Rijksbrede Risicoanalyse Nationale Veiligheid

Analistennetwerk Nationale Veiligheid

Rijksbrede Risicoanalyse Nationale Veiligheid

Analistennetwerk Nationale Veiligheid

Colofon

De Rijkbrede Risicoanalyse Nationale Veiligheid is opgesteld door
het Analistennetwerk Nationale Veiligheid in opdracht van de NCTV.

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)
Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael' (Clingendael)
SEO Economisch Onderzoek (SEO)
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Contactpersoon: ir. L. Gooijer (leendert.gooijer@rivm.nl)

Inhoudsopgave

Voorwoord

Deze Rijksbrede Risicoanalyse (RbRa) gaat over dreigingen die onze samenleving kunnen ontwrichten. We signaleren de dreigingen en geven een risico-inschatting wat de impact van deze dreigingen is voor de nationale veiligheid. Het overzicht van al die verschillende dreigingen en de bijbehorende risico's kan worden gebruikt bij de ontwikkeling van de Rijksbrede Veiligheidsstrategie (RbVS). Voor de strategievorming bestaat namelijk behoefte aan inzicht in de belangrijkste risico's voor de nationale veiligheid van het Koninkrijk der Nederlanden in de komende jaren. De Rijksbrede Risicoanalyse kan als input dienen voor deze strategie en is tevens bruikbaar voor de weerbaarheidsinschatting en de crisisbeheersing.

De RbRa is niet de eerste risicoanalyse die het Analistennetwerk Nationale Veiligheid (ANV) uitbrengt. Tot 2014 heeft het ANV de Nationale Risicobeoordeling (NRB) uitgebracht, waarin elk jaar enkele dreigingen werden geanalyseerd in de vorm van scenario's. In 2016 verscheen het Nationaal Veiligheidsprofiel (NVP) en in 2019 was er de Geïntegreerde risicoanalyse (GRA). Al deze analyses bevatten een all hazard overzicht van de belangrijkste risico's voor de nationale veiligheid.

Bij het opstellen van de RbRa is voortgebouwd op de kennis en ervaring opgedaan in het kader van deze eerdere analyses. Tegelijkertijd zijn er belangrijke aanpassingen en aanvullingen gedaan. Zo zijn reeds bestaande scenario's herzien, zijn er nieuwe scenario's geselecteerd en geanalyseerd, gaan we in op sluimerende dreigingen en hebben de onderwerpen digitalisering en internationalisering explicieter een plek gekregen in de methodiek.

Qua werkwijze vormt het ontwikkelen en beoordelen van scenario's ook bij de RbRa de belangrijkste basis. Voor de duiding van de meer dan zestig opgestelde scenario's, is een groot aantal expertsessies gehouden waarbij experts op het specifieke thema de impact en waarschijnlijkheid van voorliggende scenario's hebben beoordeeld. Via deze weg willen we de betrokken experts bedanken voor hun bijdrage aan deze sessies en het helpen vormgeven van de beschouwde scenario's. Wat deze ronde expertsessies bijzonder maakte, was dat de meeste expertsessies digitaal zijn gehouden. De sessies zijn namelijk georganiseerd in januari en februari 2022, ten tijde van de COVID-19-pandemie.

Het is goed om te melden dat enkele van de in de RbRa beschouwde dreigingen tijdens het uitvoeren van de analyse daadwerkelijk hebben plaatsgevonden. Zoals hierboven reeds is vermeld, hebben de RbRa expertsessies, maar ook de hieraan voorafgaande analyses, plaatsgevonden midden in de COVID-19-pandemie. Verder waren er in de zomer van 2021 grootschalige overstromingen in Limburg, België en Duitsland en anno 2022 heerst de vogelgriep in Nederland. Bovendien was er ten tijde van het vastleggen van de resultaten van de RbRa de Russische inval in de Oekraïne[1] en bij het schrijven van dit voorwoord (eind juni 2022) vinden er door heel Nederland protesten plaats vanwege het stikstofbeleid.

[1] De Russische inval en de oorlog in Oekraïne vonden plaats nadat de expertsessies (januari/februari 2022) voor deze risicoanalyse zijn gehouden, zodat daar niet expliciet op is ingegaan. Daarbij is het type dreiging wel expliciet meegenomen (o.a. in de vorm van een scenario waarin wordt ingegaan op de tijdelijke bezetting van een EU-lidstaat), en maakt de Russische assertiviteit en agressie deel uit van de context van meerdere themarapporten, in het bijzonder die betreffende internationale en militaire dreigingen. Zie verder het Nawoord.

Deze gebeurtenissen laten zien dat risicoanalyses zoals de RbRa niet alleen een papieren exercitie zijn, maar dat dreigingen en de bijbehorende risico's zich ook daadwerkelijk kunnen manifesteren. Een gegeven dat de waarde van risicoanalyses en het periodiek uitvoeren hiervan benadrukt, in het bijzonder voor de verbetering van de nationale veiligheid.[2]

Zoals gemeld is de RbRa uitgevoerd door het Analistennetwerk Nationale Veiligheid. Het ANV is een kennisnetwerk dat sinds 2011 analyses maakt van risico's en bedreigingen voor de nationale veiligheid. Het ANV bestaat uit een vast kern van zeven organisaties (RIVM, TNO, Instituut Clingendael, SEO, AIVD, MIVD, WODC) en een bredere kring van organisaties zoals kennisinstellingen, veiligheidsregio's en andere overheidsdiensten, bedrijven en onderzoeksbureaus.[3]

Naast dit RbRa hoofdrapport is er een aparte rapportage met een risicoanalyse voor het Caribisch deel van het Koninkrijk opgesteld en zijn er negen themarapportages beschikbaar waarin dieper ingegaan wordt op de afzonderlijke dreigingsthema's.

[2] Dat is ook een van de lessen en aanbevelingen van de Onderzoeksraad van de Veiligheid n.a.v. de aanpak coronacrisis. Zie: Onderzoeksraad voor Veiligheid, 2022. Aanpak coronacrisis. Deel 1: tot september 2020. In het rapport is ook uitgebreid ingegaan op het pandemiescenario dat het ANV eerder heeft uitgewerkt (p. 98/99).

[3] In bijlage 1 is een meer gedetailleerde beschrijving van het ANV opgenomen.

Samenvatting

Inleiding

De Rijksbrede Risicoanalyse (RbRa) geeft een overzicht van een breed scala aan dreigingen met een mogelijk ontwrichtend effect op het Koninkrijk der Nederlanden. Hierbij wordt niet alleen ingegaan op de eigenschappen van de dreiging zelf, maar ook op het bijbehorende risico. De resultaten van de RbRa dienen onder meer als input voor de Rijksbrede Veiligheidsstrategie. Bij het vertalen van de RbRa naar strategie of beleid, dienen wel enkele keuzes te worden gemaakt. Zo kan binnen de analyse onderscheid worden gemaakt tussen dreigingen met een grote impact op de samenleving, een hoge waarschijnlijkheid van optreden of een combinatie van beide. Het maken van de keuze op welk type dreiging wordt ingezet in een nieuwe strategie, ligt niet binnen de kaders van de RbRa. Een keuze die potentieel wordt gecompliceerd door het feit dat uit de analyse ook onderlinge verwevenheden, afhankelijkheden en overkoepelende onderwerpen naar voren komen die juist een meer integrale benadering vragen.

Kader van de risicoanalyse

De nationale veiligheidsbelangen vormen de basis voor de analyse van dreigingen binnen de RbRa. Als één of meer van de zes nationale veiligheidsbelangen ernstig worden aangetast, is er sprake van maatschappelijke ontwrichting en kan worden gesteld dat een dreiging potentieel de nationale veiligheid van het Koninkrijk der Nederlanden kan raken. De zes nationale veiligheidsbelangen zijn (i) territoriale veiligheid, (ii) fysieke veiligheid, (iii) economische veiligheid, (iv) ecologische veiligheid, (v) sociale en politieke stabiliteit en (vi) internationale rechtsorde en stabiliteit. Deze belangen kunnen door veel verschillende soorten dreigingen worden aangetast. Daarom is in de RbRa een *all hazard* aanpak gehanteerd; zowel moedwillige *(security)* als niet-moedwillige *(safety)* en zowel interne als externe dreigingen zijn in de analyse beschouwd.

Voor het in kaart brengen van de risico's van de verschillende dreigingen, zijn deze dreigingen vertaald naar scenario's. Tijdens expertsessies zijn deze scenario's op basis van een vastgelegde methodiek beoordeeld op waarschijnlijkheid van optreden en impact op de veiligheidsbelangen. Voor beide assen wordt een vijfpuntsschaal gehanteerd: van zeer onwaarschijnlijk tot zeer waarschijnlijk en van beperkt tot catastrofaal. Doordat alle scenario's op dezelfde wijze worden beoordeeld, zijn de risico's onderling vergelijkbaar. De Rijksbrede Risicoanalyse plaatst de verschillende risico's zo in vergelijkend perspectief.

In totaal zijn meer dan zestig scenario's uitgewerkt, verdeeld over negen dreigingsthema's:

- Klimaat- en natuurrampen;
- Infectieziekten;
- Zware ongevallen;
- Polarisatie, extremisme en terrorisme;
- Ongewenste inmenging en beïnvloeding democratische rechtsstaat;
- Internationale en militaire dreigingen;
- Economische dreigingen;
- Cyberdreigingen;
- Bedreiging vitale infrastructuur.

Bovenstaande dreigingsthema's zijn allemaal afzonderlijk geanalyseerd en voor elk thema is een eigen thema-rapportage opgesteld. Naast uitgewerkte scenario's is in de themarapporten ingegaan op relevante ontwikkelingen en sluimerende dreigingen. De resultaten van de losse thema's zijn bruikbaar om dieper in te gaan op specifieke dreigingen en bijbehorende risico's en zijn nuttig voor het uitvoeren van weerbaarheidsinschattingen en de versterking van de crisisbeheersing. De resultaten behorende tot de negen dreigingsthema's zijn vervolgens samengebracht en vormen de basis voor de overkoepelende resultaten van de RbRa.

Resultaten van de risicoanalyse vanuit drie perspectieven
Voor de beantwoording van de vraag welke dreigingen de komende de jaren de grootste risico's vormen voor de nationale veiligheid kunnen verschillende perspectieven worden gehanteerd.

Grootste waarschijnlijkheid
Als je kijkt naar de dreigingen met de grootste waarschijnlijkheid van optreden, dan valt op dat er relatief veel scenario's zijn die als zeer waarschijnlijk worden gezien (de hoogste waarschijnlijkheidsbeoordeling binnen de gehanteerde methodiek). Het gaat om scenario's uit verschillende thema's en betreffen zowel safety (natuurbranden, griepepidemie) als security dreigingen (hybride operaties, verstoringen internationale handel, collateral damage cyberaanvallen). Aangezien de waarschijnlijkheid van optreden van dit type dreigingen relatief groot is, is het belangrijk om voorbereid te zijn op het kunnen mitigeren van de impact.

Grootste impact
Er zijn veel scenario's waarvan de impact 'ernstig' of hoger is. Als we inzoomen op de dreigingen met de twee hoogste impactcategorieën (zeer ernstig en catastrofaal), blijkt dat ook hier een mix van zowel safety en security als interne en externe dreigingen is vertegenwoordigd. De grootste impact is te verwachten bij fysieke dreigingen uit de thema's klimaat- en natuurrampen en infectieziekten, namelijk bij een overstroming vanuit zee en een nieuwe pandemie vergelijkbaar met COVID-19. In beide gevallen is de impact zeer groot en worden meerdere veiligheids-belangen catastrofaal geraakt.
Ook hier geldt dat het van belang is om weerbaar te zijn tegen deze type dreigingen, waardoor uiteindelijk de kans dat een catastrofale impact optreedt, wordt verminderd. Denk hierbij aan de maatregelen die al langdurig worden getroffen om Nederland te beschermen tegen een overstroming uit zee.

