Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

30 821 Nationale Veiligheid

Nr. 175

BRIEF VAN DE MINISTERS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES, VAN DEFENSIE, VAN BUITENLANDSE ZAKEN, VAN ECONOMISCHE ZAKEN EN KLIMAAT, VAN ONDERWIJS, CULTUUR EN WETENSCHAP, VAN SOCIALE ZAKEN EN WERKGELEGENHEID EN VOOR BUITENLANDSE HANDEL EN ONTWIKKELINGSSAMENWERKING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 28 november 2022

Hierbij bieden de Ministers van Binnenlandse Zaken en Koninkrijksrelaties, van Defensie en van Justitie en Veiligheid uw Kamer het door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) gepresenteerde Dreigingsbeeld Statelijke Actoren 2 (DBSA 2) aan. Met deze brief bieden de bovengenoemde Ministers en de Ministers van Buitenlandse Zaken, van Economische Zaken en Klimaat, van Onderwijs, Cultuur en Wetenschap, van Sociale Zaken en Werkgelegenheid en voor Buitenlandse Handel en Ontwikkelingssamenwerking tevens een beleidsreactie op het DBSA 2. De brief schetst de strategische inzet van het kabinet om de weerbaarheid te verhogen tegen dreigingen die uitgaan van statelijke actoren[1]. Met deze brief wordt tevens invulling gegeven aan de nadere uitwerking van het coalitieakkoord (bijlage bij Kamerstuk 35 788, nr. 77) en verschillende moties en toezeggingen op het gebied van onder meer vitale infrastructuur, kennisveiligheid en ongewenste buitenlandse inmenging.

Ontwikkelingen in de dreiging: nationale veiligheidsbelangen onder druk

Het geopolitieke klimaat in de wereld is onmiskenbaar guurder en instabieler geworden. Het DBSA 2 gaat in op een verhoogde dreiging van een agressiever Rusland dat meermaals nucleaire retoriek heeft geuit. Daarnaast is een assertiever China zichtbaar, dat de internationale rechtsorde in zijn voordeel wil veranderen, en een toenemende (geo)poli-

[1] Deze brief volgt op de twee eerdere Kamerbrieven over de aanpak van statelijke dreigingen (Kamerstuk 30 821, nr. 72 en Kamerstuk 30 821, nr. 125).

kst-30821-175
ISSN 0921 - 7371
's-Gravenhage 2022

tisering van de (wereld)economie waarbij economische instrumenten als machtsmiddel worden ingezet. Zoals ook volgt uit het advies «De Oekraïne-oorlog als geopolitieke tijdschok» van de Adviesraad Internationale Vraagstukken heeft de Russische oorlog in Oekraïne in het bijzonder laten zien dat ons open en internationale karakter ons ook kwetsbaar kan maken.[2] Dit beeld wordt nog eens bevestigd door het rapport «De Russische invasie in Oekraïne: Implicaties voor Nederland» van het *Hague Centre for Strategic Studies*. Daarnaast is de dreiging van ongewenste inmenging in diasporagemeenschappen onverminderd aanwezig.

Als gevolg van deze ontwikkelingen worden Nederland en de Europese Unie steeds vaker openlijk en heimelijk geconfronteerd met handelingen van statelijke actoren, die bewust of onbewust onze belangen, waaronder onze nationale veiligheidsbelangen[3], kunnen schaden. Dat dit een reële dreiging is bleek met het uitwijzen van 17 Russische inlichtingenofficieren in maart van dit jaar, die werkzaam waren onder een diplomatieke dekmantel.[4] Statelijke actoren gebruiken niet-traditionele machtsmiddelen, waarbij de inzet heimelijk of met dubbele agenda's plaatsvindt: dit noemen we hybride dreigingen. Hybride dreigingen zijn dreigingen voor de nationale veiligheid, die zich grotendeels manifesteren onder het niveau van een openlijk gewapend conflict, waarbij sprake is van een meervoudig gebruik van middelen door statelijke en/of niet-statelijke actoren, met als doel bepaalde strategische doelstellingen te bereiken. Voorbeelden hiervan zijn militaire intimidatie, spionage en sabotage, cyberaanvallen, desinformatiecampagnes, ongewenste buitenlandse inmenging in diasporagemeenschappen, kennisdiefstal of de inzet van economische instrumenten. Deze middelen worden al dan niet in samenhang ingezet.

Deze dreigingen raken de veiligheid van NAVO-landen en EU-lidstaten, de internationale rechtsorde en de open Nederlandse samenleving en (kennis-) economie, allen cruciale Nederlandse publieke belangen. Nederland, de Europese Unie en internationale partners moeten zich wapenen tegen dit brede palet aan hybride dreigingen. Het DBSA 2 constateert dat de internationale rechtsorde in toenemende mate onder druk is komen te staan. Dit belang wordt door verschillende statelijke actoren ter discussie gesteld en neergezet als een westers construct, en daarmee structureel aangetast. Ook worden internationale normen als non-interventie, non-proliferatie en vreedzame geschillenbeslechting geschonden en vormen internationale instituties steeds meer het toneel waarop statelijke actoren de internationale rechtsorde proberen te ondermijnen. Dat raakt ook Nederland als een van de meest open en internationaal verbonden landen ter wereld.

Het DBSA 2 constateert ook toegenomen conventionele en nucleaire statelijke dreigingen, onder meer vanuit Rusland, China, Noord-Korea en Iran. Nederland stelt zich primair in NAVO-verband tegen deze dreigingen te weer. Deze brief gaat verder niet in op deze dreigingen, maar beperkt zich tot hybride dreigingen.

---

[2] Een kabinetsreactie op het AIV-advies is in voorbereiding en komt uw Kamer toe.

[3] De zes nationale veiligheidsbelangen van Nederland staan verwoord in de Nationale Veiligheidsstrategie (NVS) van 2019 en zijn: territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, de politieke/sociale stabiliteit en de internationale rechtsorde.

[4] Kamerstuk 35 925 V, nr. 86.

Versterking en uitbreiding aanpak statelijke dreigingen noodzakelijk

Onze aanpak van statelijke dreigingen moet, in het licht van het onguurdere en instabielere geopolitieke klimaat, in een hogere versnelling. Het is cruciaal dat Nederland, in nauwe samenwerking met EU-partners, bondgenoten en gelijkgezinden, in staat is om deze dreigingen, nu en in de toekomst, het hoofd te kunnen bieden, en beschikt over een instrumentarium gericht op voorkomen, mitigeren *en* reageren. De staande aanpak tegen statelijke dreigingen zal worden bestendigd, versterkt en uitgebouwd. Hiermee beschermen we onze democratische rechtsorde en nationale veiligheid.

Daarmee dragen wij ook bij aan het beschermen van de internationale rechtsorde en het open en vrije karakter van onze samenleving, economie, onderwijs en wetenschap. Dit doen we onder meer door minder afhankelijk van de *just in time economy* te worden en de veerkracht en weerbaarheid van de vitale infrastructuur te versterken. Daarnaast zetten we in op vergroting van de open strategische autonomie van de EU en vermindering van risicovolle strategische afhankelijkheden. Tegelijkertijd is het van belang dat Nederland een open samenleving en economie houdt waarin we andere landen niet de rug toekeren, maar in gesprek blijven. Dit vergt keuzes met keerzijden, bijvoorbeeld omdat ze tot hogere kosten, minder *efficiency* of minder flexibiliteit kunnen leiden. Het gevolg zijn ingewikkelde afwegingen waarvan de uitkomst niet bij voorbaat vaststaat en die per geval gemaakt moeten (kunnen) worden.

Om de hybride dreigingen die uitgaan van statelijke actoren het hoofd te bieden is een samenhangende en diverse set aan maatregelen en instrumenten nodig die Nederland in staat stelt zich hiertegen te verweren. Zowel in het civiele als militaire domein[5]. Deze brief beschrijft de maatregelen en de kaders waarbinnen deze gecoördineerd kunnen worden ingezet en is het Nederlandse antwoord op deze hybride statelijke dreigingen.

