Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Nationaal Coördinator Terrorismebestrijding en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.nctv.nl

Ons kenmerk
2573867

Bijlagen
1

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 18 april 2019
Onderwerp Tegengaan statelijke dreigingen

Inleiding

Een open samenleving met een open economie vormt de grondslag voor de inrichting van onze maatschappij en de basis voor onze welvaart. Onze open samenleving staat in het teken van vrijheden, democratie, rechtsstaat en een internationale oriëntatie. Door deze openheid profiteren Nederland en Nederlanders van de kansen en mogelijkheden die bijvoorbeeld digitalisering en globalisering bieden. Een open economie en vrijhandel liggen sinds jaar en dag aan de basis van het Nederlandse verdienvermogen. Dit brengt ons namelijk de noodzakelijke financiering, schaalvoordelen, uitwisselen van talen en kennis en essentiële concurrentieprikkels. Dit is een grote kracht en heeft van Nederland als relatief klein land een wereldspeler gemaakt waar het gaat om kennis, innovatie, handel en investeringen. Verwevenheid van de internationale economie met wederzijdse afhankelijkheden kan bovendien bijdragen aan een vreedzame samenwerking en welvaartsgroei en kan deuren openen voor Nederland in het buitenland om ook politieke zaken te agenderen. Kortom, onze open samenleving en open economie zijn een groot goed dat wij moeten beschermen.

<u>De wereld om ons heen verandert</u>

Tegelijkertijd verandert de wereld ook en dat heeft gevolgen voor onze open samenleving en open economie. De wereld is in hoog tempo gedigitaliseerd en geopolitiek, economie en veiligheid zijn steeds meer met elkaar verweven geraakt. Nieuwe (digitale) technologieën nemen bovendien een snellere vlucht en worden belangrijker of zelfs onmisbaar voor het functioneren van onze maatschappij. Daarnaast vindt er een heropleving van machtspolitieke concurrentie tussen staten plaats, die verschuivingen binnen het geopolitieke speelveld teweeg brengt. Door globalisering is sprake van groeiende economische interactie, internationalisering van arbeidsmarkten en productieprocessen en liberalisering van het vestigings- en investeringsbeleid. Dit biedt meer mogelijkheden voor (heimelijke) verwerving van Nederlandse technologie en bedrijven. Nieuwe spelers hebben het wereldtoneel betreden en traditionele bondgenootschappen verdwijnen of veranderen van samenstelling. Staten proberen daarbij op steeds assertievere wijze hun eigen belangen te behartigen waardoor bestaande verhoudingen veranderen. Daarbij hanteren zij in toenemende mate andere regels, normen en waarden dan die waaraan Nederland en de internationale (westerse) gemeenschap zo gewend zijn geraakt. Zoals in de jaarverslagen van de AIVD en de MIVD is te lezen proberen staten inzicht te krijgen in besluitvorming en deze te beïnvloeden (inclusief de publieke opinie), digitale sabotage van vitale infrastructuur mogelijk te maken, bedrijfsgeheimen te stelen of hun (ex-)landgenoten te intimideren en te beïnvloeden. Steeds meer landen richten zich op politieke en/of economische spionage waarbij digitale spionage steeds complexer wordt. Zij maken daarbij

gebruik van cyberaanvallen, heimelijke beïnvloeding en economische machtsmiddelen om machtspolitieke agenda's te realiseren. Dit past in een breder wereldwijd beeld dat niet alleen Nederland raakt maar ook onze bondgenoten.[1] In deze veranderende wereld staat het kabinet pal voor de opdracht om onze open samenleving en open economie te koesteren en beschermen door open te zijn waar het kan en waakzaam te zijn voor statelijke dreigingen zodat bescherming kan worden geboden waar nodig.

Het is een ongemakkelijke paradox dat de vrijheden die deze openheid garanderen, kwaadwillende statelijke actoren ook de ruimte bieden om activiteiten te ondernemen die onze nationale veiligheid ondermijnen en daarmee onze vrijheden aantasten. 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. Risico's ten aanzien van onze nationale veiligheid moeten zo goed mogelijk worden beheerst, waarbij steeds een weging plaatsvindt tussen het veiligheidsbelang en mogelijke gevolgen voor de open samenleving en open economie. Hierbij moet de snelheid van ontwikkelingen in de wereld om ons heen, waaronder de digitale wereld, niet uit het oog te worden verloren.

