de brede definitie van economische veiligheid aangehouden zoals beschreven in de NVS 2019[29]. Er is sprake van een toenemende verwevenheid van economische, geopolitieke en veiligheidsrisico's. Dit vraagt steeds om een zorgvuldige afweging van belangen, en vervolgens de inzet van het juiste beleid en instrumentarium, waarbij het kabinet onderscheid aanbrengt tussen enerzijds risico's voor de concurrentiekracht zonder dat nationale veiligheidsbelangen in het geding zijn en anderzijds risico's voor economische veiligheid[30]. Nederland is gebonden aan strikte internationale afspraken (zoals staatssteunregels etc.) waar het de concurrentiekracht betreft. Risico's voor de concurrentiekracht worden dan ook geadresseerd via de daarvoor bestaande economische en handelspolitieke instrumenten. De aanpak van economische veiligheidsdreigingen richt zich zoals aangegeven in de Kamerbrief tegengaan statelijke dreigingen specifiek op: continuïteit van vitale processen, de

[28] Kamerstuk 35 228, nr. 33.
[29] Kamerstuk 30 821, nr. 81.
[30] Kamerstuk 30 821 nr. 73.

integriteit en exclusiviteit van informatie en kennis en het voorkomen van ongewenste strategische afhankelijkheden[31]. Deze punten worden in het dreigingsbeeld als essentieel voor de economische veiligheid aangeduid.

De afgelopen tijd zijn diverse maatregelen genomen om de weerbaarheid op het gebied van economische veiligheid te verhogen:

- In 2019 zijn diverse aanvullende beschermingsmaatregelen aangekondigd om de veiligheid en integriteit van telecomnetwerken te waarborgen. Zo zullen bij ministeriële regeling nadere technische en organisatorische maatregelen aan de telecomaanbieders worden gesteld. De ontwerpregeling hiervoor is op 11 november voorgelegd voor een internetconsultatie. Ook kunnen telecomaanbieders bij beschikking worden verplicht om in kritieke onderdelen van hun netwerken uitsluitend gebruik te maken van anderen dan de daarbij genoemde, oftewel voor inschakeling in die kritieke onderdelen uitgesloten, partijen. Momenteel worden deze beschikkingen voorbereid. De juridische grondslag voor deze beide maatregelen is de algemene maatregel van bestuur, het Besluit veiligheid en integriteit telecommunicatie, van 5 december 2019.
- Ook op Europees niveau is aandacht voor de beveiliging van (5G-) telecomnetwerken. In maart 2019 heeft de Europese Commissie een aantal aanbevelingen gedaan om de weerbaarheid van de 5G-netwerken te verhogen. Naar aanleiding daarvan is er onder andere een toolbox gepubliceerd bestaande uit een set van instrumenten die lidstaten kunnen gebruiken om telecomnetwerken weerbaarder te maken. Recent heeft de Europese Commissie de voortgang die is gemaakt sinds de aanbevelingen als positief geëvalueerd.
- Er is voor de telecomsector een structureel proces ingericht waarin samen met relevante stakeholders bekeken worden op welke manier de telecomnetwerken ook in de toekomst weerbaar kunnen blijven tegen veranderingen in het dreigingsbeeld en technologische ontwikkelingen. Focus ligt hierbij op het doen van risicoanalyses, het inzichtelijk maken van afhankelijkheden en in kaart brengen waar adaptieve maatregelen mogelijk zijn. Hiermee is de aanpak adaptief in het bepalen van wat kritiek en niet kritiek is in de telecomnetwerken, conform de motie van het lid van den Berg[32].
- De structurele aanpak die voor de telecomsector is ingericht is een mooi voorbeeld hoe kan worden ingezet op de opbouw van diepgaande sectorale expertise. Daarnaast zien we dat vanuit deze kennis en ervaring ook de sector-overstijgende expertise kan worden versterkt, bijvoorbeeld op het gebied van risicoanalyses, strategische afhankelijkheden en informatiedeling. De komende periode wordt in kaart gebracht wat er nodig is (qua mensen, middelen en expertise) om deze structurele aanpak op telecom te verbreden naar andere vitale processen, zoals op het vitaal proces elektriciteit dat sterke intersectorale afhankelijkheden kent. Dit is conform de motie van de leden Buitenweg en Yesilgöz-Zegerius over dit onderwerp[33].
- Met het stelsel van investeringstoetsing breidt het kabinet haar instrumentarium voor het tegengaan van ongewenste investeringen, fusies en overnames verder uit. De wettelijke grondslag voor dit stelsel is op dit moment in voorbereiding en gaat specifiek voorzien in het mitigeren van risico's voor de nationale veiligheid bij overnames en investeringen binnen het toepassingsbereik van de toets. Het wetsvoorstel ziet op drie categorieën bedrijven: vitale aanbieders, specifieke toeleveranciers van vitale aanbieders en bedrijven die beschikken over sensitieve technologie die raakt aan de nationale

