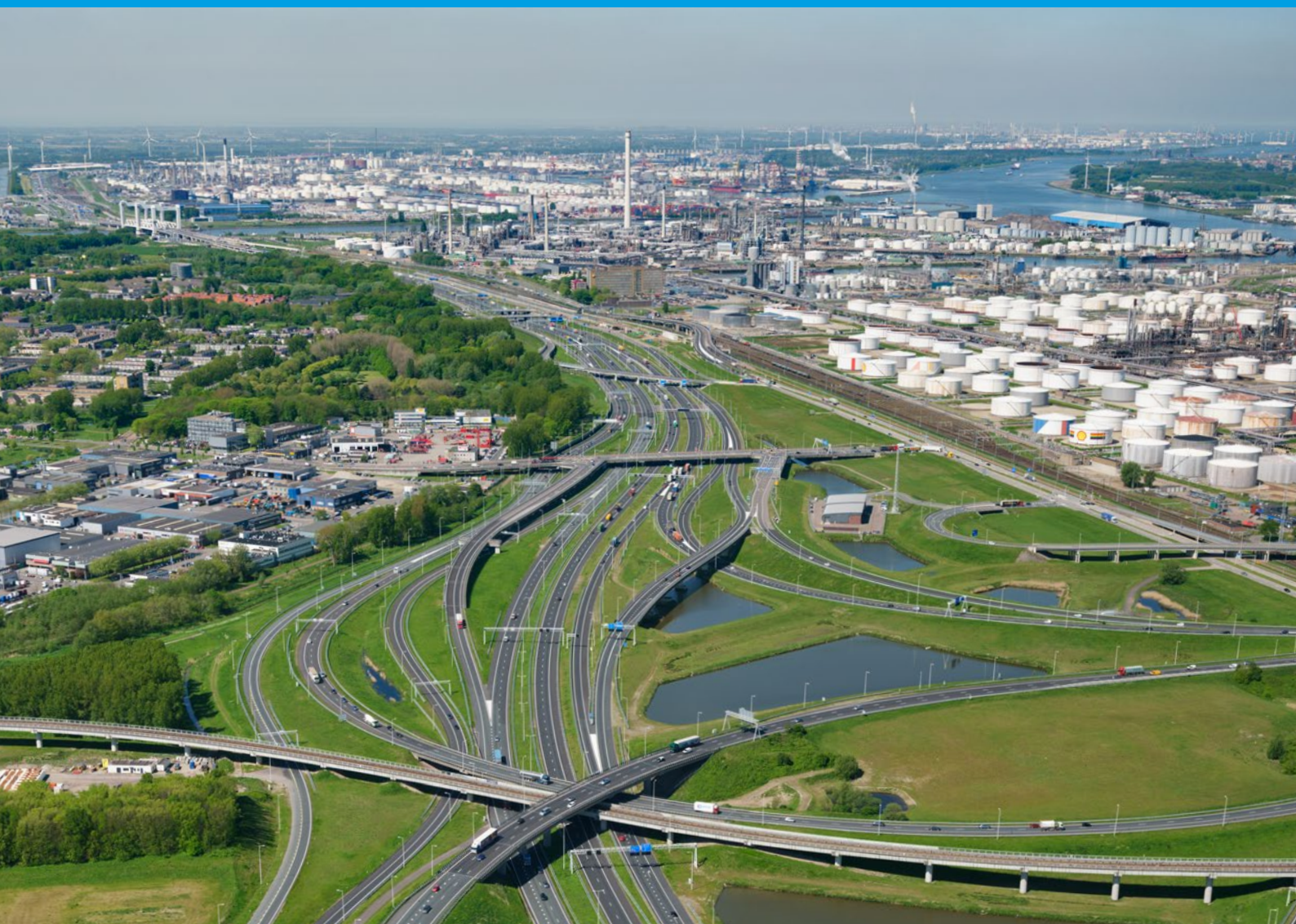
Nationale Veiligheid Strategie

2019

Inhoudsopgave



Samenvatting

Nationale veiligheid is een dynamisch en veelzijdig begrip, dat vraagt om een aanpak die robuust en flexibel is. In deze Nationale Veiligheid Strategie (NVS) staat wat de nationale veiligheidsbelangen zijn die we moeten beschermen, hoe die belangen op dit moment worden bedreigd en op welke wijze we deze risico's en dreigingen het hoofd bieden.

Met de strategische cyclus van de Nationale Veiligheid Strategie, die dit proces iedere drie jaar herhaalt, is Nederland in staat om zich te blijven beschermen tegen de ontwikkeling van dreigingen en risico's en wordt de nationale veiligheidsaanpak toekomstbestendig versterkt.

Voorkomen van maatschappelijke ontwrichting en beschermen van de democratische rechtsorde

We onderscheiden hiervoor zes nationale veiligheidsbelangen:

1. *Territoriale veiligheid*
2. *Fysieke veiligheid*
3. *Economische veiligheid*
4. *Ecologische veiligheid*
5. *Sociale en politieke stabiliteit*
6. *Internationale rechtsorde*

De nationale veiligheid is in het geding wanneer een of meerdere nationale veiligheidsbelangen zodanig bedreigd worden, dat er sprake is van (potentiële) maatschappelijke ontwrichting. Nederland is voor het realiseren van de nationale veiligheid meer dan ooit afhankelijk van het functioneren van het internationale stelsel van normen en afspraken. Daarom is *het functioneren van de internationale rechtsorde* toegevoegd als nationaal veiligheidsbelang. Dit veiligheidsbelang staat niet op zichzelf, maar is nauw verweven met de andere vijf veiligheidsbelangen en met andere belangen en waarden van de Nederlandse samenleving. Alle veiligheidsbelangen kunnen ook via de digitale ruimte geraakt worden: digitale veiligheid is daarom verweven in alle belangen. De beschikbaarheid, vertrouwelijkheid en integriteit van essentiële informatiediensten is in deze NVS toegevoegd als criterium voor territoriale veiligheid en daarmee onderdeel van de nationale veiligheid.

Strategische agenda die periodiek getoetst wordt

Met deze NVS start een strategische cyclus, die periodiek wordt herhaald om te blijven toetsen of de bescherming van de nationale veiligheidsbelangen in de pas loopt met ontwikkelingen en dreigingen of risico's die de nationale veiligheid kunnen raken. Deze cyclus kent een omlooptijd van drie jaar, maar wordt tussentijds herijkt aan eventuele nieuwe ontwikkelingen en dreigingen of risico's voor de nationale veiligheid. De NVS vervult op deze wijze de functie van strategische agenda, die in kaart brengt welke dreigingen en risico's de nationale veiligheid bedreigen en in hoeverre er is voorzien in een integrale aanpak om de dreiging te verminderen en de weerbaarheid te vergroten. Deze inzet kan in de loop der tijd zodoende veranderen, en heeft daarmee een flexibel karakter.

Versterkte aanpak van risico's

De huidige ontwikkeling van dreigingen en risico's laat zien dat de volgende veiligheidsvraagstukken vragen om een versterkte aanpak:

- **Statelijke dreigingen** worden aangepakt. Deze aanpak bestaat uit generieke maatregelen, gericht op het verhogen van de weerbaarheid tegen verschillende uitingen van statelijke dreigingen.
- **Polarisatie** kan onze open samenleving ondermijnen. Om polarisatie tegen te gaan wordt ingezet op een brede overkoepelende aanpak gericht op de bevordering van samenleven. Gemeenten, maatschappelijke organisaties en de veiligheidsketen leveren hieraan een belangrijke bijdrage.

- Veel dreigingen en risico's kunnen leiden tot verstoring van de **vitale infrastructuur**. Om deze te beschermen, zet het kabinet in op een versterkte aanpak om kennis, kunde en expertise te bundelen om nationale veiligheidsrisico's ten behoeve van de vitale infrastructuur adequaat te adresseren.
- Bestrijding van **terrorisme en extremisme** vergt onverminderd de aandacht. Het is van groot belang de versterkte inzet waar nodig op basis van actuele dreigingsbeelden te intensiveren. Daarnaast zal er 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.
- Nederland kan **militaire dreigingen** alleen tegengaan door effectieve samenwerkingen en actief internationaal beleid, in onder andere 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.
- In de aanpak van **ondermijnende criminaliteit** wordt ingezet op een breed pakket van maatregelen in een coalitie van overheid, bedrijfsleven en samenleving. Daarnaast is er een ambitieuze wetgevingsagenda, waarin goed rekening wordt gehouden met zowel wensen vanuit de uitvoeringspraktijk als met rechtsstatelijke uitgangspunten. Zo wordt, samen met alle betrokken partners in het veld, een stevige impuls gegeven aan de aanpak van ondermijnende criminaliteit.
- Dreigingen en risico's rondom **cybersecurity en digitale dreigingen** worden door het kabinet op geïntegreerde wijze geadresseerd met de Nederlandse Cyber Security Agenda (NCSA) uit april 2018[1]. Deze is flexibel vormgegeven, zodat nieuwe of toenemende dreigingen adequaat het hoofd kunnen worden geboden.

Versterkte inzet betekent dat de dreiging van dien aard is dat het onderwerp – geïntegreerd, maar binnen de reeds bestaande taken en verantwoordelijkheden van betrokken organisaties – extra aandacht behoeft om de geïdentificeerde dreigingen of risico's het hoofd te blijven bieden. De genoemde versterkte inzet behoeft, onder verantwoordelijkheid van de betrokken vakdepartementen, nog wel nadere concretisering.

Onverminderde inzet op weerbaarheid

De ontwikkeling van dreigingen en risico's laat zien dat onderstaande veiligheidsvraagstukken een onverminderde inzet vragen. Op hoofdlijnen is die is als volgt:

- Nederland zet internationaal in op het behoud en het **versterken van multilaterale stelsels**, met afspraken en regels die gebaseerd zijn op universele waarden. Deze inzet is verder uitgewerkt in de Geïntegreerde Buitenland- en Veiligheid Strategie (GBVS).[2]
- Met het oog op **bestrijding en voorkoming van natuurrampen** richt de inzet zich op klimaatverandering, droogte, stijging van het waterpeil, natuurbranden, aardbevingen, bodemdaling en zonnestormen. Er worden onder andere maatregelen genomen die gericht zijn op CO_2-reductie en op een klimaatbestendig grond- en oppervlaktewatersysteem, ruimtelijke inrichting en grondgebruik. Nederland blijft zich inzetten om de doelstellingen van het akkoord van Parijs te halen. 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. In het kader van natuurrampen als bosbranden en aardbevingen volstaat de gebruikelijke crisisvoorbereiding op lokaal, regionaal en nationaal niveau. Er worden veel maatregelen genomen om de kans op aardbevingen in verband met de Groningse gaswinning en de gevolgen ervan te verminderen. In het geval van een aardbeving staat het systeem van crisisbeheersing paraat.
- Aangezien de potentiële impact van **CBRN**-conflicten of incidenten op de Nederlandse nationale veiligheidsbelangen groot is, heeft deze dreiging onze onverminderde aandacht. Een ander belangrijk element in de aanpak is het verhogen van de maatschappelijke weerbaarheid tegen eventuele CBRN-incidenten.
- In Nederland is de last van **infectieziekten** relatief beperkt. De opkomst van antibioticaresistentie is echter zorgwekkend en kent daarom een integrale en gecoördineerde aanpak. Afgelopen jaren zijn er voor besmettelijke dierziekten en zoönosen geen significante veranderingen waargenomen die de nationale veiligheid zouden kunnen raken.

1 Kamerstukken 2017-2018, 26643, nr. 536.

2 Kamerstukken 2017-2018, 33694, nr. 12.

Generiek instrumentarium ontwikkelen

Naast de aanpak van voornoemde dreigingen en risico's, zet Nederland in op het versterken van een aantal generieke instrumenten voor de bescherming van de nationale veiligheid, zoals het **generieke systeem van risico- en crisisbeheersing**, om (dreigende) incidenten en crises adequaat en eenduidig het hoofd te bieden. Daarnaast wordt de ontwikkeling van **kennis en wetenschappelijk onderzoek naar dreigingen en risico's** geïntegreerd en zullen **nieuwe technologieën en hun toepassingsmogelijkheden** gemonitord worden op risico's voor de nationale veiligheid. Tot slot wordt de **cyclus van de NVS** periodiek herhaald en ontwikkeld. De volgende NVS is beoogd in 2022 en kan, wanneer de ontwikkeling van dreigingen en risico's hiertoe aanleiding geven, tussentijds worden aangepast.

Figuur 1 **De drie pijlers van de veiligheidsaanpak in de GBVS**

Inleiding

Nederland is volop in ontwikkeling. Technologische ontwikkelingen gaan snel en mensen, producten, organisaties en informatie raken meer en meer met elkaar verbonden. Dit betekent dat nationale en internationale ontwikkelingen meer dan ooit met elkaar verweven zijn.

Klimaatverandering door de opwarming van de aarde stelt ons voor nieuwe uitdagingen. Naast kansen voor economische groei en maatschappelijke ontwikkeling, leiden deze ontwikkelingen ook tot nieuwe dimensies bij veiligheidsvraagstukken. Bovendien kunnen nieuwe (digitale) dreigingen zich soms snel ontwikkelen, en gevolgen hebben voor *safety* en *security*.