Combinatie van impact en waarschijnlijkheid
Tot slot kan worden gekeken naar dreigingen die zowel een relatieve grote impact als waarschijnlijkheid hebben. Dit type dreiging komt terug in een groot aantal van de dreigingsthema's. Als we kijken naar de top negen scenario's wat betreft de combinatie van impact en waarschijnlijkheid, is vooral het dreigingsthema klimaat- en natuurrampen sterk vertegenwoordigd. Binnen dit thema betreft het enkele scenario's die vallen binnen de categorie extreem weer, te weten de scenario's hitte/droogte en orkanen. Het scenario orkanen is één van de grootste risico's voor het Caribisch deel van het Koninkrijk. Ook het scenario natuurbrand scoort hoog op zowel impact als waarschijnlijkheid. Bij het dreigingsthema klimaat- en natuurrampen is klimaatverandering een belangrijke driver voor de verschillende risico's.

Binnen het thema infectieziekten zijn ook meerdere scenario's met een hoge beoordeling op zowel impact als waarschijnlijkheid. In het geval van zowel een griep-epidemie als een pandemie zoals COVID-19 kunnen er naast grote aantallen doden en zieken (met als gevolg ernstige druk op de medische sector) ook (afhankelijk van de situatie en de genomen maatregelen) grote gevolgen voor de economie en de samenleving optreden.

Binnen het thema economische dreigingen laten de twee scenario's die zich in de top negen bevinden wat betreft zowel impact als waarschijnlijkheid, vooral de risico's zien van afhankelijkheid. Deze risico's kunnen zich mogelijk manifesteren zodra er schaarste dreigt of als er spanningen tussen betrokken actoren zijn. Het gaat hier specifiek om de scenario's met betrekking tot een verstoring van de handel door productieproblemen in het buitenland en (problemen met) de import van fossiele energie.

Tot slot zijn ook het thema ongewenste inmenging en beïnvloeding van de democratische rechtsstaat (scenario hybride operaties Rusland waarbij meerdere instrumenten worden ingezet) en het thema cyberdreigingen (scenario aanval cloud service provider) vertegenwoordigd in de top negen. Uit de analyse volgt dat bij cyberdreigingen soms niet goed in te schatten valt welke vervolgeffecten er precies zullen optreden, waaruit een bepaalde mate van onvoorspelbaarheid naar voren komt.

Alhoewel de bovenstaande thema's de hoogst scorende scenario's bevatten wanneer het gaat om de combinatie van impact en waarschijnlijkheid, wil dit niet zeggen dat de andere thema's vanuit dit perspectief gezien niet relevant zijn. Binnen het thema internationale en militaire dreigingen gaat het bijvoorbeeld om mogelijke instabiliteit rondom de Europese Unie en het Koninkrijk. Denk aan gebeurtenissen als het ineenstorten van de Venezolaanse staat of spanningen op de Balkan. Binnen het thema polarisatie, extremisme en terrorisme komt vanuit hetzelfde perspectief maatschappelijke polarisatie naar voren en vanuit het thema verstoring vitale infrastructuur een black out van de elektriciteitsvoorziening. Kortom, ook vanuit het perspectief van zowel impact als waarschijn-lijkheid komt een scala aan typen dreigingen naar voren.

Gebruik van de resultaten
De drie perspectieven die hierboven zijn gebruikt voor de duiding van de risico's kunnen ook dienen ter ondersteuning van het vervolg op de RbRa:
- Bij de dreigingen met een *hoge waarschijnlijkheid* lijkt het zinnig om daar als samenleving op voorbereid te zijn en na te gaan of de weerbaarheid op orde is. Denk aan natuurbranden, aanslagen door een alleenhandelende dader of de nevenschade als gevolg van een cyberaanval.

- Voor de dreigingen die tot de *grootste impact* op de nationale veiligheid kunnen leiden, ligt het voor de hand om de kans op voorkomen te minimaliseren. Daarbij is het uiteraard de vraag wat in onze eigen macht ligt om die kans zo klein mogelijk te maken of te houden en of extra investeringen wel in relatie staan tot de gerealiseerde veiligheidswinst.
- Voor het stellen van prioriteiten vanuit het risico-perspectief kunnen de dreigingen met een relatief *grote impact én hoge waarschijnlijkheid* worden gebruikt. Verdere analyse van de betreffende dreigingen kan inzicht geven of reductie van het risico eerder aan de kant van de waarschijnlijkheid of van de impact gezocht dient te worden.
- Door in te zoomen op de specifieke gevolgen van een bepaalde dreiging kan een weerbaarheidsanalyse worden geconcretiseerd en kunnen de resultaten gebruikt worden voor de versterking van de crisis-beheersing. Bij sommige dreigingen zal bijvoorbeeld het aantal slachtoffers groot zijn, waarbij de vraag kan worden gesteld of daar de benodigde hulp voor beschikbaar is dan wel hoe die beschikbaar kan worden gemaakt. Op deze manier kan een directe koppeling tussen risicoanalyse en weerbaarheids-inschatting worden gemaakt.

Onderlinge verwevenheid en overkoepelende constateringen

Naast de mogelijkheid om vanuit deze risicoanalyse in te zoomen op specifieke risico's, volgt uit de analyse de grote mate van *onderlinge verbondenheid en verwevenheid* tussen de verschillende risico's waar rekening mee moet worden gehouden. Denk hierbij aan de verwevenheid en afhankelijkheden tussen vitale processen en digitalisering (waar met name de afhankelijkheid van elektriciteit en telecom eruit springen) en tussen economische en internationale ontwikkelingen.

In aanvulling daarop zijn er in de analyse enkele overkoepelende onderwerpen naar voren gekomen, te weten *klimaatverandering, energietransitie, spanningen in de samenleving* en *hybride dreigingen*. Bij deze onderwerpen komen verschillende ontwikkelingen samen die relevant zijn voor de nationale veiligheid. Zo is klimaatverandering een driver die negatieve gevolgen zal hebben op zowel de impact als waarschijnlijkheid van meerdere dreigingen. Daarbij gaat het dus niet alleen om het thema klimaat- en natuurrampen (zoals toenemende kans op weersextremen met onder andere gevolgen voor de vitale infrastructuur), maar kan klimaatverandering ook maatschappelijke en internationale spanningen versterken. Rondom de energietransitie spelen diverse vraagstukken, denk aan een grotere afhankelijkheid van en druk op het elektriciteitsnet en afhankelijkheden van bronnen, materialen, technologie en (buitenlandse) actoren. Spanningen in de samenlevingen kunnen zowel bij moedwillige dreigingen als bij niet-moedwillige scenario's worden aangewakkerd. Zo kunnen spanningen ontstaan in het kader van de uitdagingen die zowel klimaatverandering als energietransitie met zich meebrengen, maar kunnen ze ook het resultaat zijn van de acties van extremistische of statelijke actoren. Het aanwakkeren van deze spanningen door statelijke actoren kan onderdeel zijn van een hybride dreiging. Bij hybride dreigingen ligt de focus op de moedwillige inzet van meerdere instrumenten door statelijke actoren onder de drempel van gewapend conflict die los van elkaar de nationale veiligheid niet zwaar hoeven te raken, maar als geheel wel de nationale veiligheid kunnen aantasten. Bijvoorbeeld het opzetten van desinformatiecampagnes en het uitvoeren van cyberaanvallen. Hybride dreigingen zijn niet beperkt tot één bepaald type handeling en dus ook niet tot één bepaald type dreiging.

Bovenstaande overkoepelende onderwerpen kunnen integraal geanalyseerd worden vanuit het perspectief van de weerbaarheid en crisisbeheersing. De onderlinge verbondenheid en afhankelijkheden leiden tot een zekere mate van onvoorspelbaarheid van gevolgen als een risico zich manifesteert. Dit vraagt een meer integrale benadering, waarbij vraagstukken als complex systeem benaderd kunnen worden.

Afsluitend

Binnen RbRa is een groot aantal dreigingen en bijbehorende risico's beschouwd. Waar voor sommige van deze dreigingen geldt dat deze al geruime tijd niet zijn voorgekomen in het Koninkrijk der Nederlanden of in de toekomst als (zeer) onwaarschijnlijk worden gezien, zijn anderen reeds werkelijkheid geworden of is de inschatting dat het waarschijnlijk is dat we hier als samenleving de komende jaren (wederom) mee zullen worden geconfronteerd. Het in de RbRa geschetste dreigingsbeeld is nadrukkelijk niet statisch van aard, maar is onderhevig aan onder andere maatschappelijke, internationale en technologische ontwikkelingen. Het is van belang om als samenleving goed op de hoogte te zijn en te blijven van de set aan dreigingen die de nationale veiligheid kan aantasten, onder meer door het uitvoeren van periodieke analyses zoals die in de RbRa. Aan de hand hiervan ontstaan handvatten voor het creëren van een weerbaar Koninkrijk der Nederlanden.

1. Inleiding

1.1 Het kader van de Rijksbrede Risicoanalyse

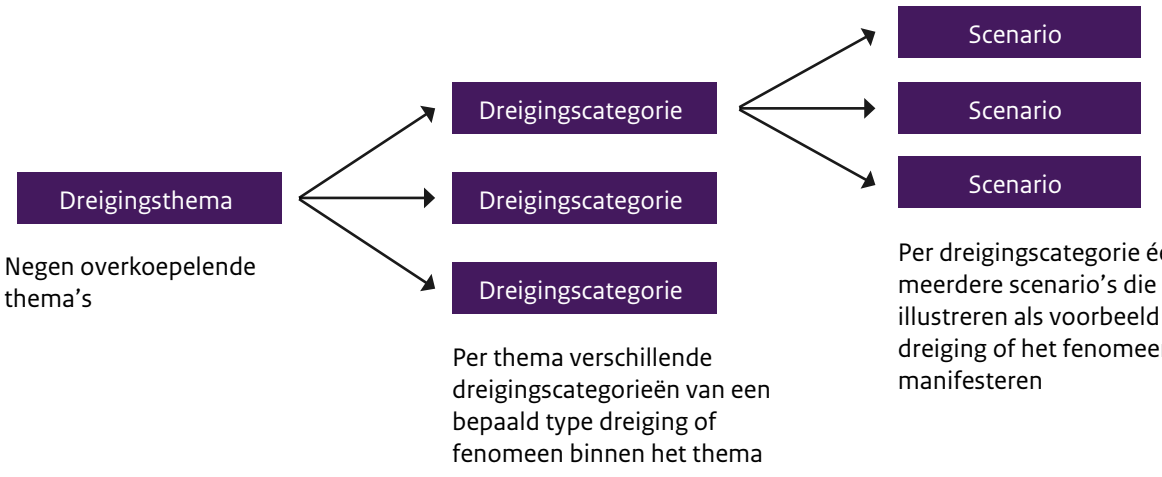
Voor u ligt het hoofdrapport van de Rijksbrede Risicoanalyse Nationale Veiligheid 2022 (RbRa), opgesteld door het Analistennetwerk Nationale Veiligheid (ANV). Deze analyse geeft een overzicht van een breed scala aan dreigingen die onze samenleving kunnen ontwrichten en de bijbehorende risico's. Een groot aantal dreigingen is geïdentificeerd en vervolgens aan de hand van concrete scenario's geanalyseerd langs de assen van impact en waarschijnlijkheid om inzicht te verschaffen in de risico's die hierin schuilen. De resultaten van de RbRa vormen input voor de Rijksbrede Veiligheidsstrategie. Dit hoofdrapport vormt een synthese van negen onderliggende door het ANV opgestelde RbRa themarapporten.