Dit antwoord is een robuuste aanpak, die de inzet van overheidspartijen, bedrijfsleven en kennisinstellingen verbindt, en zich richt op het beschermen van onze publieke belangen en het versterken van het vermogen om dreigingen te detecteren, aan te pakken en waar nodig te voorzien van een reactie. Deze aanpak wordt vormgegeven binnen de volgende accenten:

1. *Proactief optreden wanneer Nederlandse publieke belangen worden geschaad,*
2. *Bevorderen en beschermen van de economische veiligheid, waaronder kennisveiligheid,*
3. *Tegengaan van ongewenste buitenlandse inmenging, en*
4. *Beschermen van democratische processen en instituties.*

De aanpak van statelijke dreigingen vindt sinds 2019 plaats. Concrete stappen die het kabinet hierin de afgelopen jaren heeft gezet zijn:

- De Wet veiligheidstoets investeringen fusies en overnames,
- De Rijksbrede aanpak van ongewenste buitenlandse inmenging,

[5] De krijgsmacht heeft als Grondwettelijke taak (artikel 97) om de belangen van het Koninkrijk te beschermen en te verdedigen. Dit geldt onder normale- én in buitengewone (oorlogs-)omstandigheden. Deze taak ziet op de integriteit van het eigen en bondgenootschappelijk grondgebied en betreft zowel de (klassieke) militaire taakuitoefening als de civiele taakuitoefening door bijstand te leveren aan de civiele autoriteiten binnen het Koninkrijk. De krijgsmacht is daarbij een structureel en integraal onderdeel van het crisisbeheersingsinstrumentarium waarover de Nederlandse overheid beschikt.

- De vormgeving van het Rijksbreed responskader dat Nederland in staat stelt gecoördineerd te reageren op hybride dreigingen,
- Een pakket aan maatregelen op het terrein van kennisveiligheid, en
- Een wetsvoorstel uitbreiding van de strafbaarstelling van spionage.

Het kabinet heeft binnen de bovengenoemde accenten onder meer aandacht voor strategische afhankelijkheden met risico's voor de nationale veiligheid, zoals de toegang tot kritieke grondstoffen en mondiale distributie- en transportroutes. Om de risico's van strategische afhankelijkheden te mitigeren is in de afgelopen jaren een grote hoeveelheid nationale en Europese beleidstrajecten in gang gezet. Daarbij gaat het zowel om bestaande als mogelijk toekomstige risicovolle strategische afhankelijkheden. Het is noodzakelijk om de komende tijd op het tegengaan van risicovolle en strategische afhankelijkheden voort te bouwen en deze aanpak te versterken. Voor de bescherming van de open strategische autonomie van de EU en onze economische veiligheid zet het kabinet in op stimulerend economisch beleid, beschermende maatregelen, het ontwikkelen van coalities van gelijkgezinde landen rond onderwerpen als economische dwang, behoud en verder ontwikkelen van een internationale op regels gebaseerde rechtsorde in samenhang. Om de ambities ook met betrekking tot stimulerend economisch beleid waar te kunnen maken, zal het kabinet in de reguliere besluitvormingsmomenten bezien in hoeverre de bestaande middelen hiervoor toereikend zijn.[6]

Versterkte aanpak vitale infrastructuur

Uit het DBSA 2 en Cybersecuritybeeld Nederland 2022[7] (CSBN 2022) blijkt dat meerdere vitale processen doelwit zijn van statelijke actoren en digitale aanvallen. De grootste digitale dreiging gaat uit van China, Rusland en in mindere mate van Iran en Noord-Korea. Zo zet China zijn cybercapaciteiten onder andere in om hoogwaardige technologie te bemachtigen, onderneemt Iran bijvoorbeeld digitale spionageactiviteiten tegen universiteiten en is van Noord-Korea bekend dat het inzet op diefstal van digitale valuta ter financiering van zijn staatskas. Rusland richt zich onder meer op prepositie voor sabotage tegen vitale infrastructuur. Om die reden heeft het Kabinet in 2021 de versterkte aanpak ter bescherming van de vitale infrastructuur aangekondigd. De Nederlandse cybersecuritystrategie die in oktober van dit jaar werd gepresenteerd, adresseert de dreiging die uitgaat van digitale aanvallen op vitale processen eveneens. Het kabinet wil voorkomen dat risico's een bedreiging vormen voor de continuïteit, integriteit en vertrouwelijkheid van de Nederlandse vitale processen en werkt daartoe aan adequate weerbaarheid.

De versterkte aanpak vitaal zet in op het verbeteren van de bescherming van de Nederlandse vitale infrastructuur door maatregelen te treffen om de weerbaarheid van de vitale processen te vergroten en het vitaal beleid, de beleidscyclus en het vitaalstelsel te herzien. Ook wordt relevante wetgeving tegen het licht gehouden en waar nodig in de komende periode uitgebreid of aangepast. Hierbij worden de *Critical Entities Resilience Directive* (CER) en de *Network- and Information Security 2 Directive* (NIS2) betrokken. Naar verwachting worden beide richtlijnen voor het einde van dit jaar door de Europese Unie vastgesteld. Op dit moment worden interdepartementaal voorbereidingen getroffen voor de

---

[6] Zie ook de recent verzonden Kamerbrief over Open Strategische Autonomie voor meer informatie over de kabinetsvisie op strategische afhankelijkheden en een actief industriebeleid, zoals via IPCEI's. (Kamerstuk 35 982, nr. 9).

[7] Kamerstuk 26 643, nr. 891.

implementatie van beide richtlijnen. Hierover wordt uw Kamer begin volgend jaar geïnformeerd.

De sabotage van Nordstream 1 en 2 heeft nogmaals het belang van deze versterkte aanpak onderstreept. De veranderde veiligheidscontext vraagt ook om een verbeterd zicht op de weerbaarheid van de Nederlandse vitale infrastructuur. Als onderdeel hiervan wordt gewerkt aan een afhankelijkhedenanalyse met het doel risicovolle afhankelijkheden in beeld te brengen. Deze analyse zal ingaan op intersectorale afhankelijkheden, op afhankelijkheden van specifieke grondstoffen, producten of specifieke landen. De opvolging van de motie van het lid Rajkowski c.s. (Kamerstuk 26 643, nr. 874) die vraagt om een scan uit te voeren op de aanwezigheid van apparatuur of programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda in de vitale infrastructuur is onderdeel van dit onderzoek. Uw Kamer wordt hierover eveneens geïnformeerd in de brief over de versterkte aanpak vitale infrastructuur die begin 2023 wordt gepresenteerd.

Uitgangspunten versterkte aanpak statelijke dreigingen

Het dreigingsbeeld toont de noodzaak voor het kabinet om zich vol in te zetten voor de bestendiging, versterking en uitbouw van de aanpak van statelijke dreigingen. Ook de samenwerking met lokale en regionale veiligheidspartners, het bedrijfsleven en kennisinstellingen wordt versterkt; veel dreigingen van statelijke actoren manifesteren zich immers op lokaal of regionaal niveau, bijvoorbeeld bij een bedrijf, universiteit of lokale gemeenschappen. De aanpak van statelijke dreigingen vraagt ook een nauwe samenwerking met onze Europese en internationale partners.

Met de in het coalitieakkoord vrijgemaakte middelen zet het kabinet in op het verbeteren van de inlichtingen- en informatiepositie. Doel hiervan is beter zicht krijgen op dreigingen, het verhogen van bewustwording bij zowel overheden, bedrijfsleven als kennisinstellingen en het versterken van preventieve maatregelen: voorkomen is immers beter dan genezen. Door een integrale aanpak *(connecting the dots)* kan de overheid sneller interveniëren waar we risico vermoeden, in nauwe samenwerking met partijen binnen en buiten de overheid, en neemt het vermogen toe in te grijpen en/of te reageren wanneer nationale veiligheidsbelangen worden geschaad. De middelen voor versterking van Defensie[8] dragen hier tevens aan bij.