Om de nationale veiligheid te beschermen, behoort Nederland daarom te beschikken over een dynamische veiligheidsaanpak, die kan meebewegen met de ontwikkelingen en dreigingen of risico's[3] en mate van weerbaarheid. De Nationale Veiligheid Strategie (NVS) biedt een overzicht van dreigingen en risico's, urgentie ten aanzien van de mate van weerbaarheid en samenhang in de aanpak van de nationale veiligheid, en draagt zo bij aan het beschermen van de maatschappelijke continuïteit en de democratische rechtsorde.[4]

Nauw verbonden met de GBVS, Defensienota en overige strategieën

De Nationale Veiligheid Strategie (**NVS**) verbindt de internationale, nationale en lokale inzet ter bescherming van de nationale veiligheid. Waar opportuun, verwijst de NVS naar onderliggende deelstrategieën waarin de strategische inzet op de aanpak van specifieke dreigingen en risico's is opgenomen, zoals bijvoorbeeld de Contraterrorisme strategie en de Nederlandse Cybersecurity Agenda (NCSA), maar ook het Deltaprogramma en de kamerbrief Tegengaan Statelijke Dreigingen. De NVS geeft, in nauwe samenhang met de Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS) en de Defensienota, de strategische inzet weer op nationaal niveau. Hierbij besteedt de NVS specifieke aandacht aan de raakvlakken met Nederlandse inzet in het buitenland. Gebeurtenissen buiten Nederland kunnen immers significante gevolgen hebben voor de (organisatie van) veiligheid in Nederland. Dit plaatst de nationale veiligheid nadrukkelijker in een internationaal verband, zoals ook in het rapport 'Veiligheid in een wereld van Verbindingen' van de Wetenschappelijke Raad voor het Regeringsbeleid is opgemerkt. De toegenomen verwevenheid van interne en externe veiligheid en de noodzaak tot een meer geïntegreerde benadering van de nationale veiligheid krijgt zijn beslag in de NVS.

De veiligheidsaanpak in de **GBVS** is gestoeld op drie pijlers: Voorkomen, Verdedigen, en Versterken. Daarbinnen worden specifieke doelen gedefinieerd om de komende jaren urgente dreigingen het hoofd te bieden. De inzet is een anticiperende, preventieve veiligheidsaanpak gericht op de lange termijn. De strategie focust op het voorkomen van onveiligheid waar mogelijk. Evenals een effectieve en moderne aanpak van het verdedigen van Nederland tegen onveiligheid waar noodzakelijk. Dit betreft onder andere geloofwaardige afschrikking in bondgenootschappelijk verband en aandacht voor de grondoorzaken van terrorisme, irreguliere migratie, armoede en klimaatverandering, zoals in het regeerakkoord benoemd. Ten slotte is het versterken van het veiligheidsfundament – de bevordering van de internationale rechtsorde en een effectief multilateraal systeem – cruciaal voor de veiligheid van het Koninkrijk. De Defensienota 2018 hanteert drie uitgangspunten:

- **Veilig blijven** – in het Koninkrijk en Europa
- **Veiligheid brengen** – rondom Europa
- **Veilig verbinden** – van het knooppunt Nederland en de aan- en afvoerlijnen

3 De termen 'dreiging' en 'risico' worden in dit document naast elkaar gebruikt en als elkaar aanvullende begrippen gezien. Een 'risico' wordt omschreven als: 'het samenspel van de waarschijnlijkheid dat een incident zich voordoet en de impact die dat kan hebben'. 'Dreiging' wordt gerelateerd aan aanwezigheid, concreetheid en acuutheid van gevaar (soms nog als een stip aan de horizon die via early warning onderkend moet worden). Bij 'dreiging' gaat het dus om aanwezig en aanwijsbaar gevaar, bij 'risico' om potentieel gevaar.

4 Waaronder wordt begrepen: het van rechtsstatelijke en democratische waarborgen voorziene fundament van de Nederlandse samenleving.


SAMSUNG
SAMSUNG

De cyclus van de nationale veiligheid

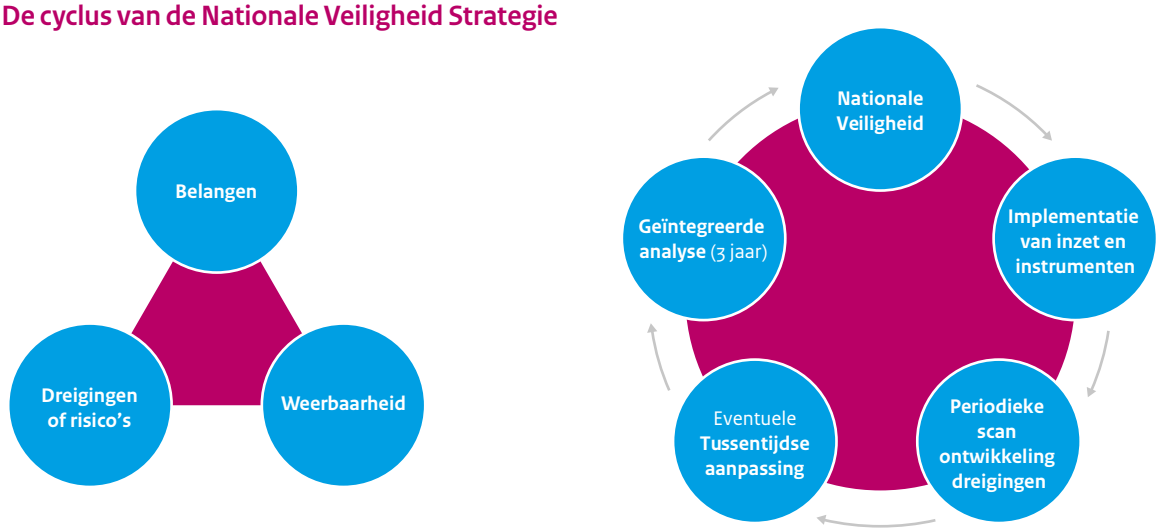
De NVS vervult de functie van strategische agenda, gericht op het voorkomen van maatschappelijke ontwrichting en het beschermen van de democratische rechtsorde. In deze agenda wordt weergegeven wat er nu aan inzet nodig is om, gegeven de ontwikkeling van dreigingen en risico's, de nationale veiligheid te beschermen. Deze inzet kan in de loop der tijd zodoende veranderen, en heeft daarmee een flexibel karakter.

Met deze NVS start een nieuwe strategische cyclus, die periodiek herhaald wordt om continu te toetsen of de bescherming van de nationale veiligheidsbelangen in de pas loopt met ontwikkelingen van dreigingen en risico's die de nationale veiligheid kunnen raken. In de NVS staat wat de belangen zijn die we moeten beschermen, hoe die belangen op dit moment worden bedreigd en op welke wijze we deze dreigingen of risico's het hoofd bieden.

Identificeren van nationale veiligheidsbelangen

De strategische cyclus start met het identificeren van de nationale veiligheidsbelangen die, wanneer ze in ernstige mate geraakt worden, kunnen leiden tot maatschappelijke ontwrichting, waaronder schade aan de democratische rechtsorde. Deze belangen zijn methodisch uitgewerkt in impactcriteria die inzichtelijk maken in welke mate de belangen geschaad kunnen zijn. De belangen en hun uitwerking zijn onderdeel van de methodiek van het Analistennetwerk Nationale Veiligheid (ANV). Het ANV is een multidisciplinair netwerk van kennisinstellingen dat als doel heeft de continuïteit, borging van kennis en multidisciplinaire aanpak rondom analyses op het gebied van nationale veiligheid te versterken.

Figuur 2 **De cyclus van de Nationale Veiligheid Strategie**



Ontwikkelingen en dreigingen of risico's in kaart brengen

Wanneer de nationale veiligheidsbelangen gedefinieerd zijn, wordt vervolgens in een onafhankelijke analyse in kaart gebracht welke veiligheidsontwikkelingen en dreigingen of risico's hierop van invloed zijn. Deze analyse integreert bestaande (deel-)analyses zoals het Cybersecuritybeeld Nederland, het dreigingsbeeld terrorisme Nederland, de strategische monitor, het Nationaal Veiligheidsprofiel en rapportages van de inlichtingen- en veiligheidsdiensten. Deze geïntegreerde analyse geeft zo een *all hazard*, *safety* én *security* beeld van de belangrijkste dreigingen en risico's voor de nationale veiligheid weer, waarbij de interne en externe veiligheidsdimensie met elkaar worden verbonden. Om tussentijdse ontwikkelingen in het dreigingsbeeld adequaat het hoofd te kunnen bieden, wordt een *mid-term* scan uitgevoerd om te bezien of er aanpassing van of aanvulling op de NVS noodzakelijk is.

Strategische inzet op weerbaarheid

De NVS is gericht op het waarborgen van de weerbaarheid van Nederland: het vermogen om dreigingen of risico's adequaat het hoofd te bieden. Hierbij worden alle partijen betrokken die een (deel)verantwoordelijkheid hebben in preventie, 'pro-actie', preparatie, respons en nazorg (integraliteit). Met de dreigings- en risicoanalyse als basis, worden in de NVS de volgende vragen op hoofdlijnen beantwoord:

1. *Beschikt Nederland over een geïntegreerde aanpak om deze dreiging of dit risico het hoofd te bieden?*
2. *Voldoet deze aanpak, gegeven de ontwikkeling van de dreiging of het risico, om Nederland weerbaar(der) te maken?*

Daar waar aanvullende inzet op de aanpak van een dreiging of risico noodzakelijk is, wordt dit zichtbaar in deze afweging en opgenomen in de NVS. Dit betekent echter **niet** dat wanneer een dreiging of risico geen aanvullende inzet vergt, de dreiging of het risico tegen de nationale veiligheid daarmee afgenomen is. De constatering dat de huidige aanpak afdoende is, gaat uit van de onverminderde (bestaande) inzet op het verhogen van de weerbaarheid tegen deze dreiging.

Nationale veiligheid als begrip

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.

Nederland hanteert bovenstaande definitie van nationale veiligheid. Twee essentiële elementen vormen de afbakening:

1. *De Nederlandse vitale, ofwel nationale veiligheidsbelangen, dienen in het geding te zijn;*
2. *en de bedreiging van deze belangen dient dermate ernstig te zijn, dat sprake is van (potentiële) maatschappelijke ontwrichting.*

Zes nationale veiligheidsbelangen

We onderscheiden de volgende nationale veiligheidsbelangen:

1. Territoriale veiligheid	Het ongestoord functioneren van Nederland en haar EU- en NAVO-bondgenoten als onafhankelijke staten in brede zin, dan wel de territoriale veiligheid in enge zin.
2. Fysieke veiligheid	Het ongestoord functioneren van de mens in Nederland en zijn omgeving.
3. Economische veiligheid	Het ongestoord functioneren van Nederland als een effectieve en efficiënte economie.
4. Ecologische veiligheid	Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland.
5. Sociale en politieke stabiliteit	Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtstaat en daarin gedeelde waarden.
6. Internationale rechtsorde	Het functioneren van het internationale stelsel van normen en afspraken, gericht op internationale vrede en veiligheid.

Nationale veiligheid kan ook via de digitale ruimte[5] geraakt worden; digitale veiligheid is daarom verweven in alle andere veiligheidsbelangen. Daarbij is de integriteit van de digitale ruimte toegevoegd als uitwerking van territoriale veiligheid, waaronder begrepen beschikbaarheid, vertrouwelijkheid en integriteit van essentiële informatiediensten. Wanneer deze in ernstige mate geraakt of bedreigd worden, kan maatschappelijke ontwrichting ontstaan. Voorbeelden van dreigingen hiertegen zijn digitale aanvallen gericht op sabotage of spionage, maar ook uitval door moedwillige of natuurlijke oorzaken.

Hoe deze belangen kunnen worden geschaad, is uitgewerkt in zogeheten impactcriteria (zie daarvoor bijlage 2). Deze criteria maken – op basis van ernst en waarschijnlijkheid – inzichtelijk wat de mogelijke gevolgen voor de nationale veiligheidsbelangen zijn. De weging van deze elementen is echter meer dan een simpele optelsom. We zien dat sommige dreigingen of risico's een meer sluipend effect kunnen hebben. Of dat uitingsvormen van meerdere dreigingen of risico's in zichzelf niet ernstig zijn, maar dat het geheel een ondermijnend effect kan hebben op de democratische rechtsorde en daarmee in potentie kan leiden tot

5 Het conglomeraat van ict-middelen en –diensten dat alle entiteiten die digitaal verbonden kunnen zijn bevat permanente, tijdelijke en plaatselijke verbindingen, en gegevens die zich in dit domein bevinden (o.a. data, programmacode en informatie), waarbij geen geografische beperkingen zijn gesteld.

maatschappelijke ontwrichting. Ook moeten we ons rekenschap blijven geven van het feit dat de maatschappij verandert en daarmee de weerbaarheid ook. Zo kan iets waar nu de schouders over worden opgehaald, op termijn tot maatschappelijke onrust leiden. Tegelijkertijd behoort de overheid terughoudend te zijn met het identificeren van maatschappelijke ontwikkelingen als een dreiging voor de nationale veiligheid. Zeker wanneer deze ontwikkelingen zich binnen een open en democratische samenleving ontplooien. De aard van nationale veiligheid impliceert immers dat de ernst van dit algemene belang rechtvaardigt dat de overheid, indien nodig, zich met alle instrumenten in zal spannen om maatschappelijke ontwrichting te voorkomen.Dit vraagt telkens weer om zorgvuldige weging op basis van transparante criteria, die in de definitie van nationale veiligheid zijn verankerd.

De internationale rechtsorde als belang; nationale veiligheid als invalshoek

Nederland is van oudsher een sterk internationaal verbonden land, met fysieke en digitale knooppunten. Denk hierbij aan de haven in Rotterdam en de luchthaven Schiphol, de toegang tot de trans-Atlantische zeekabel en een van de grootste *internet exchanges* van Europa. Nederland is door die verbindingen en de mogelijke effecten van internationale dreigingsontwikkeling meer dan ooit afhankelijk van het functioneren van het internationale stelsel van normen en afspraken en voor het beschermen van de nationale veiligheid. Daarom is **het functioneren van de internationale rechtsorde** toegevoegd als nationaal veiligheidsbelang. Dit veiligheidsbelang staat niet op zichzelf, maar is nauw verweven met de andere vijf veiligheidsbelangen en met andere belangen en waarden van de Nederlandse samenleving.