Integrale aanpak

De dreigingen voor de nationale veiligheid die uitgaan van deze staten zijn van betekenis voor verschillende beleidsterreinen. Zo raken deze statelijke dreigingen aan democratische processen, digitalisering, economische veiligheid, internationale vrede en veiligheid, krijgsmacht en sociale stabiliteit. Deze thema's worden onder verantwoordelijkheid van verschillende bewindspersonen vormgegeven. Zowel bij het kijken naar statelijke dreigingen als bij het formuleren van tegenmaatregelen is *connecting the dots* van essentieel belang. Deze perspectieven worden bijeen gebracht om voortdurend te toetsen waar onze nationale veiligheidsbelangen in het geding kunnen komen door statelijke actoren en welke tegenmaatregelen noodzakelijk zijn.

Specifiek ten aanzien van economie en veiligheid zijn maatwerk, proportionaliteit en aandacht voor de verschillende belangen gewenst. Op hoofdlijnen ziet het kabinet twee manieren om ons beter te wapenen tegen de risico's op dit terrein. Ten eerste door de Nederlandse en Europese economie sterker te maken door in te zetten op het versterken van de interne markt, het mededingingsrecht en een modern innovatie- en industriebeleid. Een innovatieve economie is namelijk ook een minder kwetsbare economie. Bovendien zet het kabinet zich met de handelspolitieke inzet in op het versterken van het gelijke speelveld, wederzijdse markttoegang en bescherming van intellectueel eigendom. Deze inzet draagt bij aan het voorkomen van eenzijdige strategische afhankelijkheden. In de Kamerbrief Europese concurrentiekracht zal worden aangegeven hoe het kabinet hier (ook) in de Europese context invulling aan wil geven. Ten tweede is het kabinet daarbij waakzaam op de aantasting van de integriteit en exclusiviteit van kennis en informatie en de aantasting van continuïteit van dienstverlening van vitale diensten en processen voor de Nederlandse economie. In de bijlage vindt u de resultaten van de analyse die is uitgevoerd naar kwetsbaarheden in vitale sectoren. Dreigingen die uit kunnen gaan van statelijke actoren is hierbij slechts één van de mogelijke risico's. Het kabinet kijkt bij de aanpak van deze economische veiligheidsrisico's[2] ook breder. In de bijlage vindt u eveneens de aanvullende maatregelen die hiervoor van belang zijn, zoals een betere benutting en aanscherping van huidige wet- en

[1] Jaarverslagen AIVD, MIVD, CSBN, GBVS, Defensienota, Nationaal veiligheidsprofiel 2016, Horizonscan NV 2018, Strategische monitor 2018-2019.

[2] zoals is uiteengezet is in de nota Tussen Naïviteit en Paranoia en de opvolgende voortgangsrapportages Economische Veiligheid.

regelgeving, aandacht voor nationale veiligheid bij inkoop en aanbesteding en de uitwerking van een investeringstoets op nationale veiligheidsrisico's bij overnames en investeringen als laatste redmiddel. Nationale veiligheid is in eerste instantie een nationale competentie, maar meer Europese samenwerking is wenselijk. Het kabinet is er waakzaam voor dat de instrumenten die worden ingezet om de nationale veiligheid te garanderen geen onnodige schade berokkenen aan ons vestigings- en investeringsklimaat. Juist vanwege het open karakter van de Nederlandse en Europese economie moet er voor gewaakt worden dat maatregelen voor economische veiligheid in feite worden ingezet voor economisch protectionistische doeleinden.

Ook niet-statelijke actoren kunnen een risico vormen voor economische veiligheid, maar daar ligt niet de focus van deze brief. Met deze brief informeer ik u namens het kabinet over het beeld van de risico's door statelijke dreigingen, over het kabinetsbeleid over het tegengaan van statelijke dreigingen en de accenten in de aanpak voor de komende tijd. De aanpak rondom het tegengaan van statelijke dreigingen wordt ook opgenomen in de Nationale Veiligheid Strategie die voor de zomer verschijnt. Hierin wordt de kabinetsbrede strategische inzet op nationale veiligheid gedefinieerd.