De volgende uitgangspunten zijn onverkort leidend in de aanpak van statelijke dreigingen:

- De overheid is verantwoordelijk voor de nationale veiligheid en staat een maatschappijbrede aanpak voor waarin publieke en private partijen samenwerken aan nationale veiligheid. De overheid staat in deze aanpak voor de publieke belangen, stimuleert eigen verantwoordelijkheid van alle stakeholders en geeft het goede voorbeeld.
- De aanpak van statelijke dreigingen is flexibel, adaptief en gericht op samenwerking, en bevordert informatiedeling tussen betrokken partijen om risico's en dreigingen vroegtijdig te kunnen signaleren.
- De aanpak van statelijke dreigingen is landenneutraal; maar waar nodig worden gerichte(re) maatregelen getroffen om de dreiging van statelijke actoren te verminderen, statelijke actoren te ontmoedigen of de weerbaarheid van Nederland te vergroten.
- Hiermee wordt de integrale aanpak van verschillende beleidsterreinen die samen de weerbaarheid tegen de dreiging door statelijke actoren vormgeven versterkt en doorontwikkeld. Bestaande rolverdelingen en

[8] Defensienota 2022, Kamerstuk 36 124, nr. 1.

verantwoordelijkheden blijven ongewijzigd, maar worden op basis van een gedeeld beeld, in afstemming en coördinatie ingezet.

Geïntegreerde aanpak en doelstellingen statelijke dreigingen

Hybride dreigingen zijn per definitie pluriform en kunnen zich overal manifesteren. Dit vraagt om een stevig instrumentarium voor Nederland, voor de Europese Unie en voor andere internationale en multilaterale partners. Dit vraagt ook om coördinatie van inzet op hybride dreigingen op het nationale, internationale en Europese niveau; in Nederland berust de coördinatie bij de NCTV, in nauwe samenwerking met het Ministerie van Buitenlandse Zaken dat in den brede coördinerend is voor de Nederlandse inzet in de EU en de NAVO en onder meer de Ministeries van Defensie, Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Klimaat en Onderwijs, Cultuur en Wetenschap, de inlichtingen- en veiligheidsdiensten, het Nationaal Cybersecurity Centrum, nationale politie en partners binnen de vitale infrastructuur. Hieronder volgt een overzicht van concrete doelstellingen, maatregelen en ontwikkelingen waar het kabinet aan werkt. Dit wordt als benoemd vormgegeven binnen de volgende accenten van de aanpak:

1. *Proactief optreden wanneer Nederlandse publieke belangen worden geschaad,*
2. *Bevorderen en beschermen van de economische veiligheid, waaronder kennisveiligheid,*
3. *Tegengaan van ongewenste buitenlandse inmenging, en*
4. *Beschermen van democratische processen en instituties.*

1. Proactief optreden wanneer Nederlandse belangen worden geschaad

De hierboven geschetste voorbeelden laten zien dat Nederland, Europese partners en bondgenoten geconfronteerd kunnen worden met een breed palet aan dreigingen door statelijke actoren. Het kabinet wil, vanuit een Rijksbrede aanpak, in staat zijn bij een (mogelijke) dreiging van een statelijke actor snel en proactief te kunnen handelen wanneer Nederlandse publieke belangen geschaad (kunnen) worden. Om die reden werkt het kabinet aan een Rijksbreed responskader dat voorziet in de mogelijkheid assertief op te treden en terug te duwen tegen een kwaadwillende statelijke actor. Bij de opzet van dit kader zijn alle departementen betrokken zodat een breed beeld ontstaat over de activiteiten van statelijke actoren. Ook maakt de Rijksbrede opzet het mogelijk een breed instrumentarium in te zetten. Het doel van het responskader is tweeledig:

1) De betreffende actor af te schrikken en te bewegen schadelijke activiteiten richting Nederland, Nederlandse of Europese belangen of de belangen van bondgenoten na te laten dan wel te staken;
2) Mitigeren van de impact van de acties van de actor of actoren, danwel deze actoren de mogelijkheden te ontzeggen nog langer schadelijke acties uit te voeren.

Inzet van het kader zal alleen plaatsvinden na een politiek besluit en bij voorkeur in Europees en bondgenootschappelijk verband. Momenteel loopt een *pilot* tot de zomer van 2023 waarin het Rijksbreed responskader wordt uitgewerkt. Na een evaluatie van deze pilot zal het responskader vanaf het najaar van 2023 kunnen worden ingezet.

Het kabinet constateert dat de aanpak van hybride statelijke dreigingen inmiddels ook stevig op de internationale agenda staat. Zowel in EU- als in NAVO-verband lopen initiatieven voor een geïntegreerde aanpak tegen hybride dreigingen. In EU-verband wordt gewerkt aan de vaststelling van een hybride toolbox en een FIMI toolbox (buitenlandse informatiemanipu-

latie en inmenging). Op 21 juni 2022 zijn hierover door de Europese Unie Raadsconclusies aangenomen. Momenteel wordt gewerkt aan de implementatie van richtsnoeren om deze beide toolboxen te operationaliseren. De hybride toolbox is bedoeld als een overkoepelend kader dat bestaande en mogelijke nieuwe instrumenten samenbrengt om in EU-kader een gecoördineerde respons tegen hybride dreigingen en campagnes te bieden. De FIMI toolbox, die tevens werd aangekondigd in het EU Strategisch Kompas[9], richt zich specifiek op de bestrijding van informatiemanipulatie en inmenging. De EU heeft in het Europees Democratie Actieplan aangekondigd een instrumentarium te ontwikkelen dat gebruikt kan worden bij het tegengaan van FIMI.

Op de NAVO-top van Madrid van afgelopen juni werd het nieuwe Strategisch Concept aangenomen. Hierin wordt nogmaals onderstreept dat hybride operaties tegen NAVO-lidstaten het niveau kunnen bereiken van een gewapende aanval en dus kunnen leiden tot het inroepen van Artikel 5 van het Noord Atlantisch Verdrag.

Onderzoek en kennisopbouw over hybride dreigingen

Zoals ook in de Defensienota 2022[10] en in het kader van het EU Strategisch Kompas wordt benoemd vereist het begrip van hybride dreigingen en op welke manier hiertegen opgetreden kan worden voortdurende kennisontwikkeling. De bestaande onderzoeksmiddelen worden dan ook blijvend aangewend om onze kennis van statelijke en hybride dreigingen te vergroten en er vindt doorlopend onderzoek plaats naar de weerbaarheid van Nederland, Europese en internationale partners. Zo start begin 2023 een nieuw vierjarig onderzoek van TNO, waar de steeds transformerende aard van hybride dreigingen, detectie, afschrikking en responsopties centraal staan. Ook neemt Nederland deel aan het *European Centre of Excellence for Countering Hybrid Threats* en aan het EU-consortium *EU-HYBNET*. De Ministeries van Buitenlandse Zaken en Defensie continueren in 2023 de studie over hybride afschrikking bij het *Hague Centre for Strategic Studies* en een onderzoek naar de implementatie van de hybride toolbox van de EU door Clingendael. Deze onderzoeken dragen bij aan de kennisopbouw in Nederland op het gebied van hybride dreigingen.

2. Bevorderen en beschermen van de economische veiligheid, waaronder kennisveiligheid

Het DBSA 2 concludeert dat Nederland steeds vaker openlijk en heimelijk geconfronteerd wordt met dreigingen tegen de economische veiligheid. Daarbij zijn vitale processen kwetsbaar voor sabotage door statelijke actoren en ook, bijvoorbeeld als gevolg van investeringen en overnames, voor ongewenste invloed van buitenlandse actoren. Ook is er sprake van een toename van misbruik van bepaalde strategische afhankelijkheden. De Europese afhankelijkheid van Russisch gas heeft dat recent duidelijk gemaakt. Tot slot zijn Nederlandse bedrijven, kennisinstellingen en wetenschappers op grote schaal doelwit van activiteiten om hoogwaardige technologie buit te maken. China vormt op dat gebied de grootste dreiging voor de Nederlandse kennisveiligheid. Diefstal en het weglekken van kennis brengt het risico van oneerlijke concurrentie en ongewenst eindgebruik voor bijvoorbeeld militaire doeleinden met zich mee.

