Midterm review 2021
Nationale Veiligheid Strategie

Inhoudsopgave

Inleiding

Nederland is een open, diverse en internationaal georiënteerde samenleving. Als open economie bepalen handel en investeringen ons verdienvermogen en onze welvaart. Onze welvaart is ook gebaat bij open wetenschap, waarvoor internationale gerichtheid eveneens onmisbaar is. Ons internationale engagement is principieel en dus benoemt onze grondwet het belang van de internationale rechtsorde.

Onze openheid brengt ons veel en maakt ons kwetsbaar tegelijk. Zo heeft het verharden van de geopolitieke verhoudingen - nog eens aangewakkerd door Covid-19 - gevolgen voor onze veiligheid. Sommige landen aarzelen niet langer om uit eigenbelang onze openheid tegen onszelf te gebruiken, en om politieke of economische druk op ons uit te oefenen. Dat kan negatief uitpakken, bijvoorbeeld omdat onze economie sterk is verweven met de rest van de wereld. Bijgevolg is zij erg gevoelig voor invloeden van buitenaf, bijvoorbeeld voor onderbrekingen in mondiale logistieke ketens. Los daarvan biedt moderne technologie de mogelijkheid om over grenzen heen te beïnvloeden, te verstoren of te spioneren.

Onze samenleving is zo sterk gedigitaliseerd, en de afhankelijkheid van digitale middelen is inmiddels dermate groot, dat geavanceerde technieken allerlei vitale processen korter of langer kunnen verlammen. Covid-19 heeft aangetoond hoe gevoelig onze gedigitaliseerde samenleving is voor verstoring van de gewone gang van zaken. Net als tastbaar geweld kunnen 'onzichtbare' infectieziekten, desinformatie of cyberaanvallen ons welzijn, onze vrijheid of onze welvaart aantasten. Daarnaast is Nederland alleen al door zijn ligging kwetsbaar voor bijvoorbeeld zeespiegelstijging, terwijl onze waterkeringen dat zijn voor cyberaanvallen.

Covid-19 heeft bovendien een katalyserende werking op al sluimerend maatschappelijk ongenoegen. Sinds de uitbraak van het virus heeft ontevredenheid in de samenleving zich zowel online als offline sterker gemanifesteerd. Op verschillende thema's vinden individuen en groepen - geholpen door sociale media - elkaar in gevoelens van onbehagen, onrechtvaardigheid of een andere werkelijkheidsbeleving. Dat geeft brandstof aan wantrouwen tegen traditionele instellingen als de overheid, de wetenschap of reguliere media.

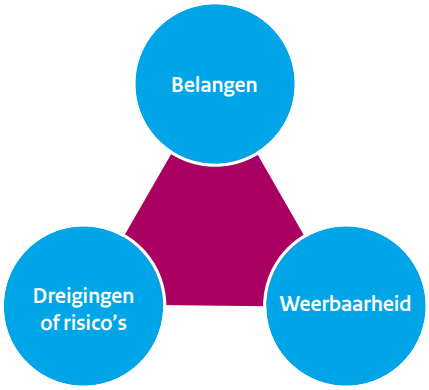
Al met al stellen de dreigingen van vandaag en morgen Nederland voor een forse uitdaging. Deze zijn groter, complexer en veelomvattender dan voorheen. Onze openheid in combinatie met verslechterde geopolitieke verhoudingen maakt ons land kwetsbaar voor statelijke en niet-statelijke dreigingen. Die kwetsbaarheid betreft vooral digitale veiligheid en economische veiligheid. Tegelijk zijn er binnen onze samenleving dreigende tendensen te signaleren. Om onze vrijheden, welvaart, openheid en internationale positie te beschermen is veiligheid een essentiële voorwaarde. Dit verlangt een nieuwe manier van kijken naar veiligheid en een integrale aanpak van onveiligheid.

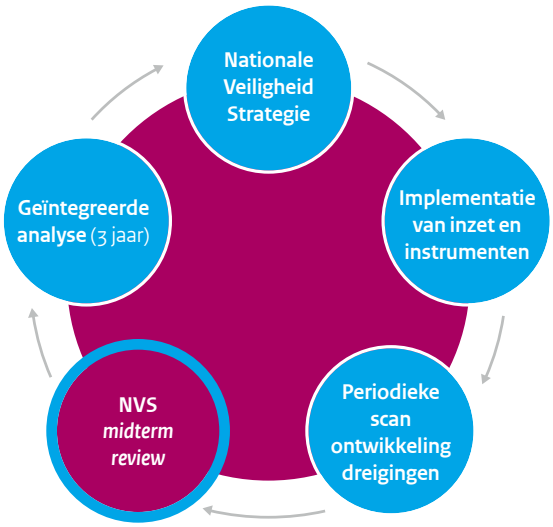
In de zomer van 2019 zag de Nationale Veiligheid Strategie (NVS 2019) het licht.[1] Het uitbrengen van de NVS markeerde de start van een meerjarige cyclus. Onderdeel van die cyclus is deze tussentijdse evaluatie (*midterm review*), waarin het kabinet de ontwikkelingen op het gebied van nationale veiligheid sinds het uitkomen van de NVS nader beschouwt. De NVS 2019 vormt daarmee het uitgangspunt voor dit document.[2] De NVS 2019 is geschreven vanuit de optiek van het doorlopen van de systematiek die is opgebouwd uit de driehoek belangen, dreigingen/risico's en weerbaarheid. Welke belangen beschermen we, wat bedreigt die belangen dusdanig dat sprake kan zijn van maatschappelijke ontwrichting en wat kunnen we doen om de weerbaarheid tegen die bedreigingen te vergroten? Ook in deze *midterm review* staat de methodiek van die driehoek centraal.

In dit document analyseren we de ontwikkeling van de risico's en dreigingen ten aanzien van de nationale veiligheid en de weerbaarheid tegen die risico's en dreigingen sinds het schrijven van de NVS. We doen dat door per in de NVS beschreven thema te kijken naar de ontwikkeling van de dreigingen/risico's en van de weerbaarheid. Daarbij wordt ook gekeken of de huidige aanpak volstaat, of moet worden bijgesteld.

Ten behoeve van de NVS 2019 heeft het Analistennetwerk Nationale Veiligheid (ANV) de dreigingen en risico's voor de nationale veiligheid uitgewerkt in een geïntegreerde risicoanalyse (GRA 2019). Voor deze *midterm review* heeft het ANV de risico's en dreigingen opnieuw bezien tegen de achtergrond van de ontwikkelingen in Nederland en de wereld. De bevindingen zijn opgenomen in de *Horizonscan 2020* (als bijlage met dit document meegestuurd). In de beschouwing van de thema's uit de NVS 2019 zijn de bevindingen uit de Horizonscan 2020, naast andere bevindingen, waar nuttig kort verwerkt onder de terugkerende kop 'Ontwikkeling van de dreiging en de risico's'.

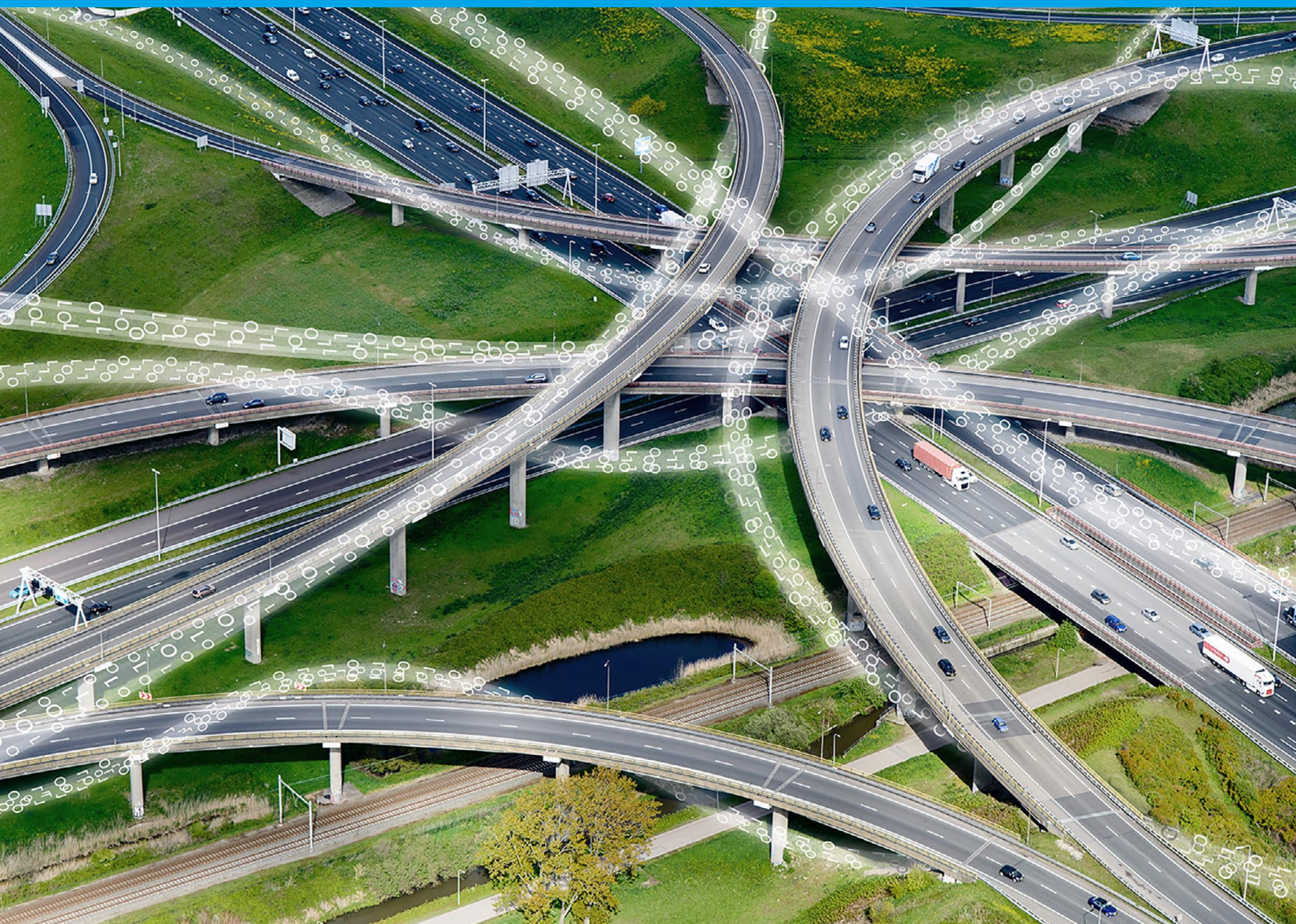
De cyclus van de Nationale Veiligheid Strategie





1 Tweede Kamer 2018-2019, 3 0821, nr. 81.

2 Waar in de NVS de focus ligt op nationale veiligheid in brede zin, ligt in de Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS) de focus op de wereldwijde inzet van het kabinet. Samen met ook de Defensienota en Defensievisie vormen deze documenten de strategische kaders voor de inzet van het kabinet voor een veilig Nederland. De GBVS richt zich met name op externe veiligheid, in het bijzonder op menselijke dreigingen ('security'). Hierbij wordt gebruikgemaakt van de drie V's van Veiligheid: Voorkomen, Verdedigen en Versterken. In de GBVS zijn enkele strategische doelen geformuleerd die raken aan de zes gestelde urgente veiligheidsdreigingen. In de GBVS-tussenrapportage (Tweede Kamer 2019-2020, 33 694, nr.57) is over de behaalde resultaten gerapporteerd en is vooruitgeblikt op de verwachte dreigingsontwikkeling. Zowel de GBVS als de NVS zijn tot stand gekomen na intensieve samenwerking en informatiedeling tussen departementen en relevante partners.



Ontwikkelingen per thema uit de NVS 2019

Statelijke dreigingen tegengaan

Korte samenvatting NVS 2019

Een open samenleving met een open economie vormt de grondslag voor de inrichting van de Nederlandse maatschappij en welvaart. Door deze openheid profiteren Nederland en Nederlanders van de kansen en mogelijkheden die bijvoorbeeld digitalisering en mondialisering bieden.

De vrijheden die deze openheid garanderen, bieden kwaadwillende statelijke actoren evenwel ook de ruimte om activiteiten te ontplooien die de nationale veiligheid ondermijnen en daarmee onze vrijheden aantasten. Deze statelijke actoren zetten, teneinde hun eigen belangen te behartigen en geopolitieke doeleinden te behalen, steeds vaker een breed scala aan middelen in die potentieel ondermijnend kunnen zijn voor onze rechtsstaat en de stabiliteit en openheid van de Nederlandse samenleving.

De strategische aanpak gericht op het tegengaan van statelijke dreigingen bestaat uit generieke maatregelen, gericht op het verhogen van de weerbaarheid tegen verschillende uitingen van statelijke dreigingen. Daarnaast ligt het accent van de aanpak gezien de dreiging, de te beschermen belangen en recente casuïstiek de komende tijd op de thema's sociale en politieke stabiliteit en economische veiligheid.[3]

Ontwikkeling van de dreiging en de risico's

De ontwikkeling van de dreiging en de risico's wordt beschreven in het dreigingsbeeld statelijke actoren (DBSA) dat in februari 2021 aan de Tweede Kamer is aangeboden. Hierin wordt geconcludeerd dat de verschillende nationale veiligheidsbelangen kwetsbaar zijn en door statelijke actoren substantieel bedreigd en aangetast worden, maar niet in dezelfde mate. Deze kwetsbaarheid is niet alleen afhankelijk van de dreiging door statelijke actoren, maar ook van het effect van tegenmaatregelen in Nederland of in een internationale context. Op dit moment heeft geen van de statelijke actoren de benodigde combinatie van intentie en capaciteit om de nationale veiligheid[4] op de korte termijn (tot twee jaar) aan te tasten. Ontwikkelingen op middellange en lange termijn geven reden tot zorg.