Dreigingen en risico's

Om hun eigen belangen te behartigen en geopolitieke doeleinden te behalen, zetten statelijke actoren steeds vaker een breed scala aan middelen in, die potentieel ondermijnend kunnen zijn voor onze rechtsstaat en de stabiliteit en openheid van onze samenleving. Hun activiteiten zijn vaak doelbewust, stelselmatig en heimelijk en onder de drempel van wat we in internationaal recht verstaan onder gewapend conflict. De door statelijke actoren ingezette middelen c.q. ontplooide activiteiten kunnen de gehele breedte van het overheidsinstrumentarium bestrijken en kunnen al dan niet worden toegepast als onderdelen van een doelgerichte strategie van *hybride conflictvoering*[3]. Ondanks dat dit zich afspeelt onder de drempel van gewapend conflict maakt de militaire dimensie hier wel onderdeel van uit. Ook militaire middelen kunnen buiten een militaire conflictsituatie worden ingezet om een bepaald strategisch doel te bereiken. Onderstaand worden enkele manifestaties beschreven die in het actuele dreigingsbeeld voorkomen en waar Nederland, evenals de Europese Unie en NAVO, mee geconfronteerd worden.

Digitale middelen

De grootste dreiging op het digitale vlak wordt gevormd door statelijke actoren. Digitale middelen worden door staten ingezet voor manipulatie (bijvoorbeeld van gegevens) en sabotage (bijvoorbeeld door het verstoren van onze vitale processen), desinformatie (bijvoorbeeld in de verspreiding van onjuiste informatie rondom verkiezingen, via onder meer sociale media) en digitale spionage (bijvoorbeeld voor het vergaren van gevoelige of vertrouwelijke informatie).[4] Niet alleen het aantal staten dat digitale aanvalscapaciteiten ontwikkelt neemt toe, de aanvallen worden ook steeds complexer. Het ongestoord functioneren van digitale middelen is essentieel voor onder andere vitale processen binnen bedrijfsleven en overheid, het verdienvermogen van ondernemingen en het dagelijks leven van burgers. Incidenten in de afgelopen jaren hebben duidelijk gemaakt dat digitale aanvallen een grote impact op de samenleving kunnen hebben en kunnen leiden tot

[3] *Understanding hybrid threats. EPRS At a Glance* , juni 2015); Munich Security Report 2015. Collapsing Order, Reluctant Guardians? (MSC, 2015);*Irregular Adversaries and Hybrid threats: an assessment 2011* (US Joint Irregular Warfare Center, 2011); Hoffman, F., *Conflict in the 21st century: the rise of hybrid wars* (Potomac Institute for Policy Studies, december 2007), *Chimaera. Een duiding van het fenomeen 'hybride dreiging'*, NCTV april 2019 (herdruk van rapport juli 2017), www.nctv.nl

[4] Cyber Securitybeeld Nederland 2018, jaarverslagen AIVD en MIVD.

aantasting van de nationale veiligheid.

Economische middelen
De economische verwevenheid met staatsgeleide economieën roept vragen op over economische veiligheid[5]. Door overnames van en investeringen in vitale infrastructuur of bedrijven die hoogwaardige technologie ontwikkelen, kan een ongewenste afhankelijkheid ontstaan met risico voor het functioneren van de Nederlandse economie en democratische rechtsorde. De continuïteit van onze vitale processen kan in het geding komen of vertrouwelijke of gevoelige informatie kan weglekken. Een vergelijkbaar risico kan ontstaan door inkoop van cruciale diensten en producten. Ook economische spionage is een belangrijke manifestatie van sommige staten.

Ongewenste buitenlandse inmenging
Ondermijning door statelijke actoren is meestal een sluipend proces dat op langere termijn kan leiden tot ernstige ontwrichting en disfunctioneren van de democratische rechtsorde en open samenleving. Denk daarbij aan de integriteit van politieke en bestuurlijke besluitvorming, onafhankelijke rechtspraak, vrije en eerlijke verkiezingen en fundamentele vrijheden zoals persvrijheid, academische vrijheid en vrijheid van meningsuiting. Daarnaast kan ongewenste buitenlandse inmenging leiden tot spanningen binnen en tussen bevolkingsgroepen in Nederland en een barrière opwerpen voor de binding met de Nederlandse samenleving.[6] Statelijke actoren kunnen met ongewenste inmenging gebruik maken van verschillende beïnvloedingsmethodes en –doelgroepen, zoals diaspora, studenten, media of politici. Soms kan sprake zijn van heimelijke financiering. Ook de verspreiding van desinformatie behoort tot de gebruikte tactieken[7].