Omdat de nationale veiligheid door veel verschillende soorten dreigingen kan worden aangetast, is een all hazard aanpak gebruikt. Zowel moedwillige (security) als niet-moedwillige (safety) en zowel interne als externe dreigingen worden beschouwd. Om te assisteren bij het in kaart brengen van de impact en waarschijnlijkheid van soms abstracte dreigingen, zijn deze dreigingen vertaald naar één of meerdere concrete scenario's. In totaal zijn meer dan zestig scenario's uitgewerkt, verdeeld over negen dreigingsthema's:

- Klimaat- en natuurrampen;
- Infectieziekten;
- Zware ongevallen;
- Polarisatie, extremisme en terrorisme;
- Ongewenste inmenging en beïnvloeding democratische rechtsstaat;
- Internationale en militaire dreigingen;
- Economische dreigingen;
- Cyberdreigingen;
- Bedreiging vitale infrastructuur.

Elke van de negen dreigingsthema's is onderverdeeld in meerdere dreigingscategorieën, elk met een aantal bijbehorend scenario's. Zo bestaat het thema klimaat- en natuurrampen uit de dreigingscategorieën overstroming, aardbeving, extreem weer en natuurbrand. Binnen bijvoorbeeld de categorie overstroming zijn dan weer verschillende scenario's uitgewerkt, zoals een overstroming vanuit de zee of vanuit een rivier. Het figuur hieronder geeft de verhouding weer tussen thema, categorie en scenario. Een complete lijst van dreigingsthema's en categorieën is opgenomen in bijlage twee.

Figuur 1 Relatie thema, categorie en scenario



De verschillende scenario's zijn allemaal op dezelfde wijze beoordeeld, aan de hand van de door het ANV opgestelde methodiek nationale veiligheid. Deze methodiek is gebaseerd op zes nationale veiligheidsbelangen die worden gebruikt voor het bepalen van de gevolgen van een dreiging voor de samenleving. Deze zes belangen betreffen niet alleen territoriale, fysieke, economische en ecologische veiligheid, maar ook sociale en politieke stabiliteit en tot slot de internationale rechtsorde en stabiliteit. Onderstaande tabel geeft de beschrijving van de nationale veiligheidsbelangen. Voor een verdere beschrijving van de werkwijze en de methodiek van het ANV wordt verwezen naar bijlage twee.

Tabel 1 Nationale veiligheidsbelangen

De zes nationale veiligheidsbelangen	
Territoriale veiligheid	Het ongestoord functioneren van het Koninkrijk der Nederlanden en haar EU en NAVO bondgenoten als onafhankelijke staten in brede zin, dan wel de territoriale veiligheid in enge zin.
Fysieke veiligheid	Het ongestoord functioneren van de mens in het Koninkrijk der Nederlanden en zijn omgeving.
Economische veiligheid	Het ongestoord functioneren van het Koninkrijk der Nederlanden als een effectieve en efficiënte economie.
Ecologische veiligheid	Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij het Koninkrijk der Nederlanden.
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 democratische rechtsstaat van het Koninkrijk der Nederlanden en daarin gedeelde waarden.
Internationale rechtsorde en stabiliteit	Het goed functioneren van het internationale stelsel van normen en afspraken, gericht op het bevorderen van de internationale vrede en veiligheid, inclusief mensenrechten, en effectieve multilaterale instituties en regimes, alsmede het goed functioneren van staten grenzend aan het Koninkrijk der Nederlanden en in de directe omgeving van de Europese Unie.

De nationale veiligheid is in het geding als één of meer van de nationale veiligheidsbelangen zodanig worden bedreigd dat er sprake is van (potentiële) maatschappelijke ontwrichting.

In vergelijking met eerdere door het ANV uitgevoerde analyses zoals het Nationaal Veiligheidsprofiel 2016 en de Geïntegreerde risicoanalyse 2019, zijn de nationale veiligheidsbelangen en de uitwerking hiervan in impactcriteria, alsmede de bijbehorende analyse op enkele onderdelen aangepast en aangevuld ten behoeve van de RbRa. Zo hebben aspecten die samenhangen met digitalisering en internationalisering explicieter een plek gekregen in de methodiek.

Verder is ook de reikwijdte van deze analyse breder dan vorige edities. Er wordt gekeken naar dreigingen voor het gehele Koninkrijk der Nederlanden, inclusief het Caribisch deel van het Koninkrijk.

Een andere aanvulling is de opname van sluimerende dreigingen. Naast dreigingen die in de vorm van de meer dan 60 reguliere scenario's zijn geanalyseerd en waarbij een tijdshorizon wordt gehanteerd van ongeveer vijf jaar, is in deze analyse ook aandacht gegeven aan meer sluimerende dreigingen of ontwikkelingen die vooral op de langere termijn (10 – 20 jaar) relevant kunnen zijn. Zo kan een indruk worden gekregen van onderwerpen die mogelijk over 10-20 jaar pas relevant zijn, maar wellicht nu al actie vereisen. Daarnaast hebben we op sommige plekken de randen van het voorstelbare opgezocht in de vorm van wild cards. De sluimerende dreigingen en wild cards zijn kwalitatief beschreven en zijn aanvullend op de risico's die in de vorm van scenario's zijn geanalyseerd en beoordeeld tijdens expertsessies op waarschijnlijkheid en impact. Een aantal van de sluimerende dreigingen komen terug in hoofdstuk 13, welke ingaat op enkele overkoepelende onderwerpen in het kader van de RbRa. Voor de wild cards wordt verwezen naar de verschillende themarapportages.

Voor de verdere beschrijving van de werkwijze en de methodiek wordt verwezen naar bijlage 2.

1.2 Doel en reikwijdte

Doel van deze risicoanalyse is het geven van een overzicht van relevante risico's voor de nationale veiligheid van het Koninkrijk der Nederlanden, zodat er onderbouwde keuzen kunnen worden gemaakt qua prioritering en kan worden gekeken naar de beschikbare en benodigde weerbaarheid. De RbRa komt zelf niet tot een prioritering van dreigingen, maar vormt hiertoe input voor de Rijksbrede Veiligheidsstrategie (RbVS).[4]

1.3 Leeswijzer

Dit rapport bestaat uit verschillende onderdelen. Deel één gaat per dreigingsthema in op de voornaamste resultaten van de risicoanalyse. In de bijbehorende hoofdstukken twee tot en met tien komen de volgende dreigingsthema's aan bod:

- Hoofdstuk 2: Klimaat- en natuurrampen;
- Hoofdstuk 3: Infectieziekten;
- Hoofdstuk 4: Zware ongevallen;
- Hoofdstuk 5: Polarisatie, extremisme en terrorisme;
- Hoofdstuk 6: Ongewenste inmenging en beïnvloeding democratische rechtsstaat;
- Hoofdstuk 7: Internationale en militaire dreigingen;
- Hoofdstuk 8: Economische dreigingen;
- Hoofdstuk 9: Cyberdreigingen;
- Hoofdstuk 10: Bedreiging vitale infrastructuur.

Elk van deze hoofdstukken bevat naast een kwalitatieve omschrijving van de belangrijkste resultaten ook het risicodiagram van het thema in kwestie.[5] Hier worden de binnen het thema geanalyseerde scenario's weergegeven langs de assen van impact en waarschijnlijkheid. Hoofdstuk 11 gaat vervolgens in op risico's voor het Caribisch deel van het Koninkrijk. Per dreigingsthema en voor het Caribisch deel van het Koninkrijk is tevens een aparte thema-rapportage opgesteld. Deze themarapportages gaan in meer detail in op voor het thema relevante ontwikkelingen, de door het ANV opgestelde scenario's en de voorziene gevolgen en waarschijnlijkheid hiervan. Dit hoofdrapport bevat voor elk van de bovenstaande thema's een synthese van de belangrijkste uitkomsten en observaties uit het betreffende themarapport.

Deel twee van dit rapport gaat in op de resultaten van de RbRa als geheel alsmede de dwarsverbanden tussen de verschillende dreigingsthema's en het bredere dreigingslandschap nationale veiligheid. Hoofdstuk 12 bevat de algehele uitkomsten van de RbRa in de vorm van het risicodiagram waarin alle uitgewerkte scenario's worden weergegeven langs de assen van impact en waarschijnlijkheid. Dit diagram wordt gebruikt voor het presenteren, bespreken en duiden van de resultaten. Hoofdstuk 13 gaat in op enkele overkoepelende onderwerpen die naar voren zijn gekomen in meerdere dreigingsthema's. Hoofdstuk 14 bevat een beschouwing van het dreigingslandschap nationale veiligheid als een complex systeem.

Het derde en laatste deel van deze rapportage bevat tenslotte de slotbeschouwing van deze risicoanalyse (hoofdstuk 15), waarin onder andere enkele richtingen worden beschreven over hoe met de resultaten van de RbRa kan worden verdergegaan. In de bijlagen kan niet alleen meer informatie worden gevonden over het ANV en de door het ANV gehanteerde methodiek nationale veiligheid, maar ook een overzicht van alle dreigingsthema's.

[4] Zoals gemeld is de reikwijdte van deze analyse het gehele Koninkrijk der Nederlanden, inclusief het Caribisch deel. In dat kader kan de vraag naar voren komen of de term 'nationale veiligheid' wel de juiste is en wellicht een alternatief als 'Rijksbrede veiligheid' beter is. Aangezien 'nationale veiligheid' een meer gangbare term is, wordt deze hier gehanteerd.

[5] Voor referenties betreffende (onder andere) de in de themahoofdstukken gehanteerde definities, wordt verwezen naar de onderliggende themarapportages.

DEEL 1:
Resultaten per dreigingsthema

Dit onderdeel van het RbRa hoofdrapport bevat voor elk van de negen dreigingsthema's en de analyse voor het Caribisch deel van het Koninkrijk een overzicht van de voornaamste resultaten. Voor aanvullende informatie wordt verwezen naar de achterliggende door het ANV opgestelde themarapporten.

2. Klimaat- en natuurrampen

Binnen het thema klimaat- en natuurrampen zijn vier verschillende typen klimaat- en natuurrampen in kaart gebracht, die de nationale veiligheid kunnen raken, namelijk overstromingen, extreem weer, natuurbranden en aardbevingen. Het gaat hierbij om (potentiële) rampen die veroorzaakt worden door natuurgeweld.[6] Daarbij ligt de focus op klimaat- en natuurrampen in Nederland met effecten in Nederland, maar is in dit thema ook ingegaan op orkanen die kunnen plaatsvinden in het Caribisch deel van het Koninkrijk. In totaal zijn voor acht scenario's de impact en waarschijnlijkheid in kaart gebracht. In onderstaande figuur worden deze scenario's in vergelijkend perspectief weergegeven.

Figuur 2 Risicodiagram klimaat- en natuurrampen

Catastrofaal		• Overstroming zee			
Zeer ernstig	• Geïnduceerde aardbeving		• Overstroming rivier	• Orkaan • Hitte/droogte	
Ernstig			• Sneeuwstorm		• Natuurbranden
Aanzienlijk			• Natuurlijke aardbeving		
Beperkt					
	Zeer onwaarschijnlijk	**Onwaarschijnlijk**	**Enigszins waarschijnlijk**	**Waarschijnlijk**	**Zeer waarschijnlijk**

[6] Aardbevingen kunnen een natuurlijke oorzaak hebben of worden geïnduceerd door de mens. Beide typen aardbevingen zijn meegenomen. Daarbij valt op te merken dat geïnduceerde aardbevingen door menselijk handelen veroorzaakt worden, en dus geen natuurlijke oorzaak hebben. Desondanks nemen we deze dreiging ook mee onder natuurrampen, aangezien hierbij natuurgeweld naar voren komt.