Het internationale stelsel van normen en afspraken is een robuust geheel, dat niet bij iedere aantasting schade toebrengt aan de Nederlandse nationale veiligheid. Daarom geldt vooral voor het functioneren van de internationale rechtsorde, dat er sprake moet zijn van **ernstige of zeer ernstige** aantasting of het komen te vervallen van de internationale rechtsorde, wat kan leiden tot maatschappelijke ontwrichting, voordat het de nationale veiligheid direct raakt. Deze impactcriteria zijn door het ANV uitgewerkt en opgenomen in de systematiek van de risicoanalyse

Maatschappelijke ontwrichting

Het tweede deel van de definitie van nationale veiligheid gaat over maatschappelijke ontwrichting. Dit betekent dat een ontwikkeling pas bedreigend is voor de nationale veiligheid wanneer deze dermate ernstig is dat er sprake is van (potentiële) maatschappelijke ontwrichting en/of de continuïteit van de samenleving in het geding is. Dit komt bijvoorbeeld tot uiting in het wegvallen van sociale of politieke stabiliteit, maar kan zich ook voordoen wanneer de ecologische leefomgeving in ernstige mate geraakt wordt of het basisvertrouwen in het functioneren van de samenleving wegvalt.

Maatschappelijke ontwrichting omvat daarmee een fysiek aspect, dat zich kan uiten in aantallen slachtoffers, schade of uitval van vitale functies. Daarnaast heeft het ook een sociaalpsychologisch aspect, zoals verstoring van het dagelijks leven, handelingsperspectieven tijdens en na het zich voordoen van de dreiging of risico, verwachtingspatronen over verwijtbaarheid, legitimiteit van beleid (billijkheid) en vertrouwen in herstel.[6] Maatschappelijke ontwrichting dreigt ook wanneer de continuïteit of beschikbaarheid van vitale processen wordt geraakt. Deze processen vormen samen de Nederlandse vitale infrastructuur. Transport en distributie van elektriciteit, toegang tot internet en levering van drinkwater zijn voorbeelden van vitale processen. Tot slot kan maatschappelijke ontwrichting ook sluipenderwijs ontstaan. Denk daarbij bijvoorbeeld aan criminele ondermijning of aantasting van de democratische rechtsorde met verlies van vertrouwen in instituties als gevolg.

Verschillende dimensies van nationale veiligheid

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) maakt in zijn rapport 'Veiligheid in een Wereld van verbindingen' onderscheid tussen de dimensies national security, human security en flow security. Door het prisma van de nationale veiligheidsbelangen centraal te stellen in de aanpak van nationale veiligheid worden deze dimensies alle drie door deze NVS gedekt.

Internationale beleidsvergelijking

Een verkenning van de nationale veiligheidsstrategieën van soortgelijke landen[7] leert dat daarin veelal dezelfde dreigingen of risico's worden gesignaleerd die kunnen leiden tot maatschappelijke ontwrichting: terrorisme, cybersecurity en klimaatverandering zijn gedeelde, terugkerende dreigingen. Andere landen omvatten in grotere mate de effecten van internationale problematiek op nationale veiligheid. Bijvoorbeeld effecten van mislukte staten, falende governance en instabiliteit in en aan de randen van hun invloedssfeer. Dergelijke effecten van internationale problematiek op de nationale veiligheid zijn voor de Nederlandse context uitgewerkt in de Geïntegreerde Buitenland- en Veiligheidsstrategie.

6 Uit: Maatschappelijke ontwrichting en overstromingen (2014), Planbureau voor de Leefomgeving.

7 Duitsland, Zweden, het Verenigd Koninkrijk, de Verenigde Staten, Australië, Canada, Frankrijk en België.

Uitgangspunten: veiligheid als gezamenlijke verantwoordelijkheid

In onze democratische rechtsstaat is het belangrijk dat mensen en maatschappelijke organisaties zich in vrijheid en veiligheid kunnen ontplooien. Het zorgen voor deze veiligheid is een kerntaak van de overheid. Alleen dan kunnen de waarden van de democratische rechtsstaat en de grondwettelijke vrijheden beschermd worden. Tegelijkertijd is deze veiligheid niet (meer) alléén te realiseren door de overheid. Ook het bedrijfsleven, maatschappelijke organisaties en burgers hebben een belangrijke rol bij het zorgen voor (nationale) veiligheid en het bevorderen van de weerbaarheid. De overheid heeft hierin een regierol en dient herkenbaar, transparant en rolvast op te treden bij dreigingen of risico's. Daarbij gelden de volgende uitgangspunten:

- **De overheid draagt zorg voor het beschermen en bevorderen van de nationale veiligheid**, zodat mensen en maatschappelijke organisaties zich in vrijheid en veiligheid kunnen ontplooien binnen onze democratische rechtsstaat. Vanzelfsprekend opereert de overheid rechtsstatelijk in het beschermen van de nationale veiligheid.
- **Nederland zet hierbij in op een maatschappijbrede aanpak**, waarbij overheidsorganisaties, veiligheidsdiensten, het bedrijfsleven en maatschappelijke organisaties samenwerken aan de nationale veiligheid.[8] In de implementatie en ontwikkeling van de NVS-systematiek worden al deze partijen betrokken. Ook wordt ingezet op vergroten van *awareness* en het formuleren van handelingsperspectief voor de dominante risico's. Zelfredzame en mondige burgers organiseren ook veel zelf. De overheid staat in deze aanpak voor de publieke belangen, stimuleert de eigen verantwoordelijkheid van partijen en geeft het goede voorbeeld.
- **Nederland zet in op het vroegtijdig detecteren en signaleren van risico's en dreigingen** voor de nationale veiligheid. Dit betekent dat informatiedeling tussen publieke partijen onderling en tussen publieke en private partijen zoveel mogelijk wordt bevorderd. Deze informatiedeling dient evenwel binnen de geldende wettelijke kaders en waarborgen versterkt te worden.
- **100% veiligheid bestaat niet.** Schokkende gebeurtenissen zijn niet altijd te voorkomen of te voorzien, ongeacht de inspanningen van alle betrokken partijen. Nederland zet zich in om zoveel mogelijk dreigingen en risico's te voorkomen, en waar ze zich voordoen, adequaat en snel te kunnen reageren. Ook wordt geleerd van incidenten, door te evalueren en waar nodig beleids- en planvorming aan te passen. Zo blijft de Nederlandse veiligheidsaanpak zich ontwikkelen.
- **De nationale veiligheidsaanpak is geïntegreerd en beweegt mee** met de ontwikkeling van de dreigingen of risico's en weerbaarheid.[9] Daarbij is het maken van **keuzes onvermijdelijk;** als de samenleving geen enkel risico zou accepteren, worden veiligheidsmaatregelen al snel draconisch en onbetaalbaar.
- **Nationale veiligheid houdt niet op bij de landsgrenzen:** internationale ontwikkelingen hebben een toenemende weerslag op de nationale veiligheid. Interne en externe veiligheid zijn meer en meer met elkaar verweven en vragen om meer integratie van de nationale veiligheidsaanpak. Niet alleen in het fysieke, maar ook in het digitale domein. Waar mogelijk werkt Nederland daarom ook in Europees of breder internationaal verband aan het versterken van de eigen nationale veiligheid en het beschermen van de Nederlandse veiligheidsbelangen. Deze internationale inzet is vastgelegd in de GBVS.

8 Zo wordt bijvoorbeeld in de aanpak cybersecurity nadrukkelijk verbinding gezocht met het bedrijfsleven en in de aanpak tegengaan radicalisering met lokale overheden en maatschappelijke organisaties.

9 Bij weerbaarheid hoort ook de ontwikkeling van de dreigingsperceptie, zoals beschreven in het WODC-rapport *Op weg naar een weerbare open samenleving*, Kamerstukken 2018/19, 30821, nr. 52.

Trends en ontwikkelingen die de nationale veiligheid beïnvloeden

Nederland is een open samenleving, waarin mensen kunnen profiteren van maatschappelijke en economische ontwikkelingen. Digitalisering, technologische ontwikkeling en de internationale oriëntatie van Nederland bieden Nederlandse burgers en bedrijven veel kansen.

Tegelijkertijd maakt de openheid en internationale verbondenheid van Nederland dat interne en externe ontwikkelingen onze nationale veiligheid op termijn kunnen beïnvloeden. In dit hoofdstuk worden (mega)trends en ontwikkelingen benoemd die van invloed kunnen zijn of worden op de ontwikkeling van (nieuwe) dreigingen of risico's en de bescherming van de nationale veiligheid.

Internationale (politieke) ontwikkelingen[10]

Multi-orde wereld: verschuiving van de internationale machtsbalans

Er is sprake van spanningen tussen grote mogendheden, met name tussen de Verenigde Staten (VS) en de Europese Unie (EU) aan de ene kant en Rusland en China aan de andere kant. De toenemende assertiviteit van China en Rusland op het internationale toneel springt daarbij in het oog. Tegelijkertijd wordt duidelijk dat de trans-Atlantische relatie niet langer vanzelfsprekend is.

Door de verschuiving van de internationale machtsbalans naar een meer multipolaire orde, komt het multilateralisme als vermogen tot samenwerking onder druk te staan. Dit heeft gevolgen voor bijvoorbeeld de financieel-economische orde en klimaatafspraken. Het kan tegelijkertijd een effectieve aanpak van cyber- en hybride dreigingen en de risico's van extremisme en terrorisme in de weg staan. De wereldorde na de Tweede Wereldoorlog orde, die gestoeld is op de democratische rechtstaat, de liberale markteconomie en de kernwaarden van onze maatschappij (zoals mensenrechten, fundamentele vrijheden en gelijkwaardigheid) staat steeds vaker ter discussie. Deze Multi-Orde wereld leidt tot nieuwe vormen van mondiale spanningen en polarisaties tussen Oost en West.

Politieke instabiliteit in de EU

Een sterk Europa vormt een belangrijk fundament voor onze nationale veiligheid. De EU Global Strategy vormt de basis voor het stabiliteits- en veiligheidsbeleid binnen de EU. Niettemin wordt het 'project EU' als geheel door sommigen vaker in twijfel getrokken. Het vertrek van het Verenigd Koninkrijk uit de EU is hiervan het meest verregaande voorbeeld, maar ook de populariteit van anti-EU partijen in meerdere lidstaten (waaronder Frankrijk, Hongarije, Italië, Oostenrijk, Nederland, Polen, Zweden) is tekenend. De verschillende opvattingen binnen de EU over onderwerpen als migratie (kloof Oost - West) en economie (kloof Noord - Zuid) voeden het populisme en vormen een risico voor het vertrouwen in de EU en diens instituties. Tot slot is in enkele EU-landen een zorgwekkende afbrokkeling van de rechtsstaat te zien.

Hier staat tegenover dat de Eurobarometer de afgelopen jaren juist toenemende steun en draagvlak voor de EU laat zien. Brexit is weliswaar een tegenslag, tegelijkertijd is de EU sterk eensgezind in de reactie hierop.

10 Zoals ook in de GBVS beschreven.

Ook weet de EU wel degelijk in gezamenlijkheid externe dreigingen te identificeren en te adresseren, bijvoorbeeld richting eerdergenoemde assertieve grootmachten. Er is met andere woorden wel reden tot zorg en alertheid, maar niet tot het luiden van de noodklok.

Politieke instabiliteit rond de EU

Ook de voortdurende instabiliteit in landen en regio's rond de EU brengt mogelijke risico's met zich mee. Sommige landen vormen een toevluchtsoord voor criminele, extremistische of terroristische groeperingen. Het risico bestaat dat omringende landen worden meegezogen in een neerwaartse spiraal van geweld en falend bestuur. Ook kan de (irreguliere) migratiedruk op Europa toenemen. Dit kan een destabiliserend effect hebben op de Europese samenwerking, solidariteit en verdraagzaamheid. Daarnaast kan het polarisatie aanwakkeren en het draagvlak voor reguliere migratie en het asielsysteem verkleinen. Irreguliere migratie gaat in veel gevallen gepaard met vormen van grensoverschrijdende criminaliteit, zoals mensensmokkel en –handel. De inkomsten hiervan kunnen dienen ter financiering van terroristische activiteiten. Tot slot kunnen terroristische individuen 'meeliften' met de irreguliere migratiestromen richting Europa.
De verwachting is dat de irreguliere migratiedruk uit de instabiele landen en regio's rond Europa de komende jaren groot blijft.

Ontwikkeling van grondoorzaken en dreiging van terrorisme

Jihadistische varianten van de politieke islam zullen blijven voortbestaan, ook nadat ISIS zijn territorium heeft moeten opgeven in Irak en Syrië. De grondoorzaken waarop deze en andere groeperingen kunnen groeien zijn namelijk niet weggenomen en vooral in Afrika en het Midden-Oosten blijven zij een mogelijke katalysator van geweld. Hoewel ISIS territoriaal grotendeels verslagen en sterk verzwakt is, zal het de komende jaren naar alle waarschijnlijkheid in andere verschijningsvormen een veiligheidsrisico blijven. Het is daarbij in toenemende mate transnationaal van karakter en maakt daarbij gebruik van nieuwe technologieën (digitale middelen, sociale media). Het verlies van ISIS-grond-gebied maakt de problematiek van terugkeerders extra urgent. Strijdervaring en het behouden van jihadistisch gedachtengoed maakt dat er van specifieke groepen dreiging uitgaat.

Ook andere vormen van terrorisme blijven in ontwikkeling. Rechts-extremistisch terrorisme is weer in opkomst, en er zijn tekenen dat in reactie hierop, links-extremistische groeperingen actiever worden in de EU. Dit wordt ook besproken bij het thema 'demografisch-maatschappelijk'.