---

[9] Kamerstuk 21 501-02, nr. 2474.
[10] Kamerstuk 36 124, nr. 1.

De Nederlandse economie is gebaat bij een sterk mondiaal handels- en investeringssysteem en een sterke internationale positie als kennisland. Een groot deel van onze welvaart hebben we te danken aan onze handelsactiviteiten, grensoverschrijdende kapitaalstromen, kennis en innovatie. Hoogwaardig onderwijs en excellent (wetenschappelijk) onderzoek zijn essentieel om in de toekomst een relevante speler te blijven. Samenwerking tussen bedrijven en kennisinstellingen – zowel nationaal als internationaal – levert een bijdrage aan kapitaal, talent en kennis, en aan het uitwisselen van technologieën en ideeën ten behoeve van de maatschappelijke uitdagingen van vandaag en morgen. Nederland moet dan ook nadrukkelijk de openheid, kansen en samenwerking blijven zoeken, in het bijzonder binnen de EU en met belangrijke bondgenoten als de Verenigde Staten, het Verenigd Koninkrijk en Australië. Maar ook, met inachtneming van de risico's, met landen waarmee een complexere betrekking bestaat. Hier is Nederland bij gebaat.

Onze kenniseconomie, met sterke innovatiekracht en hoogwaardige hightech-ecosystemen, maakt evenwel dat we ook een aantrekkelijk doelwit zijn voor landen die kennis en technologie op ongeoorloofde of onwenselijke wijze willen vergaren, ten gunste van hun eigen (technologische) positie. Hierdoor kunnen Nederlandse publieke belangen, zoals ons verdienvermogen, de maatschappelijke uitdagingen genoemd in het coalitieakkoord[11] en onze nationale veiligheid onder druk komen te staan. Economische veiligheid is daarom al enige tijd een prioriteit in de aanpak van statelijke dreigingen.

Bewustwording blijft aandacht vergen

Het bewustzijn van risico's binnen de Rijksoverheid en medeoverheden neemt toe. Dit geldt ook voor het bedrijfsleven en kennisinstellingen, onder andere door verbeterde samenwerking en het uitwisselen van informatie. Desondanks blijft bewustwording onverminderd een punt van aandacht. We blijven dan ook inzetten op verhoging van bewustwording en informatie- en kennisdeling tussen publieke en private partijen. Voor het *bedrijfsleven* richt de Rijksdienst voor Ondernemend Nederland (RVO) in opdracht van het Ministerie van Economische Zaken en Klimaat om die reden een Rijksbreed aanspreekpunt in om informatie te verstrekken aan bedrijven over economische veiligheid. De planning is dat dit loket in het voorjaar van 2023 zal starten. In januari 2022 is in opdracht van het Ministerie van Onderwijs, Cultuur en Wetenschap het loket kennisveiligheid al bij de RVO geopend. Hier kunnen *kennisinstellingen* terecht voor advies over de kansen en risico's die zijn verbonden aan internationale samenwerkingen, en hoe dat zo veilig mogelijk kan worden ingericht. Daarnaast wordt, door een stevige financiële impuls in het coalitieakkoord voor de inlichtingendiensten en het Nationaal Cyber Security Centrum gebouwd aan meer en beter zicht op potentiële dreigingen en kwetsbaarheden die door statelijke actoren kunnen worden misbruikt. Ook wordt het *postennetwerk* versterkt, dit draagt bij aan een beter zicht op potentiële dreigingen uit het buitenland.

Het beleid rondom economische veiligheid kent de volgende doelstellingen:

[11] Waaronder in het bijzonder klimaatambities en energietransitie.

a) Het mitigeren van risico's voor de nationale veiligheid als gevolg van overnames

Naast sectorale investeringstoetsen (gas, telecom, elektriciteit) is de Wet veiligheidstoets investeringen, fusies en overnames (Vifo) inmiddels aangenomen door de Eerste en Tweede Kamer. De aanname van deze wet is een belangrijke mijlpaal in de bescherming van onze nationale veiligheid tegen de risico's van investeringen, fusies en overnames. De Wet Vifo zal het toepassingsbereik van het stelsel van investeringstoetsing uitbreiden met meer vitale aanbieders, bedrijven die actief zijn op sensitieve technologie, en beheerders van campussen waar sensitieve technologie aanwezig is. Voor een optimale werking van de wet werkt het kabinet aan twee algemene maatregelen van bestuur die gegeven de afhankelijkheid van de doorlooptijden van advies- en uitvoeringsinstanties, alsmede van voorhang in uw Kamer, op zijn vroegst in het eerste helft van 2023 in werking treden en terugwerkende kracht hebben tot 8 september 2020. Met deze wet zet het kabinet een grote stap in het voorkomen van ongewenste zeggenschap in vitale processen, sensitieve technologie en bedrijfscampussen. Om de sectorale investeringstoetsen en de uitvoering van Wet Vifo mogelijk te maken is het Bureau Toetsing Investeringen (BTI), onderdeel van het Ministerie van Economische Zaken en Klimaat, inmiddels twee jaar operationeel. Verder werkt het kabinet aan de sectorspecifieke investeringstoets voor de defensie-industrie. Deze wet ziet op essentiële bedrijven in de toeleveringsketen van het vitale proces «Inzet Defensie». Deze investeringstoets zal naar verwachting in 2023 gereed zijn en wordt ook met uw Kamer gedeeld. Het kabinet is zich er daarbij van bewust dat investeringen, fusies en overnames niet alleen per bedrijf moeten worden bezien, maar tevens in relatie tot de gehele sector in het licht van strategische afhankelijkheden.

b) Veilig inkopen en aanbesteden

Vanwege de dreiging van statelijke actoren moeten risico's voor de nationale veiligheid bij de inkoop en het gebruik van producten en diensten bij de (rijks- en lokale) overheid en vitale aanbieders worden geïdentificeerd en beperkt. Het uitgangspunt is bij iedere inkoopopdracht risico's voor de nationale veiligheid in kaart te brengen en hier waar nodig maatregelen op te treffen. Ter ondersteuning van dit beleid heeft het kabinet instrumentarium ontwikkeld dat organisaties handvatten biedt bij het maken van een risicoanalyse en het treffen van maatregelen. Momenteel werkt het kabinet aan de doorontwikkeling en aanscherping van dit instrumentarium. Doel is met het instrumentarium bij te dragen aan het identificeren en mitigeren van risico's bij dienstverleners en in de (toe)leverancierskeketen. De toepassing van dit instrumentarium wordt verplicht gesteld voor relevante inkoopopdrachten binnen het Rijk.

Het kabinet werkt tevens aan een Rijksbrede regeling voor aanbestedingen die de nationale veiligheid raken (ABRO, Algemene beveiligingseisen Rijksoverheid opdrachten). Dit betreft een doorontwikkeling vanuit de huidige ABDO (Algemene beveiligingseisen Defensie opdrachten) van het Ministerie van Defensie. De nieuwe regeling zal eisen stellen aan opdrachtnemers op het gebied van fysieke beveiliging, (digitale) informatiebeveiliging en cybersecurity, (wijzigingen in) eigendomsstructuren, economische veiligheid, screening van personeel en procedures bij incidenten. Het (laten) meewegen van nationale veiligheid bij inkoop en aanbestedingen in de vitale infrastructuur zal in de versterkte aanpak vitaal worden meegenomen. Daarnaast wordt ook in dit traject doorlopend ingezet op bewustwording van de dreiging die uitgaat van statelijke actoren bij inkopers, binnen de Rijksoverheid en bij vitale aanbieders. In aanvulling op deze brief wordt uw Kamer tot slot voor het

eind van het jaar nader geïnformeerd over de inzet van het kabinet op veilig inkopen en aanbesteden, naar aanleiding van de motie Rajkowski en van Weerdenburg[12] en de motie Rajkowski c.s.[13]

c) Voorkomen van ongewenste kennis- en technologieoverdracht

Om spionage en sabotage tegen te gaan, de nationale veiligheid te borgen en technologisch leiderschap te behouden is het van belang ongewenste overdracht van hoogwaardige kennis en technologie te voorkomen. Om invulling te kunnen geven aan noodzakelijke maatregelen en daarbij het open karakter van onze academische wereld en economie te bewaken moet met elkaar worden afgestemd welke (onderdelen en toepassingen van) kennis en technologie we precies willen beschermen. Exportcontrole is een van de middelen om ongewenste kennis- en technologieoverdracht tegen te gaan. Voorafgaand aan de uitvoer van strategische goederen toetst de overheid op het gevaar voor de Nederlandse en internationale veiligheid. Het kabinet zal hier de komende jaren ook onverminderd op inzetten. De Minister voor Buitenlandse Handel en Ontwikkelingssamenwerking informeert uw Kamer hier nader over.