De territoriale veiligheid van het EU-grondgebied en het NAVO-bondgenootschap staan onder druk door de aanzienlijke toename van het Russische conventionele en nucleaire militair vermogen. Ondanks een assertief en agressief Russisch buitenland- en veiligheidsbeleid wordt de fysieke territoriale veiligheid de komende twee jaar zeer waarschijnlijk niet direct bedreigd. Er gaat wel concrete dreiging uit van activiteiten door statelijke actoren in het digitale domein. Behalve digitale spionage gaat het hier ook om voorbereidingsactiviteiten vanuit onder meer Rusland en Iran voor digitale verstoring en sabotage. Nederland kan daarnaast geconfronteerd worden met nevenschade uit digitale aanvallen in andere landen. De sociale en politieke stabiliteit wordt geschaad door staten wier doelstelling het is om de democratische rechtsorde in andere landen te ondermijnen, zoals Rusland, en door staten met een actieve diasporapolitiek, zoals Iran en Turkije.

De economische veiligheid wordt geschaad door spionage van diverse landen, waaronder Rusland en China, en door bepaalde economische activiteiten van China. Economische spionageactiviteiten zijn met name gericht op Nederlandse topsectoren en kennisinstellingen. Economische activiteiten zoals investeringen in en samenwerking bij de ontwikkeling van sensitieve technologieën vormen een dreiging, omdat kennis- en technologieoverdracht die

3 De thema's ongewenste buitenlandse inmenging gericht op diaspora en beschermen democratische processen en instituties werden in de kamerbrief statelijke dreigingen in 2019 apart benoemd, maar in de huidige aanpak samengevoegd onder sociale en politieke stabiliteit.

4 Het begrip 'nationale veiligheid' wordt in de Nationale Veiligheid Strategie 2019 omschreven als: "*De nationale veiligheid is in het geding als één of meer vitale belangen van de Nederlandse staat en/of samenleving zodanig bedreigd worden dat sprake is van (potentiële) maatschappelijke ontwrichting.*"

vanuit het oogpunt van nationale veiligheid ongewenst is kan plaatsvinden en omdat (ongewenste) strategische afhankelijkheid kan ontstaan. De internationale rechtsorde, hoeksteen voor onze veiligheid en welvaart, staat vanuit verschillende kanten onder druk. Rusland en China streven ernaar de internationale rechtsorde naar eigen inzicht om te vormen. Zij spelen hierin, gezien hun omvang, militaire en economische macht en hun positie als permanente leden van de VN-Veiligheidsraad, een grote rol.

Ontwikkeling van de weerbaarheid

Sinds het presenteren van de aanpak statelijke dreigingen in april 2019 zijn belangrijke stappen gezet om de weerbaarheid tegen statelijke dreigingen te verhogen. Hierover is in februari 2021 aan de Tweede Kamer over gerapporteerd.[5] Er worden zowel op het fysieke als digitale domein maatregelen genomen om de weerbaarheid te verhogen en er wordt actief gezocht naar kansen om gezamenlijk op te trekken, bijvoorbeeld in EU, bilateraal of like-minded verband. Binnen de aanpak statelijke dreigingen worden generieke maatregelen genomen om de weerbaarheid te verhogen en maatregelen om de weerbaarheid aangaande de politieke en sociale stabiliteit en economische veiligheid te verhogen.

Onder de generieke maatregelen valt bijvoorbeeld de ontwikkeling van een domeinoverstijgend Rijksbreed Responskader (RBRK) statelijke dreigingen, om actieve handelingsperspectieven tegen statelijke dreigingen – onder de drempel van een gewapend conflict - voor besluitvormers binnen de rijksoverheid in kaart te brengen. Daarnaast richt de aanpak statelijke dreigingen zich op de verhoging van bewustwording onder verschillende doelgroepen. Door middel van (kleine) bijeenkomsten, voorlichting en de ontwikkeling van communicatiemateriaal, groeit de kennis op het thema statelijke dreigingen. Ook wordt aan diverse onderzoeken bijgedragen ter verbetering van het begrip van statelijke dreigingen en wat ertegen gedaan kan worden en verdiept Defensie de geïntegreerde benadering van militaire en civiele middelen.

Ter verhoging van de weerbaarheid van de sociale en politieke stabiliteit, worden uiteenlopende algemene, preventieve en repressieve maatregelen getroffen. Voor het tegengaan van ongewenste buitenlandse inmenging richting in Nederland wonende gemeenschappen met een migratie-achtergrond wordt gewerkt volgens de in 2018 ontwikkelde 'OBI-aanpak'. Hierbinnen wordt onverminderd ingezet op het versterken van onze informatiepositie, onder andere door de inlichtingen- en veiligheidsdiensten. De vraag om welke actoren, dreigingen en kwetsbaarheden het daarbij gaat, speelt een centrale rol. Daarnaast wordt sinds 2019 ingezet op verschillende sporen om de verspreiding van desinformatie tegen te gaan.[6] Het eerste spoor is preventie, acties die het doel hebben om te voorkomen dat desinformatie impact heeft en zich verspreidt, zoals het creëren van bewustwording bij alle betrokkenen (burgers, bedrijven, overheidsorganisaties, etc.) Het tweede spoor betreft het verstevigen van de informatiepositie; door onder andere betere informatiedeling is er tijdiger zicht op en duiding van de (potentiële) dreigingen. Het derde spoor bestaat uit reactieve acties, en het vergroten van het handelingsperspectief bij desinformatie. Naast de generieke inzet tegen desinformatie rondom specifieke gebeurtenissen zoals het strafproces MH17, de coronacrisis of de Tweede Kamerverkiezingen 2021 houdt het kabinet samen met alle betrokken partijen de vinger aan de pols en neemt het waar nodig aanvullende stappen om te voorkomen dat de integriteit van de Nederlandse democratische rechtsorde en instituties worden ondermijnd. Wat betreft het tegengaan van ongewenste buitenlandse geldstromen werkt het kabinet aan het vergroten van het zicht op de herkomst van buitenlandse geldstromen, bijvoorbeeld door middel van het wetsvoorstel transparantie maatschappelijk organisaties. Dit wetsvoorstel geeft het Openbaar Ministerie en burgemeesters de bevoegdheid om –indien er aanleiding toe is- inzicht te kunnen eisen bij maatschappelijke organisaties in Nederland naar financiële stromen vanuit het buitenland.

Met betrekking tot economische veiligheid zijn er ook diverse weerbaarheidsverhogende maatregelen genomen. Met het stelsel van investeringstoetsing breidt het kabinet haar instrumentarium voor het tegengaan van ongewenste investeringen, fusies en overnames verder uit. De wettelijke grondslag voor dit stelsel is op dit moment in voorbereiding en gaat specifiek voorzien in het mitigeren van risico's voor de nationale veiligheid bij overnames en investeringen binnen het toepassingsbereik van de toets. Het wetsvoorstel ziet op drie categorieën bedrijven: vitale aanbieders, specifieke toeleveranciers van vitale aanbieders en bedrijven die beschikken over sensitieve technologie die raakt aan de nationale veiligheid. Ook wordt een nieuwe sectorale investeringstoets geïntroduceerd op het gebied van de defensie-industrie, waarmee specifieke maatregelen kunnen worden genomen bij ongewenste investeringen, fusies en overnames binnen de toeleveringsketen van Defensie. Voor inkoop en aanbesteding wordt het instrumentarium, dat in 2018 is ontwikkeld, herzien en beschikbaar gesteld aan de Rijksoverheid, decentrale overheden en speciale sector bedrijven die actief zijn in de vitale infrastructuur. Met betrekking tot de telecomsector zijn in 2019 diverse aanvullende beschermingsmaatregelen aangekondigd om de veiligheid en integriteit van telecomnetwerken te waarborgen. Ook is er voor de telecomsector een structureel proces ingericht waarin samen met relevante stakeholders bekeken wordt op welke manier de telecomnetwerken ook in de toekomst weerbaar kunnen blijven tegen veranderingen in het dreigingsbeeld en technologische ontwikkelingen. De komende periode wordt in kaart gebracht wat er nodig is (qua mensen, middelen en expertise) om deze structurele aanpak op telecom te verbreden naar andere vitale processen, zoals op het vitaal proces elektriciteit dat sterke intersectorale afhankelijkheden kent.

5 Tweede Kamer 2020-2021, 30 821, nr. 125.
6 Tweede Kamer 2018-2019, 30 821, Nr. 91 en 112.

Om ongewenste kennis- en technologieoverdracht in het hoger onderwijs en wetenschap tegen te gaan, is op 27 november 2020 door het kabinet een pakket aan maatregelen aangekondigd, aanvullend op het bestaande exportcontroleregime en bestaande sanctieregelgeving.. Het gaat daarbij om een combinatie van bewustwording en zelfregulering binnen de sector en een bindend toetsingskader op bepaalde risicovakgebieden. Ook wordt geïnvesteerd in de kennisopbouw aangaande zogenaamde sensitieve technologieën, die raken aan de nationale veiligheid. Hierbij worden de technologische toepassingen in kaart gebracht die raken aan de nationale veiligheid en criteria ontwikkeld, op basis waarvan opkomende technologieën kunnen worden geïdentificeerd die bescherming behoeven in het licht van de nationale veiligheid.[7] Met betrekking tot het voorkomen van ongewenste strategische afhankelijkheid is het van belang te bezien welke strategische afhankelijkheden er bestaan en welke vanuit nationale veiligheidsoverwegingen onwenselijk zijn.[8] Tot slot wordt onderzocht op welke wijze vorm gegeven kan worden aan aanvullende strafbaarstelling van spionage.

Ontwikkeling van de aanpak

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

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

Vanuit deze bredere blik worden de huidige maatregelen binnen de aanpak statelijke dreigingen onder de loep genomen en indien nodig versterkt. De aanpak kent een aantal generieke maatregelen en richt zich meer specifiek op de sociale en politieke stabiliteit en de economische veiligheid. De aanpak statelijke dreigingen hangt sterk samen met de versterkte aanpak vitale infrastructuur en de aanpak digitale dreigingen.

7 Zoals ook gevraagd in de gewijzigde motie van het lid Van den Berg (Kamerstuk 30 821, nr. 110)'

8 Zie ook de kabinetsbrief aan de Tweede Kamer over nationale veiligheid, strategische afhankelijkheid en planbureau van 10 februari 2021

Polarisatie tegengaan

Korte samenvatting NVS 2019

Mensen maken zich zorgen over de samenleving en kunnen een groeiend gevoel van onbehagen en soms gevoelens van onmacht ervaren. Dit maatschappelijk onbehagen kan een voedingsbodem zijn voor polarisatie en het uitvergroten van maatschappelijke tegenstellingen. Op de langere termijn kan polarisatie zorgen voor het afzwakken van de sociale stabiliteit in Nederland. Daarom gaat de overheid intensiever samenwerken tegen polarisatie via een brede overkoepelende aanpak gericht op de bevordering van samenleven.

Juist bij polarisatie, waar het gaat om een uitvergroting van maatschappelijke tegenstellingen, is het belangrijk dat de overheid alle vormen van maatschappelijke onrust adresseert in haar beleid en communicatie. Communicatie is hierin een belangrijk beleidsinstrument. Gemeenten en instanties zijn volop bezig om polarisatie en de effecten ervan tegen te gaan. Ook de veiligheidsketen kan een belangrijke bijdrage leveren, bijvoorbeeld met wijkagenten die vaak het eerste aanspreekpunt zijn in een wijk.

Ontwikkeling van de dreiging en de risico's

De Horizonscan 2020 signaleert dat meer aandacht nodig is voor 'niet-gewelddadig extremisme'. Maatschappelijke ontwikkelingen, bijvoorbeeld een toename van tegenstellingen (sociaaleconomisch én sociaal-cultureel), het toenemende belang van ervaren primaire identiteit, en toename van complotdenken vormen een voedingsbodem voor niet-gewelddadig extremisme en polarisatie. Deze trends kunnen op hun beurt weer worden gefaciliteerd door mogelijkheden en ontwikkelingen op het gebied van informatietechnologie. Met name de mogelijkheden voor een snelle verspreiding van des- en misinformatie vormen hierbij het ideale middel om denkbeelden en standpunten breed, dan wel gericht, te communiceren. Algoritmen sturen gebruikers naar onlinebronnen of platforms die als echokamers van het eigen gelijk kunnen gaan fungeren. Samen kan dit leiden tot de versterking van complottheorieën, acties en/of demonstraties over bepaalde onderwerpen waarover de meningen binnen de samenleving (sterk) verdeeld zijn. Onderwerpen als 5G, windturbines en de maatregelen rondom Covid-19 zijn hier concrete voorbeelden van. Ook kunnen maatregelen rondom klimaat en milieu, zoals het terugdringen van de uitstoot van stikstof leiden tot maatschappelijke discussie en polarisatie. Daarbij geldt dat dit ook een internationale dimensie heeft en dezelfde onderwerpen leiden tot acties en demonstraties in andere (Europese) landen. Bovendien kunnen kwaadwillende buitenlandse actoren dergelijke polarisatie over specifieke onderwerpen uitbuiten in het kader van buitenlandse beïnvloeding (via

hybride operaties). Zij kunnen middels gerichte informatiecampagnes angst en verdeeldheid zaaien en zo polarisatie van het publieke debat verder aanwakkeren. Verder geldt dat de geschetste ontwikkelingen en uitingen door binnenlandse en buitenlandse actoren die weliswaar niet-gewelddadig zijn maar wel extremistisch mogelijk op termijn de sociale cohesie kunnen aantasten, anti-overheidssentimenten doen toenemen en kunnen zorgen voor het verminderen van het vertrouwen in de overheid en instituties. Dit kan vervolgens op termijn leiden tot het aantasten en ondermijnen van de principes van de democratische rechtsstaat en open samenleving.