Informatietechnologische ontwikkelingen

Cognitie en autonomie van informatiesystemen

Er vindt een verschuiving plaats van systemen die geprogrammeerd zijn om afgebakende taken volgens vaste protocollen uit te voeren, naar zelflerende systemen die zichzelf (zonder menselijke tussenkomst) nieuwe taken en gedrag aanleren, en systemen die op basis van kennis improviseren en zelf beslissingen nemen. Gebruik van dit soort *Artificial Intelligence*-systemen (AI-systemen) en *Machine Learning* kan leiden tot consequenties voor de nationale veiligheid.

AI-systemen worden getraind met behulp van grote hoeveelheden data. Wanneer hiervoor gebruik gemaakt wordt van een *biased* (ondoordachte, onvolledige of manipuleerde) dataset, kan een zelflerend systeem vooringenomenheid ontwikkelen en daarnaar gaan handelen. Na verloop van tijd is niet meer te achterhalen waar bepaald gedrag vandaan komt. Wanneer het systeem beslissingen neemt die impact kunnen hebben op personen of organisaties, kunnen de gevolgen ernstig zijn.

De interactie van meerdere autonoom werkende systemen kan leiden tot onvoorziene verstoring van maatschappelijke processen, als autonoom werkende systemen niet afdoende op elkaar afgestemd worden. Denk hierbij aan verkeersongevallen die kunnen ontstaan doordat autonoom functionerende systemen niet goed met elkaar samenwerken. De risico's die uitgaan van autonome systemen worden groter naarmate zij in meer verschillende domeinen worden toegepast, en binnen eenzelfde domein steeds dominanter worden. Omdat zij (vaak) niet in een isolement kunnen opereren maar interactie vereisen, en die veelal plaatsvindt via internet, zijn autonome systemen vatbaar voor ongewenste inmenging van buitenaf.

Verbondenheid en verwevenheid van systemen en netwerken

Steeds meer apparaten – van huis-, tuin- en keukenvoorwerpen tot bruggen en sluizen – zijn verbonden met het internet. Door kwetsbaarheden in de hard- en software van apparaten kunnen kwaadwillende partijen toegang krijgen tot de apparaten zelf, het netwerk waar de apparaten deel van uitmaken en de data die deze apparaten verzamelen en verwerken over hun gebruikers en het gebruik van de apparaten.

Gebruikers en aanbieders van dergelijke apparaten houden vaak geen of onvoldoende rekening met de potentieel schadelijke effecten van deze kwetsbaarheden, omdat zij zelf niet direct de pijn voelen als het misgaat. Digitale informatiesystemen zijn cruciaal voor de continuïteit van bedrijven en organisaties. Het platleggen of uitvallen van dergelijke systemen kan leiden tot grote bedrijfseconomische gevolgen.

Afhankelijkheid van informatietechnologie

Onze maatschappij is sterk afhankelijk geworden van informatietechnologie. De groeiende afhankelijkheid van grote buitenlandse techbedrijven zorgt ervoor dat het realiseren van *governance* in het digitale domein lastiger wordt. Steeds moet worden bekeken wat deze afhankelijkheid betekent voor de borging van publieke belangen en op welke wijze, nationaal of internationaal, borging kan worden gerealiseerd.

De EU streeft op het gebied van defensie en veiligheid naar strategische autonomie. Op dit moment is er in informatietechnologie ook op deze gebieden een sterke afhankelijkheid van buitenlandse bedrijven. De benodigde hard- en software wordt bijvoorbeeld gemaakt door niet-Europese bedrijven. *De facto* zijn Nederland en andere Europese landen dus afhankelijk van deze spelers voor kritieke onderdelen van hun vitale (digitale) infrastructuur.

Mondiale financieel-economische ontwikkelingen

Herstructurering van de mondiaal financieel-economische orde

Er is een herschikking gaande in de internationaal financieel-economische orde waarvan de economische en veiligheidsconsequenties nog niet zijn uitgekristalliseerd. De grote economische vitaliteit van China ondersteunt de mondiale economie. Zodoende is er een Chinees belang bij de huidige financieel-economische orde. Tegelijkertijd stelt China de spelregels van de liberale marktorde ter discussie en probeert deze naar zijn hand te zetten. Ook investeert China in de oprichting van parallelle instituten en nieuwe netwerken die de institutionele orde aantasten. Op de lange termijn heeft de verschuiving van de economische machtsbalans van het Westen naar China politieke gevolgen die van invloed kunnen zijn op de nationale veiligheid.

Technologische ontwikkelingen in de financieel-economische sector

Cryptovaluta kunnen door middel van nieuwe technieken als *blockchain* privaat worden uitgegeven en zijn onafhankelijk van een centrale bank. De grootste risico's die crypto's met zich meebrengen, is dat zij bij uitstek geschikt zijn voor het witwassen van met criminele activiteiten verdiend geld en het financieren van terroristische activiteiten. Daarom is op EU-niveau besloten om crypto's onder de reikwijdte van de anti-witwasrichtlijn te brengen en wordt er gewerkt aan internationale anti-witwasstandaarden voor crypto's. Vanaf begin 2020 zullen cryptodienstverleners die actief zijn in Nederland een vergunning in het kader van de Wet op witwassen en financieren van terrorisme moeten aanvragen. Op het hoogtepunt van de cryptobubbel, eind 2017, was onbekend hoe groot de gevolgen van crypto's voor de stabiliteit van het financiële systeem waren. Inmiddels blijkt uit nationale en internationale onderzoeken dat de risico's voor de financiële stabiliteit momenteel beperkt zijn. Desalniettemin blijven zowel nationale als internationale instanties de ontwikkelingen rondom crypto's en de mogelijke gevolgen voor de financiële stabiliteit monitoren.

Economische instabiliteit van de EU

De financiële crisis (2007-2011) heeft geleid tot meer economische instabiliteit binnen de EU. De gevolgen daarvan zijn tot op de dag van vandaag merkbaar. Oost- en Zuid-Europese banken kampen nog altijd met een hoog volume aan problematische leningen op hun balans. Dit kan directe gevolgen hebben voor de economieën van andere EU-lidstaten, waaronder Nederland, doordat negatieve overloopeffecten hiervan hun systeembanken raken. Daarnaast kennen Griekenland, Italië en Portugal nog steeds een hoge overheidsschuld en structurele tekorten op hun begrotingen. De groeiende euroscepsis binnen de EU, gecombineerd met een niet onmogelijk geachte nieuwe kredietcrisis, zouden de Eurozone en het vertrouwen daarin schade kunnen berokkenen.

Demografische en maatschappelijke ontwikkelingen

Groeiende kloof tussen bevolkingsgroepen

De groeiende kloof tussen bevolkingsgroepen manifesteert zich langs zowel sociaal-culturele als sociaaleconomische scheidslijnen: zo is er bijvoorbeeld sprake van een duidelijke verharding van het (online) maatschappelijke debat. De versnippering of 'parallellisering' van de samenleving kan worden versterkt door het gebruik van sociale media en de zogenoemde 'media bubble', waarin gebruikers continu bevestiging vinden in hun mening en weinig in aanraking komen met andere opvattingen. Ook gevoelens van economische achterstelling of effecten van technologische ontwikkelingen op arbeidsparticipatie kunnen leiden tot parallellisering. Versnippering is altijd al aanwezig geweest in de Nederlandse samenleving, al neemt het de laatste jaren steeds grotere vormen aan. Bepaalde groeperingen wijzen fundamentele aspecten van de democratische rechtsstaat af en kunnen daarmee een dreiging (gaan) vormen voor de democratische rechtsorde. De weerbaarheid van de maatschappij ten opzichte van deze opvattingen is in het algemeen nog steeds hoog.

Fluctuatie in mate van vertrouwen in instituties

Dit alles hangt samen met een verlies aan vertrouwen in de politiek en de overheid. Het vertrouwen in gezaghebbende instituten is groot in Nederland, en blijft dat naar verwachting ook. Het vertrouwen in het functioneren van personen binnen die instituten verschilt echter en fluctueert. Er zijn hierbij grote verschillen tussen de diverse subgroepen in de samenleving. Het vertrouwen in traditionele media is bijvoorbeeld onder sommige groepen jongeren scherp afgenomen. Daarom zoeken zij hun informatie in alternatieve bronnen.

Ecologische ontwikkelingen

Klimaatverandering

De aarde warmt op en dit heeft gevolgen voor het klimaat. Verschijningsvormen van extreem weer die een risico kunnen gaan vormen voor de nationale veiligheid zijn met name extreme hagelbuien, hevige neerslag waarbij de hoeveelheid hemelwater niet verwerkt kan worden en coïncidentie waarbij twee fenomenen van extreem weer bij elkaar komen. Als tweede ontwikkeling wordt de opkomst van exoten relevant geacht. Planten en dieren uit zuidelijkere regio's trekken verder noordwaarts. Mensen, planten en dieren kunnen door de opkomst van deze exoten te maken krijgen met nieuwe infectieziekten.

Vermindering biodiversiteit en biomassa

Biodiversiteit duidt de verscheidenheid van het leven op aarde aan: diversiteit aan genen, soorten en ecosystemen. Door een verder verlies aan biodiversiteit en biomassa kunnen de natuurlijke omgeving en landbouw significant verschralen. Dit kan op termijn de ecologische veiligheid van Nederland schade toebrengen

Milieudruk

De negatieve gevolgen van menselijke activiteiten richting bodem, water en lucht wordt gezien als milieudruk. Menselijk handelen gericht op korte termijn (bijvoorbeeld grondwaterstandbeheer ten behoeve van landbouw) kan op de lange termijn tot schade leiden (verzilting). Dit kan leiden tot een wezenlijke verandering en kwaliteitsvermindering van het bodem-, water- en luchtsysteem.

Dominante risico's voor de nationale veiligheid

De trends en ontwikkelingen op macroniveau, kunnen hun weerslag hebben in actuele dreigingen en risico's voor de nationale veiligheid. Welke dreigingen en risico's dit zijn, en hoe die de nationale veiligheid bedreigen, is uitgewerkt in een geïntegreerde risicoanalyse van het ANV.

Voor de leesbaarheid zijn de risicocategorieën uit de risicoanalyse geclusterd naar in dit hoofdstuk opgenomen veiligheidsvraagstukken (zie bijlage 1 voor deze clustering).

De risicoanalyse brengt van een dreiging of risico het volgende in beeld:

- De impact waarmee (een of meerdere van) de nationale veiligheidsbelangen wordt getroffen;
- en de waarschijnlijkheid dat de dreiging/het risico (die volgt uit de middellange termijn ontwikkeling) zich daadwerkelijk zal voordoen.

Daaruit volgen elf dominante risico's en dreigingen voor de nationale veiligheid, die hieronder nader zijn beschreven. Dit zijn dreigingen en risico's die een of meerdere van de zes nationale veiligheidsbelangen ernstig tot zeer ernstig aantasten.

Ongewenste inmenging en beïnvloeding door statelijke actoren

(Heimelijke) inmengings- en beïnvloedingsactiviteiten van buitenlandse overheden tasten de nationale veiligheid aan. Enerzijds kan het gaan om heimelijke inmenging van buitenlandse overheden, gericht op het aan zich binden en controleren van hun diasporagemeenschappen. Methoden zoals intimidatie en chantage worden hierbij vaak niet geschuwd. Dit heeft impact op het veiligheidsbelang 'Sociale en politieke stabiliteit'. Anderzijds kan het gaan om ongewenste beïnvloedingsactiviteiten en verstoringsoperaties die gericht zijn op het direct compromitteren, verzwakken, ondergraven en destabiliseren van Nederland zelf, zijn democratische rechtsstaat en open samenleving. Dit heeft impact op de veiligheidsbelangen 'Internationale rechtsorde', 'Sociale en politieke stabiliteit' en in het geval van fysiek geweld: 'Fysieke veiligheid'. Ondermijning door statelijke actoren via ongewenste beïnvloedingsactiviteiten en verstoringsoperaties gebeurt onder meer middels hybride operaties. Hybride conflictvoering is niets nieuws. Wel nieuw zijn de schaal en frequentie waarmee steeds assertiever wordende staten dit inzetten. Er is sprake van een constante internationale competitie tussen landen waarbij heimelijke hybride operaties om een andere samenleving te ondermijnen steeds vaker worden toegepast. Kwetsbaarheden in de maatschappij en politiek worden daarbij uitgebuit en kunnen bij een samenloop van omstandigheden en met de juiste combinatie van beïnvloedingsactiviteiten een grote impact hebben (bijvoorbeeld op de vitale infrastructuur). Bovendien faciliteren ontwikkelingen in het cyber- en informatiedomein deze manier van beïnvloeding en ondermijning.

Dreigingen tegen multilaterale instituties en economische weerbaarheid

De internationale orde is sterk aan het veranderen. Op allerlei terreinen wordt in steeds wisselende coalities samengewerkt. In combinatie met polarisatie tussen bevolkingsgroepen die onze democratieën en de consensus over internationale samenwerking onder druk zet, zorgt dat voor onzekerheid en het draagt bij aan een verslechterende internationale veiligheidssituatie. Bovendien geldt dat belangen van individuele landen (en de normen en waarden waarop hun samenleving gestoeld is) steeds belangrijker worden geacht. Mede hierdoor komt multilaterale, institutionele samenwerking onder druk te staan. De toenemende macht en invloed van China in westerse economieën kan op de lange termijn grote gevolgen hebben voor zowel het financieel-economisch bestel (van de EU) als voor de werking van de multilaterale instituties.

Zoals in het vorige hoofdstuk wordt beschreven, wordt Europa, en dus Nederland geconfronteerd met een 'ring' van toenemende instabiliteit en conflict, waarbij de kans op een nieuw conflict aanwezig blijft. In dit klimaat van onzekerheid en toenemende dreigingen en risico's is het voor Nederland des te belangrijker dat de twee organisaties waarin Nederland zijn veiligheidsbelangen wil waarborgen, de EU en de NAVO, goed functioneren.