Het valt op dat zowel de impact als de waarschijnlijkheid van de scenario's sterk uiteenloopt. De impact is daarbij relatief hoog. Dit heeft voornamelijk te maken met de omvang van de gebieden die getroffen kunnen worden door klimaat- en natuurrampen. Doordat grote gebieden geraakt kunnen worden, door bijvoorbeeld een overstroming, een orkaan (Caribisch deel) of extreme hitte en droogte, kan er ook op grote schaal aantasting van het grondgebied of de ecologie plaatsvinden, kunnen er veel slachtoffers vallen, kan er een groot gebrek aan primaire levensbehoefte ontstaan en kan in een groot gebied de dagelijkse gang van zaken verstoord raken. Door de omvang van de getroffen gebieden bestaat tijdens de herstelperiode tevens het gevaar dat mensen in het ene gebied het gevoel krijgen slechter af te zijn dan mensen in andere gebieden, door keuzes die worden gemaakt tijdens het herstel. Dit kan tot onbegrip en woede leiden onder de getroffenen.

Opvallend is dat klimaat- en natuurrampen een brede impact hebben. Vrijwel alle nationale veiligheidsbelangen kunnen worden geraakt. Het gaat hierbij om de belangen territoriale, fysieke, economische en ecologische veiligheid en sociaal-politiek stabiliteit. Alleen het belang internationale rechtsorde wordt door klimaat- en natuurrampen niet geraakt. Het belang fysieke veiligheid wordt het ernstigst geraakt. Hierbinnen vallen de criteria doden, gewonden en chronisch zieken en gebrek aan primaire levensbehoefte. Alle drie de criteria kunnen door klimaat- en natuurrampen sterk getroffen worden. Opvallend zijn vooral de hoge scores op het criterium ernstig gewonden en chronische zieken. Hierbij gaat het enerzijds om mensen die direct gewond raken, bijvoorbeeld door vallende brokstukken bij een aardbeving of onderkoeling bij een overstroming. Anderzijds kan een ramp mentale problemen veroorzaken, in de vorm van depressie, angst of posttraumatische stressstoornis, zowel in het getroffen gebied als daarbuiten. Ook dit raakt de nationale veiligheid wanneer hier op grote schaal sprake van is.

Klimaat- en natuurrampen hebben een sterke koppeling met vitale processen. Bij vrijwel alle typen klimaat- en natuurrampen kunnen vitale processen als elektriciteits-, drinkwater- en gasvoorziening en telecommunicatie worden geraakt. Dit geldt niet alleen binnen het direct getroffen gebied, maar ook daarbuiten kan een deel van de vitale processen uitvallen door cascade-effecten. Uitval van vitale processen zorgt ervoor dat het dagelijks leven verstoord raakt en er gebrek aan primaire levensbehoeften kan ontstaan.

Ook is er een sterke koppeling met economische dreigingen. Door verschillende type klimaat- en natuurrampen kan bijvoorbeeld de knooppuntfunctie van Nederland bedreigd worden, doordat bepaalde transportmogelijkheden tijdelijk niet bruikbaar zijn. De aan- en afvoer van goederen van en naar het achterland wordt hierdoor beperkt. Dit leidt tot de toename van transportprijzen, welvaartsverliezen en tekorten van bepaalde producten.

Zoals gezegd loopt ook de waarschijnlijkheid van de scenario's sterk uiteen. Sommige dreigingen treden al vaker op, maar de impact blijft tot nog toe relatief beperkt. Het is echter goed voorstelbaar dat de impact groter zal worden en de dreiging daadwerkelijk zal uitgroeien tot een ramp. Een voorbeeld hiervan is natuurbranden. Gemiddeld komt vrijwel elk jaar een onbeheersbare natuurbrand voor. Door het intensieve gebruik van natuurgebieden is de kans op slachtoffers groot. Daarbij komt dat wanneer meerdere branden tegelijk ontstaan, dit uitdagingen oplevert voor de verdeling van bestrijdingscapaciteiten. Daarnaast worden er nauwelijks beheersmaatregelen genomen om het risico te verkleinen. Het is volgens de deskundigen daarom niet de vraag of maar wanneer een onbeheersbare natuurbrand optreedt, waarbij ernstige gevolgen zullen ontstaan.

Het uitgewerkte scenario van een geïnduceerde aardbeving wordt als zeer onwaarschijnlijk ingeschat. Dit volgt uit de combinatie van de verschillende factoren van het scenario, namelijk een zware aardbeving en daarbij grote gevolgen, zoals slachtoffers en het instorten van gebouwen. Dit neemt niet weg dat er meermaals geïnduceerde aardbevingen, met een lager magnitude dan in het scenario, in Nederland voorkomen, met name in Groningen. Deze aardbevingen hebben in het getroffenen gebied grote impact, maar hierbij is geen sprake van dodelijke slachtoffers en ingestorte gebouwen.

In deze analyse ligt de nadruk op dreigingen die het Koninkrijk binnen nu en vijf jaar kunnen raken. Om meer sluimerende dreigingen in beeld te krijgen, is ook gekeken naar ontwikkelingen die op langere termijn, 10 tot 20 jaar, tot dreigingen kunnen leiden of die van invloed zijn op de impact en waarschijnlijkheid van de dreigingen en er daardoor voor kunnen zorgen dat op termijn de nationale veiligheid ernstiger of sneller geraakt wordt.

Klimaatverandering is een belangrijke ontwikkeling die van invloed is op de impact en waarschijnlijkheid van vrijwel alle dreigingscategorieën (behalve aardbevingen). Hier wordt in hoofdstuk 13 verder op ingegaan. Naast klimaatverandering zijn de economische groei en demografische ontwikkeling in Nederland van invloed op de impact van de dreigingscategorieën. Door economische groei en bevolkingsgroei in gebieden die vatbaar zijn voor overstromingen, natuurbranden of aardbevingen neemt de mogelijke impact hiervan toe. De economische schade zal hoger zijn, maar ook het aantal potentiële slachtoffers neemt toe. Een voorbeeld hiervan zijn de doorgaande investeringen in woningen en infrastructuur in de laagstgelegen delen van Nederland. Door de lange levensduur van deze investeringen, krijgen deze zeker te maken met de langetermijneffecten van klimaatverandering. Daarbij komt dat de maatschappij steeds kwetsbaarder wordt voor klimaat- en natuurrampen als extreem weer en aardbevingen.

Ook zijn er opkomende technologische ontwikkelingen, die, naast voordelen, ook dreigingen binnen het thema klimaat- en natuurrampen met zich mee kunnen brengen. Een voorbeeld hiervan is geo-engineering: de grootschalige beïnvloeding van het klimaat om de opwarming van de aarde en de effecten daarvan tegen te gaan. Verschillende landen passen al technieken van geo-engineering toe, bijvoorbeeld om extreme hitte tegen te gaan of om neerslag op te wekken, en hebben de intentie dit steeds vaker te gaan doen. De neveneffecten van geo-engineering op lange termijn voor het klimaat, het milieu en ecosystemen zijn niet bekend en mogelijk risicovol, doordat bijvoorbeeld juist extreem weer kan ontstaan of de ozonlaag aangetast kan worden. Ook kan geo-engineering, zowel bewust als onbewust, leiden tot geopolitieke spanningen. Wanneer wereldwijd klimaatbeleid faalt, wordt de kans groter dat meerdere landen geo-engineering gaan inzetten om de gevolgen van klimaatverandering te bestrijden.

3. Infectieziekten

Binnen het thema infectieziekten zijn er vier verschillende dreigingscategorieën onderscheiden:
- Humane infectieziekten en zoönosen;
- Dierziekten en plantenziekten;
- Antimicrobiële resistentie (AMR);
- Voedselcrises.

Het onderscheid tussen de eerste twee dreigingscategorieën is voornamelijk gebaseerd op de manier van overdracht tussen mensen, dieren en planten. Bij humane infectieziekten vindt er overdracht tussen mensen plaats, terwijl bij zoönose de verspreiding van dier op mens gaat. Dat kan vervolgens ook verder gaan van mens op mens zoals de COVID-19-pandemie laat zien. Bij de categorie dierziekten en plantenziekten vindt er geen overdracht naar de mens plaats. De dreigingscategorieën AMR en voedselcrisis zijn apart beschouwd, omdat deze typen dreigingen anders van aard zijn en er naast de belangrijke link met infectieziekten ook andere factoren meespelen. Hiervoor zijn geen scenario's uitgewerkt. Zowel AMR als een voedselcrisis worden als sluimerende dreiging gezien. In onderstaande risicodiagram zijn de geanalyseerde scenario's weergegeven.

Figuur 3 Risicodiagram Infectieziekten

	Zeer onwaarschijnlijk	Onwaarschijnlijk	Enigszins waarschijnlijk	Waarschijnlijk	Zeer waarschijnlijk
Catastrofaal			• Pandemie door een mens overdraagbaar respiratoir virus		
Zeer ernstig			• Griep pandemie		
Ernstig					• Griep epidemie
Aanzienlijk				• Uitbraak MKZ onder koeien	
Beperkt			• Uitbraak zoönotische variant vogelgriep		

Humane infectieziekten en zoönosen

Uit het risicodiagram valt ten eerste de hoge waarschijnlijkheid van de griepepidemie op. Dit is gebaseerd op het feit dat er bijna elk jaar een griepepidemie voorkomt die wordt veroorzaakt door bestaande typen influenzavirussen. Een pandemie heeft een lagere waarschijnlijkheid, maar heeft wel een grote impact op de nationale veiligheid. Uit de analyse volgt dat de impact van een pandemie veroorzaakt door een nieuw mensoverdraagbaar respiratoir virus groter is dan die van een grieppandemie. De pandemie veroorzaakt door een nieuw mensoverdraagbaar respiratoir virus is gebaseerd op de COVID-19-pandemie. Dit kan van oorsprong een zoönose zijn die mensoverdraagbaar is.

De impact bij humane infectieziekten is vooral zichtbaar op het gebied van doden en zieken en bij een ernstige pandemie ook wat betreft het gebrek aan voldoende acute zorg. Daarnaast zijn de kosten hoog, die in geval van zware maatregelen om een pandemie te bestrijden tot de maximale beoordeling kunnen oplopen. Tenslotte is er bij de pandemiescenario's een grote verstoring van het dagelijks leven, als gevolg van uitval door zieken en/of als gevolg van maatregelen zoals een lockdown. Dit leidt potentieel tot sociaal-maatschappelijke impact, zoals polarisatie, afnemende solidariteit en rellen. Dit is zeker bij het scenario van een uitbraak van een nieuw mens overdraagbaar respiratoir virus voorstelbaar. Hier is een koppeling met het thema polarisatie, extremisme en terrorisme te maken, waar onder meer het wantrouwen tegen overheidspartijen naar voren komt als onderwerp.

De snelheid van verspreiding wordt vooral bepaald door de vraag of de ziekteverwekker van mens tot mens overdraagbaar is, of de transmissie van ziekteverwekkers via de lucht of direct contact kan plaatsvinden en door de responstijd. Daarbij is (zeker ook door de COVID-19-pandemie) duidelijk dat globalisering (inclusief toerisme) een factor is die de verspreiding wereldwijd versterkt.

Om de responstijd te minimaliseren is met name aandacht voor een snelle detectie van de ziekteverwekker en een goede herkenning en erkenning van mogelijke signalen van een epidemie van belang. Voornamelijk op het vlak van de detectie en signalering van mogelijke uitbraken van ziekteverwekkers zijn er de laatste jaren gunstige ontwikkelingen geweest. Er worden steeds meer geavanceerde moleculaire technieken ingezet om in combinatie met bioinformatica sneller en nauwkeuriger diagnostiek te kunnen bedrijven om aard en omvang van de uitbraken te kunnen vaststellen. Daarnaast loopt er een geïntegreerde signaleringsstructuur tussen humane infectieziekten en besmettelijke dierziekten (de One Health aanpak). Deze signaleringsstructuur is ook gebruikt tijdens de COVID-19-pandemie.