Kennisveiligheid als gezamenlijk initiatief overheid en kennissector

Nederlandse kennis- en onderwijsinstellingen en het bedrijfsleven beschikken over veel kennis en hoogwaardige technologie. Deze sectoren zijn dan ook het doelwit van statelijke actoren in hun (heimelijke) zoektocht naar buitenlandse kennis. Tegelijkertijd is internationale samenwerking de zuurstof voor de Nederlandse kennissector. We hebben het nodig om de kwaliteit van onze wetenschap op peil te houden, evenals ons innovatie- en verdienvermogen. Om kennis en innovaties afdoende te beschermen is het voor bedrijven en kennisinstellingen van belang te beschikken over enerzijds voldoende bewustzijn van de dreiging op het gebied van kennis en innovatie en anderzijds over voldoende inhoudelijk inzicht om specifieke dreigingen tijdig te kunnen signaleren, ook bij snel veranderende technologie. De Rijksoverheid heeft daarom in het kader van kennisveiligheid een pakket aan maatregelen genomen met drie uitgangspunten: 1) het tegengaan van ongewenste kennisoverdracht, 2) het voorkomen van heimelijke beïnvloeding en 3) ethische kwesties. In deze aanpak moeten de kennissector en overheid nauw samen optrekken.

Een belangrijke stap in de aanpak van kennisveiligheid bij kennisinstellingen is de implementatie van de Nationale Leidraad Kennisveiligheid. Dit is een gezamenlijk initiatief van het Rijk én de kennissector met als doel ervoor te zorgen dat internationale wetenschappelijke samenwerking veilig kan plaatsvinden, met een goede balans tussen de kansen en risico's, én met respect voor en inachtneming van de academische kernwaarden. Andere belangrijke maatregelen zijn de uitvoering van de risicoanalyses door de kennisinstellingen, de externe audit naar de implementatie van de leidraad en (onder andere naar aanleiding van de motie Van der Woude en Van der Molen (Kamerstuk 31 288, nr. 979)) de aanpak en uitkomsten van de risicoanalyses, de bestuurlijke gesprekken

[12] Kamerstuk 26 643, nr. 830: een onderzoek te doen naar hoe apparatuur en programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda geweerd kunnen worden uit aanbestedingen van de Rijksoverheid en een scan te maken van apparatuur of programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda die aanwezig is binnen (de kernsystemen van) de vitale sector en deze resultaten te betrekken bij het toegezegde onderzoek met betrekking tot aanbestedingen van de Rijksoverheid.

[13] Kamerstuk 26 643, nr. 874: te komen met een richtlijn voor de Rijksoverheid en haar leveranciers dat producten of diensten van organisaties en bedrijven uit landen met een offensieve cyberagenda gericht tegen Nederland uit bepaalde aanbestedingen geweerd kunnen worden.

en de opening van het eerdergenoemde loket kennisveiligheid. Ook in EU-verband zijn stappen gezet om kennisveiligheid op de agenda te zetten en de Europese Commissie heeft verschillende initiatieven op dit terrein genomen. Nederland zet zich actief in voor kennisveiligheid in de EU en internationaal en blijft samenwerken met gelijkgezinde landen om te leren van hun aanpak en hierover uit te wisselen. Eind dit jaar zal de Minister van Onderwijs, Cultuur en Wetenschap uw Kamer informeren over de voortgang en uitwerking van de zojuist genoemde kennisveiligheidsmaatregelen. Daarbij zal hij ook ingaan op de voorstellen voor een toetsingskader. Hiermee kunnen personen uit derde landen worden getoetst op risico's op ongewenste kennis- en technologieoverdracht wanneer zij bij kennisinstellingen op sensitieve technologiegebieden actief zullen zijn.

Kennismigranten en oneigenlijk gebruik erkend referentschap

Een van de manieren waarop statelijke actoren kunnen proberen om via bedrijven toegang te verkrijgen tot hoogwaardige kennis en technologie is door middel van kennismigranten en bedrijven die misbruik maken van het erkend referentschap dat benodigd is om kennismigranten naar Nederland te halen. De regelingen rondom kennismigranten, en het daarmee verbonden erkend referentschap, maken het voor bedrijven en kennisinstellingen eenvoudiger en sneller om niet-Europese hoogopgeleide immigranten in dienst te nemen. De kennismigrantenregeling is cruciaal voor het faciliteren van de instroom van kenniswerkers uit het buitenland en levert daarmee een belangrijke bijdrage aan de innovatiekracht van Nederland. De samenstelling van deze instroom van kenniswerkers is het resultaat van de vraag van Nederlandse werkgevers naar talent. Echter is het ook van belang dat erop wordt toegezien dat regelingen rondom kennismigranten en het erkend referentschap niet gebruikt kunnen worden voor oneigenlijke doeleinden. Momenteel wordt door alle betrokken ministeries en organisaties gezamenlijk onderzocht hoe ongewenste kennis- en technologieoverdracht via bedrijven, onder meer via kennismigranten en bedrijven die erkend referent zijn, kan worden tegengegaan.

Hiermee wordt ook verdere opvolging gegeven aan de motie van het voormalig lid Wiersma[14] en het vertrouwelijke dreigingsbeeld dat daaropvolgend is opgesteld, zoals benoemd in de brief aan uw Kamer van 24 september 2021.[15] Het traject behelst verschillende sporen, te weten het bepalen van de scope van de te nemen maatregelen, het op de korte en lange termijn creëren van bewustwording onder het bedrijfsleven alsook het uitwerken van een handelingsperspectief rondom het verstrekken van verblijfsvergunningen en het toekennen van het erkend referentschap aan bedrijven. In het kader van bewustwording worden bijeenkomsten georganiseerd voor bedrijven die werken met gevoelige technologieën en/of kennis. Doel van de bijeenkomsten is het creëren van bewustzijn bij de bedrijven en het uitwisselen van perspectieven over ongewenste kennis- en technologieoverdracht. Onlangs heeft een eerste bijeenkomst plaatsgevonden tussen vertegenwoordigers van speciaal genodigde bedrijven en de betrokken departementen en uitvoeringsorganisaties.

d) Uitbreiding strafbaarstelling spionage

In het Coalitieakkoord 2021–2025 «Omzien naar elkaar, vooruitkijken naar de toekomst» is opgenomen dat buitenlandse inmenging wordt tegengegaan «o.a. door spionage strafbaar te stellen». Het Wetboek van

[14] Kamerstuk 35 680 nr. 17.
[15] Kamerstukken 19 637 en 30 821, nr. 2770.

