Bijlage: Accenten van de aanpak statelijke dreigingen

De aanpak rondom het tegengaan van statelijke dreigingen bestaat uit een aantal generieke maatregelen, zoals beschreven in de brief. 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 voor een deel al belangrijke stappen gezet en zijn ook weer nieuwe facetten onderkend die een versterkte aanpak behoeven. In deze bijlage treft u de aanpak op deze thema's aan inclusief uitkomsten ex-ante analyses op economische veiligheid.

1. Ongewenste buitenlandse inmenging gericht op diaspora

Ongewenste buitenlandse inmenging gericht op de diaspora betreft doelbewuste, vaak stelselmatige en in vele gevallen heimelijke activiteiten van statelijke actoren (of actoren die aan statelijke actoren zijn te relateren) in Nederland of gericht op Nederlandse belangen, die door de nagestreefde doelen, de gebruikte middelen of ressorterende effecten het politieke en maatschappelijke systeem kunnen ondergraven.
Nederlandse burgers moeten, ongeacht hun achtergrond, in de Nederlandse rechtsstaat in staat zijn om in vrijheid eigen keuzes te maken als het gaat om de inrichting van hun leven, politieke voorkeur en de band met hun land van oorsprong of dat van hun ouders. Contacten vanuit een statelijke actor met Nederlandse burgers dienen op transparante wijze plaats te vinden en op basis van vrijwilligheid en mogen niet leiden tot het exporteren van spanningen naar Nederlands grondgebied of een negatieve invloed op de integratie of de binding met de Nederlandse samenleving.

In het afgelopen jaar zijn verschillende voorbeelden geweest van ongewenste buitenlandse inmenging gericht op diaspora waarover uw Kamer is ingelicht.[1] De aanpak op ongewenste buitenlandse inmenging is een generieke – landen neutrale – aanpak waarover uw Kamer eerder is ingelicht.
Betrokken departementen en diensten staan doorlopend in nauw contact om op basis van een gezamenlijke en gestructureerde werkwijze een beeld te vormen en indien nodig te besluiten tot gecoördineerde actie en opschaling. Bij (dreigende) incidenten wordt gebruik gemaakt van een divers instrumentarium. Dit loopt uiteen van monitoren en informeren, tot maatregelen in het kader van de openbare orde en veiligheid. Daarnaast heeft het kabinet verschillende diplomatieke instrumenten, zoals het voeren van een dialoog met landen van zorg of een diplomatieke vertegenwoordiger in Nederland *persona non grata* verklaren, om ongewenste buitenlandse inmenging tegen te gaan.

Ook zet het kabinet in op maatregelen om de weerbaarheid van betrokken gemeenten en gemeenschappen te verhogen als het gaat om ongewenste buitenlandse inmenging. Het gaat hier zowel om het creëren van bewustwording als het ondersteunen van gemeenten en gemeenschappen bij de ontwikkeling van een handelingsperspectief om ongewenste buitenlandse inmenging die de integratie kunnen belemmeren tegen te gaan.

Ongewenste buitenlandse inmenging blijft een actueel thema (motie Becker[2], waarover u voor de zomer wordt geïnformeerd en financiering als modus operandi van statelijke actoren [3]), maar ook vanwege ontwikkelingen in andere landen en veranderingen in de migratiestromen. Dit rechtvaardigt een onverminderde inzet op dit onderwerp.

---

[1] Onder meer via de volgende Kamerstukken:

- Beantwoording Kamervragen over het bericht dat de Turkse president Erdogan campagne wil voeren in het buitenland voor de Turkse presidents- en parlementsverkiezingen in juni,TK, vergaderjaar 2017-2018, 2591
- Antwoorden Kamervragen over het bericht 'Russische trollen ook actief in Nederland' /ingezonden 7 sept 2018. Kamerstuk nr 14250
- Brief sancties Iran, 8 januari 2019, Tweede Kamer, vergaderjaar 2018–2019, 35 000 V, nr. 56
- Tweede Kamer, vergaderjaar 2018–2019, 32 735, nr. 209
- Beantwoording Kamervragen over *het bericht «So werden Erdogan-Kritiker in Deutschland per App denunziert»*) Tweede Kamer, vergaderjaar 2018–2019, Aanhangsel

[2] Motie van het lid Becker c.s. over een contrastrategie ten aanzien van ongewenste diasporapolitiek, Tweede Kamer, 30821-56.