Sinds de uitbraak van Covid-19 heeft maatschappelijk ongenoegen zich zowel online als offline verder gemanifesteerd, waarbij sociale media een faciliterende en mobiliserende rol spelen. Alhoewel een groot deel van deze groepen of individuen zich houden aan de spelregels van de democratische rechtsstaat en ongenoegen over beleidsmaatregelen ventileren of zich richten op de emancipatie van groepen in de Nederlandse samenleving, is er ook een deel dat elkaar vindt in het stelselmatig afwijzen van de overheid of het overheidsbeleid. Dit gebeurt niet zozeer met ideologische motieven, maar vanwege gevoelens van onrechtvaardigheid, groot onbehagen of een andere werkelijkheidsbeleving. Mensen die de overheid, wetenschap en traditionele media al langer wantrouwen, kunnen hun denkbeelden bovendien bevestigd zien in complottheorieën, misinformatie en desinformatie; sinds de uitbraak van Covid-19 verspreiden complottheorieën zich sneller van de marges van het internet naar mainstreamkanalen. Er is een (online) context ontstaan waarbinnen de drempel om tot extremistische gedragingen te komen wordt verlaagd. Deze context versterkt polarisatie en leidt in een enkel geval tot verharding, intimidatie of (oproepen tot) geweld. Wel bestaat er een grote discrepantie tussen digitale uitingen van ongenoegen en de omvang van protesten in de fysieke ruimte. Offline komen verschillende groepen samen in anti-lockdownprotesten, die wat betreft omvang en ongeregeldheden geenszins in vergelijking staan met protesten in bijvoorbeeld Duitsland, maar wel kunnen leiden tot (gewelddadige) verstoringen van de openbare orde. De demonstraties brengen deelnemers op de been vanuit een breed scala aan onderwerpen. Behalve de relatief brede, gemêleerde activistische bovenlaag die gebruikt maakt van de rechten die ze hebben in een democratische rechtsstaat bestaat er een radicale onderstroom met extremistische gedragingen, zoals het belagen van politici en journalisten en het intimideren van politiemensen. Diverse groepen boze burgers zoeken ook aansluiting bij bijvoorbeeld de aanhoudende boerenprotesten. Bij een gedeelte van de boerenprotesten is sprake van een zekere verharding, bijvoorbeeld door het uiten van dreigementen richting politici, journalisten en andersdenkende medeboeren.

Ontwikkeling van de weerbaarheid

Polarisatie en ook het beschreven onbehagen is latent aanwezig en is niet per se negatief of van directe invloed op de veiligheid.

Tegelijk kan polarisatie, met name als het gaat om die radicale onderstroom, in een extreme vorm schade toebrengen aan de sociale stabiliteit en de democratische rechtsstaat. Daarom richt het kabinet zich op het vergroten van de weerbaarheid van samenleving en vroegsignalering. Vroegsignalering heeft als doel om te de-escaleren bij onwenselijke maatschappelijke spanningen en polarisatie, en radicalisering en extremisme voor te zijn dan wel te herkennen. Centraal in deze benadering staan: het weerbare individu, de weerbare groep, de weerbare samenleving en de weerbare (lokale) overheid. Door te investeren in de weerbaarheid op individueel en gemeenschapsniveau kunnen het individu en de gemeenschap zich teweerstellen tegen polariserende en onverdraagzame boodschappen. Door te werken aan preventie van ongewenste polarisatie, maatschappelijke spanningen, radicalisering en problematisch gedrag, versterkt het kabinet het vermogen om op te veren na een drastische verandering of tegenslag.

Zo is onder andere ingezet op het 'leren': het kunnen omgaan met polarisatie, door het vertalen van kennis over (omgaan met) polarisatie naar de alledaagse praktijk. Ook is ingezet op het vergroten van de kennis over het demonstratierecht bij gemeenten en hun bestuurders. Deze kennis wordt breed gedeeld.

Ontwikkeling van de aanpak

In de NVS 2019 is sprake van een versterkte aanpak op polarisatie en dit blijft noodzakelijk. De inzet gericht op het leren omgaan met polarisatie in de samenleving en het als overheid kunnen anticiperen op demonstraties blijft belangrijk en actueel, gelet op de zorgen in de samenleving en de beeldvorming hierover. De kennis hierover wordt door het kabinet verder opgebouwd en verspreid binnen de context van een aanpak die gericht het samenleven wil bevorderen. Dit leidt tot meer handelingsperspectief en bruikbare beleidsinterventies om polarisatie tegen te gaan.

Problematisch gedrag, radicalisering of in het uiterste geval (gewelddadig) extremisme kunnen voortkomen uit ongewenste buitenlandse beïnvloeding en vragen om een multidisciplinaire aanpak gericht op preventie en repressie. De aanpak is onder andere verdeeld naar actoren, inzicht in de doelen en geldstromen van buitenlandse organisaties en problematisch gedrag, met als doel om groepen in Nederland beter tegen die beïnvloeding bestand te maken en de ongewenste maatschappelijke effecten af te zwakken.[9]

9 Zie ook Tweede Kamer 2020-2021, 35 228, nr. 33.

Versterkte aanpak beschermen vitale infrastructuur

Korte samenvatting NVS 2019

Processen worden vitaal verklaard vanwege de voorziene impact op Nederlandse veiligheidsbelangen bij uitval of verstoring. De complexiteit van dreigingen en risico's laat zien dat ook integriteit van informatie, toegang tot (besturings-)systemen, en zeggenschap over (onderdelen van) de vitale infrastructuur belangrijke factoren zijn geworden in het waarborgen van de nationale veiligheidsbelangen. Deze staan onder druk, gezien de toenemende dreiging van statelijke actoren en cybercriminelen, de toegenomen (digitale) verwevenheid van systemen en organisaties en de daaruit voortvloeiende ketenafhankelijkheden. Welke processen en aanbieders (bedrijven, organisaties) we moeten beschermen en hóe we deze zouden moeten beschermen is daarmee aan constante verandering onderhevig. Dit vraagt een nieuwe blik op de werking van het systeem. De verantwoordelijkheid voor en kennis van vitale processen is bij de overheid sterk verdeeld over ministeries en het bedrijfsleven en kent daarnaast ook regionale en lokale componenten.

Het kabinet acht het van groot belang dat bij het toetsen van nationale veiligheidsrisico's voor de vitale infrastructuur, gebruik wordt gemaakt van consistente en technisch *up to date* zijnde criteria, en dat, omwille van het tijdig anticiperen op ontwikkelingen, inzichtelijk is hoe de Nederlandse vitale infrastructuur zich technisch en organisatorisch ontwikkelt. Daarom zal het kabinet, in samenwerking met al deze partijen, een versterkte aanpak van bescherming van de vitale infrastructuur ontwikkelen.

Ontwikkeling van de dreiging en de risico's

De Nederlandse vitale infrastructuur wordt gevormd door processen die zo belangrijk zijn voor onze samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Omdat vitale infrastructuren onderling afhankelijk zijn, kan het (technisch) falen van één vitaal proces leiden tot diverse keteneffecten. De afhankelijkheden tussen vitale processen zijn in veel gevallen niet direct en eenduidig. De uitval of verstoring van vitale processen kan met name een impact hebben op de veiligheidsbelangen 'Fysieke veiligheid', 'Sociale en politieke stabiliteit' en 'Economische veiligheid', maar eigenlijk op vrijwel alle nationale veiligheidsbelangen (en alle onderliggende impactcriteria). Daardoor heeft uitval of verstoring van de vitale infrastructuur tevens een versterkend effect op het optreden van andere dominante risico's voor de nationale veiligheid. Maar dit geldt ook andersom; vrijwel alle dreigingen of risico's kunnen effect hebben op de vitale infrastructuur.

De digitale dreiging vanuit statelijke actoren gericht op het verstoren of saboteren van vitale systemen blijft een zorg. Er is een duidelijke trend in de toename van autonome systemen in allerlei sectoren, zoals de elektriciteitssector, de financiële sector of de industrie. Deze systemen kunnen vaak niet in isolement opereren, waardoor communicatie en interactie tussen verschillende entiteiten (veelal via het internet) plaatsvinden. Dit maakt de systemen vatbaarder voor ongewenste inmenging van buitenaf. Waakzaamheid ten aanzien van digitale dreigingen en daaraan gerelateerde *supply chain* risico's blijft geboden. Daarnaast worden binnen het Deltaprogramma maatregelen genomen om de weerbaarheid van de vitale infrastructuur tegen de effecten van klimaatverandering te versterken.

Ontwikkeling van de weerbaarheid

Naar aanleiding van de zorgelijke ontwikkeling van digitale en statelijke dreigingen worden meerdere weerbaarheidsverhogende maatregelen ontwikkeld en geïmplementeerd die de weerbaarheid van de vitale infrastructuur versterken. Hierbij moet gedacht worden aan de implementatie van de Wet beveiliging netwerk- en informatiesystemen (Wbni) om de digitale veiligheid van de vitale infrastructuur te versterken, aan bewustwordingsactiviteiten rond *supply chain* risico's en het beschikbaar stellen van een instrumentarium om *supply chain* risico's te adresseren, aan wetgeving gericht op het voorkomen van ongewenste overnames en investeringen en aan maatregelen om de weerbaarheid van de vitale infrastructuur tegen de effecten van klimaatverandering te versterken.

Ontwikkeling van de aanpak

Op de gesignaleerde risico's wordt momenteel vanuit verschillende programma's actie ondernomen. Deze acties dienen in een samenhangende en geactualiseerde aanpak geborgd te worden. In het kader van de Rijksbrede aanpak vitale infrastructuur wordt daarom momenteel gewerkt aan een versterkingsprogramma. Binnen dit versterkingsprogramma wordt de scope van de aanpak vitale infrastructuur opnieuw bezien, onder andere met het oog op digitale ontwikkelingen en door de *supply chain* (het vitale proces inclusief de toeleveranciers) een structurele plek te geven in de aanpak. Daarnaast heeft het programma tot doel de activiteiten van de overheid die raken aan de bescherming van vitale infrastructuur te stroomlijnen; onder andere door de beleidslijnen gericht op fysieke en digitale weerbaarheid nadrukkelijker op elkaar af te stemmen en economische veiligheid mee te nemen in de *all hazard* aanpak van vitaal. Fysiek, digitaal en economisch veiligheidsbeleid worden daarom zoveel mogelijk gebundeld ten behoeve van één aanpak: het samenvoegen van digitale en fysieke veiligheid, ketenafhankelijkheden én *supply chain* security in één gecoördineerde aanpak vitale infrastructuur.

Terrorisme en extremisme tegengaan

Korte samenvatting NVS 2019

De afgelopen jaren is ingezet op de versterking van de integrale aanpak, in lijn met de Contraterrorisme Strategie 2016-2020 en passend bij de terroristische dreiging. Gezien het dreigingsbeeld is deze aanpak langs een aantal lijnen versterkt, namelijk:

- Vroegtijdige onderkenning van dreiging, door intensivering van inlichtingenonderzoek naar radicalisering en salafisme, in het kader van contraterrorisme.
- Borging aanpak van financiering van extremisme en terrorisme.
- Versterking van digitale weerbaarheid en aanpak extremisme online.
- Investeren in deradicalisering, re-integratie en strafrechtelijke aanpak.
- Versterking internationale inzet.

Verschillende vormen van extremisme, waaronder rechts-extremisme en identitair extremisme, nemen toe. Daarom zal ingezet worden op het toepassen van de integrale aanpak op alle vormen van extremisme, van welke ideologische signatuur dan ook, zodat ook 'nieuwe' dreigingen het hoofd geboden kunnen worden. Het blijft van belang om periodiek te reflecteren op de resultaten van de aanpak: passen de maatregelen nog tegen de actuele dreiging? In dit kader worden onderdelen van de aanpak steeds geëvalueerd. Op basis van deze bevindingen zal de nieuwe CT-strategie samengesteld worden.