Zowel de EU als de NAVO worden echter sterk uitgedaagd door een aantal externe en interne factoren. Stond in het verleden samenwerking voorop en gaven de gezamenlijke belangen veelal de doorslag bij trans-Atlantische spanningen, nu lijken de gezamenlijke belangen steeds beperkter te worden geïnterpreteerd. Op sommige dossiers is het een uitdaging om eensgezindheid onder EU-lidstaten te bereiken, om zo voldoende eigen gewicht in de schaal – ofwel de internationale orde – te leggen. Dit risico kan effect hebben op de veiligheidsbelangen 'Territoriale veiligheid', 'Sociale en politieke stabiliteit', en 'Internationale rechtsorde'.

Verstoring van de vitale infrastructuur

De Nederlandse vitale infrastructuur wordt gevormd door processen die zo vitaal zijn voor het functioneren van onze samenleving, dat verstoring ervan grote gevolgen voor onze samenleving heeft. Omdat vitale infrastructuren onderling afhankelijk zijn, kan het (technisch) falen van van één vitaal proces leiden tot diverse keteneffecten. De afhankelijkheden tussen vitale processen zijn in veel gevallen niet direct en eenduidig.

Vanwege het belang van de vitale processen voor de continuïteit van de samenleving leidt ernstige verstoring ervan tot aantasting van de nationale veiligheid. 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.

Recente analyses benadrukken in het bijzonder de digitale dreiging vanuit statelijke actoren, die er op gericht is om vitale systemen te verstoren of zelfs te saboteren. Er is een duidelijke trend in 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.

Terrorisme en extremisme

Extremisme is het actief nastreven van diep ingrijpende veranderingen in de samenleving die een gevaar kunnen opleveren voor de democratische rechtsorde, eventueel met het gebruik van ondemocratische middelen die het functioneren van de democratische rechtsorde ernstig kunnen aantasten. De gebruikte ondemocratische middelen kunnen zowel gewelddadig als niet-gewelddadig van aard zijn. Van de gewelddadige ondemocratische middelen is terrorisme de uiterste vorm.

Extremisme in Nederland en zijn omgeving vertoont tekenen dat de tweedeling van rechts- en linksextremisme in de komende jaren misschien minder van toepassing zal zijn en dat nieuwe fenomenen zoals 'identitair extremisme' of 'anti-overheidsextremisme' mogelijk die klassieke tegenstelling overstijgen. Er zijn groepen opgestaan die vanuit ideologische standpunten ernaar streven om 'het blanke ras zuiver te houden' en zich keren tegen de 'rassenvermenging' en 'omvolking'. Daarnaast zijn er boze burgers (groepen of individuen) die zich om verschillende redenen afzetten tegen de overheid. Ondanks de toename van zulke sentimenten, die vooral online geuit worden, is het onzeker of ook de geweldsbereidheid van extremisten in Nederland op korte termijn groter zal worden.

Terroristische dreigingen in Nederland komen momenteel bijna volledig voort uit het jihadisme, waarbij ISIS-aanhangers een gevaar blijven vormen. Maar ook de potentie van (kern) Al Qa'ida moet niet worden onderschat. Een potentiële dreiging voor de komende jaren ontstaat wanneer gedetineerde jihadisten die volharden in hun jihadistische ideeën, worden vrijgelaten. Zowel aanslagen door eenlingen als grootschalige aanslagen worden (zeer) voorstelbaar geacht. Er zijn (enige) aanwijzingen dat ze zich (ook in diverse soortgelijke varianten) daadwerkelijk kunnen voordoen. Het valt daarnaast niet uit te sluiten dat de komende jaren andere politiek of etnisch geïnspireerde vormen van terrorisme belangrijker kunnen worden.

Militaire dreigingen

Oplopende spanningen tussen grootmachten en instabiliteit aan de Europese buitengrenzen vergroten de kans op een gewapend conflict. Militaire ontwikkelingen dragen daaraan bij. De wereldwijde bestedingen aan defensiematerieel waren sinds de Koude Oorlog nog nooit zo hoog als in het laatst gemeten jaar, 2017. De grootste stijgers zijn China, Rusland, Saoedi-Arabië, maar ook de Europese NAVO-landen (bij elkaar opgeteld). Andere indicatoren wijzen eveneens op een toenemende militaire dreiging. Agressievere retoriek, grootschaligere militaire oefeningen en de vele schendingen van territoriale wateren en het luchtruim weerspiegelen de toenemende spanningen tussen staten. Deze spanningen kunnen ook een bedreiging zijn voor Nederlandse aan- en afvoerlijnen, wat zich door vertaalt naar mogelijke aantasting van het financieel-economisch bestel. Het risico van militaire dreigingen in al zijn vormen vormt een dreiging voor de nationale veiligheid.

Vanuit de koppeling tussen interne en externe veiligheid komt vanuit dit dominante risico de koppeling met digitale dreigingen en hybride conflictvoering duidelijk naar voren. Bijvoorbeeld bij een militaire dreiging die uitloopt op een militair conflict, waar Nederland bij betrokken zou raken. Dit kan gebeuren via artikel 5 van het NAVO-verdrag als er een militair conflict optreedt tussen een NAVO-lidstaat en een statelijke actor. In een dergelijk geval zullen naast militaire inzet ook andere hybride instrumenten, waaronder cybermiddelen, ingezet worden. Een spannende situatie kan zich zelfs voordoen wanneer artikel 5 nog niet in werking is gesteld, maar er wel sprake is van internationaal oplopende escalatie waardoor artikel 5 zou kunnen worden ingeroepen. Het is denkbaar dat Nederland als transitland voor andere NAVO-eenheden in een dergelijk geval al vroegtijdig als belangrijk (cyber)doelwit wordt beschouwd. Manifesteert dit dominante risico zich, dan heeft dat impact op de veiligheidsbelangen 'Territoriale veiligheid' en 'Internationale rechtsorde'.

Criminele ondermijning

In een aantal steden en gemeenten zijn tendensen waargenomen die het lokale bestuur afwijzen, tegenwerken, verstoren en ondergraven. Denk daarbij aan criminele groeperingen die het ontstaan van 'no go areas' nastreven. In Nederland gebeurt dit echter (nog) niet in dezelfde mate als in andere Europese landen. Toch kan dit op termijn het gezag van de overheid aantasten. Criminele inmenging in het bedrijfsleven en van daaruit beïnvloeding van het openbaar bestuur, of rechtstreekse criminele beïnvloeding daarvan, kan resulteren in wantrouwen richting betrokken (overheids)partijen. Uit de analyse komt naar voren dat als dit risico zich manifesteert, het vooral impact heeft op het veiligheidsbelang 'Politieke en sociale stabiliteit', met een ernstige aantasting van de democratische rechtsstaat en een significante sociale maatschappelijke impact. Omdat criminele ondermijning reeds optreedt in een aantal steden en gemeenten en de impact ervan groot is, is het een dominant risico voor de nationale veiligheid.

Polarisatie en dreigingen tegen sociale cohesie

Toenemende polarisatie ondermijnt onze open samenleving. Het kan een voedingsbodem zijn voor zowel niet-gewelddadig als gewelddadig extremisme en eventueel zelfs terrorisme. Statelijke actoren kunnen hierop inspelen, al dan niet aan de hand van hybride operaties. Ontwikkelingen die polarisatie in de hand werken zijn een internationaal fenomeen, ze doen zich niet alleen binnen Nederland voor. Dit dominante risico heeft impact op het veiligheidsbelang 'Sociale en politieke stabiliteit'.

Behalve polarisatie door het verspreiden van on- of antidemocratische boodschappen, kunnen extremistische groeperingen proberen eigen parallelle samenlevingen (enclaves) af te dwingen. Bijvoorbeeld door onze open samenleving actief af te wijzen; door bestuurders en politici in hun functioneren te hinderen; door democratische instituties te ondermijnen; en/of door burgers in hun grondrechten te belemmeren.

Ook statelijke actoren kunnen polarisatie (moedwillig) versterken, onder andere via digitale middelen. In de internationale machtscompetitie worden middelen ingezet die de soevereiniteit en machtspositie van staten ondermijnen. Dit uit zich bijvoorbeeld in zogenoemde 'lange-arm-activiteiten' of hybride operaties, die tot polarisatie tussen bevolkingsgroepen kunnen leiden.

Cyberdreigingen

Digitale aanvallen van statelijke actoren met als doel spionage, beïnvloeding, verstoring en sabotage, vormen de grootste digitale dreiging voor de nationale veiligheid, met een grote impact en een hoge waarschijnlijkheid. Daarnaast hebben de activiteiten van cybercriminelen grote impact. Cyberdreigingen hebben een relatief hoge waarschijnlijkheid.

Technologische ontwikkelingen vergroten de afhankelijkheid, verwevenheid, complexiteit en onbeheersbaarheid van systemen en processen. Bovendien werkt de strategische afhankelijkheid van buitenlandse partijen als (toe)leveranciers, producenten en dienstverleners, de kwetsbaarheid voor spionage, verstoring en sabotage in de hand. Toenemende digitalisering zorgt ervoor dat de potentiële schade van digitale aanvallen (en het profijt dat een kwaadwillende actor ervan kan hebben) toeneemt. Analyses tonen bovendien aan dat, onder andere vanwege snelle ontwikkelingen, de weerbaarheid tegen cyberaanvallen achterop dreigt te raken. Verder geldt dat digitale dreigingen niet op zichzelf staan. Zo is er een wisselwerking met andere risico's. Verstoring van elektriciteit kan bijvoorbeeld leiden tot een verstoring van informatiesystemen en vice versa. Het onderscheid tussen cyberdreigingen en andere dreigingen met gevolgen voor het digitale domein, is daardoor niet altijd strikt te duiden.

Natuurrampen

Dit dominante risico treedt op als gevolg van natuurgeweld, veelal een ramp met een natuurlijke oorzaak. Overstromingen (vanuit zee en/of vanuit een rivier), natuurbranden en aardbevingen kunnen ernstige gevolgen hebben voor de samenleving. Dat geldt ook voor extreem weer zoals zware stormen, sneeuwstormen en ijzel. Een extra risico bij extreem weer is het fenomeen coïncidentie: het samenkomen van twee effecten, zoals bijvoorbeeld piekafvoeren van de grote rivieren in combinatie met een westerstorm. Hierdoor wordt het water vanuit de zee of het IJsselmeer opgestuwd. De rivieren kunnen het water vervolgens niet afvoeren naar zee, waardoor het risico op overstromingen vanuit de rivieren wordt vergroot. Klimaatverandering, in combinatie met de (versnelde) zeespiegelstijging, is door dit risico een belangrijke ontwikkeling. Door klimaatverandering zullen weersextremen waarschijnlijk vaker voorkomen en neemt op de langere termijn de kans op natuurrampen toe.

CBRN-dreigingen

Door recente technologische ontwikkelingen zijn er zorgen rondom de mogelijke inzet van biologische wapens. Ook nucleaire wapenarsenalen worden wereldwijd gemoderniseerd en uitgebreid, terwijl de nucleaire wapenbeheersingsverdragen wankelen (*Intermediate-Range Nuclear Forces*-verdrag), aflopen (New START) of worden genegeerd (Non-Proliferatieverdrag). De doctrines voor het gebruik van nucleaire wapens in een conflict zijn aan het veranderen. Daarnaast zijn er zorgen dat nucleair en radiologisch materiaal in handen kan vallen van niet-statelijke actoren zoals groeperingen met een gewelddadig extremistische of terroristische intentie.

Het risico van een wankel wapenbeheersingsregime en de (mogelijke) inzet van CBRN-middelen door statelijke actoren heeft impact op verschillende criteria binnen het veiligheidsbelang 'Internationale rechtsorde'. Het gebruik van massavernietigingswapens (waaronder CBRN-middelen) tast staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting aan. Het veiligheidsbelang van een goed functionerende internationale rechtsorde kan worden aangetast zonder dat dit op korte termijn impact heeft op een van de andere veiligheidsbelangen. Maar omdat het de norm van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting met voeten treedt, slaat het een bres in de fundamenten van de internationale rechtsorde. Dit kan straffeloosheid en precedentwerking in de hand werken. Het zorgt voor meer onzekerheid en instabiliteit in internationale verhoudingen. Daarnaast valt CBRN-proliferatie onder de aantasting van multilaterale instituties (het wapenbeheersingsregime vormt een belangrijk stelsel van internationale verdragen en afspraken). Tot slot valt inzet van nucleaire wapens onder zeer ernstige aantasting van mensenrechten.

Infectieziekten

Dit risico gaat over acute dreigingen voor de gezondheid als gevolg van een crisis in de vorm van een grootschalige uitbraak van een infectieziekte. Het gaat daarbij om een grieppandemie (alhoewel ook andere infectieziekten mogelijk zijn), zoönose of dierziekte. Als dit risico optreedt, dan heeft het impact op de veiligheidsbelangen 'Fysieke veiligheid', 'Sociale en politieke stabiliteit' en 'Economische veiligheid'.

Op basis van het aantal (ernstige) grieppandemieën in de laatste 100 jaar en de frequentie waarin ze voorkomen, is het waarschijnlijk dat er een grieppandemie optreedt de komende jaren. Het is niet vooraf duidelijk of het om een ernstige of milde variant zal gaan. De maatschappelijke gevolgen zullen vooral groot zijn als een groot percentage van de bevolking ziek is. De uitbraak van een dierziekte (zoals mond-en-klauwzeer of Afrikaanse varkenspest) blijft in Nederland waarschijnlijk, ook ondanks de getroffen voorzorg en voorbereiding. Dit heeft onder meer te maken met het grote aantal landbouw- en huisdieren en het wereldwijde transport van dieren.

De vaccinatiegraad in Nederland en antimicrobiële resistentie (AMR) zijn ontwikkelingen om alert op te blijven. Bij een verdere daling van de vaccinatiegraad zou op de langere termijn de kans dat infectieziekten optreden toe kunnen nemen. Nederland moet zich voldoende blijven weren tegen de toenemende dreiging door insleep van AMR uit andere landen.