De mondiale uitbraak van COVID-19 heeft kwetsbaarheden met betrekking tot bekende aandachtspunten in de respons blootgelegd. Denk hierbij aan de beschikbaarheid van specialistische zorg (met name de IC zorg en beademingsapparaten) en de mogelijkheden voor aparte verpleging (quarantaine) die nodig kan zijn bij een nieuwe pandemie. Daarnaast is de leveringszekerheid en beschikbaarheid van persoonlijke beschermingsmiddelen en vaccins minder stuurbaar door de productie hiervan door slechts enkele wereldspelers op een mondiale markt. De urgentie van vaccinontwikkeling tegen varianten van SARS-Cov-2 heeft de mondiale samenwerking tussen bedrijfsleven en academica wel versterkt. De COVID-19-pandemie heeft laten zien dat er binnen de samenleving spanningen naar voren kunnen komen en er discussies over onder ander vaccins optreden. Dergelijke discussies kunnen potentieel door buitenlandse actoren worden gevoed. Daarbij is er een link met hybride dreigingen met het verspreiden van desinformatie als mogelijk instrument (zie ook hoofdstuk 6).

Dierziekten en plantenziekten

De recente uitbraken van varianten van Aviaire influenza (vogelgriep) hebben laten zien dat een goede voorbereiding en uitvoering van een nationale respons noodzakelijk is en blijft. In de uitwerking is ervoor gekozen om alleen voor dierziekten een scenario uit te werken en te boordelen op de waarschijnlijkheid van optreden en de impact op de nationale veiligheid. Dit omdat voor plantenziekten er niet direct een aantasting van de nationale veiligheid zal plaatsvinden.

Uit de analyse volgt dat de kans dat de komende jaren een uitbraak van een dierziekte, zoals varkenspest, MKZ of (niet-zoönotische) vogelgriep plaats vindt, relatief groot is. Wat betreft de impact volgt uit de beoordeling dat veel criteria worden geraakt en de totale impact aanzienlijk is. De financiële schade en de sociaal-maatschappelijke impact zijn in dit geval het grootst. Hierbij is duidelijk dat de gevolgen van een dergelijke dierziekte de mensen en bedrijven in de betreffende sector significant raken. Dat zie je verder terug bij het verwachtte aantal mensen met mentale aandoeningen en de impact op het dagelijks leven. Daarnaast kunnen er uitingen van woede en frustratie ontstaan in de vorm van geweld en intimidatie over getroffen maatregelen. Een gevoel van onrecht kan leiden tot verharding en polarisatie, waarbij er wederom een link is met het thema polarisatie, extremisme en terrorisme.

Antimicrobiële resistentie

De problematiek van AMR nu en in de komende jaren vormt geen bedreiging voor de nationale veiligheid, maar gezien de wereldwijde toename van resistentie kan AMR nog steeds als 'sluipmoordenaar' worden beschouwd en het is daarom van belang om dit goed te blijven monitoren.

In ons land is carbapenem resistentie (CRE) één van de meest zorgwekkende ontwikkelingen, omdat bacterie-infecties kunnen optreden die vanwege resistentie niet of nauwelijks meer zijn te behandelen. Het vóórkomen van deze CRE wordt nauwlettend gemonitord en verspreiding wordt zo goed mogelijk voorkomen, onder meer door screening, vroegsignalering en adequate maatregelen bij incidentele gevallen en uitbraken. Hierbij blijft de 'One Health' benadering, waarin alle facetten van menselijke gezondheid in relatie tot de gezondheid van dieren en het milieu integraal worden beschouwd, zeer belangrijk.

Voedselcrisis

Grootschalige voedselcrises komen niet vaak voor, en op basis van de eerdere analyse is het beeld dat de impact in geval van optreden beperkt zal blijven. Op basis hiervan is de conclusie dat het belangrijk is voldoende aandacht te blijven houden voor voedselveiligheid, maar dat incidenten en crises met voedsel geen bedreiging vormen voor de nationale veiligheid. Naar verwachting zal dit de komende jaren niet veranderen.

Binnen het themarapport klimaat- en natuurrampen komt voedselschaarste aan de orde bij het onderwerp klimaatverandering. Als gevolg van klimaatverandering (en ook als gevolg van internationale conflicten) kunnen in delen van de wereld voedselschaarste ontstaan, waardoor voedselprijzen toenemen en migratiebewegingen op gang kunnen komen.

4. Zware ongevallen

Binnen het thema zware ongevallen is ingegaan op de risico's van niet-moedwillige stralingsongevallen, chemische ongevallen en transportongevallen. Binnen de categorieën stralingsongevallen en chemische ongevallen zijn voor vier scenario's de gevolgen en waarschijnlijkheid in kaart gebracht, in beide categorieën twee scenario's. In onderstaande figuur worden deze scenario's in vergelijkend perspectief weergegeven.

Figuur 4 Risicodiagram zware ongevallen

Catastrofaal					
Zeer ernstig					
Ernstig	• Kerncentrale Borssele • Treinramp met gaswolkbrand				
Aanzienlijk	• Stralingsongeval in Europa • Falen opslagtank ammoniak				
Beperkt					
	Zeer onwaarschijnlijk	**Onwaarschijnlijk**	**Enigszins waarschijnlijk**	**Waarschijnlijk**	**Zeer waarschijnlijk**

Als we naar het risicodiagram kijken valt als eerste op dat de binnen dit thema uitgewerkte scenario's allemaal een lage waarschijnlijkheid van optreden hebben (zeer onwaarschijnlijk). De reden om zeer onwaarschijnlijke scenario's uit te werken is om na te gaan in hoeverre het thema zware ongevallen de nationale veiligheid kan raken of dat het vooral op lokaal of regionaal niveau relevantie heeft.

De beschouwde categorieën hebben een brede impact. De meeste veiligheidsbelangen worden geraakt, waarbij geldt dat de impact relatief vaak aanzienlijk of ernstig is met soms een zeer ernstige impact. De impact op de nationale veiligheid komt vooral naar voren bij de belangen fysieke, economische en territoriale veiligheid en sociaal-politieke stabiliteit. In het kort gaat het dan met name om slachtoffers, financiële schade en verstoring van het dagelijks leven door deze ongevallen.

Bij deze constateringen is het goed om wel nuance aan te brengen en verschil te maken tussen de stralingsongevallen enerzijds en chemische ongevallen anderzijds. Zo vallen er bij een ongeval bij een kerncentrale geen directe dodelijke slachtoffers als gevolg van de blootstelling aan straling. Bij chemische ongevallen is dat wel het geval. Daarbij kunnen zowel bij brand en explosie als bij een giftige wolk zowel doden als gewonden vallen. Hierbij is één van de vragen of er capaciteitsproblemen zullen ontstaan als er acuut zorg nodig is voor enkele honderden mensen.

Bij stralingsongevallen kunnen wel enkele doden vallen tijdens de evacuatie van mensen in de omgeving, omdat mensen in paniek zijn. Ook kunnen mensen ziek worden (inclusief psychische klachten), waaronder mensen die door de blootstelling kanker krijgen en op langere termijn als gevolg daarvan overlijden.

Verder is een deel van de impact bij stralingsongevallen gekoppeld aan de maatregelen die getroffen zullen worden. Zo zal de agrarische sector financiële gevolgen oplopen door een graasverbod na een groot stralingsongeval. Die maatregel kan ook getroffen worden mocht er in een centrale elders in Europa een groot ongeval plaatsvinden en de resulterende wolk met radioactief materiaal door een ongunstige windrichting Nederland bereikt. Tenslotte zal de impact voor bewoners in de nabijheid van een centrale groot zijn als bewoners moeten evacueren en voor een langere periode elders moeten verblijven.

Voor zowel chemische ongevallen als bij stralingsongevallen is het voorstelbaar dat er een maatschappelijke discussie ontstaat over het ongeval zelf, de activiteiten bij de betreffende installatie en over eventuele maatregelen. Denk daarbij aan discussie over kernenergie of juist het vervoer van gevaarlijke stoffen via het spoor. Naast discussie is het bij een zwaar ongeval mogelijk dat er naast uitingen van emoties als woede ook bedreigingen of intimidatie van verantwoordelijken zullen plaatsvinden.

Net als bij chemische ongevallen kunnen bij transportongevallen grote aantallen doden en gewonden vallen. Dat geldt in het bijzonder bij ongevallen met een vliegtuig of bij een cruiseschip vanwege de grote aantallen passagiers. De kans van optreden is ook hier gelukkig laag. Een transportongeval kan verder leiden tot cascade-effecten en bijvoorbeeld de logistieke functie (knooppunt-functie) van Nederland of andere vitale processen verstoren. Hier ligt een koppeling met de thema's economische dreigingen en bedreiging vitale infrastructuur.

Wat meer indirect liggen er vanuit het thema zware ongevallen koppelingen met enkele moedwillige dreigingen. Binnen het thema cyberdreigingen is onder andere gekeken naar een cyberaanval waarbij een bedrijf in de chemische sector wordt getroffen en er bewust een gevaarlijke stof vrijkomt. De waarschijnlijkheid hiervan is relatief laag, maar is wel groter ingeschat dan het niet-moedwillige scenario. Verder is bij het thema internationale en militaire dreigingen aandacht gegeven de moedwillige inzet van CBRN-middelen.

Tenslotte zijn er vanuit de categorieën stralingsongevallen, chemische ongevallen en transportongevallen verbindingen gelegd met de energietransitie. Een eventuele discussie over kernenergie na een ongeval bij een centrale is al genoemd, en dat zal ook kunnen spelen in het kader van de energietransitie. Verder geldt dat in de energietransitie stoffen zoals waterstof een belangrijke rol kunnen gaan spelen. Een rol waaraan risico's gekoppeld zijn waar rekening mee moet worden gehouden. Als gevolg van transportongevallen kunnen cascade-effecten optreden die het energiesysteem raken, bijvoorbeeld bij een scheepvaart-ongeval waarbij een windpark beschadigd raakt. Naast deze aspecten die hier kort zijn aangestipt, zijn er meerdere facetten van de energietransitie die relevant zijn voor de nationale veiligheid. In hoofdstuk 13 wordt hier nader op ingegaan.

5. Polarisatie, extremisme en terrorisme

Het thema polarisatie, extremisme & terrorisme bestaat uit vier verschillende dreigingscategorieën: maatschappelijke polarisatie, niet-gewelddadig extremisme, gewelddadig extremisme en terrorisme. Maatschappelijke polarisatie betreft een toename van 'wij-zij denken' in de maatschappij en een situatie waarbij groepen steeds meer tegenover elkaar komen te staan, met onderlinge spanningen als gevolg. In sommige gevallen kan polarisatie bijdragen aan de voedingsbodem voor radicalisering. Naarmate groepen meer onderlinge tegenstellingen ervaren en zich sterker tegen elkaar af beginnen te zetten, kunnen gehanteerde standpunten uitgroeien tot radicale opvattingen. Extremisme refereert op zijn beurt naar het actief nastreven en/of ondersteunen van diepingrijpende veranderingen in de samenleving die een gevaar kunnen opleveren voor (het voortbestaan van) de democratische rechtsorde, eventueel met het hanteren van ondemocratische methodes die afbreuk kunnen doen aan het functioneren van de democratische rechtsorde. Extremisten kunnen hun doelen proberen te verwezenlijken door gebruik van zowel gewelddadige als niet-gewelddadige middelen. Terrorisme, tot slot, is het uit ideologische motieven dreigen met, voorbereiden of plegen van op mensen gericht ernstig geweld, dan wel daden gericht op het aanrichten van maatschappij-ontwrichtende schade, met als doel maatschappelijke veranderingen te bewerkstelligen, de bevolking ernstige vrees aan te jagen of politieke besluitvorming te beïnvloeden. Alle vier de categorieën hebben op enige wijze betrekking op de inrichting van de Nederlandse democratische rechtsorde en de mogelijke herschikking hiervan. Naarmate van polarisatie naar terrorisme wordt bewogen, neemt de mate van geweldsgebruik toe.