Ontwikkeling van de dreiging en de risico's

De dreiging op het gebied van terrorisme en extremisme is veranderlijk van aard en omvang. Sinds het verschijnen van de NVS in 2019 is het dreigingsniveau weliswaar verlaagd van 4 naar 3, maar dat neemt niet weg dat er nog altijd een aanzienlijke dreiging is. Er is sprake van dreiging vanuit terroristische organisaties als ISIS en Al Qaida, de terugkeer van uitreizigers in de Nederlandse samenleving, de ontwikkeling en mogelijke opkomst van andere terroristische groeperingen en er kan sprake zijn van (onvoorziene) geopolitieke ontwikkelingen die mogelijk terrorisme en/of extremisme in de hand werken. Ook zal Nederland nog in toenemende mate te maken krijgen met ex-gedetineerden die terugkeren in de samenleving maar waarvan een deel hun extremistische gedachtegoed mogelijk nog niet heeft afgezworen en wellicht nieuwe onwenselijke connecties heeft gemaakt tijdens detentie. Tot slot moeten we bedacht zijn op de mogelijkheid van een gewelddadige daad gepleegd door een geïnspireerde eenling. Al deze ontwikkelingen maken dit thema complex. De dreiging komt daarbij niet alleen van islamitisch terroristische groeperingen.

De uitbraak van Covid-19 en de genomen overheidsmaatregelen hebben niet geleid tot een verhoogde dreiging van rechts- en links-extremisme in Nederland. De maatregelen hebben logischerwijs gezorgd voor een tijdelijke stilstand van fysieke activiteiten bij activistische en extremistische bewegingen. Maar ook bij demonstraties tegen de maatregelen speelden links- en rechtsextremistische groeperingen een marginale rol. Online koppelden groepen en personen aan beide kanten de ontwikkelingen rond Covid-19 aan hun eigen thema's, om hun gedachtegoed te propaganderen en om te bepleiten dat de crisis het falen van het huidige politieke systeem blootlegt. Dit gebeurt bijvoorbeeld door de pandemie te koppelen aan immigratie, globalisering, wereldwijde ongelijkheid of het plaatsen van economische belangen boven mensenlevens. Door de langetermijngevolgen van Covid-19 kan mogelijk meer ruimte ontstaan voor radicale standpunten. Evenals voor de uitbraak van Covid-19 is er een toename van personen die, mede gevoed door extreemrechtse ideeën, online dreigen met geweld. Hoewel de ernst en vooral de waarschijnlijkheid van de dreiging niet in alle gevallen heel groot lijkt, blijft dit een punt van aandacht. Het risico dat rechtsextremistische eenlingen of kleine groepen naar geweld grijpen wordt groter geacht dan in het verleden. Daarnaast hebben extreemrechtse groepen en individuen geprobeerd aan te haken op online circulerende complottheorieën of antilockdown-sentimenten, om de eigen agenda te dienen. Het is exemplarisch dat deze groepen tijdens de anti-lockdown-demonstraties slechts beperkt aanwezig en niet richtinggevend waren, terwijl juist andere groepen zich hebben laten zien.

Ontwikkeling van de weerbaarheid

Met de introductie van het Actieprogramma Integrale Aanpak Jihadisme en radicalisering, inmiddels opgevolgd door de Integrale aanpak terrorisme, is ingezet op het behoud van onze veiligheid en de democratische rechtsorde. Dit alles in lijn met de Nationale CT-Strategie 2016-2020. Deze inzet heeft geleid tot een verbetering van de weerbaarheid op lokaal, regionaal en nationaal niveau. Daarnaast stopt terrorisme niet bij de landsgrenzen en heeft intensieve internationale samenwerking geleid tot een verbeterde weerbaarheid op internationaal niveau. Dankzij de Nederlandse inzet kunnen we potentiële dreiging vroegtijdiger detecteren, aanslagdreiging eerder wegnemen en onze belangen beter beschermen. Ook zijn we beter in staat om bij een eventuele aanslag de schade zoveel mogelijk te beperken en (potentiële) daders op te sporen en te vervolgen.

Ontwikkeling van de aanpak

Terroristische dreiging is geen statisch gegeven. Er zijn periodes waarin de dreiging intensiveert en er zijn periodes waarbij zij weer wat lijkt af te nemen. Bij een periode van verminderde dreiging ligt tevens vermindering van aandacht voor het thema op de loer, met als risico dat we onvoldoende voorbereid zijn als het nodig is. Hoewel de huidige dreiging iets minder lijkt dan de periode 2014-2019, is het van groot belang om alert te blijven. Dit wordt geïllustreerd door de recente aanslagen in Frankrijk en Oostenrijk. In dat kader wordt voorzien dat de nieuwe CT Strategie 2021-2025 inzet op behoud van kennis én kunde, zodat bij een toename van de dreiging lokale, regionale en nationale partijen voldoende in staat zijn om deze dreiging het hoofd te bieden.

Militaire dreigingen tegengaan

Korte samenvatting NVS 2019

De afgelopen jaren is de eerste hoofdtaak van de krijgsmacht, de bescherming van het eigen en bondgenootschappelijke grondgebied, steeds belangrijker geworden. Tegelijkertijd neemt het belang van de andere hoofdtaken niet af.

Andere landen maken grote stappen met hun militaire capaciteiten, waardoor militair overwicht van Nederland en zijn bondgenoten geen vanzelfsprekendheid meer is. Nederland kan deze dreigingen alleen tegengaan door effectieve samenwerkingen en actief internationaal beleid, in de EU, de NAVO, de OVSE en de VN. Om een geloofwaardige bondgenoot en partner te blijven, wordt de slagkracht, het voortzettingsvermogen en de inzetbaarheid van onze krijgsmacht versterkt en verbeterd. We moeten inspringen op nieuwe technologische ontwikkelingen, de dominante(re) rol die informatie gaat spelen in zowel conflictpreventie en oorlogsvoering onderkennen en ons voorbereiden op conflicten die zich tegelijkertijd in verschillende domeinen ontvouwen, inclusief het cyberdomein. Dit vraagt nauwe civiel-militaire samenwerking in de aanpak van digitale en statelijke dreigingen.

Ontwikkeling van de dreiging en de risico's

Sinds de publicatie van de NVS is de competitie tussen verschillende staten verder toegenomen en de taal verder verhard. De oplopende geopolitieke spanningen worden zichtbaarder en leiden op plekken al tot ontvlambare situaties. Een deel van de spanningen doet zich bovendien binnen het NAVO-bondgenootschap voor, of aan de randen daarvan. De militarisering van het conflict tussen Turkije en Griekenland over gas en maritieme grenzen is daar een voorbeeld van, net als het oplaaiende geweld tussen Armenië en Azerbeidzjan in en om Nagorno-Karabach. Deze ontwikkelingen spelen zich af terwijl de Verenigde Staten terugtrekkende bewegingen uit Europa maakt. Mede daardoor staat de strategische stabiliteit die we de afgelopen decennia hebben genoten onder druk, want onze veiligheid blijft in de komende jaren sterk afhankelijk van Amerikaanse solidariteit. Onder andere de Adviesraad voor Internationale Vraagstukken (AIV) concludeert dat de positie van Europa hierdoor kwetsbaarder wordt.[10] Europa moet sterker worden, ook op militair vlak. Dat maakt vervolgens ook de NAVO weer sterker.

De veranderende geopolitieke verhoudingen en de minder vanzelfsprekende politieke cohesie van onze internationale partnerschappen zorgen dat 'oude' dreigingen weer terug op de radar komen. Tegelijkertijd neemt, mede door het gebruik van geavanceerde technologie door potentiële tegenstanders, het militair-technologisch overwicht van de NAVO (en EU) af. Ondanks de

10 *Europese Veiligheid: Tijd voor nieuwe Stappen*, Adviesraad Internationale Vraagstukken, nr. 112, 19 juni 2020.

coronacrisis verhoogde China bijvoorbeeld het defensiebudget dit jaar tot 178,2 miljard dollar. Rusland investeert in de ontwikkeling van hypersone wapens, robots, drones, lasers, en in manieren om anderen succesvol de toegang te ontzeggen tot gebieden en in het gebruik van desinformatie voor politiek-strategische doeleinden. In hun inhaalslag richten potentiële tegenstanders zich veelal op het incorporeren van nieuwe technologische mogelijkheden, oftewel nieuwe manieren van vechten. Het cyberdomein en het gebruik van de ruimte spelen daarbij een steeds belangrijkere rol, naast de meer traditionele domeinen van land, lucht en zee. Militarisering van het cyberdomein en de ruimte kunnen ook gevolgen hebben voor de nationale veiligheid, aangezien hier een deel van de Nederlandse vitale infrastructuur is geherbergd.

Ontwikkeling van de weerbaarheid

De afgelopen jaren is de focus voor het tegengaan van militaire dreigingen veranderd. Tot een aantal jaren geleden lag deze focus vooral op het bestrijden van terroristische groeperingen in onherbergzame gebieden. De veranderde dreiging heeft het besef gebracht dat we beter in staat moeten zijn om het eigen fysieke en digitale grondgebied te beschermen. Er is meer aandacht voor het kunnen optreden in het hogere geweldsspectrum en dat zal de komende jaren, mede door gericht met partners te oefenen, verder moeten groeien.

Dit betekent onder andere dat Nederland rekening moet houden met mogelijk grootschalige doorvoeroperaties om bondgenoten te kunnen laten ontplooien in Europa. Het Nationaal Plan Militaire Mobiliteit[11] geeft verder richting aan het verbeteren van militaire mobiliteit voor zowel EU- als NAVO-activiteiten. Het gaat hierbij niet alleen om het kunnen ontvangen van eenheden, maar ook om het kunnen ondersteunen van de daaropvolgende logistieke operatie. Dit vergt bewaking en beveiliging van bijvoorbeeld haventerminals, logistieke hubs en corridors waarlangs verplaatst wordt. Het in 2020 opgerichte Territoriaal Operatiecentrum (TOC) van de Koninklijke Landmacht heeft daarbij een ondersteunende *command* en *control* functie. Dit kabinet heeft, met de investeringen in Defensie, ingezet op het vergroten van de weerbaarheid tegen militaire dreigingen. Er worden stappen gezet in het vergroten van de slagkracht in zowel de 'traditionele domeinen' als in het cyberdomein. De Defensievisie 2035 (van oktober 2020) geeft hier een overzicht van.[12]

De kennis en kunde in het cyberdomein is vergroot, waarmee ook de weerbaarheid tegen statelijke dreigingen uit die hoek groeit. De NAVO had het cyberdomein in 2016 al erkend als operationeel domein en Nederland speelt internationaal op dit vlak al op hoog niveau mee. Eind 2019 is ook de ruimte door de NAVO erkend als een operationeel domein. Zowel Buitenlandse Zaken als Defensie hebben extra capaciteit gezet op dit thema en in het voorjaar van 2021 wordt de Defensie-ruimte-agenda gepubliceerd. Informatiegestuurd optreden was al aangeduid als een van de prioiriteiten in de Defensienota 2018 en is in de Defensievisie 2035 gemaakt tot een van de 'make or break' eigenschappen van Defensie.

Ontwikkeling van de aanpak

Het dreigingsbeeld wordt diverser, complexer en verontrustender. Defensie moet daarop kunnen anticiperen en, in het geval van een crisis, direct op kunnen reageren. Ondanks de belangrijke investeringen in de ondersteuning en de modernisering van onze krijgsmacht van dit kabinet, luidt de conclusie in de Defensievisie 2035 dat met de huidige inrichting en staat van de organisatie Defensie niet adequaat is toegerust voor de huidige en toekomstige dreigingen. In die visie, die op 15 oktober 2020 is aangeboden aan de Tweede Kamer, staat het vinden van een oplossing hiervoor centraal. De visie kijkt vijftien jaar vooruit en inventariseert wat er nodig is richting 2035. Dit helpt volgende kabinetten om, in het spanningsveld van behoeften en budget, beleidsprioriteiten te kunnen stellen.

11 Tweede Kamer 2020-2021, 35 570-X, nr. 75.
12 Tweede Kamer 2020-2021, 34 919, nr. 71.

Aanpak criminele ondermijning

Korte samenvatting NVS 2019

De problematiek van ondermijnende criminaliteit is voor een belangrijk deel grensoverschrijdend en internationaal van karakter, maar is tegelijkertijd sterk geworteld in de lokale samenleving. Anders gezegd, het gaat om criminele structuren die mondiaal zijn vertakt, maar lokaal wortelen en investeren. Dat betekent dat zowel een lokale/regionale aanpak én een landelijke/ internationale aanpak nodig zijn. Het kabinet ziet de aanpak van ondermijnende criminaliteit als een belangrijke opgave en heeft daarom gekozen voor een stevige programmatische aanpak. Die aanpak bestaat uit een breed pakket aan zowel preventieve als repressieve maatregelen, met een coalitie van overheid, bedrijfsleven en samenleving en op basis van een meerjarig versterkingsprogramma. Dat gebeurt in de eerste plaats door de inzet van extra financiële middelen uit het regeerakkoord die de regio's en de landelijke organisaties in staat stellen de aanpak een krachtige impuls te geven.

Met deze inzet van de extra middelen wordt een belangrijke stap gezet om het zicht op de ondermijningsproblematiek verder te verbeteren en de uitvoeringskracht en de overheidsbrede samenwerking te versterken. Ook bieden de extra middelen de mogelijkheid om de aanpak meer thematisch vorm te geven en daarbij via concrete pilots en projecten de aanpak ook te innoveren, met behulp van moderne technologieën.