Strafrecht bevat op dit moment al verschillende bepalingen die kunnen worden ingezet om strafrechtelijk op te treden tegen gedragingen die samenhangen met spionage, zoals de strafbaarstellingen van de schending van staats- en bedrijfsgeheimen. Deze strafbaarstellingen bieden echter onvoldoende mogelijkheden om op te treden tegen spionageactiviteiten waarbij geen sprake is van een schending van (staats- of bedrijfs-) geheimen of waarbij het gaat om andere gedragingen ten behoeve van een buitenlandse mogendheid dan het verstrekken van informatie, terwijl ook dergelijke gedragingen de Nederlandse belangen zoals de nationale veiligheid, vitale infrastructuur, de integriteit en exclusiviteit van hoogwaardige technologieën en de veiligheid van personen ernstig kunnen schaden. Een wetsvoorstel waarin de strafbaarheid wordt uitgebreid tot dergelijke schadelijke spionageactiviteiten is inmiddels in consultatie geweest en vervolgens aan de Afdeling advisering van de Raad van State (Raad van State) voorgelegd. Op dit moment wordt het advies van de Raad van State verwerkt. Ik verwacht het wetsvoorstel op korte termijn aan uw Kamer te kunnen aanbieden.

e) Mitigeren van de risico's van strategische afhankelijkheden

In de Kamerbrief Open Strategische Autonomie is uiteengezet dat het kabinetsbeleid ten aanzien van de *open strategische autonomie van de EU* zich richt op drie pijlers: 1. Structurele politiek-economische versterking van de EU, 2. Het mitigeren van risicovolle strategische afhankelijkheden, en 3. Het vergroten van het geopolitiek handelingsvermogen van de EU. Voor een meer gedetailleerde uiteenzetting van de beleidstrajecten ten aanzien van strategische afhankelijkheden, kan de Kamerbrief Open Strategische Autonomie geraadpleegd worden. Belangrijke elementen in de aanpak op het terrein van open strategische autonomie die hieronder nader worden uiteengezet zijn de inzet op technologisch leiderschap en toegang tot kritieke grondstoffen.

Om ook in de toekomst onze publieke belangen op het vlak van nationale veiligheid, verdienvermogen en maatschappelijke uitdagingen te kunnen verdedigen, is het belangrijk te investeren in de digitale transformatie van Nederland en de EU en toegang te hebben en houden tot cruciale technologieën en toepassingen. *Technologisch en digitaal leiderschap* in cruciale sectoren (onder andere semicon, kwantum en de ruimte, maar ook op het gebied van diensten en datastromen) is nodig om de positie van Nederland en de EU in de wereld te behouden en te versterken.[16] Dat vraagt om een slim samenspel tussen het behoud van zo goed mogelijke toegang tot cruciale technologieën en toepassingen wereldwijd enerzijds en het versterken van technologische capaciteiten binnen Nederland en de EU anderzijds, zonder ongerechtvaardigde marktverstoringen. Het is essentieel om in te blijven zetten op hoogwaardig onderwijs en excellent (wetenschappelijk) onderzoek om in de toekomst een relevante speler te blijven en technologisch leiderschap te behouden. Verder is *internationale samenwerking*, in de EU maar ook daarbuiten, met onder meer de Verenigde Staten, Japan, Zuid-Korea en Australië, van cruciaal belang. Technologisch leiderschap stelt Nederland en andere EU-lidstaten in staat om toegang te houden tot technologie elders, maar ook om ons (militair) te kunnen verdedigen, spelregels internationaal te bevorderen en de koers van technologische ontwikkeling mede te bepalen volgens onze waarden.

[16] Het kabinet werkt onder coördinatie van EZK aan een nadere invulling van de digitale autonomie van de digitale economie en infrastructuur. Deze invulling is naar verwachting voor de zomer van 2023 gereed.

Door de groeiende digitalisering en de klimaattransitie worden *kritieke grondstoffen* steeds belangrijker. Hierdoor krijgen kritieke grondstoffen een sterker geopolitiek karakter. Europa – en daarmee ook Nederland – is voor kritieke grondstoffen in hoge mate afhankelijk van onder andere China, de Democratische Republiek Congo en Australië. Er wordt momenteel gewerkt aan een Nederlandse grondstoffenstrategie met als doel de leveringszekerheid op de korte en (middel)lange termijn van deze kritieke grondstoffen veilig te stellen en daarnaast ook duurzame mineralenketens te bevorderen. Het streven is deze grondstoffenstrategie eind dit jaar aan te bieden aan uw Kamer. Een groot deel van de inzet is optreden in EU-verband, er wordt dan ook actief aansluiting gezocht bij de *Critical Raw Materials Act* die de EU naar verwachting in 2023 publiceert.

3. Tegengaan van ongewenste buitenlandse inmenging

Ongewenste buitenlandse inmenging (OBI) is in onze vrije en open maatschappij niet acceptabel. Het DBSA 2 constateert dat Nederland en zijn bondgenoten doelwit blijven van (heimelijke) beïnvloedingsactiviteiten van statelijke actoren. Statelijke beïnvloedingsactiviteiten zetten, bedoeld en onbedoeld, druk op de cohesie binnen de Nederlandse samenleving. Bovendien blijven diasporagemeenschappen en opposanten van autoritaire regimes doelwit van verschillende openlijke en heimelijke vormen van beïnvloeding en inmenging door herkomstlanden.

Personen binnen diasporagemeenschappen voelen zich regelmatig onder druk gezet, geïntimideerd of rechtstreeks bedreigd door de activiteiten die andere landen in Nederland ontplooien. Uitgangspunt van het kabinet is dat mensen in Nederland zich vrij en ongehinderd dienen te kunnen ontplooien, zonder angst voor ongewenste of heimelijke inmenging van andere landen. Hiervoor is het belangrijk dat zowel in de communicatie met andere landen, als voor mensen in Nederland helder is waar de normale vorm van interactie met andere landen ophoudt en ongewenste inmenging begint. Het kabinet zet bij de aanpak van ongewenste buitenlandse inmenging in op drie sporen:[17]

- Het *diplomatieke* spoor: het aangaan van de dialoog met landen die zich schuldig maken aan ongewenste inmenging en hen daar consequent op aanspreken, en indien nodig ook diplomatieke stappen ondernemen tegen de betreffende landen;
- Het *weerbaarheidsspoor*: het verhogen van de weerbaarheid van de kwetsbare groepen die mogelijkerwijs vatbaar zijn voor ongewenste buitenlandse inmenging;
- Het *bestuurlijk/strafrechtelijke* spoor: het gecoördineerd optreden en verstoren bij actuele of dreigende incidenten, waarbij we een mix van bestuurlijke en strafrechtelijke maatregelen inzetten. Het hierboven reeds genoemde wetsvoorstel voor de uitbreiding van de strafbaarstelling van spionage zal in dit spoor tot een toename van juridische slagkracht leiden.

De komende jaren zal de analyse en duiding van bestaande en nieuwe vormen van ongewenste buitenlandse inmenging door middel van een vijfslag verder worden geïntensiveerd. Deze vijfslag bestaat uit 1) welke statelijke *actoren* zitten er precies achter de potentiële inmenging? 2) Met welke *intenties* zijn deze statelijke actoren actief? 3) Op welke *doelgroepen* of *doelwitten* richten de statelijke actoren zich? 4) Welke *middelen* zetten statelijke actoren in richting die specifieke doelgroepen of doelwitten? 5) Welke ongewenste maatschappelijke *effecten* treden op ten gevolge van ongewenste buitenlandse inmengingsactiviteiten? In lijn met deze

[17] Kamerstukken 30 821 en 26 643, nr. 42.

vijfdeling, zal voor het versterken van de aanpak de komende jaren worden ingezet op twee lijnen in het bijzonder: het anticiperen op dreigingen door nieuwe statelijke *actoren* en het vergroten van de bewustwording rond ongewenste inmenging bij (potentiële) *doelgroepen/ doelwitten*. Daarbij is samenwerking met onze internationale partners, met name binnen de Europese Unie, van belang om te leren van elkaars kennis en ervaringen.