[3] Kamerbrief Integrale aanpak Problematisch gedrag en ongewenste buitenlandse financiering van maatschappelijke en religieuze instellingen, Tweede Kamer, 2018-2019, 29614 nr. 108

2. Beschermen democratische processen en instituties

Het tweede accent van de aanpak richt zich op het tegengaan van het ondermijnen van de democratische rechtsstaat door statelijke actoren. Via verschillende maatregelen wordt hier op ingezet:

Tegengaan politieke beïnvloeding door staten

Al eerder werd in het kader van ongewenste buitenlandse inmenging aangekondigd dat wordt ingezet op het vergroten van de weerbaarheid van – met name lokale – politieke ambtsdragers. Daarbij richten we ons op twee lijnen, te weten (1) het beschermen van politieke ambtsdragers (hierbij gaat het om het zorgdragen voor de veiligheid en integriteit van politieke ambtsdragers) en (2) het toerusten van politieke ambtsdragers (gericht op het versterken van de kennis, kunde en het handelingsvermogen van politieke ambtsdragers) om ondermijning van de democratische rechtsorde effectief tegen te kunnen gaan. Verder vindt rondom het handelingsvermogen en het verhogen van transparantie in het politiek-bestuurlijke domein een verkenning plaats naar de wenselijkheid en mogelijkheid van een registratieplicht voor lobbyisten. De Verenigde Staten, Australië en Canada, kennen al een dergelijke registratieplicht.

Veilige verkiezingen

Acties van statelijke actoren kunnen schade toebrengen aan de politieke en bestuurlijke integriteit wanneer deze onafhankelijke volksvertegenwoordiging, besluitvorming of rechtspraak compromitteert, of wanneer er twijfel is over de vrijheid, eerlijkheid en anonimiteit van verkiezingen. De democratische samenleving komt onder druk te staan, wanneer inmengingsactiviteiten bijdragen aan een gebrek aan acceptatie van de legitimiteit van de overheid of een gebrek aan solidariteit in de samenleving, polarisatie en enclavevorming. Of wanneer intolerantie verspreid wordt en vrijheden beperkt worden. Verschillende departementen en operationele en lokale partners dragen, onder coördinatie van de minister van BZK, tezamen zorg voor veilige verkiezingen vanuit de eigen verantwoordelijkheid. Binnen het Europees verkiezingsnetwerk worden kennis en expertise tussen de lidstaten en de instellingen uitgewisseld. Het kabinet heeft daarbij met name oog voor de onderkenning van bijzondere signalen, ongewenste beïnvloeding en desinformatie.

Tegengaan desinformatie

De verspreiding van desinformatie met als doel de democratische rechtsorde te ondermijnen en te destabiliseren is een reële dreiging. Deze dreiging manifesteert zich veelal online. Het kabinet ziet de verspreiding van desinformatie als een probleem waarbij van verschillende partijen in de samenleving gevraagd wordt dat zij hun verantwoordelijkheid nemen, zoals private actoren, de media en wetenschap[4]. De inzet van het kabinet is daarbij met name gericht op het tegengaan van heimelijke beïnvloeding van de publieke opinie door statelijke actoren (of actoren die aan statelijke actoren zijn te relateren). Belangrijke uitgangspunten voor het kabinet bij het zoeken naar een juiste reactie zijn onder andere dat waarborging van de vrijheid van meningsuiting en vrije pers, democratie en rechtsstaat voorop staan en de focus op campagnes in plaats van individuele nieuwsberichten. Wanneer echter sprake is van een bedreiging van de economische of politieke stabiliteit of nationale veiligheid door inmenging van statelijke of daaraan gelieerde actoren, is een reactie van de overheid gegrond.