Met (ondermijnende) criminaliteit worden ook criminele opbrengsten gegenereerd. Bij het bestrijden van georganiseerde criminaliteit en bredere geldgedreven criminaliteit wordt méér focus gelegd op het blootleggen van criminele geldstromen, om van daaruit effectieve interventies te bepalen en te plegen. Daarbij wordt ingezet op vier actielijnen: financieel-economisch perspectief aan de voorkant van het opsporingsonderzoek; verder leren, ontwikkelen en integraal verbinden; internationalisering; en monitoren en (bij)sturen.

Ontwikkeling van de dreiging en de risico's

Georganiseerde misdaad is van alle tijden, maar het karakter ervan is de afgelopen jaren veranderd. Met extreem grof en steeds roekeloozer geweld wordt gepoogd opgebouwde machtsposities en gewaande onaantastbaarheid binnen de omvangrijke illegale economie te beschermen. Veel vaker dan voorheen worden onschuldige Nederlanders daar het slachtoffer van. Dit is ondermijning in de meest gevaarlijke vorm. De rechtsstaat komt daarmee onder druk te staan.

De georganiseerde ondermijnende criminaliteit is in toenemende mate complex doordat zij sterk is geprofessionaliseerd en optimaal profiteert van de open economie, gunstige geografische ligging van Nederland en een goede logistieke, financiële en digitale infrastructuur. De mondiaal opererende criminele netwerken wortelen lokaal in de wijken. De gevaren voor de samenleving van de illegale drugsindustrie zijn evident: drugslabs in woonwijken, de intimiderende aanwezigheid van criminele motorbendes, en handgranaten als dreigmiddel bij restaurants en cafés. Kwetsbare jongeren worden de harde drugscriminaliteit in gezogen, en in sommige wijken ontstaat een parallelle samenleving waarin meedoen aan deze criminaliteit normaal lijkt. Er is in toenemende mate sprake van – dreiging met– extreem en grof geweld, niet alleen tegen concurrenten maar ook tegen de overheid en specifieke beroepsgroepen (contrastrategieën). De strafrechtelijke en fiscaalrechtelijke aanpak van de georganiseerde ondermijnende criminaliteit vergt een langdurige strategie, waarbij ook onorthodoxe en innovatieve maatregelen worden ingezet.

Een afschuwelijk dieptepunt in deze ontwikkeling is de moord op een advocaat op 18 september 2019, volgend op de moord op de broer van een kroongetuige in 2018. Liquidaties, witwassen, de versmelting van de onder- en bovenwereld; het gevaar dat uitgaat van georganiseerde ondermijnende criminaliteit is duidelijk en mag niet worden onderschat.

Ontwikkeling van de weerbaarheid

Sinds 2019 is intensief overleg gevoerd met alle relevante partijen, om te komen tot structurele intensiveringen op het gebied van onder meer regionale versterking, preventie en de normalisering van drugsgebruik.

Een balans tussen landelijke inzet, van onder andere kennis en middelen, en gebiedsgericht maatwerk is nodig om weerbaarder op te kunnen treden ten aanzien van ondermijnende criminaliteit. Daarnaast heeft het verhinderen c.q. voorkomen van het afglijden van kwetsbare personen naar criminaliteit ook de focus. Het weerbaarder maken van deze doelgroep kan door het vergroten van het toekomstperspectief door het verstevigen van de sociale structuren en in te zetten op kansen voor een zinvol bestaan en bijdrage aan de samenleving. Ook dient er speciale aandacht te zijn voor het weerbaarder maken van professionals en burgers in het sociale, onderwijs- en veiligheidsdomein. Zo is de bewaking en beveiliging van advocaten, officieren van justitie en rechters een noodzakelijk instrument en wordt nog meer aandacht besteed aan het waarborgen van de veiligheid van een melder van een ongebruikelijke transactie.

Ontwikkeling van de aanpak

In de periode 2019-2021 is incidenteel 100 miljoen vanuit het regeerakkoord geïnvesteerd in de regionale aanpak van ondermijnende criminaliteit. Vanaf 2020 zijn extra gelden beschikbaar gekomen ten behoeve van het breed offensief.[13] Met inzet van deze middelen wordt de aanpak geïntensiveerd en wordt ook kracht bijgezet met een uitgebreide wetgevingsagenda. Sinds de zomer van 2020 is binnen het ministerie van Justitie en Veiligheid een programmadirecteur-generaal georganiseerde en ondermijnende criminaliteit aangesteld. Zodoende coördineert één rijksbrede coördinator samen met alle betrokken partners het thema georganiseerde ondermijnende criminaliteit en wordt de integrale aanpak ondermijning geborgd, die bestaat uit preventieve en repressieve maatregelen volgens het devies 'oprollen, afpakken en voorkomen'.

In alle regio's en in enkele landelijke projecten hebben kabinet en partners geïnvesteerd in de integrale aanpak van georganiseerde ondermijnende criminaliteit. Er worden belangrijke stappen gezet om de aanpak van georganiseerde ondermijnende criminaliteit naar een steeds hoger niveau te tillen. Zo wordt toegezien op een totaalaanpak om deze complexe problematiek effectief te bestrijden. Het breed offensief wordt ingezet op een combinatie van repressieve en preventieve maatregelen zoals onder meer; het oprichten van het multidisciplinair interventieteam (MIT), het intensiveren van het stelsel bewaken en beveiligen, het verder ontwikkelen van kennis en expertise en de preventieve lokale aanpak om te verhinderen dat kwetsbare personen worden verleid af te glijden naar criminaliteit.[14]

Het MIT is een nieuw en uniek samenwerkingsverband binnen de Nederlandse rechtshandhaving en richt zich op de bestrijding van de georganiseerde ondermijnende criminaliteit. Het MIT gaat opereren op het snijvlak van (inter-)nationale georganiseerde ondermijnende criminaliteit en de daarmee gepaard gaande criminele geldstromen. Het team is een aanvulling op en werkt actief samen met de bestaande diensten die zich nu al succesvol inzetten binnen de integrale aanpak van ondermijning. Het doel van het MIT is het duurzaam verstoren van ondermijnende criminele bedrijfsprocessen, ook in het buitenland. Dit dient te gebeuren door het structureel opsporen en ontmantelen van criminele netwerken, het oppakken van kopstukken, het in beslagnemen van crimineel vermogen en het opwerpen van barrières voor crimineel handelen en voor het verkrijgen van crimineel geld. Naar verwachting kunnen de eerste MIT-teamleden in 2021 operationeel zijn.

Al eerder is het stelsel van de bewaking en beveiliging van advocaten, officieren van justitie en rechters geïntensiveerd. In de komende periode wordt de structurele versterking en flexibilisering van de stelsels Bewaken en Beveiligen en Getuigenbescherming doorontwikkeld. Om blijvend het hoofd te kunnen bieden aan huidige en toekomstige dreigingen in een complexer geworden samenleving zal een onafhankelijke commissie het stelsel bewaken en beveiligen beoordelen en voorstellen doen om het toekomstbestendig te maken.

Ten behoeve van de preventieve lokale aanpak hebben acht gemeenten voor 2020-2022 incidentele middelen gekregen om hun preventieve aanpak van ondermijning te versterken in sociaaleconomische kwetsbare wijken. De gemeenten investeren onder andere in dader- en gedragsgerichte interventies en voor toekomstvastheid en optimale effectiviteit wordt de preventieve aanpak lerend geëvalueerd. Voor het waarborgen van continuïteit en/of verder ontplooien van succesvolle activiteiten betreffende de regionale aanpak worden vanuit het breed offensief ook gelden in de komende twee jaar vrijgemaakt.

Op het gebied van landelijke kennisdeling wordt een strategisch kenniscentrum opgericht om samen met partners en wetenschappers trends en ontwikkelingen van georganiseerde ondermijnende criminaliteit te analyseren en te duiden. Dit strategisch kenniscentrum staat niet op zichzelf. Zo komen ook fenomeentafels, waarin de partners op geprioriteerde thema's de integrale aanpak gaan vormgeven, met concreet handelingsperspectief voor lokale en regionale partners. Ook wordt het algehele kennisfundament betreffende ondermijning verder versterkt door een nationale Kennisagenda Ondermijning. Deze agenda gaat onderzoek doen naar thema's waar nog onvoldoende kennis over bestaat, en zetten we in op systematische analyse en praktische toepassing van bestaande wetenschappelijke kennis.

Vanaf 2022 komt 150 miljoen euro per jaar extra beschikbaar voor de intensivering van de aanpak van georganiseerde ondermijnende criminaliteit. Dit geld wordt primair ingezet op het toekomstbestendig maken van het stelsel Bewaken en Beveiligen en de inrichting en werkzaamheden van het MIT.

13 Tweede Kamer 2019-2020, 29 911, nr. 256.
14 Tweede Kamer 2019-2020, 29 911, nr. 254.

Aanpak digitale dreigingen

Korte samenvatting NVS 2019

Risico's rondom digitale veiligheid worden door het kabinet op geïntegreerde wijze geadresseerd met de Nederlandse Cybersecurity Agenda (NCSA) uit april 2018. Deze is flexibel vormgegeven, zodat nieuwe of toenemende dreigingen adequaat het hoofd kunnen worden geboden.

De permanente dreiging, de weerbaarheid die onder druk staat en verregaande afhankelijkheden vragen om een versterking en versnelling van de aanpak. Daarom wordt voor alle vitale sectoren ingezet op structurele en adaptieve risicobeheersing. Concreet betekent dit dat er gewerkt wordt aan bewustwording van de risico's en het noodzakelijke niveau van digitale weerbaarheid, het versterken van digitale weerbaarheid en het toezicht hierop, en het vergroten van regie om ervoor te zorgen dat partijen hun verantwoordelijkheid nemen en waar nodig ingegrepen wordt.

De toenemende digitale dreiging, onderlinge afhankelijkheden en de opkomst van nieuwe technologieën vereisen een risicogestuurde benadering van wat beschermd moet worden. Met de verantwoordelijke departementen en toezichthouders wordt gewerkt aan een versterking van het toezicht op de digitale weerbaarheid. Hiertoe worden basisniveaus en beveiligingsdoelen per sector opgesteld. Hiermee worden partijen in staat gesteld nader invulling te geven aan de zorgplicht die uit de Wet beveiliging netwerk- en informatiesystemen (Wbni) vloeit.

Om ervoor te zorgen dat de digitale weerbaarheid structureel op een voldoende niveau is, moet er gezamenlijk geoefend en getest worden. Daarom stelt dit kabinet een breed, publiek-privaat, oefen- en testprogramma op. Voorts wordt een certificeringsraamwerk voor producten, diensten en processen voortvloeiend uit de Europese *Cyber Security Act* ingevoerd.

Ontwikkeling van de dreiging

Digitale onveiligheid is momenteel de grootste bedreiging van onze nationale veiligheid. Elke dag krijgt Nederland talloze grotere en kleinere cyberaanvallen te verduren, uitgevoerd door statelijke actoren en criminelen, die zich soms door staten laten inhuren. De voortdurende en steeds geavanceerdere aanvallen nemen toe in aantal en in omvang. Onze digitale veiligheid en weerbaarheid houden hiermee geen gelijke tred, terwijl ons land wel in hoog tempo verder digitaliseert. Intussen onderstreept de coronacrisis nog eens de onmisbaarheid van digitale middelen en onze digitale infrastructuur. Cyberaanvallen kunnen vitale processen (energie, communicatie, betaalverkeer, enzovoorts) verregaand verstoren of zelfs verlammen.

Door toenemende cognitie, autonomie en complexiteit in IT-systemen worden nieuwe typen kwetsbaarheden geïntroduceerd die kunnen leiden tot technisch falen, zo signaleert de Horizonscan 2020. Bij cyberdreigingen zijn er vernieuwde aanvalsmiddelen en -werkwijzen. Er is bijvoorbeeld een ontwikkeling gaande richting het geautomatiseerd zoeken naar kwetsbaarheden in systemen met behulp van nieuwe, geavanceerdere middelen (zoals zelflerende aanvalssystemen, of autonome malware). Ook op militair gebied worden autonome onbemande systemen steeds vaker ingezet.

In termen van 'vernetting' is er volgens de Horizonscan 2020 risico op cascade-effecten. Door de koppeling van databronnen en informatiesystemen is onvoldoende inzicht in cascade-effecten bij uitval. Zo kan een systeem verstoord raken doordat gekoppelde systemen of diensten verstoord zijn (*supply chain* risico's). Dit levert ook nieuwe routes voor sabotage en cyberaanvallen. Als voorbeeld: kwaadwillenden maken steeds vaker gebruik van autonoom opererende programma's om grootschalige DDoS- (*Distributed Denial of Service*) -aanvallen uit te voeren op internetdiensten. Bovendien is er professionalisering bij cybercriminelen te zien inclusief het cybercrime-as-a-servicemodel, waarbij kwaadwillenden derden betalen om cyberaanvallen uit te voeren.

De risico's en dreiging zijn in het afgelopen jaar toegenomen, zoals ook is beschreven in het Cybersecuritybeeld Nederland 2020 (CSBN 2020).[15] In de afgelopen periode heeft de digitale dreiging zich een aantal keer prominent gemanifesteerd, zoals bij de problematiek rond kwetsbaarheden in Citrix-systemen (december 2019), waar onder andere de Rijksoverheid gebruik van maakt. Daarnaast is de afhankelijkheid van de Nederlandse samenleving van digitale middelen zichtbaarder geworden toen een verstoring in 2019 zorgde voor onbereikbaarheid van het noodnummer 112 en meer recentelijk het landelijke telefoonnummer van de politie. Door de Covid-19 pandemie is het gebruik van digitale technologie en diensten verder toegenomen waardoor de samenleving en economie ook afhankelijker hiervan zijn geworden. Dat maakt het belang van digitale veiligheid groter.