Weging van dreigingen en risico's: wat vergt extra inzet?

Veiligheid is een kerntaak van de overheid. Waar zich dreigingen of risico's voordoen, spant de overheid zich in om met preventie, pro-actie, preparatie, respons en (waar nodig) nazorg Nederland weerbaar(der) te maken. Er gebeurt al veel. Veiligheidsdiensten, overheidsorganisaties, bedrijven en burgers werken samen om Nederland veilig te houden en om de weerbaarheid te vergroten.

Tegelijkertijd blijft de wereld om ons heen veranderen en is een robuuste en flexibele aanpak van dreigingen en risico's noodzakelijk. Volgens de cyclus van de Nationale Veiligheid Strategie is voor deze NVS 2019 de ontwikkeling van dreigingen en risico's afgezet tegen de huidige strategische inzet die de overheid met alle maatschappelijke partners pleegt om deze het hoofd te bieden. Daarbij zijn – met inachtneming van de uitgangspunten - de volgende vragen beantwoord:

1. *Beschikt Nederland over een geïntegreerde aanpak om deze dreiging of dit risico het hoofd te bieden?*
2. *Voldoet deze aanpak, gegeven de ontwikkeling van de dreiging of het risico, om Nederland weerbaar(der) te maken?*

In dit hoofdstuk zijn de onderwerpen opgenomen die leiden tot een versterkte strategische inzet. Versterkte inzet betekent dat de dreiging van dien aard is dat het onderwerp – geïntegreerd, maar binnen de reeds bestaande taken en verantwoordelijkheden van betrokken organisaties – extra aandacht behoeft om de geïdentificeerde dreigingen of risico's het hoofd te blijven bieden. De genoemde versterkte inzet behoeft, onder verantwoordelijkheid van de betrokken vakdepartementen, nog wel nadere concretisering. Versterkte inzet is nodig op de aanpak van statelijke dreigingen, het tegengaan van polarisatie, het beschermen van de vitale infrastructuur, het tegengaan van terrorisme, de aanpak van militaire dreigingen, de aanpak ondermijning en cybersecurity.

1. Statelijke dreigingen worden aangepakt

Een open samenleving met een open economie vormt de grondslag voor de inrichting van de Nederlandse maatschappij en welvaart. Onze open samenleving staat in het teken van vrijheden, democratie, rechtsstaat en een internationale oriëntatie. Door deze openheid profiteren Nederland en Nederlanders van de kansen en mogelijkheden die bijvoorbeeld digitalisering en 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. Digitale middelen worden door staten ingezet voor manipulatie (bijvoorbeeld van gegevens) en sabotage (bijvoorbeeld door het verstoren van onze vitale processen), desinformatie (bijvoorbeeld in de verspreiding van onjuiste informatie rondom verkiezingen, via onder meer sociale media) en digitale spionage (bijvoorbeeld voor het vergaren van gevoelige of vertrouwelijke informatie).

Door overnames van en investeringen in vitale infrastructuur of bedrijven die hoogwaardige technologie ontwikkelen, kan een ongewenste afhankelijkheid ontstaan met risico voor het functioneren van de Nederlandse democratische rechtsorde. De continuïteit van vitale processen kan in het geding komen en/of vertrouwelijke of gevoelige informatie kan weglekken. Een vergelijkbaar risico kan ontstaan door inkoop van cruciale diensten en producten. Ook (digitale) economische spionage is een belangrijk middel dat sommige staten inzetten.

Ondermijning door statelijke actoren is meestal een sluipend proces dat op langere termijn kan leiden tot schade aan de democratische rechtsorde en open samenleving. Denk daarbij aan de integriteit van politieke en bestuurlijke besluitvorming, onafhankelijke rechtspraak, vrije en eerlijke verkiezingen en fundamentele vrijheden zoals persvrijheid, academische vrijheid en vrijheid van meningsuiting. Daarnaast kan ongewenste buitenlandse inmenging leiden tot spanningen binnen en tussen bevolkingsgroepen in Nederland en een barrière opwerpen voor de binding met de Nederlandse samenleving.[11] Statelijke actoren kunnen met ongewenste inmenging gebruik maken van verschillende beïnvloedingsmethodes en –doelgroepen, zoals diasporagemeenschappen, studenten, media of politici. Soms kan sprake zijn van heimelijke financiering. Ook de verspreiding van desinformatie behoort tot de gebruikte tactieken.[12]

De strategische aanpak gericht op het tegengaan van statelijke dreigingen is op 18 april jl. aan de Kamer gestuurd.[13] De aanpak 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 de recente casuïstiek de komende tijd op de thema's:

1. *Ongewenste buitenlandse inmenging gericht op diasporagemeenschappen;*
2. *beschermen democratische processen en instituties;*
3. *aanpak economische veiligheid.*

Ook het Nederlandse exportcontrolebeleid draagt bij aan het weerbaar maken tegen statelijke dreigingen door te voorkomen dat export van strategische *dual-use* goederen, diensten of technologieën ongewenste gevolgen hebben.

2. Polarisatie tegengaan door brede aanpak gericht op samenleven

Mensen maken zich zorgen over de samenleving en ervaren een groeiend gevoel van onbehagen en soms gevoelens van onmacht. Ook zijn er zorgen die zich bijvoorbeeld richten op immigratie of integratie. Andere mensen voelen zich niet gelijkwaardig in de Nederlandse samenleving en hebben het gevoel blijvend behandeld te worden als tweederangsburgers. 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. Het continue onderzoek Burgerperspectieven (1e kwartaal 2019) van het Sociaal-Cultureel Planbureau (SCP) wijst op zorgen onder burgers over vergrote tegenstellingen en polarisatie. 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.

3. Versterkte aanpak beschermen vitale infrastructuur

De integriteit van de vitale infrastructuur is een essentiële factor voor de nationale veiligheid. Zo'n 80% van de vitale processen is daarbij in handen van private partijen. 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. Daarin moet ook de toepassing van de beschermende maatregelen op niet alleen de vitale aanbieders en processen, maar ook hun ketenafhankelijke factoren, bedrijven, organisaties of netwerken worden meegenomen. 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

11 Nationaal Veiligheidsprofiel 2016 (Analistennetwerk Nationale Veiligheid, 2016) en ook Kamerstukken 2017/18, 22233, nr.63.

12 Kamerstukken 2018/19, 30 821, nr. 51.

13 Kamerstukken 2018/19, 30821, nr. 72.

criteria, en dat, omwille van het tijdig anticiperen op ontwikkelingen, inzichtelijk is hoe de Nederlandse vitale infrastructuur zich technisch en organisatorisch ontwikkeld. Daarom zal het kabinet, in samenwerking met al deze partijen, een versterkte aanpak van bescherming van de vitale infrastructuur ontwikkelen. Onderdeel van deze versterkte aanpak is een structuur om kennis, kunde en expertise te bundelen om nationale veiligheidsrisico's ten behoeve van de vitale infrastructuur, nu en in de toekomst, adequaat te adresseren.

4. Terrorisme en extremisme: evalueren, versterken en blijven ontwikkelen

Bestrijding van terrorisme en extremisme vergt onverminderde aandacht. Er zijn nog steeds kwaadwillenden die zich bezighouden met aanslagplanning binnen Nederland, zoals ook de recente gebeurtenissen in Utrecht hebben laten zien. De dreiging van terrorisme en extremisme blijft in ontwikkeling.

De herovering van het door ISIS bezette gebied, de daarmee veranderende strategie van IS, de terugkeer van uitreizigers in de Nederlandse samenleving, de ontwikkeling en opkomst van andere terroristische groeperingen en mogelijk (onvoorziene) geopolitieke ontwikkelingen zijn een aantal uitdagingen die het vraagstuk onverminderd complex maken. Ook zal Nederland te maken krijgen met ex-gedetineerden die terugkeren in de samenleving maar die hun gedachtegoed mogelijk niet hebben afgezworen en nieuwe connecties hebben gemaakt tijdens detentie.

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 er 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.

Vanuit de wetenschap dat de dreiging dynamisch en onzeker is, blijft het 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 de CT-strategie 2016-2020. Op basis van deze bevindingen zal de nieuwe CT-strategie samengesteld worden.

5. Militaire dreigingen tegengaan door effectieve samenwerking en verbeteren slagkracht

De veiligheid van Nederland is verknoopt met die van de buitenwereld. De afgelopen jaren is de eerste hoofdtaak van de krijgsmacht, de bescherming van het eigen en bondgenootschappelijke grondgebied, steeds belangrijker geworden.[14] Tegelijkertijd neemt het belang van de andere hoofdtaken niet af. De diversiteit en complexiteit van dreigingen waarmee Europa wordt geconfronteerd, maakt dus dat Nederland (en Europa) de bakens moeten verzetten, om ook in de toekomst onze veiligheid te kunnen blijven beschermen.

Andere landen maken grote stappen met hun militaire capaciteiten, waardoor militair overwicht van Nederland en zijn bondgenoten geen vanzelfsprekendheid meer is. Er is sprake van een toenemende en geïntegreerde Russische dreiging tegen bondgenootschappelijke, Europese en (daarmee) Nederlandse belangen. Deze dreiging heeft naast een hybride-, spionage- en cybercomponent, ook een nucleaire component.[15] Rusland kan met moderne wapensystemen (tijdelijk) de toegang tot betwiste gebieden op zee, op land en in de lucht voorkomen of bemoeilijken. Ook kan het de bewegingsvrijheid binnen deze gebieden beperken.

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.

Naast een verdieping van het NAVO-bondgenootschap en de Europese defensiesamenwerking, harnast onze krijgsmacht zich ook op andere manieren voor de toekomst. De samenwerking met civiele autoriteiten, het bedrijfsleven en bijvoorbeeld ngo's moet robuuster en vanzelfsprekender worden. 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.

14 Kamerstukken 2018/19, 34919, nr.1.

15 Conceptversie Openbaar Jaarverslag MIVD 2018.

Het doel van de nieuwe Defensienota, die gepland staat voor 2020, is het presenteren van een visie en strategie die laat zien welke rol Defensie, gezien het veranderende dreigingsbeeld, in de toekomst moet kunnen vervullen en welke stappen nodig zijn om daar te komen.

6. Stevige programmatische aanpak criminele ondermijning[16]

Bij ondermijnende criminaliteit gaat het om een breed scala aan criminele fenomenen en de ondermijnende werking die daarvan uitgaat op de samenleving. «Ondermijning» verwijst vooral naar de effecten van de georganiseerde criminaliteit: de verwevenheid van onder- en bovenwereld, de innesteling in woonwijken en in legale sectoren. Georganiseerde criminaliteit is altijd geworteld in de lokale samenleving. Plegers van georganiseerde criminaliteit maken gebruik van dezelfde legale structuren en voorzieningen als gewone burgers: transportvoorzieningen, financiële en juridische dienstverlening, recreatieterreinen, de vastgoedsector etc. Deze verwevenheid met de legale wereld heeft vergaande consequenties. De combinatie van omvangrijke criminele vermogens en de toegang tot zware geweldsmiddelen stelt criminele netwerken in staat invloed te verwerven in maatschappelijke sectoren en ongewenste sociale druk uit te oefenen in de samenleving. Dit gaat gepaard met bedreiging van de integriteit van het openbaar bestuur en van overheidsambtenaren. Dit leidt tot aantasting van het rechtsgevoel en van de rechtsstaat en zijn instituties.[17]

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. De internationale aanpak vindt plaats met bronlanden, transitlanden, binnen de EU en met buurlanden.

Het huidige 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 de extra financiële middelen uit het regeerakkoord die de regio's en de landelijke organisaties in staat stellen de aanpak een krachtige impuls te geven. Van de beschikbare € 100 miljoen gaat 85 miljoen naar de regio's en € 15 miljoen naar landelijke organisaties en taken.

Het kabinet heeft er voor gekozen om robuuste plannen «van onderop» te laten ontwikkelen, vanuit de partijen die verantwoordelijk zijn voor de uitvoering: bij de professionals ter plaatse zit de kennis en expertise over hoe de aanpak het beste kan worden versterkt.

Daarnaast is er een ambitieuze wetgevingsagenda, waarin goed rekening wordt gehouden met zowel wensen vanuit de uitvoeringspraktijk als met rechtsstatelijke uitgangspunten. Er is een Strategisch Beraad Ondermijning ingesteld dat de minister van Justitie en Veiligheid adviseert over de besteding van de extra financiële middelen en over mogelijkheden tot verdere verbetering van de aanpak. Daarnaast is er een aanjaagteam ingericht dat het land in gaat om samen met de operationele partijen te kijken hoe de aanpak concreet verbeterd en versneld kan worden. Het aanjaagteam werkt nauw samen met de RIECs en het LIEC. Door het inrichten van een tussentijdse evaluatie wordt het lerend vermogen van de betrokken organisaties vergroot en kunnen *best practices* snel beschikbaar komen voor bredere uitwisseling en waar van toepassing voor landelijke uitrol. De verantwoordingslijnen richting de Tweede Kamer lopen reeds via het programma Anti-ondermijning.

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. Zonder het afpakken van die opbrengsten ontstaat een aanzuigende werking op het plegen van strafbare feiten met bijbehorende wezenlijke verstoringen van onze samenleving. Ook het rechtsgevoel van individuele burgers die erop moeten kunnen vertrouwen dat de overheid hiertegen effectief optreedt komt onder druk te staan. Extra inspanningen zijn nodig en daar maakt het kabinet samen met alle partners zich sterk voor. Bij het bestrijden van georganiseerde criminaliteit en breder geld gedreven 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, die zijn neergelegd in de brief aan de Tweede Kamer van 13 maart jl.[18]: financieel-economisch perspectief aan de voorkant van het opsporingsonderzoek; verder leren, ontwikkelen en integraal verbinden; internationalisering; en monitoren en (bij)sturen. Door het vorige kabinet is in de miljoenennota 2018 € 30 miljoen incidenteel beschikbaar gesteld ter versterking van de aanpak van het afpakken van crimineel vermogen.