In de brede aanpak[5] wordt gewerkt aan maatregelen om voorbereid te zijn op desinformatie, signalen te herkennen, deze te duiden, mogelijke proportionele respons te formuleren en indien gewenst uit te voeren zonder afbreuk te doen aan de eerdergenoemde vrijheden.
Doordat desinformatie zich veelal online manifesteert, stopt het niet bij de grens. Nederland hecht daarom waarde aan internationale samenwerking en kennisuitwisseling op dit onderwerp. In dat kader verwelkomt Nederland het Europese Actieplan Desinformatie, zoals ook uiteengezet in het BNC-fiche Actieplan Desinformatie (d.d. 25 januari 2019). Een voortvloeisel uit het Actieplan is de Nederlandse deelname in EU-verband aan het Europees Verkiezingsnetwerk en het *Rapid Alert System* (RAS). In het Europees Verkiezingsnetwerk wordt de overkoepelende aanpak van desinformatie en bescherming van verkiezingen besproken en kennis uitgewisseld tussen lidstaten en EU-instellingen. Het RAS verbindt analisten en beleidsmakers uit EU-lidstaten en de StratCom Taskforces van EDEO om *real time* informatie uit te wisselen als er sprake is van desinformatiecampagnes. Het Nationaal Crisis Centrum van de NCTV vervult de rol van nationaal Point of Contact voor het RAS, het ministerie van BZK vervult een dergelijke rol voor het Europees verkiezingsnetwerk waarbij alle relevante departementen zijn aangesloten.

---

[4] Kamerbrief van de minister van BZK inzake desinformatie en beïnvloeding verkiezingen (13 december 2018)

[5] Tweede Kamer, vergaderjaar 2018-2019, 30821, nr 51

Tevens is Nederland lid van de informele 'International Partnership to Counter State Sponsored Disinformation' waarin onder meer de VS, het VK, Baltische en Noordse staten vertegenwoordigd zijn. Het partnerschap heeft tot doel analyses en rapportages over de verspreiding van desinformatie te delen en samenwerking richting techbedrijven te faciliteren.

3. **Aanpak Economische Veiligheid**

Een derde accent is gericht op economische veiligheid. Hieronder vindt u de resultaten van de analyse die is uitgevoerd naar kwetsbaarheden in vitale sectoren alsmede de aanvullende beheersmaatregelen die van belang zijn om de risico's voor de nationale veiligheid op het gebied van economische veiligheid verder te beperken.

Sectorale ex-ante analyses

In het Regeerakkoord heeft het kabinet de bescherming van vitale sectoren aangekondigd, na zorgvuldige analyse van risico's voor nationale veiligheid. In deze analyses is er bijzondere aandacht voor de risico's als gevolg van veranderende zeggenschap.[6] Het doel is om potentiële risico's voor de nationale veiligheid per vitale sector te identificeren, en om daarbij te bepalen in hoeverre het bestaande instrumentarium van de overheid voldoende waarborgen biedt. In deze brief deel ik de uitkomsten van de sectorale ex-ante analyses met u en daarbij kom ik tegemoet aan de motie-Van den Berg c.s.[7] en de motie-Graus.[8]

Uit de analyses blijkt dat vrijwel alle vitale sectoren op enigerlei wijze beschermd zijn tegen ongewenste zeggenschap. Daarbij is er een divers beeld van de mate en aard van de bescherming. Een aantal sectoren is in overheidshanden. De Nederlandse overheid kan daardoor (mede) bepalen aan wie en onder welke voorwaarden een bedrijf wordt verkocht. Daarbij worden ook nationale veiligheidsbelangen meegewogen. Een aantal sectoren worden beschermd door sectorale wetgeving. Uit de analyse op telecommunicatie blijkt dat in deze sector ongeadresseerde risico's bij verandering in zeggenschap bestaan. Het kabinet heeft al in een eerder stadium besloten hier direct actie op te nemen en heeft inmiddels een wetsvoorstel over ongewenste zeggenschap in de telecommunicatiesector ter consultatie aangeboden aan uw Kamer[9]. Conclusies sectorale ex-ante analyses:

- De vitale sectoren, de inzet politie, inzet defensie, de nucleaire sector, openbare drinkwatervoorziening, vitale kerende en beherende objecten en de mainports Schiphol en Rotterdam zijn (grotendeels) in handen van de overheid. Voor een groot deel betreft dit kerntaken van de overheid, waarvan de zeggenschap van de overheid niet verandert. De risico's voor de nationale veiligheid als gevolg van verandering van zeggenschap zijn hier daarom niet van toepassing.
- De vitale sector energie is voor wat betreft de transport- en distributienetwerken in handen van de overheid. De energielevering is verspreid over meerdere aanbieders, wat de risico's verkleint. Daarnaast heeft de Minister van Economische Zaken en Klimaat de taak en bevoegdheid om een eventuele verandering van zeggenschap binnen de gas- en energieproductie te beoordelen.[10] De risico's voor de nationale veiligheid als gevolg van verandering van zeggenschap zijn daarom voldoende beheerst.
- De vitale sector telecommunicatie kent nationale veiligheidsrisico's als gevolg van veranderende zeggenschap, die nog onvoldoende kunnen worden beheerst door wettelijke normen te stellen en daar toezicht op te houden. De risico's voor de nationale veiligheid als gevolg van verandering van zeggenschap zullen daarom geborgd worden met aanvullende wetgeving.
- De vitale sectoren betalingsverkeer en chemie kennen strenge normen, en bijhorend publiek toezicht, om respectievelijk de integriteit van gegevens en de fysieke veiligheid te borgen die de belangrijkste risico's voor de nationale veiligheid vormen. De risico's voor de nationale veiligheid worden daarmee voldoende beheerst binnen deze sectoren.

Uit de analyses blijkt dat de continuïteit en inzetbaarheid van (vrijwel) alle vitale processen, zowel in handen van overheid als bedrijfsleven, sterk afhankelijk zijn van private ondernemingen die

[6] Regeerakkoord 'Vertrouwen in de toekomst', paragraaf 2.4.
[7] Tweede Kamer, vergaderjaar 2016-2017, 29 826, nr. 84.
[8] Tweede Kamer, vergaderjaar 2017-2018, 34 775 XIII, nr. 116.
[9] Tweede Kamer, vergaderjaar 2018-2019, 35 153, nr. 5
[10] Zie de Elektriciteitswet 1998 en de Gaswet.

goederen, diensten of technologie leveren. Dat betekent dat er kwetsbaarheden kunnen ontstaan bij aanbesteding en toelevering. Het kabinet neemt daarom de volgende maatregelen.

Maatregelen

A. Oprichting Taskforce Economische Veiligheid

Er is een Taskforce Economische Veiligheid opgericht waarin, onder voorzitterschap van de NCTV, de balans tussen nationale veiligheidsbelangen en economische belangen nader verkend wordt, casuïstiek kan worden besproken en economische en veiligheidsbelangen integraal worden gewogen. Momenteel staat de Taskforce in het teken van de kwetsbaarheid van 5G telecommunicatienetwerken en welke maatregelen nodig zijn om risico's te beheersen.

B. *Betere benutting en aanscherping van huidige wet- en regelgeving ter bescherming van nationale veiligheid*

Nederland beschikt over een aantal instrumenten die (beter) kunnen bijdragen aan de bescherming van nationale veiligheidsrisico's bij private ondernemingen. Het betreft onder meer private juridische beschermingsconstructies, sectorale regelgeving, contractuele afspraken, de Ondernemingskamer en het aanwijzen van vertrouwensfuncties. Het kabinet is bezig met een evaluatie en aanscherping van huidige wet- en regelgeving, zodat deze beter kunnen worden benut.