[31] Kamerstuk 30 821, nr. 72.
[32] Kamerstuk 24 095, nr. 499.
[33] Kamerstuk 35 570 VI, nr. 38.

veiligheid. In het wetsvoorstel wordt ook de mogelijkheid tot ingrijpen opgenomen wanneer na surséance van betaling of een faillissement de zeggenschap van een onderneming in handen komt van een ongewenste partij. Het wetsvoorstel wordt zo spoedig mogelijk, waarschijnlijk in het eerste kwartaal van 2021, aan uw Kamer aangeboden.

- Het kabinet introduceert ook een nieuwe sectorale investeringstoets op het gebied van de defensie-industrie, waarmee specifieke maatregelen kunnen worden genomen bij ongewenste investeringen, fusies en overnames binnen de toeleveringsketen van Defensie[34].
- Voor inkoop en aanbesteding wordt het instrumentarium, dat in 2018 is ontwikkeld, herzien en beschikbaar gesteld aan de rijksoverheid, decentrale overheden en speciale sector bedrijven die actief zijn in de vitale infrastructuur. Er bestaat geen verplichting deze hulpmiddelen te gebruiken en het kabinet verkent hoe het gebruik nader kan worden aangemoedigd.
- Om ongewenste kennis- en technologieoverdracht in het hoger onderwijs en wetenschap tegen te gaan is, aanvullend op het bestaande exportcontroleregime en bestaande sanctieregelgeving, op 27 november 2020 door het kabinet een pakket aan maatregelen aangekondigd. Het gaat daarbij om een combinatie van bewustwording en zelfregulering binnen de sector en een bindend toetsingskader op bepaalde risicovakgebieden. Maatregelen zijn bijvoorbeeld het opzetten van een advies- en expertiseloket, het maken van bestuurlijke afspraken over het veiligheidsbeleid binnen kennisinstellingen en het stellen van mogelijke restricties aan inkomende onderzoekers, promovendi en studenten en samenwerkingsovereenkomsten op bepaalde risicovakgebieden[35].
- Het kabinet investeert in de kennisopbouw aangaande zogenaamde sensitieve technologieën, die raken aan de nationale veiligheid. Hierbij worden de technologische toepassingen in kaart gebracht die raken aan de nationale veiligheid en criteria ontwikkeld, op basis waarvan opkomende technologieën kunnen worden geïdentificeerd die bescherming behoeven in het licht van de nationale veiligheid[36].
- Met betrekking tot het voorkomen van ongewenste strategische afhankelijkheid is het van belang te bezien welke strategische afhankelijkheden er bestaan en welke vanuit nationale veiligheidsoverwegingen onwenselijk zijn[37]. Om een dergelijke afhankelijkheid te voorkomen kijkt het kabinet breed naar de inzet van maatregelen, zoals het stelsel van investeringstoetsing en een versterking van de Nederlandse technologische- en innovatiebasis. Hier wordt ook in de versterkte aanpak vitale infrastructuur (zie hiervoor) aandacht aan besteed. Daarnaast beziet het kabinet of en hoe een afwegingskader kan helpen bij het bepalen wanneer sprake is van ongewenste economische afhankelijkheden voor Nederland en hoe deze te adresseren.
- De recente casus van spionage door een Russische Inlichtingenofficier bij een aantal bedrijven en een onderwijsinstelling binnen de Nederlandse hightech sector, demonstreert de toenemende kwetsbaarheid van Nederland voor spionage. Om die reden is door het kabinet de toegevoegde waarde van de strafbaarstelling van spionage op het bestaande instrumentarium onderzocht. Het Strafrecht biedt reeds mogelijkheden om op te treden jegens misdrijven die verband houden met schending van staats-, ambts- en bedrijfsgeheimen. Echter,