Groeperingen die extremistische of terroristische activiteiten ontplooien, kunnen behoren tot een groot aantal verschillende stromingen of ideologieën zoals rechtsextremisme, anti-overheidsextremisme, linksextremisme en de radicale Islam. Voor elk van deze stromingen en bijbehorende groepen geldt dat zaken als de aantrekkingskracht die hiervan uitgaat en het geweldspotentieel van een bepaalde groep onderhevig is aan ontwikkelingen in binnen- en buitenland. In het themarapport polarisatie, extremisme & terrorisme wordt voor een aantal van deze stromingen en het onderwerp polarisatie nader ingegaan op relevante ontwikkelingen.

Verspreid over de vier dreigingscategorieën zijn voor tien scenario's de gevolgen en waarschijnlijkheid in kaart gebracht.[7] In de volgende figuur worden deze scenario's in vergelijkend perspectief weergegeven.

[7] In vergelijking met eerdere door het ANV uitgevoerde risicoanalyses zoals het Nationaal Veiligheidsprofiel 2016 en de Geïntegreerde Risicoanalyse 2019, zijn er binnen dit thema relatief veel scenario's uitgewerkt. Aangezien een aantal onderwerpen die vallen binnen het thema polarisatie, extremisme het errorisme de afgelopen jaren prominenter zijn geworden, is ervoor gekozen om een groter set aan scenario's uit te werken. Dit om recht te doen aan de diversiteit van dreigingen binnen het thema.

Figuur 5 Risicodiagram polarisatie, extremisme, terrorisme

	Zeer onwaarschijnlijk	Onwaarschijnlijk	Enigszins waarschijnlijk	Waarschijnlijk	Zeer waarschijnlijk
Catastrofaal					
Zeer ernstig					
Ernstig		• Meervoudige terroristische aanslag • Infiltratie openbaar bestuur	• Bestorming en gijzeling Tweede Kamer	• Polarisatie rond complottheorieën	
Aanzienlijk			• Aanval op pride evenement • Geweldsescalatie rechtsextremisten • Anarcho-extremisme • Ondermijnende enclaves	• Anti-overheids-extremisme	
Beperkt					• Alleenhandelende dader

In zijn algemeen valt op dat de binnen dit thema uitgewerkte scenario's relatief hoog scoren wat betreft waarschijnlijkheid. Van de tien scenario's hebben acht een waarschijnlijkheidsscore 'enigszins waarschijnlijk' of hoger. Het scenario alleenhandelende dader heeft zelfs een waarschijnlijkheidsscore van zeer waarschijnlijk. Hierbij moet echter wel worden opgemerkt dat dit scenario slechts beperkte gevolgen heeft, vooral wanneer afgezet tegen de andere scenario's binnen de categorie terrorisme.

Voor alle scenario's geldt verder dat het belang sociaal-politieke stabiliteit wordt geraakt. Vooral voor scenario's in de categorieën maatschappelijke polarisatie, niet-gewelddadig extremisme en gewelddadig extremisme geldt dat de hoogste impactscores voor het scenario zich binnen dit belang manifesteren. Primair op de criteria aantasting democratische rechtsstaat en sociaal-maatschappelijke impact. Ook voor de gevolgen van scenario's binnen de categorie terrorisme zijn deze criteria van groot belang. Echter, naarmate de aanslag toeneemt in omvang en geweldsintensiteit, komt hier het belang fysieke veiligheid om de hoek kijken als belang waar de grootste gevolgen zich manifesteren. Voor veel van de scenario's binnen de andere categorieën geldt dat alhoewel doden en gewonden niet uit kunnen worden gesloten, de aantallen hieromtrent beperkt zullen blijven.

Als we in wat meer detail kijken naar de gevolgen van de verschillende scenario's voor specifiek de democratische rechtsstaat, is er in meerdere scenario's sprake van het aantasten van de vrijheden en rechten van (groepen) burgers. Onder andere in de vorm van discriminatie, buitensluiting, bedreigingen en in sommige gevallen fysiek geweld. Ook is er in veel van de scenario's sprake van een aantasting van de veiligheid of het veiligheidsgevoel van specifiek politici, bestuurders of ambtenaren. Bedreigingen, intimiderend gedrag en in sommige gevallen fysiek geweld raken echter niet alleen de persoon waar deze op zijn

gericht, maar hebben een olievlekwerking richting de mensen die om deze persoon heen staan, bijvoorbeeld in de vorm van familieleden of collega's. Dit geldt zowel voor burgers die te maken krijgen met bijvoorbeeld buitensluiting of intimidatie als mensen werkzaam voor aan de democratische rechtsstaat verbonden instituten die het slachtoffer zijn bedreigingen. Politici durven zich minder uit te spreken over bepaalde onderwerpen uit vrees om ook slachtoffer te worden van intimiderende 'homevisits' en (potentiële) gemeenteraadsleden en wethouders haken af uit vrees voor de eigen veiligheid en die van hun gezin. Het effect van een ideologisch gemotiveerde mishandeling of intimiderend huisbezoek raakt dus niet alleen de ambtenaar, bestuurder of politicus in kwestie, maar de gehele beroepsgroep. Eenzelfde soort redenatie geldt ook voor burgers van wie vrijheden en rechten worden aangetast. Het discrimineren of intimideren van individuen heeft zijn weerslag op het veiligheidsgevoel en de ervaren vrijheid van de bredere bevolkingsgroep waar deze mensen toe behoren. De mate waarin deze doorwerking plaatsvindt hangt onder andere af van de ernst van de gebeurtenissen en hoe lang deze voortduren.

Een andere factor die hierbij van belang is, is de weerbaarheid van de maatschappij en daarmee ook de democratische rechtsstaat en overkoepelende rechtsorde tegen gebeurtenissen zoals omschreven in de scenario's binnen dit themarapport. Dit gaat dan bijvoorbeeld over de vraag of er voldoende capaciteit beschikbaar is voor het ondersteunen of beveiligen van mensen die het doelwit zijn van bedreigingen van extremisten of de mogelijkheden voor het vroegtijdig signaleren van toekomstige aanslagen.

Binnen dit thema wijken twee scenario's in positieve zin af wat betreft de waarschijnlijkheid: infiltratie openbaar bestuur en meervoudige terroristische aanslag. In beide gevallen kwam tijdens de analyse naar voren dat de weerbaarheid van dusdanige orde is, dat de waarschijnlijkheid van de gebeurtenissen naar beneden moest worden bijgesteld naar een score B (onwaarschijnlijk). Weerbaarheid is echter geen gegeven. Het is van belang om ook voor deze scenario's waakzaam te blijven met betrekking tot het niveau van weerbaarheid. Ook is het belangrijk om nader tegen het licht te houden hoe ook voor het type gebeurtenis uit de andere acht scenario's binnen dit themarapport de weerbaarheid kan worden versterkt.

Alhoewel de RbRa is opgedeeld in negen verschillende thema's, wil dit niet zeggen dat er geen verbindingen zijn tussen deze thema's. Voor maatschappelijk polarisatie geldt bijvoorbeeld dat deze kan ontstaan in het kader van een breed scala aan onderwerpen die een plek hebben in één van de andere themarapporten, waaronder vraagstukken op het gebied van klimaat en internationale samenwerking. Uiteraard kunnen spanningen rond deze en andere onderwerpen uiteindelijk ook leiden tot uitingen van extremisme of terrorisme. Het aanwakkeren van polarisatie en extremisme kan tegelijkertijd onderdeel zijn van een doelbewuste strategie van statelijke actoren om de Nederlandse maatschappij te destabiliseren, bijvoorbeeld als onderdeel van hybride operaties. Deze ongewenste inmenging door statelijke actoren heeft een plek in het thema ongewenste inmenging en beïnvloeding democratische rechtsstaat.

6. Ongewenste inmenging en beïnvloeding democratische rechtsstaat

Het thema ongewenste inmenging en beïnvloeding democratische rechtsstaat bestaat uit vier dreigingscategorieën: Ongewenste buitenlandse beïnvloeding (hybride dreigingen); spionage; ongewenste buitenlandse inmenging en georganiseerde criminaliteit. Elk van deze categorieën zal afzonderlijk worden behandeld.[8] Het risicodiagram hieronder bevat een overzicht van alle binnen het thema uitgewerkte scenario's langs de as van waarschijnlijkheid en gevolgen.

Figuur 6 Risicodiagram Ongewenste inmenging en beïnvloeding democratische rechtsstaat

	Zeer onwaarschijnlijk	Onwaarschijnlijk	Enigszins waarschijnlijk	Waarschijnlijk	Zeer waarschijnlijk
Catastrofaal					
Zeer ernstig					
Ernstig			• Crimineel geweld richting media en overheid • Ongewenste buitenlandse inmenging in diaspora-gemeenschappen	• (Heimelijke) beïnvloeding door China	• Hybride operaties Rusland - aangrijpen op maatschappelijk debat (migratie)
Aanzienlijk				• Cyberspionage overheid • Georganiseerde criminaliteit door heel Nederland • Klassieke statelijke spionage • Criminele inmenging bedrijfsleven	
Beperkt					

[8] De reden dat de categorieën in dit thema afzonderlijk worden behandeld is omdat ze onderling relatief veel van elkaar verschillen.

Ongewenste buitenlandse beïnvloeding (hybride dreigingen)

(Statelijke) actoren ontplooien diverse activiteiten die op verschillende manieren kunnen leiden tot beïnvloeding van andere staten. Dergelijke activiteiten hoeven dus niet direct gericht te zijn op het Koninkrijk der Nederlanden of bondgenoten, maar kunnen wel leiden tot aantasting van de nationale veiligheid. Deze buitenlandse beïnvloeding is voor de nationale veiligheid ongewenst, omdat op deze manier geleidelijk de Nederlandse democratische rechtstaat kan worden ondermijnd. Verschillende vormen van beïnvloeding kunnen worden gevat onder de noemer hybride dreigingen.

Omdat hybride campagnes veelal worden uitgevoerd door staten (al dan niet met hulp van niet-statelijke actoren zoals criminele organisaties), kunnen hybride dreigingen gezien worden als onderdeel van statelijke dreigingen: *dwingende, ondermijnende, misleidende of heimelijke activiteiten van of namens statelijke actoren, onder de drempel van gewapend conflict, die de nationale veiligheidsbelangen van Nederland kunnen schaden door een combinatie van nagestreefde doelen, gebruikte middelen en ressorterende effecten*.

Hybride dreigingen zijn vaak 'sluimerend' van aard, omdat deze zich niet altijd manifesteren in één evenement of gebeurtenis, zoals bij een ransomware aanval. Wat hiermee wordt bedoeld is dat een typerende hybride dreiging bestaat uit heel veel verschillende activiteiten die op zichzelf de nationale veiligheid niet hoeven aan te tasten. Sterker nog, het is in het belang van hybride actoren om zo lang mogelijk onder de radar een andere staat (en diens bevolking) te beïnvloeden, zonder dat de hybride actor wordt 'betrapt' op illegale activiteiten. Economische investeringen en culturele uitwisselingsprogramma's zijn bijvoorbeeld niet illegaal, in eerste instantie staan de (economische) voordelen juist centraal. Echter, dergelijke instrumenten kunnen ook ingezet worden ten behoeve van buitenlandse beïnvloeding, waarbij de optelsom van dergelijke legale activiteiten op de lange termijn kan leiden tot een situatie waarin een staat bijvoorbeeld in verregaande mate afhankelijk is van de andere staat die op die manier een staat naast economisch, ook politiek kan beïnvloeden. Het 'sluimerende' aan hybride dreigingen zit dus in het feit dat beïnvloeding heel ongemerkt en langzaam kan gaan, totdat het feitelijk 'te laat' is, en een staat onbedoeld op veel verschillende manieren afhankelijk is geworden van een andere staat.