Daarnaast intensiveren statelijke actoren door oplopende geopolitieke spanningen hun digitale activiteiten, onder andere via cyberaanvallen. Statelijke actoren zijn blijvend actief gebleken op het gebied van digitale spionage, het treffen van voorbereidingen voor digitale sabotage gericht op Westerse landen en bondgenootschappelijke belangen en misbruik van Nederlandse ICT-infrastructuur voor digitale aanvallen op andere landen.

Kwaadwillende actoren spelen daarnaast in op de actualiteit: door de Covid-19-pandemie is er een toegenomen interesse in onder andere farmaceutische bedrijven, onderzoekscentra, ziekenhuizen en zorginstellingen, maar ook de publieke en economische sectoren vormen een doelwit. Kwaadwillende actoren maken misbruik van de gelegenheid die de toenemende digitalisering hen biedt.

15 Tweede Kamer 2019-2020, 26643, nr. 695.

Ten slotte neemt onze afhankelijkheid van digitale technologie en de onderlinge verwevenheid van netwerk- en informatiesystemen nog steeds toe. Hierdoor neemt ook de kwetsbaarheid als gevolg van digitale aanvallen en uitval toe. Een samenleving met voldoende digitale weerbaarheid vraagt dan ook om continue inspanning.

Ontwikkeling van de weerbaarheid

De uitvoering van de Nederlandse Cybersecurity Agenda (NCSA) is inmiddels in volle gang. Daarnaast zijn er afgelopen jaar aanvullende maatregelen aangekondigd binnen het zogenaamde versterkingsprogramma cybersecurity, naar aanleiding van het CSBN 2019 en het WRR-rapport "Voorbereiden op digitale ontwrichting".[16]

Alle maatregelen beogen bij te dragen aan een vergroting van de digitale veiligheid, waaronder tegen verstoringen van de continuïteit en tegen ongewenste activiteiten van geavanceerde actoren, door onder andere een verhoging van inzicht in de digitale dreigingen, de weerbaarheid en passende maatregelen, de daadwerkelijke digitale weerbaarheid en het vermogen om snel te kunnen handelen bij digitale incidenten, de dienstverlening te herstellen.

Afgelopen jaar zijn er diverse concrete stappen gezet, zoals een verdere uitbreiding van het Nationaal Detectienetwerk, de uitwerking van het oefenprogramma, de voorbereidingen op de inwerkingtreding van het Besluit beveiliging netwerk- en informatiesystemen (Bbni) met als doel basisniveau van beveiliging te realiseren van netwerk- en informatiesystemen bij vitale aanbieders, het inspectiebeeld vitale infrastructuur, en het in kaart brengen van huidige wettelijke taken en bevoegdheden die het mogelijk maken informatie te delen en in het uiterste geval in te grijpen dan wel te sturen op digitale weerbaarheid bij rijksoverheid, vitale aanbieders en andere organisaties. Daarnaast zijn in Europees verband stappen gezet om de digitale weerbaarheid in de lidstaten te vergroten waaronder implementatie en evaluatie van de richtlijn betreffende de beveiliging van netwerk- en informatiesystemen (NIB-richtlijn), uitwerken cybersecuritymaatregelen ten behoeve van telecomnetwerken en oprichting van een strategisch netwerk in het kader van cybercrisisbeheersing.

Ondanks deze inspanningen dient het versterken van onze digitale weerbaarheid blijvend aandacht te krijgen. In het algemeen geldt dat de technologie en onze afhankelijkheid zich snel ontwikkelen, waardoor er constant aandacht nodig is voor het thema van digitale weerbaarheid. Onder andere geldt dit voor de doorontwikkeling van het Landelijk Dekkend Stelsel waardoor meer organisaties in Nederland toegang krijgen tot actuele dreigingsinformatie, het verstevigen van het wettelijk kader voor de digitale weerbaarheid van de vitale infrastructuur en het vergroten van de operationele slagkracht.

Ontwikkeling van de aanpak

Risico's en dreigingen nemen toe, en ondanks de maatregelen die in gang zijn gezet, moeten er nog stappen worden gezet om de digitale weerbaarheid van Nederland te verhogen én op peil te houden. Het in de NCSA uitgezette beleid vormt daarin de leidraad, met concrete versterkingen sindsdien, zoals de acties die zijn opgenomen in de kabinetsreactie op het WRR-rapport over digitale ontwrichting. Dit gaat uit van een integrale publiek-private aanpak, dat wil zeggen overheidsbreed en in samenwerking met vitale sectoren, en andere private partijen. Daarnaast wordt momenteel gewerkt aan een evaluatie van de NCSA. De planning is deze voorjaar 2021 naar de Tweede Kamer te sturen.

16 Tweede Kamer 2019-2020, 26 643, nr. 673 en Tweede Kamer 2018-2019 26 643, nr. 614.

Versterken multilaterale instituties

Korte samenvatting NVS 2019

Nederland zet in op het behoud en het versterken van multilaterale stelsels, met afspraken en regels die gebaseerd zijn op universele waarden. Daarbij maakt Nederland zich in Europees verband hard voor het dichten van gaten in de regels van de Wereld Handelsorganisatie (WTO), zodat verschillende economische systemen binnen een gelijk speelveld kunnen opereren. In het kader van het tegengaan van statelijke dreigingen, zet Nederland in op versterkte samenwerking binnen de EU en de NAVO en geeft daarmee prioriteit aan het versterken van de multilaterale instituties die bijdragen aan de nationale veiligheid.

Ontwikkeling van de dreiging en de risico's

Door geopolitieke ontwikkelingen staan de traditionele multilaterale samenwerkingsverbanden waarop de Nederlandse veiligheid steunt (NAVO; EU; VN) onder druk. Intussen groeit de kans op confrontaties en conflicten doordat landen machtspolitiek voorop gaan stellen. De Nederlandse veiligheid is juist gediend bij wederkerige en afdwingbare internationale afspraken.

Ook de Horizonscan 2020 ziet dat de tanende multilaterale wereldorde voor groeiende competitie tussen grote mogendheden zorgt en dat druk op het draagvlak voor internationale handelssystemen heeft geleid tot verder verstoorde handelsbetrekkingen Voorts is er onzekerheid over het voortduren van stabiliseringsmechanismen zoals raketbeheersingsverdrag INF. Toenemende spanningen tussen grote mogendheden kunnen leiden tot ondermijning van veiligheidsarrangementen. Tot slot kunnen grootmachten om hun macht te tonen digitale sabotage of cyberspionage bewust inzetten. Dit kan tevens onderdeel zijn van hybride operaties om zo een land te beïnvloeden.

De Horizonscan signaleert dat conflicten en fragiliteit ten zuiden van Europa kunnen zorgen voor een heropleving van terreurorganisaties. In dat geval kan de waarschijnlijkheid van terroristische aanslagen in Europa toenemen. Instabiliteit rondom Europa kan uiteindelijk leiden tot conflicten met gevolgen voor Europa en ook tot polarisatie binnen Nederland. Ook vanuit Rusland blijft een militaire dreiging uitgaan. Rusland poogt bovendien verdeeldheid te creëren onder lidstaten van zowel de EU als de NAVO. In de Caraïben vormt het conflict in Venezuela een bedreiging van de aan- en afvoerlijnen van Caribisch Nederland.

Multilaterale instellingen zijn in toenemende mate onderhevig aan uitholling, onder meer door een obstructieve rol van Rusland, het opzetten van parallelle structuren door China, een terugtrekkende rol van de VS (zoals onder de vorige Amerikaanse regering uit het Open Skies verdrag). Daarnaast blijft de dreiging van druk op de multilaterale orde zoals beschreven in NVS relevant.

Ontwikkeling van de weerbaarheid

Op politiek niveau bestaat nog steeds de wil samen te werken op EU-niveau. Echter, processen verlopen moeizaam en belangen lijken verder uit elkaar te liggen. Eigenzinnige lidstaten bemoeilijken besluitvorming op politieke niveau en gezamenlijk optrekken. Dit wordt versterkt door maatschappelijke scepsis ten aanzien van de EU die gezamenlijk optreden verder bemoeilijkt. Ook op het cyberdomein blijven partners het belang van multilaterale aanpak zien en aandringen op een gezamenlijke aanpak van dreigingen. Een voorbeeld hiervan is het ingestelde EU-cybersanctieregime.

Ontwikkeling van de aanpak

De aanpak hoeft niet te worden gewijzigd en verdere uitwerking zoals beschreven in de GBVS blijft leidraad. Nederland zal blijven inzetten op internationale aanpak gericht op goed bestuur, mensenrechten, en preventie van gewelddadig extremisme en samenwerking met en binnen de VN, de EU en de NAVO. Constructieve bijdrage van NL in multilateraal verband op contraterrorisme- en cybergebied kan rekenen op waardering van partners en Nederlandse belangen kunnen worden ingebracht. Om bij te dragen aan het versterken van multilaterale instituties zal Nederland, in samenwerking met gelijkgezinde partners, soms meer een voortrekkersrol moeten nemen om aandacht te blijven vestigen op het belang van thema's als rechtsstatelijkheid, mensenrechten en internationale samenwerking voor bevorderen van internationale veiligheid. Ook moet Nederland blijven inzetten op de internationale cyberaanpak gericht op versterking van de internationale rechtsorde in het digitale domein en cyberafschrikking en respons.

Voorkomen en bestrijden van natuurrampen

Korte samenvatting NVS 2019

Klimaatverandering
Klimaatverandering is tastbaar geworden. Het leidt steeds vaker tot extreem weer, van heftige neerslag tot hoge temperaturen. Nederland zet in op klimaatadaptatie en klimaatmitigatie, door onder andere maatregelen te nemen gericht op CO_2-reductie en op een klimaatbestendig grond- en oppervlaktewatersysteem, ruimtelijke inrichting en grondgebruik (zie ook Droogte).

Droogte
Naar aanleiding van de aanhoudende droogte in 2018 zal ingezet worden op meer structurele maatregelen gericht op een klimaatbestendig grond- en oppervlaktewatersysteem, ruimtelijke inrichting en grondgebruik. Het watersysteem, dat nu vooral gericht is op het zo snel mogelijk afvoeren van overtollig water, moet beter toegerust worden op het vasthouden en infiltreren van water. Op deze manier kan het grondwater tijdens neerslagoverschotten tijdig worden aangevuld.
De provincies hebben de regierol bij ruimtelijke borging van een klimaatrobuust watersysteem in de provinciale omgevingsvisies en de doorwerking daarvan naar het beleid van gemeenten en waterschappen.

Stijging waterpeil
Dat de zeespiegel de komende eeuw en ook daarna blijft stijgen is zeker. Het Nederlandse beleid is erop gericht om de doelstellingen uit het Akkoord van Parijs te halen (maximaal 2°C wereldwijde temperatuurstijging). Er is nog veel onzekerheid over de toekomstige emissies en de opwarming en zeespiegelstijging die daarmee gepaard gaat. Vanwege de potentieel grote implicaties voor Nederland is daarom ook gekeken naar een extreme zeespiegelstijging die het gevolg kan zijn van een emissiescenario dat leidt tot 4°C wereldwijde temperatuurstijging. In het Deltaprogramma staan de plannen hiervoor. Met het Deltaprogramma is Nederland in voldoende mate in staat de ontwikkelingen als gevolg van klimaatverandering en stijging van het waterpeil het hoofd te bieden.

Natuurbranden, aardbevingen, bodemdaling en zonnestormen
Buiten de programma's voor de aardbevingen in verband met de gaswinning zijn er geen aparte nationale programma's voor deze natuurrampen, anders dan de gebruikelijke crisisvoorbereiding op lokaal, regionaal en nationaal niveau.

Ontwikkeling van de dreiging en de risico's

De opwarming van het klimaat vergroot de kans op extreem weer. Het gaat hier specifiek om een toename in waarschijnlijkheid. Het is wel de verwachting dat intensiteit en daarmee ook de impact van hittegolven toeneemt. Klimaatbeleid en energietransitie kunnen volgens de Horizonscan 2020 leiden tot protesten en confrontaties van voor- en tegenstanders. Als het klimaatbeleid faalt, wordt de kans groter dat landen *geo-engineering* gaan inzetten met risico op geopolitieke spanningen. Hierdoor komen ook mogelijk veiligheidsarrangementen zoals de NAVO onder druk te staan, aldus de Horizonscan 2020.

Voorts meldt de Horizonscan dat de kwaliteit van drinkwaterbronnen onder druk staat door vervuiling van het grond- en oppervlaktewater. De beschikbaarheid van drinkwater kan daarmee in het geding komen. Dit is met name het geval in combinatie met extreme droogte waardoor vervuiling minder kan verdunnen in het water. Positiever is de Horizonscan over de kwaliteit van de lucht. Voor zowel stikstofdioxide als voor fijnstof is de verwachting dat de gemiddelde concentratie waar mensen aan blootgesteld worden de komende jaren afneemt. Dit heeft positieve gevolgen voor de volksgezondheid. Wel signaleert de Horizonscan dat milieubeleid (bijvoorbeeld rond stikstof) leidt tot protesten en demonstraties.