C. Beschermen van nationale veiligheid bij inkoop en aanbesteding

Het kabinet zal de nationale veiligheidsrisico's die door de afhankelijkheden kunnen ontstaan verder in kaart brengen en bezien hoe deze mogelijke risico's bij onder andere inkoop en aanbesteding beheerst kunnen worden. In 2018 is voor veilige inkoop en aanbesteding binnen het rijk een instrumentarium ontwikkeld en ingevoerd door het kabinet. Op dit moment wordt bezien hoe dit ook ingezet kan worden binnen onderdelen van de vitale infrastructuur en mede overheden. Het kabinet gaat daarnaast de mogelijkheid van het neerleggen van nationale veiligheidsrichtlijnen voor het gebruik van producten en diensten binnen de Rijksoverheid, vitale infrastructuur en medeoverheden actiever inzetten. Ook werkt het kabinet in het kader van inkoop en aanbesteding aan de Nationale Cyber Security Agenda (NCSA) aan aanvullende cybersecurity-criteria bij inkoop van eigen ICT-middelen door de overheid. Bij deze eisen zullen ook economische veiligheidsoverwegingen worden meegenomen om de weerbaarheid tegen statelijke actoren te verhogen.

D. Beschermen nationale veiligheid bij overnames en investeringen

In de EU wordt ingezet op een verdere versterking van het samenwerkingsmechanisme op het gebied van buitenlandse investeringen. Enerzijds is er tot een raamwerk besloten voor de toetsing door individuele lidstaten van buitenlandse investeringen aan nationale veiligheid of de openbare orde. Anderzijds faciliteert en verplicht de verordening tot het uitwisselen van informatie tussen lidstaten en de Europese Commissie. De verordening vraagt om het realiseren van een samenwerkingsmechanisme waarvoor ook in Nederland processen voor onder andere informatie-uitwisseling moeten worden ingericht. Het raamwerk legt geen verplichtingen op voor een investeringstoets maar stelt wel kaders voor lidstaten die een toets wensen te implementeren.

Binnen dit Europese kader werkt het kabinet aan een uitwerking van een investeringstoets. Dit is een instrument 'of last resort' voor nationale veiligheidsrisico's waarbinnen ruimte is voor maatwerk. Bestaande sectorale wetgeving zal daarbij het uitgangspunt zijn. Op deze manier krijgen, binnen het Europese kader, ook de nationale beleidswensen over de inhoud en reikwijdte van een breder beschermingsmechanismen plek. In de uitwerking zal gekeken worden naar overkoepelende 'parapluwetgeving' waar ook bestaande en toekomstige sectorale wetgeving goed op aangesloten is. Hierbij is het uitgangspunt dat een verbod in het kader van de investeringstoets alleen daar wordt ingezet indien er geen alternatieve effectieve beschermingsmaatregelen voor handen zijn.

Initiatieven die raken aan dit thema

Naast deze set aan maatregelen om nationale veiligheidsrisico's beheersbaar te maken zijn er nog een aantal andere initiatieven die onder andere raken aan dit thema. Hierbij staat de beschikbaarheid van kritische technologie en kennis centraal. Ongewenste kennis- en technologieoverdracht kan plaatsvinden in geval van bijvoorbeeld faillissementen en overname van *start-ups* en het risico van ongewenste kennis- en technologieoverdracht via de weg van (academisch) onderwijs en onderzoek. Er wordt onderzocht op welke manier de kennisregeling kan worden uitgebreid naar andere risicolanden en bijvoorbeeld opleidingen waar zeer specifieke technische kennis kan worden opgedaan[11].

[11] Zie tevens Kamerbrief, 'Verscherpen toezicht op studenten en onderzoekers uit risicolanden', Tweede Kamer, vergaderjaar 2018-2019, 30821, nr.70

Met een verkenning naar digitaal financieel economische spionage is het beeld ten aanzien van deze dreiging aangescherpt, en is bezien welk instrumentarium, complementair aan de maatregelen uit zoals de Internationale Cyber Strategie en de Nationale Cyber Security Agenda, van toepassing is om deze dreiging te mitigeren. Aanvullend instrumentarium, zoals bijvoorbeeld vergroting van het bewustzijn van deze dreiging, wordt in de verschillende beleidsterreinen opgenomen, zo ook in de aanpak tegengaan statelijke dreigingen. Het gaat hier ook om het inzetten van internationale samenwerking en diplomatieke instrumenten (inclusief attributie) zoals die in het kader van de EU Cyber Diplomacy Toolbox en om het benutten van bestaande WTO procedures ter zake waar opportuun.