Juist een onderwerp als hybride dreigingen is niet te vatten in één puntscenario (over één fenomeen), maar is typisch een dreiging die zich over de lange termijn ontwikkelt waarbij ook op de lange termijn de impact merkbaar is. Vandaar dat dit onderwerp als overkoepelend onderwerp in hoofdstuk 13 is opgenomen, waarin expliciet de koppelingen met andere thema's wordt gemaakt, waar specifieke fenomenen worden uitgelicht, maar die wel degelijk onderdeel kunnen zijn van een groter geheel. Het is van cruciaal belang om altijd een integraal perspectief te hebben op specifieke dreigingen. Het is uiteraard belangrijk om een antwoord te kunnen bieden op de individuele gebeurtenissen (zoals een cyberaanval), maar het is nog belangrijker om daarbij niet het grote plaatje uit het oog te verliezen en te proberen de verschillende gebeurtenissen met elkaar te verbinden (*connecting the dots*). Een op het oog op zichzelf staande gebeurtenis kan immers een andere lading krijgen wanneer deze eigenlijk onderdeel blijkt te zijn van een groter geheel, wat tevens impact heeft op de respons vanuit de overheid.

Spionage

Spionage is het op heimelijke wijze verzamelen van inlichtingen over bijvoorbeeld de politieke of economische situatie in een land, maar het kan ook tot doel hebben om bedrijfsgeheimen dan wel persoonsgegevens te stelen of om kennis over technologie te bemachtigen. Nederland is een aantrekkelijk doelwit voor spionage door andere landen. Ons land is lid van de Noord-Atlantische Verdragsorganisatie (NAVO) en de Europese Unie (EU) en beschikt over interessante informatie. Daarnaast zijn we gastland van tal van internationale organisaties, zoals de Organisatie voor het Verbod op Chemische Wapens (OPCW) en het Internationaal Strafhof (ICC). Ook beschikken de Nederlandse kennis- en onderwijsinstellingen en het bedrijfsleven over veel kennis en hoogwaardige technologie.

Spionage kan enerzijds plaatsvinden op de klassieke manier, door het benaderen van personen om via hen toegang te krijgen tot informatie. In dit kader zoeken medewerkers van buitenlandse geheime diensten zoeken continu naar interessante gesprekspartners (bronnen), zoals ambtenaren, militairen, wetenschappers, topfunctionarissen en journalisten. Anderzijds, wordt er tegenwoordig ook veel digitaal gespioneerd. Digitale spionage, ook wel cyberspionage genoemd, is het (ongezien) stelen van informatie door binnen te dringen in digitale systemen. Hierbij worden informatiesystemen gecompromitteerd, wat een hoge impact heeft op de integriteit van de digitale ruimte. Via (cyber)spionage verkregen informatie kan, afhankelijk van de aard hiervan, door spionerende partijen onder andere worden ingezet voor het verbeteren van de concurrentiepositie van de eigen economie, het versterken van de eigen krijgsmacht of het beïnvloeden van processen en besluitvorming binnen internationale gremia. Dit mogelijk ten koste van de Nederlands positie en belangen. Cyberspionage kan als onderdeel van het hybride instrumentarium worden ingezet voor diverse doelen, zoals het ondermijnen van andere staten. Ook kan cyberspionage worden ingezet om

waardevolle informatie te stelen, bijvoorbeeld over technologie of bedrijfsgeheimen. Uiteraard kunnen klassieke en digitale vormen van spionage ook in samenhang ingezet worden.

Spionage wordt gezien als een serieuze dreiging voor Nederland en haar bondgenoten. Staten zoals Rusland, China hebben grote geopolitieke ambities en zijn hiervoor op zoek naar informatie waarmee zij hun krijgsmacht kunnen moderniseren, hun economie kunnen versterken of politieke besluitvorming in het Westen kunnen beïnvloeden. Tegelijkertijd is er steeds meer aandacht voor de (statelijke) dreigingen die uit kunnen gaan van cyberspionage, onder andere gevoed door digitale spionagepogingen van statelijke actoren bij Nederlandse ministeries. Deze aandacht uit zich ook door de toenemende zorgen over het gebruik van technologie van buitenlandse leveranciers en de mogelijkheid dat er 'achterdeurtjes' zijn geïnstalleerd in de betreffende hard- of software waar buitenlandse inlichtingendiensten gebruik van kunnen maken. Ook spionage op, en de sabotage van onderzeese infrastructuur (zoals zeekabels), is een onderwerp dat de afgelopen tijd steeds meer in de belangstelling staat. Begin dit jaar heeft het ministerie van Justitie en Veiligheid een wetsvoorstel ingebracht ter consultatie gericht op het moderniseren van de strafbaarstelling van spionage. Dit betekent dat 'nieuwe vormen' van spionage (zoals cyberspionage) voor diverse doeleinden in de toekomst mogelijk beter aangepakt kunnen worden.

Binnen de RbRa is er een scenario uitgewerkt rond zowel klassieke als digitale spionage. Alhoewel het binnen deze scenario's en de dreigingscategorie als geheel veelal gaat om relatief kleinschalige gebeurtenissen zoals het omkopen van een enkele medewerker van defensie, kunnen de gevolgen wel degelijk groot zijn met implicaties voor de nationale veiligheid. Spionage is tevens een fenomeen met een relatief hoge waarschijnlijkheid van plaatsvinden. Welke veiligheidsbelangen vooral worden geraakt hangt sterk af van het soort informatie dat wordt verkregen door middel van spionage en welke partij is gekozen als doelwit. Het is echter niet altijd eenvoudig om de impact van (cyber) spionage op de nationale veiligheid te duiden in de praktijk, omdat het meestal onzeker is welke informatie er door wie is buitgemaakt en waarvoor de actor deze informatie wil inzetten. Zo zijn er bijvoorbeeld zorgen over de economische impact van spionage, maar zijn juist ook deze economische gevolgen ingewikkeld om te duiden.

De spionerende actor kan er bijvoorbeeld voor kiezen om belangrijke buitgemaakte informatie achter de hand kan houden, om vervolgens op een voor hem opportuun moment in te zetten. De timing en context van het gebruik van deze informatie heeft een grote invloed op de uiteindelijk gevolgen ervan voor bijvoorbeeld de Nederlandse economie. Als de store-and-forward strategie bijvoorbeeld zou worden toegepast om kritieke informatie in te zetten bij internationale onderhandelingsprocessen, zou dit zelfs de internationale rechtsorde (door middel van het beïnvloeden van multilaterale besluitvormingsprocessen) kunnen schaden. Dit betekent ook dat geopolitieke ontwikkelingen een belangrijke context vormen voor zowel de mate van waarschijnlijkheid als ook de impact van de schending.

Ongewenste buitenlandse inmenging

Onder Ongewenste Buitenlandse Inmenging (OBI) verstaan we de inmenging van statelijke actoren die kan leiden tot ernstige ontwrichting en disfunctioneren van de democratische rechtsorde en open samenleving. OBI kan schade toebrengen aan de integriteit van het Nederlands bestuur als deze de onafhankelijke volksvertegenwoordiging of rechtsspraak compromitteert, of als er twijfel ontstaat over de eerlijkheid en anonimiteit van verkiezingen. Daarnaast heeft OBI de potentie om de stabiliteit in de samenleving te ondermijnen, wanneer de acceptatie tussen verschillende bevolkingsgroepen onder druk komt te staan. Binnen deze dreigingscategorie ligt de nadruk op OBI in de vorm van Inmenging in diasporagemeenschappen in Nederland, bijvoorbeeld door te trachten de culturele afstand tussen die gemeenschappen en de andere Nederlanders te vergroten en politieke tegenstanders op te sporen en te intimideren.

Ongewenste buitenlandse inmenging (OBI) in diasporagemeenschappen vindt vaak geleidelijk en in veel gevallen ook heimelijk plaats. De scheidslijnen binnen diasporagemeenschappen worden veelal langzaam uitgediept. Zodra het voor de inmengende staat opportuun is kunnen deze scheidslijnen manifest worden gemaakt, bijvoorbeeld als leden van de diasporagemeenschap electoraal gemobiliseerd moeten worden voor verkiezingen in het land van herkomst. Dit type OBI kent echter veel verschillende gedaanten. Deze kan variëren van het eerder genoemde electoraal mobiliseren van grote kiezersgroepen tot het intimideren, of zelfs uitschakelen, van oppositieleden die in Nederland verblijven. Een eenduidige beoordeling van de gevolgen van een 'OBI-diasporagemeenschappen' is daardoor complex.

De OBI-variant die zich richt op electorale mobilisatie is veelal het meest zichtbaar voor het grote publiek en zal met name de Nederlandse sociale en politieke stabiliteit raken. Grote groepen Nederlanders tegenover elkaar komen te staan, aangewakkerd door een buitenlandse mogendheid.

Georganiseerde criminaliteit

Criminaliteit komt in verschillende vormen en gradaties voor in de Nederlandse maatschappij. Waar een groot deel van de in Nederland gepleegde delicten niet relevant zijn voor de nationale veiligheid, is dit mogelijk wel het geval

voor activiteiten die vallen onder de noemer georganiseerde criminaliteit.[9] We spreken van georganiseerde criminaliteit als wordt voldaan aan een drietal voorwaarden:

- Het gaat om systematisch gepleegde misdaden met ernstige gevolgen zoals (grootschalige) fraude, ernstige geweldsdelicten en drugscriminaliteit.
- Het gaat om misdaden die worden gepleegd door groepen die primair gericht zijn op illegaal gewin. Misdaden moeten dus voortkomen uit een groepsverband en gericht zijn op het verkrijgen van onder andere macht, geld of status. Dit in tegenstelling tot individueel handelen of een misdaad binnen de relationele sfeer.
- Men is in staat om deze misdaden op betrekkelijk effectieve wijze af te schermen. Hiervoor gebruiken criminelen onder andere facilitators in de bovenwereld: mensen werkzaam in legale sectoren die vanuit hun positie al dan niet bewust of vrijwillig faciliterende diensten verlenen aan criminelen. Denk aan makelaars en werknemers van autoverhuurbedrijven of de financiële sector die helpen de ware identiteit dan wel oorsprong van de financiële middelen van een koper, huurder of client te verhullen.

Binnen Nederland wordt regelmatig de term crimineel samenwerkingsverband (csv) gebruikt om te refereren naar de groepen criminelen die zich bezighouden met georganiseerde criminaliteit. Deze samenwerkingsverbanden houden zich bezig met een breed scala aan activiteiten die potentieel vallen onder de noemer georganiseerde criminaliteit, waaronder mensenhandel, cybercrime, fraude en vermogenscriminaliteit. Nederlandse criminelen zijn bovendien internationaal grote spelers in de handel en productie van verdovende middelen. Onder andere dankzij de geografische ligging, goede infrastructuur, aanwezigheid van diasporagemeenschappen en toegang tot de benodigde kennis is Nederland een belangrijk knooppunt voor de handel in cocaïne en (in mindere mate) heroïne. Ook is er een grote binnenlandse productie van hoofdzakelijk cannabis en synthetische drugs, met name gericht op de export. Om deze activiteiten af te schermen en te faciliteren, gaat men niet alleen over tot het witwassen van criminele verdiensten, maar poogt men ook andere mensen te beïnvloeden. Bijvoorbeeld door middel van omkoping, infiltratie, bedreiging of het uitoefenen van fysiek geweld. Deze beïnvloeding kan onder andere gericht zijn op andere criminelen, de eigen sociale omgeving, mensen werkzaam in voor criminelen interessante sectoren of ambtenaren en bestuurders.