16 De verantwoordingslijnen richting de Tweede Kamer lopen reeds via het programma Anti-ondermijning.

17 Zie uitvoeriger hierover: Sluipend gif (Politieacademie 2018), Nationaal Dreigingsbeeld georganiseerde criminaliteit (Politie 2017) en Ondermijning ondermijnd (NSOB 2016).

18 Kamerstukken II 2018/2019, 29 911 en 31 477, nr. 221.

Op basis van voorstellen van tien regionale en van nationale partners is tot een reeks concrete versterkingsprojecten besloten die van start zijn gegaan. Daarbij ligt een belangrijk accent op de versterking van de integrale samenwerking en ook het integraal afpakken met als doel het financieel-economische perspectief in de bestrijding van criminaliteit breed in het land te borgen. Daarnaast wordt het wettelijk instrumentarium geoptimaliseerd. Daarbij wordt met inbreng vanuit de praktijk en aangenomen moties bezien welke verbeterpunten in de wetgeving mogelijk zijn om het afpakken van crimineel vermogen te versterken, in het bijzonder in het kader van de aanpak van ondermijning.

Voorts is het van cruciaal belang dat de legale financieel-economische kanalen waarlangs crimineel verkregen gelden worden witgewassen worden beschermd tegen misbruik. De verplichtingen om dit te voorkomen zijn neergelegd in de Wet ter voorkoming van witwassen en terrorismefinanciering. Deze verplichtingen vloeien voort uit de internationale standaarden van de Financial Action Task Force (FATF) en de Europese anti-witwasrichtlijn. Op die manier wordt bewerkstelligd dat er in internationaal en Europees verband uniforme regels op dit terrein worden gehanteerd. De wijzigingen op de vierde anti-witwasrichtlijn worden op dit moment in Nederland geïmplementeerd. Ook is een beleidscyclus ingericht om witwasrisico's te identificeren en de effecten van de aanpak van witwassen te evalueren. De rapporten die daarover de afgelopen tijd zijn verschenen zijn reeds aan de Tweede Kamer aangeboden.[19] Voor de zomer zullen de minister van Financiën en de minister van Justitie en Veiligheid een plan van aanpak voor het tegengaan van witwassen aan de Tweede Kamer toesturen. Daarin wordt onder meer ingegaan op deze rapporten alsook op de mogelijkheden om informatiedeling met en tussen banken effectiever te maken.

7. Versterkte aanpak van digitale dreigingen

De samenleving is volledig afhankelijk geworden van digitale middelen en ook digitale veiligheid is verweven in alle nationale veiligheidsbelangen. Vrijwel alle vitale processen en diensten zijn volledig afhankelijk van ict. Door het bijna geheel verdwijnen van analoge alternatieven en de afwezigheid van terugvalopties is de afhankelijkheid van gedigitaliseerde processen en systemen zo groot geworden dat aantasting hiervan kan leiden tot maatschappij-ontwrichtende schade. Vitale processen zijn in hoge mate afhankelijk van elektriciteitsvoorziening en datacommunicatie. Uitval en verstoring hiervan hebben zeer snel, binnen enkele uren, impact op een aantal vitale processen. Vanwege de omvang van de digitale dreiging in samenhang met de huidige weerbaarheid, ontstaan risico's voor de nationale veiligheid.

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. Hiermee wordt invulling gegeven aan ambitie 7 van de NCSA om de regie op de kabinetsbrede aanpak te versterken. 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. De NCTV gaat samen met de vakdepartementen opnieuw beoordelen welke belangen in de digitale ruimte het meest van invloed zijn op de nationale veiligheid en onderzoeken of vitale organisaties zich voldoende bewust zijn van deze kwetsbaarheden.

Het belang van cybersecurity is zo groot dat partijen ondersteuning moet worden geboden en dat er op moet worden toegezien dat partijen hun verantwoordelijkheid nemen. 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 invulling nader te geven aan de zorgplicht die uit de Wet beveiliging netwerk- en informatiesystemen (Wbni) vloeit. Om ervoor te zorgen dat organisaties ook daadwerkelijk hun verantwoordelijkheid nemen en passende maatregelen treffen is effectief toezicht op digitale veiligheid noodzakelijk.

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. Het programma zorgt ervoor dat organisaties en mensen in staat zijn om bij een daadwerkelijke crisis snel en adequaat te kunnen handelen.

Voorts wordt een certificeringsraamwerk voor producten, diensten en processen voortvloeiend uit de Europese *Cyber Security Act* ingevoerd.

Nieuwe technologieën zoals 5G en AI leiden tot nieuwe, in potentie fundamentele (digitale) veiligheidsvraagstukken die aandacht zullen behoeven. Binnen de EU is Nederland steeds actiever op het gebied van cyberveiligheid, onder andere met de '*Cyber Diplomacy Toolbox*' en door het stimuleren van cybersancties.

19 Kamerstukken II 2018/19, 31477, nr. 28.

Onverminderde inzet op weerbaarheid

Waar sommige veiligheidsvraagstukken nadrukkelijk vragen om extra inzet, zijn er ook dominante risico's die reeds geïntegreerd en adequaat het hoofd worden geboden. Gezien de ontwikkeling hiervan vergen deze onverminderde inzet om de nationale veiligheid te beschermen. Afkalving van de huidige aanpak, kan leiden tot (hernieuwde) risico's en dreigingen voor de nationale veiligheid.

1. Versterken van multilaterale instituties

Nederland heeft als open samenleving en economie baat bij een multilateraal stelsel met afspraken en regels over handel, veiligheid en geschillenbeslechting, gebaseerd op universele waarden. De GBVS laat zien dat het multilaterale stelsel, zoals ontstaan na de Tweede Wereldoorlog, in toenemende mate onder druk staat. Staten richten zich steeds vaker en explicieter op het behalen van relatieve nationale economische voordelen op grond van een *zero-sum* beeld van internationale verhoudingen. Ook op (geo-)politiek gebied is hier sprake van. Dit kan gevolgen hebben voor de internationale rechtsorde, de democratische grondbeginselen en de universaliteit van mensenrechten en kan daarmee raken aan de Nederlandse nationale veiligheidsbelangen.

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.

2. Voorkomen en bestrijden van natuurrampen

Klimaatverandering

Klimaatverandering is tastbaar geworden. Het leidt steeds vaker tot extreem weer, van heftige neerslag tot hoge temperaturen. In de zomer van 2018 waren er in Nederland zestig warme dagen achter elkaar en twee hittegolven. Naast extreem warm was het ook extreem zonnig en zeer droog. In totaal registreerden KNMI-meetstations 2090 zonuren tegen 1639 normaal. Met een gemiddelde van 11,3°C was 2018 het vijfde zeer warme jaar op rij. Het was na 2014 het warmste jaar sinds het begin van de metingen. Dit beeld past in de trend van een opwarmend klimaat. 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.

Het ministerie van Infrastructuur en Waterstaat werkt samen met alle waterpartners aan deze opgave. Dat vergt inspanningen van:

- Het Deltaprogramma Zoetwater voor de verdere uitwerking van waterbeschikbaarheid.
- Het Deltaprogramma Ruimtelijke Adaptatie voor de nadere uitwerking van het thema droogte bij stresstesten en risico-dialogen.
- Het ministerie van Landbouw, Natuur en Voedselkwaliteit voor de beleidsinzet gericht op actieprogramma's Klimaatadaptatie Landbouw en Natuur.
- Gemeenten en waterbeheerders voor de uitvoering van stresstesten en het nemen van operationele maatregelen.

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. Onzeker is echter hoeveel en met welke snelheid dit zal gaan gebeuren. Dit hangt onder meer af van de emissies van broeikasgassen en dus ook van het internationale klimaatbeleid. Het Nederlandse beleid is er op 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 en daarmee ook voor het Deltaprogramma is daarom ook gekeken naar een extreme zeespiegelstijging die het gevolg kan zijn van een emissiescenario dat leidt tot 4°C wereldwijde temperatuurstijging.

De overheid wil voorkomen dat er weer een watersnoodramp gebeurt, zoals in 1953. Of dat de rivieren overstromen zoals in de jaren '90. In het Deltaprogramma staan de plannen hiervoor. De doelen zijn:

- Nederland nu en in de toekomst beschermen tegen overstromingen.
- Zorgen voor voldoende zoetwater.
- De inrichting van het land klimaatbestendig maken.

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

Alhoewel deze natuurrampen in Nederland voorkomen en de impact groot kan zijn (zonnestormen kunnen storingen veroorzaken en/of schade aanrichten aan onder andere communicatie-systemen, satellieten en de elektriciteitsvoorziening) wordt de waarschijnlijkheid als niet hoog ingeschat. 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.

3. Tegengaan van CBRN-dreigingen

Proliferatie

In de GBVS wordt gesignaleerd dat de proliferatie van massavernietigingswapens een zorgelijke ontwikkeling blijft. Sommige statelijke en niet-statelijke actoren voelen zich niet of steeds minder gebonden aan internationale afspraken. Het risico op ongelukken, incidenten of conflicten met massavernietigingswapens neemt toe. 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. Aangezien de potentiële impact van CBRN-conflicten[20] of -incidenten op de Nederlandse nationale veiligheidsbelangen enorm is, verdient deze dreiging de onversneden aandacht.

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 binnen de Nederlandse landsgrenzen 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. Grote uitdaging daarbij is het nauwgezet volgen van de capaciteiten en intenties van gewapende niet-statelijke actoren om Nederland te treffen met CBRN-middelen. Tot op heden lijkt het deze groeperingen slechts in beperkte mate te lukken hun technische en logistieke capaciteiten om te zetten in daden. Desondanks blijft dit de komende jaren een punt van zorg en dus een kwestie van blijvende investeringen in detectiemiddelen, informatie-uitwisseling en (indien nodig) preventieve actie.

Een ander belangrijk element in de aanpak is het verhogen van de maatschappelijke weerbaarheid tegen eventuele CBRN-incidenten. Hiertoe is de afgelopen jaren door diverse (hulp)organisaties gewerkt binnen een multidisciplinair, landelijk programma. Nederland is aangesloten bij het 2e EU Actieprogramma CBRN. Speerpunten hierbij zijn: het voorkomen van aanslagen, het geoefend krijgen (en houden) van personeel en het uitwisselen van kennis en kunde tussen lidstaten. Daarbij wordt de civiel-militaire samenwerking op dit gebied verstevigd.

20 CBRN staat voor: chemisch, biologisch, radiologisch en nucleair.

Stralingsongevallen

Stralingsincidenten hebben betrekking op alle activiteiten, inclusief transport en opslag, met radioactieve stoffen of toestellen die ioniserende straling kunnen uitzenden. Dit kan variëren van grote (dreigende) incidenten in nucleaire installaties tot kleine incidenten met radioactief materiaal in bijvoorbeeld een ziekenhuis.

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.

4. Infectieziektenbestrijding

In Nederland is de last van infectieziekten 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. Omdat de kennis over vaccinaties en infectieziekten toeneemt, wordt continu bekeken hoe de bescherming die het RVP biedt kan worden gemaximaliseerd. Naar aanleiding van de lichte daling van de vaccinatiegraad in Nederland heeft de staatssecretaris van VWS verbetermaatregelen gepresenteerd.[21]

In 2005 hebben de lidstaten van de WHO (waaronder Nederland) afspraken gemaakt over de signalering en bestrijding van infectieziekten. Deze afspraken zijn vastgelegd in de *International Health Regulations*. Deze zijn in Nederland verwerkt in de Wpg. 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.

De EU werkt ten slotte met de lidstaten aan het voorkomen en bestrijden van infectieziekten en het verbeteren van de weerbaarheid. Het *European Centre for Disease Control* (ECDC) speelt hierin een belangrijke rol. Het ministerie van VWS en het RIVM werken nauw samen met deze partijen. Een concreet voorbeeld van deze Europese samenwerking is de gezamenlijke aanschaf van pandemische griepvaccins door een *Joint Procurement Initiative* van de Europese Commissie.[22]

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. Over de voortgang van dit programma is de Tweede Kamer met regelmaat geïnformeerd. Vergeleken met andere landen is de situatie in Nederland relatief goed. Nederland zet zich er in internationale fora voor in om de situatie ook in andere landen te verbeteren. Het programma ABR loopt tot 2019. Voor het einde van het programma gaat de overheid samen met het veld na of er aanleiding is het programma te verlengen en welke aanpassingen nodig zijn om de dreiging van antibioticaresistentie in de toekomst het hoofd te bieden.

Zoönosen

Afgelopen jaren zijn er voor zoönosen (ziekten die van dier op mens overdraagbaar zijn) geen veranderingen waargenomen die de nationale veiligheid zouden kunnen raken. De inzet op het voorkomen, beheersen en bestrijden van zoönosen ligt besloten in de Wpg en de Gezondheids- en welzijnswet voor dieren (GWWD). De Nederlandse Voedsel- en Warenautoriteit (NVWA) houdt hierop toezicht en kan optreden. Het Centrum Zoönosen en Omgevingsmicrobiologie (Z&O) van het RIVM coördineert het 'signaleringsoverleg zoönosen'. Dit overleg signaleert en beoordeelt (nieuwe) risico's van pathogene micro-organismen die vanuit dieren, voedsel of het milieu overdraagbaar zijn naar de mens in Nederland. 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, Natuurbeheer en Voedselkwaliteit en Volksgezondheid, Welzijn en Sport beschikken over een gezamenlijke crisisstructuur en gezamenlijke crisishandboeken voor zoönosen. Deze structuren worden regelmatig geoefend.

21 Kamerstukken 2018/19, 32793, nr.338.

22 Kamerstukken 2018/19, 32793, nr.369.

Generieke instrumenten voor de nationale veiligheid

Specifieke risico's en dreigingen worden voorzien van een geïntegreerde aanpak. Naast deze specifieke instrumenten, zet Nederland in op het ontwikkelen van generieke instrumenten voor de bescherming van de nationale veiligheid. Denk hierbij aan de risico- en crisisbeheersing bij (dreigende) incidenten, rampen en crises, ongeacht welke dreiging of locatie in Nederland.