Afhankelijkheid van nieuwe (digitale) technologieën en de vitale infrastructuur
Een aantal ontwikkelingen doorsnijdt bovenbeschreven risico's en dreigingen. Nieuwe digitale technologieën, zoals *blockchains*, robotisering of kunstmatige intelligentie, transformeren de economie en samenleving in snel tempo. Digitalisering is de motor achter innovatie en bedrijvigheid[8] maar kan ook nationale veiligheidsrisico's met zich meebrengen, zoals spionage, sabotage en strategische afhankelijkheden. Dat zou kunnen leiden tot ongewenste afhankelijkheden met betrekking tot beschikbaarheid van deze technologiestandaarden. Op onze vitale infrastructuur is het bovenstaande op min of meer dezelfde wijze van toepassing. Nederland is afhankelijk van onze vitale processen, die onderling sterk met elkaar verweven zijn. Enige uitval of verstoring kan voor grote keteneffecten zorgen. Dit maakt dat de vitale infrastructuur een toegenomen doelwit is geworden, zowel digitaal als fysiek.

Voorbeelden in Nederland
Een verwijzing naar specifieke landen en de door hen ingezette manifestaties zijn onder ander te vinden in de jaarverslagen van de AIVD en MIVD. Dit beeld van risico's wordt ondersteund door de volgende voorbeelden:

- In april 2018 heeft de MIVD, samen met AIVD, een spionageoperatie van de Russische militaire inlichtingendienst GRU verstoord. Deze operatie was gericht tegen de Organisatie voor het Verbod op Chemische Wapens (OPCW) in Den Haag[9].
- Afgelopen januari zijn, mede op voordracht van Nederland, door de

[5] Investeren in Perspectief – Tweede Kamer, vergaderjaar 2018-2019,, 34 952, nr 41

[6] *Nationaal Veiligheidsprofiel 2016* (Analistennetwerk Nationale Veiligheid, 2016); *Tweede Kamerbrief Ongewenste buitenlandse inmenging* (NCTV, 16 maart 2018).

[7] Tweede Kamer, vergaderjaar 2018-2019, 30 821, nr. 51

[8] Investeren in Perspectief – Tweede Kamer, vergaderjaar 2018-2019,, 34 952, nr 41, p 21.

[9] Tweede Kamer, vergaderjaar 2018-2019, 33694 nr. 22

Europese Unie sancties opgelegd vanwege ernstige zorgen over de waarschijnlijke betrokkenheid van Iran bij vijandelijke acties op Europees grondgebied[10].

- In 2016 heeft het kabinet opgetreden naar aanleiding van berichten over rapportages die de attaché Religieuze Zaken van de Turkse ambassade in Nederland, tevens voorzitter van de Islamitische Stichting Nederland – de Nederlandse tak van Diyanet (ISN), aan Ankara stuurde over vermeende banden van Nederlandse organisaties en burgers met de Gülenbeweging. De Turkse autoriteiten hebben daarop in goed onderling overleg met het Ministerie van BZ besloten de attaché terug te trekken uit Nederland.[11]
- De Nederlandse overheid heeft signalen ontvangen van burgers die zich zorgen maken over hun familieleden in Xinjiang, die door de Chinese autoriteiten onder druk worden gezet om persoonsgegevens te delen[12].