---

[34] Kamerstuk 31 125, nr. 113.
[35] Kamerstuk 31 288, nr. 894.
[36] Zoals ook gevraagd in de motie van het lid Van den Berg (Kamerstuk 30 821, nr. 110).
[37] Zie ook de Kamerbrief over het planbureau voor de veiligheid en strategische afhankelijkheden die binnenkort aan uw Kamer wordt verzonden.

spionage – als in de heimelijke samenwerking door personen met een buitenlandse inlichtingendienst – is op dit moment op zichzelf niet als zodanig strafbaar. Het kabinet heeft vastgesteld dat een aanvullende strafbaarstelling wenselijk is en zal onderzoeken op welke wijze daaraan vorm kan worden gegeven en vervolgens een wetstraject opstarten[38].

Conclusie en vooruitblik

Sinds het presenteren van de aanpak statelijke dreigingen in april 2019 zijn belangrijke stappen gezet om de weerbaarheid tegen statelijke dreigingen te verhogen. Maar we zijn er nog niet. Het dreigingsbeeld bevestigt dat de dreiging van statelijke actoren van permanente aard is en zelfs toeneemt. De doelwitten die het beeld noemt lopen sterk uiteen. Hoewel iedere organisatie zelf verantwoordelijk is om de weerbaarheid op orde te hebben, is hier ook een taak weggelegd voor de rijksoverheid. Verdere inzet is enerzijds nodig om de eigen weerbaarheid te organiseren en anderzijds om doelgroepen die doelwit zijn van statelijke activiteiten hierin te ondersteunen.

Allereerst is het van groot belang dat we de ingezette koers voortzetten en de informatiepositie verstevigen. Helder is dat we hiervoor onze belangen in kaart moeten brengen en bepalen wat we willen beschermen op het gebied van de vitale infrastructuur en toeleveranciers, sensitieve technologieën, hoogwaardige kennis en ongewenste strategische afhankelijkheid. Hiervoor is op alle vlakken een start gemaakt, maar moet nog een specificatieslag plaats vinden. Wat betekent het bijvoorbeeld als we een technologie sensitief vinden? Welke instrumenten gaan we dan hiervoor inzetten? En als we bepalen dat we een strategische afhankelijkheid ongewenst vinden, gaan we hier dan als Nederland maatregelen op nemen of juist in Europees verband?

In de zoektocht naar de antwoorden op bovenstaande vragen staat Nederland niet alleen. Ondanks de noodzaak aan een aanpak om statelijke dreigingen tegen te gaan, zijn er ook veel landen die onze waarden en normen delen. Voor het behoud van onze samenleving en economie is het dan ook noodzakelijk om niet alleen binnen Nederland verschillende perspectieven samen te brengen, maar hiervoor ook zoveel mogelijk de samenwerking met onze Europese en like minded partners te zoeken. Alleen door een voortdurende inzet op het integraal samenbrengen van de kennis van belangen en de kennis op de dreiging kan bepaald worden op welke vlakken aanvullende maatregelen nodig zijn. Een voorbeeld hiervan is de structurele samenwerking waarbij kennis van de techniek en kennis van de dreiging wordt samengebracht om zorgvuldig te kunnen beoordelen welke maatregelen nodig zijn. Op deze manier wordt de balans tussen veiligheid en openheid, als belangrijk uitgangspunt voor de aanpak tegengaan statelijke dreigingen, gegarandeerd.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

[38] Kamerstuk 30 977, nr. 157.