Ook in 2019 en 2020 heeft het weer records gebroken, dit keer vooral als gevolg van de hoge temperaturen in de zomer. We zien nu 3 jaar op rij extreme temperaturen en droogte. Nog nooit eerder werd zo laat in het jaar een tropische dag gemeten: op 15 september 2020 steeg de temperatuur in De Bilt tot 31,4°C. In Gilze-Rijen werd het die dag zelfs 35,1°C. Na 3 jaren op rij van droogte is het neerslagtekort nog steeds groot. Landelijk gemiddeld bedraagt het neerslagtekort nu 208 millimeter. De verschillen in het land zijn echter groot. In het noorden van Noord-Holland, Twente, Gelderland en grote delen van Noord-Brabant, Limburg en Zeeland is het neerslagtekort nog hoog, met op de droogste plaatsen een tekort van meer dan 300 millimeter.

Ontwikkeling van de weerbaarheid

Stijging waterpeil
In de eerste zesjaarlijkse herijking van het Deltaprogramma, het Deltaprogramma 2021, staan voorstellen voor herijkte deltabeslissingen, strategieën en maatregelen om effectief verder te werken aan waterveiligheid, de beschikbaarheid van zoetwater en een klimaatbestendige en waterrobuuste inrichting van Nederland in 2050.

Met het Deltaprogramma en de Nationale Klimaatadaptatiestrategie (NAS2016) werkt Nederland aan klimaatadaptatie. De ruimtelijke inrichting van Nederland moet tijdig klimaatbestendig en waterrobuust gemaakt worden, zodat Nederland in 2050 volledig is aangepast op klimaatverandering. Om het proces van ruimtelijke adaptatie te versnellen hebben de gezamenlijke overheden afspraken met elkaar gemaakt over het uitvoeren van stresstesten, het vastleggen van ambities en het opstellen van uitvoeringsprogramma's. Hoe maken we bijvoorbeeld onze wegen, vaarwegen, het hoofdwatersysteem en spoorwegen zo goed mogelijk weerbaar voor extremer weer? Stresstesten leggen de kwetsbaarheden bloot.

Droogte
Op 18 december 2019 is het eindrapport van de beleidstafel Droogte (in de beleidstafel werken alle betrokken waterpartners samen om afspraken te maken) verschenen. De extreem droge zomer van 2018, die dit jaar voortduurde in Oost- en Zuid-Nederland heeft ons waterbeheer op de proef gesteld. Bij de ruimtelijke inrichting van Nederland moeten we meer rekening gaan houden met de beschikbaarheid van zoetwater. Ook moeten waterbeheerders zich beter voorbereiden op drogere zomers. De ervaringen van de afgelopen drie droge jaren laten zien dat op de hoge zandgronden en delen van Zeeland een structurele aanpak van de droogteproblematiek nodig is omdat in die gebieden geen water vanuit de rivieren kan worden aangevoerd. Dat betekent dat er extra inzet van waterbeheerders en –gebruikers nodig is om het water beter vast te houden, te bergen en op te slaan. In laag Nederland is toenemende verzilting in verband met lage rivierafvoeren een aandachtspunt.

In het eindrapport van de beleidstafel Droogte staan 46 aanbevelingen om bij een neerslagtekort en lage rivierstanden toch genoeg water van voldoende kwaliteit te hebben voor ons drinkwater, de landbouw, de scheepvaart, de natuur en andere belanghebbenden. Deze aanbevelingen worden meegenomen bij het opstellen van het uitvoeringsprogramma Zoetwater voor 2022-2027. In 2019 zijn door het Deltaprogramma Zoetwater voor heel Nederland 150 kansrijke maatregelen in beeld gebracht en is gestart met verdere prioritering.

Ontwikkeling van de aanpak

Klimaatverandering
De Nederlandse overheid wil klimaatverandering tegengaan en stelt daarom het doel dat Nederland in 2030 49% minder CO2-uitstoot ten opzichte van 1990. Om deze doelstelling te realiseren, heeft het kabinet het pakket aan maatregelen voor het Klimaatakkoord vastgesteld en gepresenteerd op 28 juni 2019. Deze "klimaatmaatregelen" hebben impact op alle Nederlanders. In het akkoord staan meer dan 600 afspraken om de uitstoot van broeikasgassen tegen te gaan.

Het Klimaatakkoord gaat over de maatregelen die we de komende jaren nemen om dit doel te halen. We doen dit om klimaatverandering tegen te gaan zoals Nederland heeft afgesproken in het klimaatverdrag Parijs. Samen met 195 andere landen heeft Nederland zich gecommitteerd om in 2050 de opwarming van de aarde te beperken tot 2 graden Celsius, en zo mogelijk 1,5 graden Celsius.

Op 11 december 2019 presenteerde de Europese Commissie haar *European Green Deal* – een groeistrategie die de Europese Unie (EU) moet transformeren in een klimaatneutrale, circulaire en grondstofefficiënte unie, waarmee Europa concurrerend blijft. De Green Deal sluit op hoofdlijnen goed aan bij het nationale Klimaatakkoord, bij de inzet van het kabinet voor een circulaire economie, het beschermen van lucht- en waterkwaliteit, de ingezette transitie naar kringlooplandbouw en het versterken van biodiversiteit. Het kabinet verwelkomt deze integrale aanpak waarin alle sectoren een rol te spelen hebben. Het is belangrijk dat Nederland deze grote uitdagingen samen met de lidstaten van de Europese Unie het hoofd biedt. Alleen door samen te werken, kan Europa hierop effectief reageren en op het wereldtoneel een leidende rol spelen. De *Green Deal* zorgt daarbij voor een gelijker speelveld in de EU, hetgeen goed is voor het Nederlandse concurrentievermogen.

Extreem weer
Hittegolven, hevige neerslag, stormen, luchtverontreiniging en vulkaanas. De toenemende kwetsbaarheid voor dit soort extreme weersomstandigheden vraagt om vroegtijdige, op impact gebaseerde waarschuwingen en adviezen. Daarom ontwikkelt het KNMI de komende jaren een Early Warning Centre (EWC), een zogenaamd nationaal waarschuwingsadviessysteem. Met het EWC kan het KNMI een grotere bijdrage leveren aan de veiligheid en welvaart van Nederland en daarbuiten.

In het EWC ligt de nadruk op samenwerking, zowel op Europees als op nationaal niveau, met marktpartijen, kennisinstellingen en medeoverheden. Gericht op 24/7 monitoring waarbij snel wordt ingespeeld op domein-overschrijdende gebeurtenissen met nieuwe producten en dienstverlening.

Het Watermanagementcentrum Nederland (WMCN) werkt verder aan de op impact gebaseerde waarschuwingen voor overstromingsdreiging en ten behoeve van maatregelen om overstromingen te voorkomen. Hierbij komt meer informatie beschikbaar over de kans van optreden van extreme gebeurtenissen op (middel)lange termijn waardoor maatregelen bij daadwerkelijke overstromingsdreiging beter voorbereid kunnen worden. Ook de informatievoorziening voor de droogte-aanpak wordt verder verbeterd door veel meer informatie online beschikbaar te maken.

Tegengaan van CBRN-dreigingen

Korte samenvatting NVS 2019

Proliferatie
De proliferatie van massavernietigingswapens blijft een zorgelijke ontwikkeling. Sommige statelijke en niet-statelijke actoren voelen zich niet of steeds minder gebonden aan internationale afspraken. Inzicht in de intenties en capaciteiten van statelijke en niet-statelijke actoren die (mogelijk) beschikken over deze wapens en hun overbrengingsmiddelen is dan ook van groot belang. Binnen Nederland wordt samengewerkt tussen de inlichtingen- en veiligheidsdiensten, politie, het ministerie van Justitie en Veiligheid, het ministerie van Defensie, het RIVM, de Autoriteit Nucleaire Veiligheid en Stralingsbescherming, maatschappelijke instellingen en lokale overheden, voor een tijdige en adequate signalering van CBRN-middelen (inclusief precursoren). Tijdige signalering kan echter alleen plaatsvinden als ook externe signalering en preventie effectief zijn georganiseerd. Daartoe wordt onder meer intensief samengewerkt met buitenlandse partners, private instellingen en multilaterale instituties.

Stralingsongevallen
De kans op een stralingsincident bij een nucleaire installatie in Nederland is klein. Deze installaties zijn zeer veilig en voldoen aan strenge eisen. Er zijn ook andere stralingsincidenten mogelijk, met een grotere waarschijnlijkheid maar een kleinere impact. Voor het vervoer van radioactieve stoffen gelden bijvoorbeeld zeer strenge voorwaarden. Als er zich toch een incident voordoet, dan treden calamiteitenplannen in werking.

Ontwikkeling van de dreiging en de risico's

De dreiging zoals in de NVS beschreven blijft onverminderd groot. De verdere proliferatie van moderne wapens (inclusief chemische, biologische, radiologische en nucleaire wapens) kan gevolgen hebben voor de nationale veiligheid. Technologische ontwikkelingen en een groeiende, vrijelijke verspreiding van kennis en informatie, met name via internet, kunnen zowel niet-statelijke als statelijke actoren in toenemende mate de capaciteit geven om met name chemische en biologische middelen voor offensieve doeleinden te ontwikkelen. De vergiftiging met een chemisch wapen van de Russische oppositieleider Navalny, de zorgwekkende nucleaire ontwikkelingen in Iran, de opstelling van Noord-Korea en het vervallen van het nucleaire akkoord INF zijn enkele voorbeelden die aantonen hoe internationale wapenbeheersings-, ontwapenings- en non-proliferatiearchitectuur onder druk staan. De impact van een aanval of incident met CBRN-middelen is per definitie grensoverschrijdend, niet alleen in termen van veiligheid en directe schade maar ook politiek en diplomatiek.

Deze internationale rechtsorde wordt aangetast door politisering van en polarisering in multilaterale fora zoals de VN-Veiligheidsraad en het Non-proliferatieverdrag (NPV). Organisaties als het Internationaal Atoomagentschap (IAEA) en de Organisatie Chemische Wapens (OPCW) spelen een belangrijke rol voor informatie-uitwisseling en het opbouwen van capaciteit en weerbaarheid tegen CBRN risico's in lidstaten; hun werk is afhankelijk van internationale betrekkingen en de bereidheid om samen te werken.

Ontwikkeling van de weerbaarheid

Nederland zet zich in voor een gebalanceerde, proportionele en defensieve reactie van de NAVO op de Russische raketdreiging met een combinatie van druk met dialoog te handhaven en niet een destabiliserende wapenwedloop te voeden.

In het licht van de groeiende strategische instabiliteit (door de verzwakking van nucleaire wapenbeheersing enerzijds en door investeringen in nucleaire capaciteiten anderzijds, maar ook door veranderende machtsverhoudingen in de wereld en de opkomst van nieuwe technologieën) heeft Nederland onvermoeid en op alle niveaus gepleit voor behoud van het New START-verdrag om een ambitieuzer wapenbeheersingsverdrag met meer partijen en meer wapensystemen mogelijk te maken. De recent aangetreden regering in de VS heeft inmiddels met de Russische Federatie overeenstemming bereikt over de verlenging.

Gezien de steeds minder voorspelbare veiligheidscontext heeft Nederland in NAVO-verband *nuclear risk reduction* op de agenda gekregen als doelstelling en beleidsthema.

Inzet op attributie is onontbeerlijk voor relevantie en slagkracht van multilaterale organisaties als OPCW, zoals met betrekking tot het gebruik van chemische wapens in Syrië. Daarnaast is implementatie van sanctieregimes van belang om druk te kunnen uitoefenen op bijvoorbeeld Noord-Korea.

Ontwikkeling van de aanpak

De aanpak moet sterker inspelen op deze risico's en dreigingen door de versnippering in CBRN-kennis en capaciteit te verkleinen. De nauwe samenwerking tussen nationale spelers zoals de ANVS, het RIVM, TNO en de ministeries van Justitie & Veiligheid, Buitenlandse Zaken en Defensie blijft gehandhaafd om de impact en weerbaarheid verder te versterken. Nederland zet daarnaast met gelijkgezinde landen actief in op het handhaven en ontwikkelen van het multilaterale regime voor ontwapening en non-pro¬liferatie van massavernietigingswapens Het is belangrijk om coalities te vormen en kansen te creëren om de politisering en polarisatie tegen te gaan. Nederland zet daarnaast in op 'nieuwe' initiatieven zoals nucleaire risicobeheersing. Ook heeft Nederland oog voor de kansen en risico's van de inzet van nieuwe technologieën. De nauwe samenwerking tussen nationale spelers als de ANVS, het RIVM, TNO en het ministerie van Buitenlandse Zaken blijft gehandhaafd om maximale impact en weerbaarheid te verzekeren.

Infectieziektenbestrijding

Korte samenvatting NVS 2019

In Nederland is de last van infectieziekten in het algemeen relatief beperkt. Het risico van een uitbraak van een (ernstige) infectieziekte zoals een grieppandemie blijft echter reëel. De Rijksoverheid voert op strategisch niveau beleid uit om hierop voorbereid te zijn. Het voorkomen en bestrijden van zeer besmettelijke of ernstige infectieziekten bij mensen is vastgelegd in de Wet publieke gezondheid (Wpg). Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) is op grond van die wet verantwoordelijk voor het Rijksvaccinatieprogramma (RVP) dat door het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) wordt georganiseerd.