Aanpak statelijke dreigingen

De volgende uitgangspunten staan centraal bij het tegengaan van statelijke dreigingen:

- De Nederlandse overheid is verantwoordelijk voor de nationale veiligheid en staat een **maatschappij-brede aanpak** voor. Hierbij worden overheidsorganisaties, veiligheidsdiensten, de krijgsmacht, bedrijfsleven en maatschappelijke organisaties actief betrokken bij de bescherming van de nationale veiligheidsbelangen. De overheid staat hierbij voor de publieke belangen, stimuleert de eigen verantwoordelijkheid van partijen en geeft het goede voorbeeld.
- Een **flexibele, adaptieve en geïntegreerde aanpak** die inspeelt op de ontwikkelingen maken dat risico's sneller zijn te detecteren en mitigeren. Interne en externe veiligheid zijn hierin onlosmakelijk verbonden. Internationale samenwerking is een belangrijk spoor in de aanpak.
- De aanpak heeft een **landen neutraal** karakter. Insteek is een generieke aanpak, toepasbaar op een dreiging vanuit elke statelijke actor, waarbij de actie van die actor potentieel leidt tot maatschappelijke ontwrichting, direct dan wel indirect via onze bondgenoten. Aan de hand van maatwerk en proportionaliteit worden deze generieke maatregelen ingezet in concrete gevallen.
- De aanpak wijzigt de bestaande rolverdelingen niet, maar zet bevoegdheden en beschikbare informatie beter op elkaar **afgestemd en gecoördineerd** in. Er wordt zoveel mogelijk gebruik gemaakt van de bestaande initiatieven, instrumentarium, samenwerkingsverbanden en informatiestromen rondom bijvoorbeeld cybersecurity, ongewenste buitenlandse inmenging en economische veiligheid.

De aanpak rondom het tegengaan van statelijke dreigingen bestaat uit een aantal generieke maatregelen die worden vermeld in onderstaande tabel. Gezien de dreiging, de te beschermen belangen en de recente casuïstiek ligt daarnaast het accent van de aanpak de komende periode op de thema's (1) ongewenste buitenlandse inmenging gericht op diaspora, (2) beschermen democratische processen en instituties en (3) economische veiligheid. Binnen deze thema's zijn al belangrijke stappen gezet en zijn ook nieuwe facetten onderkend die een versterkte aanpak behoeven. In de bijlage treft u de aanpak op deze thema's aan inclusief uitkomsten ex-ante analyses op economische veiligheid.

[10] Tweede Kamer vergaderjaar 2018-2019 35000-V, nr. 56 (Sancties tegen Iran wegen ongewenste Inmenging)

[11] Tweede Kamer, vergaderjaar 2015-2016, 32824 nr 194

[12] Tweede Kamer, vergaderjaar 2018–2019, 32 735, nr. 209

Aanpak tegengaan statelijke dreigingen	
A. Systematiek belangen dreiging weerbaarheid	Volgens een **vaste systematiek van belangen-dreiging-weerbaarheid** wordt bezien welke veiligheidsbelangen beschermd moeten worden, wat de dreiging is vanuit statelijke actoren voor de nationale veiligheid en hoe de weerbaarheid vergroot kan worden. Dit is een constant proces. Hierbij zijn bij uitstek de lidstaten van de EU en NAVO en binnen Nederland meerdere ministeries, lokaal bestuur en private organisaties betrokken. Dat vergt coördinatie en verbinding. • De minister van Justitie en Veiligheid richt zich, vanuit het perspectief van nationale veiligheid, in samenspraak met andere departementale partners op coördinatie en afstemming tussen de verschillende betrokkenen, verantwoordelijkheden, initiatieven, projecten en informatiestromen. • In deze lijn is onlangs een Taskforce Economische Veiligheid opgericht die in het teken staat van kwetsbaarheden en beheersmaatregelen van het 5G-netwerk.
B. Verbetering informatie-positie	Er wordt ingezet op **verbetering van de informatiepositie en informatiedeling** tussen en met gelijkgestemde partijen, zowel nationaal als internationaal om tijdig zicht te krijgen op en duiden van de (potentiële) dreigingen. Daartoe moet informatie delen gemakkelijker en logischer worden, waardoor een gedeeld normbeeld kan ontstaan. • Waar nodig worden interdepartementale *trusted communities* ingericht of versterkt. • Werkafspraken rondom specifieke onderwerpen zorgen er voor dat indien nodig informatie snel kan worden gedeeld en handelingsperspectief voor handen is. • Ook in internationaal verband vindt nauwe samenwerking plaats ten aanzien van dreiging en *best practices* in de aanpak. • Ambassades hebben een belangrijke monitoring- en signaleringsfunctie ter bevordering van het situationeel bewustzijn. • Nederland neemt in EU-verband deel aan het Rapid Alert System, waar direct informatie wordt uitgewisseld in geval van desinformatie campagnes. • In Nederland wordt de civiel-militaire samenwerking geïntensiveerd.
C. Bewustwording & oefenen	**Bewustwording** vormt een belangrijke schakel in het verhogen van de weerbaarheid tegen de dreiging vanuit statelijke actoren. • Er wordt fors ingezet op bewustwording bij onder andere inkopers, ambtenaren, gemeenten, vitale infrastructuur, CEO's en richting het publiek door middel van bijvoorbeeld bijeenkomsten, voorlichting en communicatiemateriaal. Een voorbeeld hiervan is de bewustwordingscampagne desinformatie die is gestart. • Op nationaal en internationaal niveau wordt **geoefend** op identificatie van en respons op statelijke dreigingen, mede door het ontwikkelen van en oefenen met scenario's. Deelname aan oefeningen van NAVO (CMX) en EU (PACE) wordt voortgezet.
D. Integrale kennisontwikkeling	Door middel van een **integrale onderzoeksagenda en kennisontwikkeling** op het gebied van weerbaarheid tegen statelijke dreigingen wordt gezamenlijk kennis opgebouwd.
E. Maatregelen ter verdediging en afschrikking	Nederland zet zich ook in voor verdere ontwikkeling van maatregelen ter verdediging en afschrikking. • Diplomatiek: Binnen het responskader heeft het kabinet verschillende diplomatieke instrumenten tot haar beschikking om statelijke dreigingen tegen te gaan. • Ter verdediging van de nationale veiligheid zet Nederland zich, waar mogelijk in samenwerking met internationale partners, in voor **verdere ontwikkeling van een effectief diplomatiek responskader**, inclusief attributie. Zo kan bij aanvallen van statelijke actoren worden gekozen om tot (publieke) attributie over te gaan. • De aanpak op ongewenste buitenlandse inmenging blijft actueel en verbreed zich naar meerdere landen.