a) Anticiperen op ongewenste inmenging door statelijke actoren

Onderzoek van het *Leiden Asia Center* uit 2021 waarschuwt dat vanuit de Chinese overheid en de Chinese Communistische Partij een basis is gelegd voor beïnvloeding van Nederlands-Chinese gemeenschappen en richting mensen die zich kritisch uitlaten over de Chinese partijstaat. Dit zal zich niet alleen uiten bij bedrijven, studenten of kennismigranten, maar ook binnen de traditionele Chinese gemeenschappen en hun organisaties. Minderheidsgroepen die het in China zelf reeds moeilijk hebben, zullen naar verwachting ook in Nederland vaker doelwit zijn van de zogenoemde «lange arm van Peking». Het kabinet is daarnaast sinds begin september op de hoogte van het bestaan van zogenoemde Chinese overzeese servicecentra. De Spaanse NGO *Safeguard Defenders* bracht hierover medio september een rapport uit. Het rapport meldt dat lokale autoriteiten in China deze overzeese politie *servicestations* zouden hebben opgezet in meerdere landen. Ten minste één van deze centra bevindt zich in Nederland. Het Ministerie van buitenlandse zaken heeft op maandag 31 oktober de Chinese ambassadeur laten weten dat deze centra onmiddellijk dienen te sluiten en dat hun activiteiten beëindigd moeten worden. De Chinese ambassadeur in Nederland liet op 3 november weten dat de betrokken personen hun werkzaamheden hebben gestaakt. Indien het kabinet aanwijzingen heeft dat er activiteiten van ongewenste buitenlandse inmenging plaatsvinden, al dan niet via overzeese service-centra, zal het niet twijfelen daartegen gepaste maatregelen te treffen. De aanpak van ongewenste buitenlandse inmenging heeft sinds 2018 de nadrukkelijke aandacht van het kabinet.[18] De extra aandacht voor China op het gebied van ongewenste buitenlandse inmenging mag vanzelf-sprekend niet ten koste gaan van de aandacht die in dit kader reeds uitgaat naar Iran. Tevens zal het kabinet aandacht blijven besteden aan Turkije. Indien dit extra capaciteit vergt, zal dit interdepartementaal tijdig worden gesignaleerd en opgepakt.

b) Vergroten van bewustwording bij doelgroepen en doelwitten

Voor het (verder) vergroten van de weerbaarheid tegen ongewenste buitenlandse inmenging, zal de NCTV de komende jaren, in nauwe samenwerking met onder meer de Ministeries van Binnenlandse Zaken en Koninkrijksrelaties en van Sociale Zaken en Werkgelegenheid, binnen de bestaande inzet op een zogenoemd «landen-neutraal bewustwordingsini-tiatief» om de bewustwording rondom dit thema verder te vergroten. Hierbij worden statelijke actoren die inmengingsactiviteiten verrichten (alsmede hun intenties) benoemd en worden de doelgroepen/doelwitten die zij onderscheiden, de instrumenten die zij inzetten en de ongewenste maatschappelijke effecten die kunnen optreden, in generieke zin beschreven. Voor het verhogen van de bewustwording rond ongewenste buitenlandse inmenging onderscheiden we verschillende doelgroepen/ ontvangers:

– (Personen/groepen binnen) Gemeenschappen die slachtoffer kunnen worden van ongewenste buitenlandse inmenging. Zij moeten zich bewust zijn van de verschillende vormen van ongewenste inmenging,

[18] Kamerstukken 30 821 en 26 643, nr. 42.

van de statelijke actoren die erachter zitten, van de intenties/doelen die deze statelijke actoren nastreven, welke instrumenten zij inzetten en (vooral) waar zij terecht kunnen als zich OBI-dreigingen aandienen.
– (Decentrale) politieke ambtsdragers (bij gemeenteraadsleden, provinciale staten, waterschappen, burgemeesters, wethouders, etc.) binnen de lopende initiatieven op het programma weerbaar bestuur. Deze groepen zijn belangrijk, omdat zij werken binnen de democratische processen die we niet aangetast willen zien. Zij moeten zich voldoende bewust zijn van de risico's van «positieve» vormen van OBI, zoals het inpalmen, fêteren, omkopen, selectief benaderen en/of positief bevoordelen van personen werkzaam in volksvertegenwoordigingen en binnen het openbaar bestuur.
– Overheidsorganisaties en (beleids)medewerkers op lokaal niveau, die te maken hebben met groepen en personen die doelgroep/doelwit kunnen zijn van ongewenste buitenlandse inmenging. Het betreft voornamelijk beleidsmedewerkers openbare orde en veiligheid bij gemeenten of bijvoorbeeld medewerkers die uit hoofde van hun functie vergunningen/(identiteits)documenten etc. verlenen, maar natuurlijk ook politieagenten. Zij moeten voldoende kennis hebben van de materie om ongewenste buitenlandse inmenging tijdig te kunnen herkennen en voldoende handvatten hebben om op te treden in geval van incidenten.

Tot slot zal voor het tegengaan van ongewenste inmenging in gemeenschappen een netwerk worden opgebouwd met andere landen – zowel in de EU als daar buiten – om te bezien of deze landen een vergelijkbare problematiek kennen en wat het antwoord daarop is. Met bovenstaande aanpak komt de Minister van Buitenlandse Zaken tegemoet aan de toezegging van het lid Piri (PvdA) van 14 juni jl.[19]

Op 20 oktober 2022 zegde de Minister van Buitenlandse Zaken, tijdens het Mensenrechtendebat in de Tweede Kamer (Kamerstuk 32 735, nr. 360), toe dat hij een verkenning zou starten naar een eventueel meldpunt voor gemeenschappen in Nederland die slachtoffer worden van ongewenste buitenlandse inmenging en waar zij activiteiten/dreigingen rond OBI zouden kunnen melden. Het kabinet is van mening dat gezien de toenemende dreiging zoals ook in het dreigingsbeeld wordt geschetst, het van belang is beter zicht te krijgen van de manifestatie en potentiële gevolgen van OBI. Het kabinet wil aansluiten bij lokale en nationale inspanningen die reeds plaatsvinden in het kader van de aanpak van ongewenste buitenlandse inmenging, waarbij OBI-meldingen die binnenkomen in het veiligheidsdomein dan wel het sociale domein, op een centrale plek bij elkaar komen. Hoe aan dit meldpunt precies invulling wordt gegeven wordt door het kabinet op dit moment bezien. De samenhang met diplomatieke, weerbaarheidsverhogende, bestuurlijke en eventueel strafrechtelijke maatregelen heeft hierbij bijzondere aandacht. Uw Kamer wordt hierover zo spoedig mogelijk nader geïnformeerd.

4. Beschermen van democratische processen en instituties

Ook in het informatiedomein is sprake van ongewenste buitenlandse inmenging en (heimelijke) beïnvloeding. Statelijke actoren stellen zich steeds assertiever op en zij maken in toenemende mate gebruik van informatieoperaties en desinformatie. Informatie is voor statelijke actoren zelfs een belangrijk instrument in de hybride aanpak geworden. Zowel de

[19] Toezegging van de Minister van Buitenlandse Zaken de Kamer een brief te sturen over beïnvloeding vanuit het buitenland door landen, waarvan veel burgers met een dubbele nationaliteit in Nederland wonen. Toezegging gedaan in het Commissiedebat Hoofdlijnen BZ van 14 juni jl. (Kamerstuk 35 925 V, nr. 110).

AIVD als MIVD noemen in het openbare jaarverslag van 2021 dat statelijke actoren over een breed palet aan middelen beschikken, waarbij desinformatie en (heimelijke) beïnvloeding veelgebruikte middelen zijn. Als landen proberen het Nederlandse politieke en sociale systeem onopgemerkt te beïnvloeden, spreken we van heimelijke beïnvloeding. Pogingen kunnen zowel in het online- als in het fysieke domein plaatsvinden, via (sociale) media of het politiek-bestuurlijk bestel.