In 2005 hebben de lidstaten van de WHO (waaronder Nederland) afspraken gemaakt over de signalering en bestrijding van infectieziekten. Op initiatief van VWS heeft Nederland zich aangemeld voor een *Joint External Evaluation* (JEE) door de WHO. Tijdens de JEE zal Nederland worden beoordeeld op de voorbereiding op volksgezondheidsrisico's, waaronder infectieziekten.

Antibioticaresistentie
De opkomst van antibioticaresistentie is zorgwekkend en vraagt om een integrale en gecoördineerde aanpak. Met het in 2015 gestarte programma antibioticaresistentie (programma ABR) geeft de regering invulling aan een integrale en strategische aanpak van het probleem. Vergeleken met andere landen is de situatie in Nederland relatief goed. Het programma ABR liep tot en met 2019 en is door Berenschot positief geëvalueerd. Het beleid dat onder het programma is gestart wordt gecontinueerd.

Zoönosen
Afgelopen jaren zijn op het gebied van zoönosen (ziekten die van dier op mens overdraagbaar zijn) geen veranderingen waargenomen die de nationale veiligheid zouden kunnen raken. De Nederlandse Voedsel- en Warenautoriteit (NVWA) houdt toezicht en kan optreden. Ieder jaar publiceert het RIVM het rapport Staat van Zoönosen, met daarin informatie en ontwikkelingen over de zoönosen die voor Nederland van belang zijn. De ministeries van Landbouw, Natuur en Voedselkwaliteit en Volksgezondheid, Welzijn en Sport beschikken over een gezamenlijke crisisstructuur en gezamenlijke crisishandboeken voor zoönosen. Deze structuren worden regelmatig geoefend. Gelet op de ontwikkelingen en de impact van zoönosen op mens, dier en maatschappij, gaan beide ministeries vooruitblikken en breder bezien wat nodig is om zoönosen in de toekomst zoveel mogelijk te voorkomen. Daartoe wordt, samen met een expertgroep, in beeld gebracht wat nodig is in de breedte van volksgezondheid, diergezondheid en milieu om het risico op het ontstaan van zoönosen zoveel mogelijk te verkleinen.

Ontwikkeling van de dreiging en de risico's

Het risico van een uitbraak van een (ernstige) infectieziekte is reëel. De aandacht voor dit risico is als gevolg van de uitbraak van Covid-19 natuurlijk wel significant toegenomen. De uitbraak van Covid-19 bewijst dat infectieziekten grote impact kunnen hebben op veiligheidsbelangen zoals fysieke veiligheid, sociale en politieke stabiliteit en economische veiligheid.

De Horizonscan 2020 signaleert dat op de achtergrond verschillende ontwikkelingen een rol spelen bij deze pandemie. Zo maken globalisering en verstedelijking een snelle verspreiding van ziekten mogelijk. Verder geldt dat door vergrijzing de groep kwetsbaren toeneemt, wat bij een pandemie gevolgen kan hebben voor het aantal ziekenhuisopnames en sterfgevallen. Dit zien we bij Covid-19 terug. Daarbij geldt ook dat na Covid-19 de dreiging niet weg zal zijn, maar een nieuwe infectieziekte zich op een bepaald moment zal aandienen.

Voor de Horizonscan 2020 is vooral de respons op de uitbraak van Covid-19-crisis van belang. De ingrijpende maatregelen hebben maatschappelijke en economische effecten op langere termijn. Vanuit de nationale veiligheid gezien is het daarbij volgens de Horizonscan 2020 opvallend dat instrumenten zijn ingezet om het aantal slachtoffers te beperken die tegelijkertijd andere veiligheidsbelangen raken, namelijk verstoring van het dagelijks leven en aantasting van de economie.

Ontwikkeling van de weerbaarheid

Naar aanleiding van de Covid-pandemie vinden er evaluaties plaats op nationaal, Europees en internationaal niveau. In Nederland is de Onderzoeksraad voor Veiligheid een evaluatie gestart; ook wordt er vanuit verschillende kanten naar de Wpg gekeken om verbeteringen door te voeren. De WHO zal de huidige *International Health Regulations* (2005) evalueren en de EU heeft al voorstellen gedaan voor wijzigingen betreffende grensoverschrijdende gezondheidsdreigingen. Naar aanleiding van de evaluaties en (wets-)wijzigingen worden de komende jaren veel veranderingen verwacht op het gebied van infectieziektebestrijding.

Uit de huidige Covid-19 crisis kunnen lessen worden getrokken die ons beter kunnen voorbereiden op een volgende uitbraak. Als straks door alle *lessons learned* allerlei zaken zijn aangepakt, zoals beschikbaarheid van persoonlijke beschermingsmiddelen en opschaling van ic's, dan is de verwachting dat we inderdaad weerbaarder worden.

Ontwikkeling van de aanpak

Het bijstellen van de aanpak zal nodig zijn, maar dat zal vooral gebeuren naar aanleiding van de bovengenoemde evaluaties.

Generieke instrumenten voor de nationale veiligheid

Crisisbeheersing

Sinds het verschijnen van de Nationale Veiligheid Strategie 2019 is Nederland geconfronteerd met verschillende incidenten en crises die de noodzaak laten zien het stelsel van crisisbeheersing in Nederland voor te bereiden op de dreigingen van morgen. Deze zijn diverser, complexer en veelomvattender dan voorheen. De Covid-19 pandemie, maar ook uitdagingen als de aanslag in Utrecht op 18 maart 2019, het onbereikbaar worden van 112 op 24 juni 2019, de impact van toenemende droogte en hitte, digitale aantastingen als de problemen met CITRIX begin 2020 en de maatschappelijke onrust rond grote protesten in 2019 en 2020 illustreren de kwetsbaarheid van onze open samenleving. De in deze *midterm review* geschetste ontwikkeling van de dreigingen en risico's onderstrepen de noodzaak te blijven investeren in een toekomstbestendig crisisbeheersingsstelsel.

Als we de afgelopen periode als samenleving iets geleerd hebben, dan is dat het feit dat het beperken en beheersen van de impact van incidenten en crises 'teamwerk' is, waarbij alle betrokkenen (burger, bedrijven, overheden) een verantwoordelijkheid dragen om samen de klus te klaren.

Deze samenwerking vormgeven en ondersteunen is een van de belangrijkste uitdagingen waar overheden op nationaal en decentraal niveau voor staan. Met de uitvoering van de agenda Risico- en Crisisbeheersing 2018-2021 (zie onder meer voortgangsbrief[17]) en gerelateerde initiatieven als de Strategische agenda van het Veiligheidsberaad worden hier stappen in gezet. De versterking van de bovenregionale en landelijke samenwerking tussen onder meer Rijk, veiligheidsregio's en crisispartners is hier een belangrijk onderdeel van. Op basis van de recente adviezen van de commissie-Muller (Evaluatiecommissie Wet veiligheidsregio's), gepaard aan onderzoeksrapporten van recente crises en evaluaties van de Inspectie Justitie en Veiligheid, zal de komende jaren door alle betrokken partijen gewerkt worden aan toekomstbestendige crisisbeheersing. Het kabinet heeft de Tweede Kamer onlangs hierover in zijn reactie op het evaluatierapport van de commissie-Muller geïnformeerd.[18]

Ontwikkelingen gezamenlijk onderzoeksprogramma

De ministeries van Buitenlandse Zaken en Defensie en de NCTV voeren een gezamenlijk onderzoeksprogramma uit naar vraagstukken op het raakvlak van interne en externe veiligheid. Dit onderzoeksprogramma vloeit mede voort uit de kabinetsreactie op het WRR-rapport "Veiligheid in een wereld van verbindingen".[19] Het programma dient er onder andere toe om de kennisbasis te versterken en de uitkomsten dienen mede als basis voor interdepartementale strategievorming. Binnen dit programma zijn tot nu toe een viertal studies uitgevoerd: een studie naar de crisisbeheersingskennisinfrastructuur in Nederland (HCSS), een studie naar Artificial Intelligence (TNO), een studie naar het conceptueel kader voor een onderzoeksagenda op het gebied van de nexus tussen de interne en externe veiligheid (Clingendael) en een nationale veiligheidsstrategieën vergelijkende studie (RAND Europe).

17 Tweede Kamer 2019-2020, 30821, nr. 102.
18 Tweede Kamer 2020-2021, 29 517, nr. 198.
19 Tweede Kamer 2017-2018, 33 763, nr. 141.

Slotwoord en vooruitblik

Nederland is door zijn open samenleving in combinatie met verslechterde geopolitieke verhoudingen kwetsbaar. Dit manifesteert zich vooral in bedreigingen voor digitale veiligheid en economische veiligheid. Ook binnen onze samenleving worden dreigende tendensen zichtbaar. Ter bescherming van onze vrijheden, welvaart, openheid en internationale positie is een integrale aanpak van veiligheid essentieel, als bouwsteen van beleid.

Ten opzichte van de NVS 2019 laat deze *midterm review* geen onverwacht beeld zien in termen van dreigingen en risico's. Dat wil niet zeggen dat er niets aan de hand is met onze nationale veiligheid. De veiligheidssituatie van Nederland was immers ook in 2019 reeds verslechterd. Covid-19 heeft bestaande tegenstellingen verscherpt in beeld gebracht en ons extra geconfronteerd met onze afhankelijkheid van digitale middelen, maar ook van de ongestoorde werking van toeleveringsketens.

Onze veiligheidssituatie is daarmee verder verslechterd. Er zijn nationaal en internationaal meer en andere dreigingen ontstaan, terwijl bestaande dreigingen – zoals criminaliteit – een gedaanteverwisseling ondergaan. Soms verbinden dreigingen zich ook met elkaar, wat de complexiteit van onze veiligheidsuitdagingen nog eens vergroot.

Onveiligheid raakt steeds meer aspecten van de inrichting van ons land, van onze manier van leven en van onze plaats in de wereld. Om onze vrijheid, welvaart en internationale positie te beschermen is het hard nodig om anders naar onze veiligheid te gaan kijken.

Wij moeten slimmer worden omdat tegenstrevers dat ook worden. Wij moeten meer opties tot handelen bedenken om in te spelen op alle dreigingen. Wij moeten strategischer afwegingen maken over capaciteiten, voorraden en processen, willen wij op bepaalde terreinen een bepaalde mate van autonomie behouden. Wij moeten internationaal en binnen de EU-partnerschappen en samenwerking sterk en relevant houden of weer maken.

Veiligheid is een noodzakelijke voorwaarde voor onze manier van leven en hoort dus een vaste waarde in het kabinetsbeleid zijn. Doorgaan op de huidige weg betekent dat wij achter de sociale, technologische en geopolitieke ontwikkelingen aanlopen.

Wij moeten instrumenten verder ontwikkelen, bestaande instrumenten effectiever maken en nieuwe instrumenten ontwikkelen om kwetsbaarheden te verkleinen en dreigingen tegen te gaan. Denk hierbij aan manieren om polarisatie, radicalisering en extremisme te voorkomen; buitenlandse beïnvloeding te beteugelen; kennis en technologie te beschermen; strategische autonomie te waarborgen; of de veiligheid van het Koninkrijk in en buiten Europa te waarborgen.

Alleen een daadwerkelijk integrale benadering - die uiteenlopende aspecten van veiligheid verbindt - kan tegenwicht bieden aan de diverse dreigingen die op ons afkomen. Het op brede schaal versterken van onze weerbaarheid speelt daarbij een essentiële rol. Dit dient door onze hele samenleving heen en over onze grenzen heen te gebeuren, dus van digitale veiligheid tot sociale cohesie en van crisisbeheersing tot terrorismebestrijding. Verder verlangt het dringend een beter besef van burgers, bedrijven en instellingen dat nationale veiligheid ook hun zaak is geworden.

Deze andere manier van kijken naar veiligheid vraagt om een nieuwe benadering van veiligheid, ten eerste door de rijksoverheid. Inmiddels is het kabinet begonnen met de voorbereiding van een rijksbrede periodieke geïntegreerde veiligheidsanalyse. De uitkomsten van deze analyse dienen als voeding voor de rijksbrede strategische inzet op het gebied van interne en externe veiligheid en de optimale verbinding tussen die twee. Het kabinet kan zich voorstellen dat de rijksbrede strategische inzet in binnen- en buitenland ten behoeve van de (inter-)nationale veiligheid op termijn vorm krijgt in een daadwerkelijk geïntegreerde, rijksbrede veiligheidsstrategie, die de bestaande strategieën op dit gebied (de NVS en de GBVS) gaat vervangen. Vanzelfsprekend is dit besluit aan een nieuw kabinet.

Omdat nationale veiligheid niet alleen een zaak van de rijksoverheid is en kan zijn, is nauwere samenwerking geboden tussen het rijk en lokale overheden; tussen civiele en militaire instanties; tussen publieke en private organisaties; en met gelijkgezinde internationale partners (bilateraal, multilateraal of in coalities). Het is de ambitie van het kabinet om de ontwikkeling van de volgende veiligheidsstrategie vanuit deze partnerschappen te starten. Verhoogde weerbaarheid van bedrijven en burgers, waar nodig gesteund en gestimuleerd door de overheid, draagt immers ook bij aan de nationale veiligheid.

Deze publicatie is een uitgave van de NCTV namens de Rijksoverheid

info@nctv.minjenv.nl