	• Politieke beïnvloeding wordt tegengegaan door toerusting en bescherming politieke ambtsdragers, een verkenning registratieplicht lobbyisten, veilig verloop van de verkiezingen door het onderkennen van bijzondere signalen, beïnvloeding en desinformatie. • In de Defensienota en het Nationaal Plan zet Defensie in op versterking van capaciteiten oa op het gebied van inlichtingen, cyber en contra-hybrid. In de nieuwe Defensienota zal volgend jaar ingegaan worden op verdere doorontwikkeling ten behoeve van nationale en internationale veiligheid.
F. Economie en Veiligheid	Het **instrumentarium om onze economische veiligheid te borgen tegen nationale veiligheidsrisico's** moet op orde zijn. Maatwerk, proportionaliteit en aandacht voor de verschillende belangen die spelen zijn daarbij belangrijke uitgangspunten van de aanpak. • Ten aanzien van economische veiligheid wordt onder andere gewerkt aan een uitwerking van een investeringstoets op nationale veiligheidsrisico's bij overnames en investeringen, aan de ontwikkeling en uitrol van beleid en richtlijnen bij inkoop en aanbesteding bij de overheid en binnen de vitale infrastructuur. Ook wordt gewerkt aan een uitbreiding van de kennisregeling ivm weglekken gevoelige technologie via het academische vlak. • Bij het toetsen van nationale veiligheidsrisico's wordt gebruik gemaakt van consistente, en technisch *up to date* zijnde criteria.
G. Digitale aanpak	Het kabinet zet middels de Nederlandse Cybersecurity Agenda (NCSA), die in april 2018 aan uw Kamer is verzonden, de Internationale Cyberstrategie en de GBVS, in op **een digitaal veilig Nederland**. In de aanpak wordt ook rekening gehouden met de invloed van statelijke actoren. • Zo wordt bijvoorbeeld geïnvesteerd in het versterken van de weerbaarheid van digitale processen en een meer robuuste infrastructuur en wordt de digitale slagkracht verder op orde gebracht om te kunnen reageren op de toename van de digitale dreiging en grootschalige cyberincidenten die de nationale veiligheid bedreigen. • In een aparte brief wordt uw Kamer, in samenhang met het CSBN 2019, nog voor de zomer geïnformeerd over de jaarlijkse voortgang van de NCSA.
H. Internationale samenwerking	Nederland zet zich in internationaal verband in lijn met de Geïntegreerde Buitenland- en Veiligheidsstrategie in voor: • **Goede samenwerking in EU- en NAVO-verband, als ook tussen EU en NAVO**, op het gebied van situationeel bewustzijn, weerbaarheid en respons. In EU-verband staan de 22 actiepunten centraal zoals geformuleerd in het *Gezamenlijk Kader voor de Bestrijding van Hybride Bedreigingen* (2016). In NAVO-verband is de *NATO Strategy on NATO's role in Countering Hybrid Warfare* (2015) het leidend kader. • Accurate (internationale) informatiepositie in nauwe samenwerking met internationale partners om informatie uit te wisselen. In EU- en NAVO verband en ad hoc met gelijkgezinde partners. • Het bevorderen van de internationale rechtsorde en een effectief multilateraal systeem op het gebied van statelijke dreigingen. Om de toenemende dreiging het hoofd te bieden zet NL, waar mogelijk en relevant, in op gezamenlijke respons en attributie van operaties. • Geloofwaardige afschrikking tegen statelijke dreigingen in bondgenootschappelijk verband, onder andere in NAVO-verband. In juli 2018 is besloten tot instelling van Counter Hybrid Support Teams (CHST), ofwel NAVO-teams die bondgenoten kunnen adviseren en assisteren rondom hybride dreigingen. • Benutting van het *European Centre of Excellence on Countering Hybrid Threats* als netwerkorganisatie en platform voor