Vaak doen statelijke actoren dit als onderdeel van een hybride campagne.[20] Gemeenten zijn voorafgaand aan de gemeenteraadsverkiezingen in maart 2022 gevraagd om een analyse te maken van de kwetsbaarheden in het verkiezingsproces waar zij een verantwoordelijkheid hebben, en dat zij, waar nodig, maatregelen treffen om kwetsbaarheden te verminderen. In de circulaire van de Minister van Binnenlandse Zaken en Koninkrijksrelaties ter voorbereiding op de provinciale staten- en waterschapsverkiezingen, worden de gemeenten en waterschappen (opnieuw) opgeroepen deze analyse uit te voeren.

Daarnaast is het van belang de weerbaarheid en onafhankelijke positie van politieke partijen te waarborgen. Daarom wordt per 1 januari 2023 de financiële transparantie van politieke partijen vergroot en wordt buitenlandse financiering van Nederlandse politieke partijen verboden. Het kabinet is voornemens met een nieuwe Wet op de politieke partijen de onafhankelijke positie van politieke partijen verder te versterken, onder andere door transparantieregels over de interne partijorganisatie en politieke advertenties.

Rijksbrede aanpak desinformatie

Uit onderzoek blijkt dat de effecten van desinformatie een reden tot zorg zijn voor Nederlanders.[21] Het kabinet heeft dan ook sinds 2019 een Rijksbrede strategie voor de aanpak van desinformatie. Deze bestaat uit de sporen preventie, verstevigen informatiepositie en reactie, en is sinds 2019 doorlopend verder ontwikkeld.[22] Een recent voorbeeld hiervan is de Werkagenda «Waardengedreven Digitaliseren» waarin onder andere ingezet wordt op het bevorderen van digitale vaardigheden en mediawijsheid, regelgeving voor online platformen en publieke alternatieven voor digitale sociale platformen.[23] Hierdoor kan de weerbaarheid van burgers versterkt worden. Burgers die mediawijs zijn, en bewust van de risico's rond desinformatie, zijn minder vatbaar om er slachtoffer van te worden. Door iemand een signaal te geven dat er mogelijk desinformatie aankomt (over een bepaald onderwerp bijvoorbeeld), is die gewaarschuwd. Dit noemen we ook wel *prebunking*. Dit is een manier van preventie, omdat ontvangers van desinformatie weerbaarder worden.

Als onderdeel van de Rijksbrede strategie desinformatie zijn voor de Tweede Kamerverkiezingen van 2021 webinars georganiseerd voor gemeenteambtenaren en voor politieke partijen met als doel de weerbaarheid voor, onder andere, desinformatie te vergroten. Voor de verkiezingen voor de provinciale staten en algemene besturen van de waterschappen in 2023 en de verkiezingen van het Europees Parlement in 2024 zullen gemeenteambtenaren wederom worden gebriefd op aspecten

---

[20] Kamerstuk 30 977, nr. 162 (jaarverslag AIVD 2021) en Kamerstuk 30 821, nr. 125 (jaarverslag MIVD 2021).

[21] Zie onder andere de Risico- en Crisisbarometer – Desinformatie voorjaar 2022 via https://www.nctv.nl/documenten/publicaties/2022/10/17/risico--en-crisisbarometer-desinformatie-voorjaar-2022.

[22] Zie onder andere Kamerstuk 30 821, nrs. 91 en 112 en Kamerstuk 30 821, nr. 119.

[23] Kamerstuk 26 643, nr. 940.

rond (digitale) veiligheid. Voor gemeenteambtenaren is tevens een workshop ontwikkeld voor het herkennen en kunnen omgaan met desinformatie.

Een ander onderdeel van de strategie is het tijdig, proportioneel en effectief reageren op desinformatie door overheidsorganisaties. Als er desinformatie is verspreid, kan deze informatie worden ontkracht. Daarnaast wordt expertise op het gebied van desinformatie in relatie tot crisiscommunicatie en nationale veiligheid uitgebreid.

Binnen de aanpak van desinformatie is desinformatie afkomstig vanuit buitenlandse, of daaraan gelieerde, actoren een specifiek aandachtspunt dat ontegenzeglijk een risico is voor de nationale veiligheid. De Europese Unie spreekt in dit verband over *Foreign Information Manipulation and Interference* (FIMI). Het tegengaan van FIMI past binnen de bredere aanpak van hybride dreigingen. Nederland draagt in EU-verband actief bij aan de (door)ontwikkeling van de FIMI-*toolbox*, een set maatregelen om informatiemanipulatie door statelijke actoren te onderkennen en tegen te gaan zowel binnen als buiten de Unie en haar Lidstaten.

Tot slot maakt het kabinet graag van deze brief gebruik om in te gaan op de motie van het lid Brekelmans[24] inzake een openbaar register voor *agents of foreign influence*. Het kabinet heeft conform de motie in Australië navraag gedaan naar de ervaringen op dit terrein aldaar. Australië kent een algemeen lobbyregister en parlementariërs mogen zich niet inlaten met lobbyisten die niet in dit register zijn opgenomen. Daarnaast bestaat er een *foreign influence transparancy scheme* dat tot doel heeft inzichtelijk te maken welke buitenlandse belangen door welke lobbyisten worden vertegenwoordigd. De complexe begripsbepaling van wanneer sprake is van buitenlandse inmenging via lobbyisten maakt dat vaststelling daarvan erg lastig en tijdrovend is. De dreiging die uitgaat van lobbyisten die werkzaam zijn ten behoeve van statelijke actoren, wordt in Nederland geadresseerd met een breed palet aan maatregelen dat tevens in deze brief wordt benoemd. Een belangrijk element in dit palet is bewustwording. Het bovengenoemde wetsvoorstel dat ziet op uitbreiding van de strafbaarstelling van spionage biedt een aanvullend element in de Nederlandse aanpak als strafrechtelijk sluitstuk. In EU-kader heeft de President van de Europese Commissie in dit licht een *Defence for Democracy*-pakket aangekondigd. Dit pakket zal naar verwachting begin 2023 worden gepresenteerd.

Tot slot

Zowel het DBSA 2 als de aanpak van statelijke dreigingen vormen een belangrijke bijdrage aan de voorbereiding van de Rijksbrede Veiligheidsstrategie die begin 2023 wordt gepresenteerd. Deze Rijksbrede Veiligheidsstrategie is de overkoepelende strategie voor de komende zes jaar om het Koninkrijk der Nederlanden weerbaarder te maken tegen dreigingen voor de nationale veiligheid die mede voortkomen uit de veranderende geopolitieke verhoudingen in de wereld, en waar ook statelijke dreigingen deel van uitmaken. Daarnaast is ook in het CSBN 2022, waarover uw Kamer in juli is geïnformeerd, (digitale) dreiging door statelijke actoren benoemd. De aanpak statelijke dreigingen hangt daarom nauw samen met de cybersecurityaanpak van het kabinet, zoals vervat in de Nederlandse Cybersecuritystrategie, die recent aan uw Kamer is aangeboden[25] en de internationale cyberstrategie die uw Kamer binnenkort toegaat.

---

[24] Kamerstuk 35 925 V, nr. 52.
[25] Kamerstuk 26 643, nr. 925.

Conclusie

In het licht van de recente en te verwachten geopolitieke ontwikkelingen vergen de dreigingen die uitgaan van statelijke actoren de blijvende aandacht van het kabinet en interactie met uw Kamer. Het kabinet bestendigt de in 2019 ingezette aanpak en versterkt deze zodat Nederland voorbereid is op de bestaande dreigingen van statelijke actoren en die van de toekomst. Uiteraard rapporteert het kabinet de voortgang op de diverse onderdelen van deze brief aan uw Kamer en ziet ernaar uit met uw Kamer in gesprek te gaan over de reeds genomen en nog te nemen stappen.

De Minister van Justitie en Veiligheid,
D. Yesilgöz-Zegerius

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
H.G.J. Bruins Slot

De Minister van Defensie,
K.H. Ollongren

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

De Minister van Onderwijs, Cultuur en Wetenschap,
R.H. Dijkgraaf

De Minister van Sociale Zaken en Werkgelegenheid,
C.E.G. van Gennip

De Minister voor Buitenlandse Handel en Ontwikkelingssamenwerking,
E.N.A.J. Schreinemacher