Maar ook het versterken van de wetenschappelijke basis krijgt aandacht, zoals het delen van kennis en de ontwikkeling van nieuwe technologieën. Deze instrumenten dragen over de breedte van het veiligheidsveld bij aan versterking van de nationale veiligheidsaanpak. Tot slot is het periodiek herijken van de NVS zelf ook een instrument voor de nationale veiligheid.

Ontwikkeling van het generieke systeem van risico- en crisisbeheersing

In geval van (dreigende) incidenten, rampen en crises werken overheidsorganisaties samen met private en semi-private partners. Afhankelijk van het crisistype valt te duiden welk beleidsterrein van de overheid op welk niveau betrokken is, welk overheidsgezag bevoegd is, welke organisaties in dat beleidsterrein een keten vormen en hoe zij zich in die keten tot elkaar verhouden. Er worden twee typen ketens onderscheiden. De algemene keten bemoeit zich met de algemene bevolkingszorg, in het bijzonder de openbare orde en publieke veiligheid, en de algemene rampenbestrijding. Partners daarin zijn bijvoorbeeld politie en veiligheidsregio's en gemeenten wat betreft bevolkingszorg. De functionele keten bemoeit zich met kwesties op specifieke terreinen, zoals energie, vervoer, scheepvaart, voedsel, milieu etc. Partners daarin zijn bijvoorbeeld het ministerie van Defensie, de waterschappen en vitale sectoren en bedrijven. Overheidsinterventie in de functionele keten vindt doorgaans centraal plaats (door de minister), in de algemene keten decentraal (door de burgemeester). Uitgangspunt is dat ook 'nieuwe/ongekende' crises zoveel mogelijk binnen de bestaande structuren worden aangepakt. Met de aanpassing van het Nationaal Handboek Crisisbesluitvorming in 2016 is hiermee al rekening gehouden door het systeem meer flexibel in te richten.

Door middel van de Agenda Risico- en Crisisbeheersing 2018-2021[23] wordt dit systeem in deze kabinetsperiode versterkt op verschillende punten. Zo wordt de werking van de wet veiligheidsregio's in de praktijk geëvalueerd. Ook zal er, mede ingegeven door eerder beschreven ontwikkelingen zoals parallellisering van de samenleving en de (perceptie van) toegenomen polarisatie, worden gewerkt aan een toekomstbestendige risico- en crisiscommunicatie gericht op het handelingsvermogen van de maatschappij. Verder vindt onder meer een intensivering plaats van de civiel-militaire samenwerking, wordt de crisisbeheersing in Caribisch Nederland aangepakt, en zal de boven regionale samenwerking en samenwerking met de buurlanden worden verstevigd.

De uitkomsten van de geïntegreerde risicoanalyse onderschrijven de noodzaak om te onderkennen dat de samenleving en de maatschappelijke risico's zich continu ontwikkelen, vaak geleidelijk, soms heel snel. Deze ontwikkelingen vereisen dat Nederland zich continu moet aanpassen aan en inspelen op veranderende maatschappelijke uitdagingen en de onzekerheden die dit met zich mee brengt. Het systeem van crisisbeheersing en de flexibele samenwerking daarbinnen dient hierop ingericht te zijn.

23 Kamerstukken 2018/19, 30 821, nr.50.

Een belangrijk aandachtspunt is de constatering dat de aard en schaal van mogelijke crises verandert. Aanslagen of digitale ontwrichting kunnen zich op heel verschillende plekken in Nederland voordoen en kunnen leiden tot verschillende keteneffecten met als gevolg zeer uiteenlopende maatschappelijke consequenties. Ook kan de bronbepaling of attributie van een mogelijke crisis, bijvoorbeeld in het cyberdomein, moeilijker worden of in toenemende mate in het buitenland liggen. Een adequate aanpak van dit type vraagstukken staat of valt steeds vaker met de mate waarin overheden, (private) veiligheidspartners (in binnen en buitenland) en burgers effectief weten samen te werken om genoemde uitdagingen het hoofd te bieden.

In het licht van bovenstaande ontwikkelingen wordt de noodzaak tot een proactieve en continue samenwerking en een gezamenlijke aanpak bij de publieke en private veiligheidspartners op landelijk en regionaal niveau zowel onderling als in een bovenregionale en internationale context steeds groter. Zo dient op het gebied van risicobeheersing de daarvoor benodigde informatie-uitwisseling te worden verbeterd. Verder kunnen *best practices* op het gebied van samenwerking in de nieuwe context in kaart gebracht worden. Ook zullen nieuwe dreigingen en risico's leiden tot aanpassingen van landelijke (nationale) crisisplannen, zoals voor ict-verstoringen.

Geïntegreerde wetenschappelijke onderzoeksagenda nexus interne/externe veiligheid

Het vrije mondiale verkeer van mensen, goederen, kapitaal en informatie biedt Nederland kansen, maar leidt ook tot dreigingen. Het grensoverschrijdende karakter van dit verkeer verbindt de ontwikkelingen op het gebied van internationale veiligheid met onze nationale veiligheid. Deze toenemende 'nexus' tussen interne en externe veiligheid vraagt om een gedeelde analyse van de dreiging, handelingsperspectieven en de benodigde en beschikbare kennis, intenties, vermogens en gelegenheid om te handelen. Een voorbeeld van intensievere interdepartementale samenwerking op onderzoeksgebied is de gezamenlijke wetenschappelijke onderzoeksagenda die de ministeries van Buitenlandse Zaken, Defensie en Justitie en Veiligheid in 2018 hebben opgezet. Een ander voorbeeld is de aandacht die wordt besteed aan het thema veiligheid binnen het missiegerichte topsectoren- en innovatiebeleid, onder coördinatie van het ministerie van EZK. Doel van de kennis- en innovatieagenda is om in samenwerking tussen bedrijven, onderzoeksinstellingen en overheid nieuwe innovatieve oplossingen voor veiligheidsvraagstukken te ontwikkelen en toe te passen. Deze initiatieven en met name de (onderzoeks-)resultaten die hieruit voortvloeien, zijn ook relevant voor de interdepartementale strategie- en beleidsvorming.

Monitoring nieuwe technologieën, toepassingsmogelijkheden en gevolgen voor de nationale veiligheid

Technologische ontwikkelingen kunnen significante implicaties hebben voor de nationale veiligheid. Nieuwe toepassingsmogelijkheden of gebruik van nieuwe technologieën kunnen leiden tot kansen én tot nieuwe dreigingen voor nationale veiligheidsbelangen. Daarom zullen periodiek de implicaties van nieuwe ontwikkelingen op dit vlak in kaart worden gebracht. In 2019 wordt onder meer door het ANV, in opdracht van de ministeries van Buitenlandse Zaken, Defensie en Justitie en Veiligheid, gekeken naar de ontwikkelingen rond artificiële intelligentie (AI), en de kansen en bedreigingen voor de nationale veiligheid die hiermee gepaard gaan.

Periodiek actualiseren van de Nationale Veiligheid Strategie

Met de NVS 2019 start een driejaarlijkse cyclus waarin ontwikkelingen die de nationale veiligheid beïnvloeden, dreigingen en risico's tegen de nationale veiligheid, als ook de mate van weerbaarheid daartegen, periodiek bezien worden op implicaties voor de strategische agenda of voor de definitie en aanpak van de nationale veiligheid. Om tussentijdse ontwikkelingen in het dreigingsbeeld adequaat het hoofd te bieden, wordt gedurende de cyclus een *mid-term* scan uitgevoerd om te bezien of er aanpassing van of aanvulling op de NVS noodzakelijk zijn. Het periodiek actualiseren van de NVS geschiedt in een proces onder regie van het ministerie van Justitie en Veiligheid (Nationaal Coördinator Terrorisme en Veiligheid (NCTV), in brede samenwerking met alle betrokken ministeries. De eerstvolgende NVS is volgens deze cyclus beoogd in 2022, of zoveel eerder als de ontwikkeling van dreigingen en risico's noodzakelijk maakt.

Ter afsluiting:
Ontwikkelen en verbreden van de nationale veiligheidsaanpak

Nationale veiligheid is een dynamisch en veelzijdig begrip, dat vraagt om een aanpak die robuust en flexibel is. Met de strategische cyclus van de Nationale Veiligheid Strategie is Nederland in staat om zich te blijven beschermen tegen de ontwikkeling van dreigingen en risico's en wordt de nationale veiligheids-aanpak toekomstbestendig versterkt.

De toegenomen verwevenheid van risico's die zichtbaar wordt in de risicoanalyse, zal zich naar verwachting doorzetten. In een wereld die meer en meer met elkaar verbonden raakt, wordt het realiseren van nationale veiligheid steeds meer afhankelijk van samenwerking en integratie van inspanningen. Juist in deze kwetsbaarheid ligt een grote kracht, want Nederland is bij uitstek een land dat in samenwerking op alle vlakken een rijke historie en grote slagkracht heeft.

Ontwikkelen van de NVS tot een maatschappijbrede aanpak

Met deze NVS wordt de basis gelegd voor een systeem van risicomanagement dat zich moet ontwikkelen tot een maatschappijbrede aanpak. Nationale veiligheid is immers van ons allemaal; overheid, bedrijfsleven, maatschappelijke organisaties, kennisinstellingen en burgers moeten in staat zijn om hun eigen verantwoordelijkheid in te vullen en zo een bijdrage te leveren aan de realisatie van nationale veiligheid.

Om te komen tot die maatschappijbrede aanpak is een brede samenwerking noodzakelijk voor de implementatie en ontwikkeling van de NVS: samenwerken aan de definitie van belangen, het identificeren van dreigingen en risico's en het organiseren van weerbaarheid. Wij zullen dit zowel strategiebreed als thematisch oppakken. Dit betekent concreet dat maatschappelijke partners (onder andere via bestaande netwerken) betrokken worden om hun kennis en kunde in te brengen ten behoeve van een gedeeld beeld van dreigingen en weerbaarheid, dat openbaar beschikbaar is. Ook zal deze kennis en kunde worden benut bij het vaststellen van de mate van weerbaarheid en de strategische inzet op awareness en handelingsperspectief. Hiermee geven we invulling aan de gezamenlijke verantwoordelijkheid en versterken we de publieke en private organisatie van nationale veiligheid om zo het effect van de systematiek van de NVS te vergroten.

Bijlage 1

Om tot een goede weging van de strategische inzet op weerbaarheid te komen, worden de risicocategorieën[24] uit de geïntegreerde risicoanalyse van het ANV[25] geclusterd naar veiligheidsvraagstukken. Deze veiligheidsvraagstukken zijn als volgt samengesteld en voorzien van een samenvatting van de risico's in in het hoofdstuk Dominante risico's voor de nationale veiligheid.

Statelijke dreigingen
- Ongewenste buitenlandse inmenging
- Ongewenste buitenlandse beïnvloeding via hybride operaties
- Bedreiging knooppuntfunctie/aan- en afvoerlijnen NL (flow security)

Multilaterale instituties en economische weerbaarheid
- Veiligheidsarrangementen onder druk
- Verstoring internationale handel

Vitale infrastructuur
- Verstoring vitale infrastructuur

Terrorisme en extremisme
- Terrorisme
- Niet-gewelddadig extremisme
- Gewelddadig extremisme

Militaire dreigingen
- Militaire dreigingen
- Hybride operaties via ongewenste buitenlandse beïnvloeding

Ondermijning lokaal gezag, criminele ondermijning
- Ondermijnende criminaliteit
- Criminele inmenging

Polarisatie en sociale cohesie
- Enclavevorming (niet gewelddadig extremisme)

Cybersecurity en digitale dreigingen
- Digitale sabotage
- Aantasten functioneren internet
- Cyberspionage
- Cybercriminaliteit

Natuurrampen
- Extreem weer
- Natuurbrand
- Overstroming
- Aardbeving

CBRN-dreigingen
- CBRN proliferatie
- Stralingsongevallen

Infectieziekten
- Infectieziekten humaan
- Dierziekten en zoönose

24 De risicocategorie Zware ongevallen uit de GRA is in zichzelf geen risico voor de nationale veiligheid, en daarom niet meegenomen in de inzet op het verhogen van weerbaarheid.

25 De geïntegreerde risico-analyse van het ANV is bij de NVS aan de Tweede Kamer verzonden.

Bijlage 2

Tabel 1

Nationaal veiligheidsbelang	Impactcriteria
1. Territoriale veiligheid	1.1 Aantasting van de integriteit van het (Nederlands) grondgebied 1.2 Aantasting van de integriteit van de internationale positie van Nederland 1.3 Aantasting van de integriteit van de digitale ruimte
2. Fysieke veiligheid	2.1 Doden 2.2 Ernstig gewonden en chronisch zieken 2.3 Gebrek aan primaire levensbehoeften
3. Economische veiligheid	3.1 Kosten 3.2 Aantasting van de vitaliteit van de Nederlandse economie
4. Ecologische veiligheid	4.1 Langdurige aantasting van het milieu en de natuur
5. Sociale en politieke stabiliteit	5.1 Verstoring van het dagelijkse leven 5.2 Aantasting van de democratische rechtstaat 5.3 Sociaal-maatschappelijke impact
6. Internationale rechtsorde	6.1 Aantasting van de normen van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting 6.2 Aantasting van de werking, legitimiteit dan wel naleving van de internationale verdragen en normen inzake de rechten van de mens 6.3 Aantasting van een op regels gebaseerd internationaal financieel-economisch bestel 6.4 Aantasting van de effectiviteit, legitimiteit van multilaterale instituties

Deze publicatie is een uitgave van de NCTV namens de Rijksoverheid.

info@nctv.minjenv.nl