	expertiseontwikkeling. Nederland is hier sinds 2018 bij aangesloten. • Verbeterde samenwerking tussen de verschillende EU instellingen om onderwerpen met de noodzakelijke samenhang te adresseren (zoals onder meer desinformatie, verkiezingen, cybersecurity, crisisbeheersing, vitale infrastructuur en buitenlandse overnames). • Met het aantreden van een nieuwe Europese Commissie in 2019 ontstaat een belangrijk momentum om een lans te breken voor een consistentere aanpak op het gebied van interne veiligheid, waaronder statelijke dreigingen.[13]

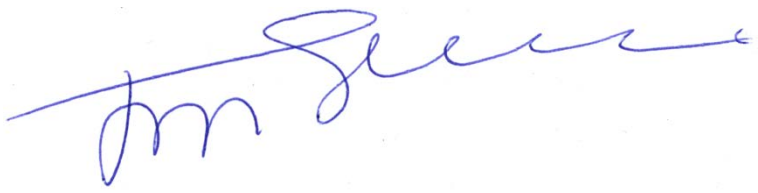
Ten slotte

Met deze brede aanpak bouwt het kabinet verder aan de weerbaarheid tegen statelijke dreigingen. Voorvallen die los bezien niet de aandacht zouden trekken in het licht van onze nationale veiligheid, kunnen in een brede aanpak beter met elkaar in verband worden gebracht en getoetst aan de mogelijkheid van een achterliggende ondermijnende of hybride strategie vanuit kwaadwillende staten of (heimelijk) door hen aangestuurde partijen.

De afgelopen periode is door verschillende departementen, in nauwe samenwerking met partijen uit de publieke én private sector en de wetenschap hard gewerkt aan deze volgende kabinetsbrede stap. De statelijke dreiging is in zijn aard veranderlijk en vraagt een adaptieve aanpak. Het kabinet zal daarom onder coördinatie van de minister van Justitie en Veiligheid bezien of partijen voldoende zijn toegerust om deze dreiging het hoofd te bieden. Dit vraagt een continue cyclus van inzicht in de dreiging en intenties van de tegenstander, het actueel houden van de te beschermen (vitale) belangen en het waar nodig verhogen van de weerbaarheid van die mensen, processen en informatie die maken dat onze samenleving open, veilig en welvarend kan blijven.

De komende maanden zullen we de ambities uit de deze aanpak waar nodig en in nauwe samenwerking met de betrokken departementen en overige partners, nader uitwerken in concrete maatregelen.

De Minister van Justitie en Veiligheid,



Ferd Grapperhaus

[13] Tweede Kamer, vergaderjaar 2018-2019 Staat van de Europese Unie 2019, 35 078, nr. 1