Over het algemeen is georganiseerde criminaliteit in Nederland relatief onzichtbaar. Het is dan ook het doel van de meeste criminelen om juist niet op te vallen en de eigen activiteiten af te schermen. Tegelijkertijd doen zich geregeld in het oog springende incidenten voor die deze onzichtbaarheid doorbreken, zoals liquidaties in de openbare ruimte. De invloed van georganiseerde criminaliteit op de maatschappij ligt zowél in deze in het oog springende incidenten, als in de permanente, sluimerende, aanwezigheid van criminaliteit. Georganiseerde criminaliteit kan zich door heel Nederland voordoet en een breed spectrum aan groepen en sectoren kan raken. De dynamiek rond georganiseerde criminaliteit is door de deels sluimerende aard moeilijk te vatten in een scenario van enkele pagina's. De drie binnen de RbRa uitgewerkte scenario's dienen dan vooral ook om het onderwerp aan te kaarten in het kader van de nationale veiligheid en om een indicatie te geven van de mogelijke gevolgen van uitingen van het fenomeen georganiseerde criminaliteit.

De gevolgen van georganiseerde criminaliteit uiten zich op relatief veel veiligheidsbelangen. Een illustratie van hoe georganiseerde criminaliteit op veel verschillende manieren de maatschappij kan beïnvloeden. De hoogste scores uiten zich met name op aantasting democratische rechtsstaat. Deze aantasting komt met name voort uit dreigementen richting overheidspersoneel, maar ook uit integriteitsschendingen en een mogelijk verlies van vertrouwen onder de bevolking in het vermogen van de overheid in brede zin om een halt toe te roepen aan georganiseerde criminaliteit. Tegelijkertijd is de waarschijnlijkheid van de scenario's aan de hoge kant.

De dreigingscategorie georganiseerde criminaliteit staat verder niet op zichzelf. Georganiseerde criminaliteit heeft een sterke link met het thema cyberdreigingen. Niet alleen maken criminelen dankbaar gebruik van technologische ontwikkelingen als de brede beschikbaarheid van end-to-end encriptiediensten, maar houdt men zich ook bezig met cybercrime. Een bekend voorbeeld hiervan is het uitvoeren van ransomware aanvallen waarbij bijvoorbeeld met gebruik van malware zich toegang verschaft tot systemen, de toegang hiertoe voor gebruikers blokkeert en vervolgens betaling eist om dit ongedaan te maken. Binnen het themarapport cyberdreigingen wordt nader ingegaan op een dergelijk ransomware scenario. Verder kunnen ook

[9] Vaak wordt in plaats van georganiseerde ook wel gesproken van ondermijnende criminaliteit. De term ondermijnende criminaliteit impliceert per definitie dat de criminele daad waar het over gaat op enige wijze het politieke of maatschappelijke systeem van Nederland aantast (ondermijnt). Georganiseerde criminaliteit is daarentegen een neutralere, overkoepelende term. Georganiseerde criminaliteit omvat grotendeels dezelfde criminele activiteiten als ondermijnende criminaliteit, maar duidt het effect op de maatschappij niet. Aangezien er binnen de nationale veiligheid niet alleen wordt gekeken naar de effecten van een dreiging op de democratische rechtsstaat, maar ook op allerlei andere vlakken, is binnen het ANV gekozen voor de term georganiseerde criminaliteit.

statelijke actoren opdracht geven tot criminele activiteiten, bijvoorbeeld als onderdeel van hybride operaties. Dit fenomeen staat bekend als '*crime as a service*'.

Tot slot is voor de ontwikkeling van georganiseerde criminaliteit van belang hoe weerbaar de maatschappij is en blijft in de toekomst. Georganiseerde criminaliteit is deels afhankelijk van de sociale omgeving voor hun activiteiten en het succesvol afschermen hiervan. Wanneer mensen vertrouwen hebben in politie en overheid en goed mee kunnen komen in de maatschappij, worden zij minder snel verleid om betrokken te raken bij georganiseerde criminaliteit of dit te faciliteren. Hiertegenover staat dat als mensen zich in een sociaaleconomisch uitzichtloze situatie bevinden en negatieve ervaringen met de overheid hebben, het uitvoeren of faciliteren van criminele activiteiten eerder als optie wordt gezien. De afgelopen paar jaar is er weer meer politieke en bestuurlijke aandacht voor (het belang van) het tegengaan van georganiseerde criminaliteit. Dit heeft zich vertaald in het ter beschikking stellen van extra financiële middelen vanuit de Rijksoverheid voor de aanpak van georganiseerde criminaliteit en een hoger niveau van bewustzijn bij bijvoorbeeld lokale overheden. Ook zijn er op landelijk niveau meerdere initiatieven ontstaan gericht op de regie en afstemming van de aanpak van ondermijnende of georganiseerde criminaliteit, waaronder de Ministeriele Commissie Aanpak Ondermijning (MCAO) en het 'programma-DG' van het ministerie van Justitie en Veiligheid. Deze toegenomen aandacht en bewustwording kan bijdragen aan de weerbaarheid tegen georganiseerde criminaliteit. Tegelijkertijd hangt deze bijdrage af van de vraag of de aandacht in kwestie structureel is. Het gevaar bestaat dat georganiseerde criminaliteit, mede door de vaak relatief onzichtbare aard, na een toename van bestuurlijke en politiek aandacht aan actualiteit inboet ten faveure van beleidsonderwerpen als klimaat, zorg en huisvesting. De komende jaren moeten uitwijzen of de extra aandacht en investeringen voor georganiseerde criminaliteit afdoende worden geborgd en deze de gewenste uitwerking hebben.

Algemene beschouwing

Ondanks het feit dat de vier binnen dit thema beschouwde dreigingscategorieën inhoudelijk van elkaar verschillen, zijn er wel degelijk een aantal dwarsverbanden te identificeren. Een eerste dwarsverband is de aantasting of ondermijning van de democratische rechtsstaat, waar de in dit thema opgenomen dreigingen een grote mate van gelijkenis vertonen. De Nederlandse rechtsstaat kan worden geraakt door zowel de activiteiten van statelijke als niet-statelijke, criminele actoren. Voor beide soorten actor geldt dat deze aantasting voortkomt uit een streven om de eigen doelen te verwezenlijken.[10] Deze statelijke actoren en de dreiging die hiervan uitgaat is een tweede dwarsverband voor in ieder geval drie van de vier dreigingscategorieën. Zowel hybride dreigingen als (digitale) spionage en ongewenste buitenlands inmenging in diasporagemeenschappen operaties vallen onder het bredere begrip statelijke dreigingen.[11] De voor dit thema uitgevoerde analyses bevestigen dan ook dat een aantal van de dreigingen die vallen onder deze noemer de democratische rechtsstaat kunnen ondermijnen. Voor georganiseerde criminaliteit geldt eveneens dat dit in sommige gevallen kan worden gezien als statelijke dreiging. Dit is het geval wanneer criminelen werken in opdracht van een statelijke actor, die bijvoorbeeld een order geeft tot het uitvoeren van een ransomware aanval.

Een laatste dwarsverband is het belang van technologische ontwikkelingen en de digitalisering van de maatschappij voor elk van de hier beschouwde dreigingscategorieën. Technologische ontwikkelingen stellen criminele actoren bijvoorbeeld in staat hun communicatie beter af te schermen door gebruik te maken van applicaties die berichten automatisch versleutelen. Het feit dat sommige onderdelen van het dagelijks leven zoals bankieren, aankopen doen en onderling communiceren zich in toenemende mate online afspelen, biedt eveneens kansen aan criminele actoren op het gebied van oplichtingspraktijken, de verkoop van verdovende middelen of cybercrime.[12] Statelijke actoren hebben op hun beurt steeds meer mogelijkheden om in Nederland woonachtige diasporagemeenschappen (online) in de gaten te houden en het uitvoeren van een desinformatiecampagne als onderdeel van hybride operaties wordt vergemakkelijkt door de brede toegang tot en het gebruik van sociale mediaplatformen en berichtendiensten. Digitalisering resulteert eveneens in een toenemende verbondenheid van netwerken en systemen alsmede de automatisering van processen. Op zijn beurt levert dit kwetsbaarheden op die door statelijke actoren kunnen worden uitgebuit bij het uitvoeren van hybride operaties, zoals offensieve cyberoperaties gericht op sabotage of spionage. Tegelijkertijd vraagt de uitrol van nieuwe technologie, zoals het opzetten van een landelijk dekkend 5G netwerk om hard- en software die mogelijk

[10] Uiteraard kan een aantasting van de democratische rechtsstaat ook voortkomen uit de activiteiten van niet statelijke, extremistische actoren. Dit wordt behandeld in het themarapport polarisatie, extremisme en terrorisme.

[11] Het begrip statelijke dreigingen refereert naar dwingende, ondermijnende, misleidende of heimelijke activiteiten van of namens statelijke actoren, onder de drempel van gewapend conflict, die de nationale veiligheidsbelangen van Nederland kunnen schaden door een combinatie van nagestreefde doelen, gebruikte middelen en ressorterende effecten

[12] In het themarapport cyberdreigingen wordt nader ingegaan op het fenomeen cybercrime.

afkomstig zijn van buitenlandse leveranciers. Alhoewel dit op zichzelf geen probleem is, zullen er landen zijn die bewust kwetsbaarheden inbouwen in hun producten om deze later eventueel te benutten voor het verkrijgen van gevoelige informatie. Naarmate de maatschappij meer digitaliseert en technologische ontwikkelingen zich aan blijven doen, is het van belang om evenwel een oog te houden op de kwetsbaarheden die dit met zich mee brengt en wat de gevolgen kunnen zijn voor de democratische rechtsstaat als kwaadwillende partijen deze kwetsbaarheden benutten.

7. Internationale en militaire dreigingen

Binnen het thema internationale en militaire dreigingen is een viertal dreigingscategorieën beschouwd, te weten (i) fragiliteit nabij het Konikrijk en/of de EU, (ii) multilaterale veiligheidsinstituties onder druk, (iii) gewapend conflict tussen de machtsblokken en (iv) proliferatie van massa-vernietigingswapens. Van de twaalf scenario's die zijn beoordeeld op de waarschijnlijkheid van manifesteren en de impact op de nationale veiligheid zijn er zes die in de eindbeoordeling relatief hoog scoren binnen het veiligheidsbelang internationale rechtsorde en stabiliteit. Dit zijn respectievelijk: IS grijpt de macht in Marokko, kernwapengebruik in het conflict Iran-Saoedi-Arabië, instorten van de Venezolaanse staat, Chinese hereniging met Taiwan, de tijdelijke bezetting van een EU-lidstaat (Finland), en het uiteenvallen van de NAVO.

Figuur 7 Risicodiagram internationale en militaire dreigingen

	Zeer onwaarschijnlijk	Onwaarschijnlijk	Enigszins waarschijnlijk	Waarschijnlijk	Zeer waarschijnlijk
Catastrofaal					
Zeer ernstig	• IS grijpt de macht in Marokko • Inzet van kernwapens Saoedi-Arabië – Iran	• Chinese hereniging Taiwan • Tijdelijke bezetting van een EU-lidstaat	• Instorten van de Venezolaanse staat • Uiteenvallen van de NAVO		
Ernstig			• Crisis in de Zuid-Chinese Zee • Tweespalt in de EU	• Desintegratie van Bosnië-Herzegovina	
Aanzienlijk		• Terroristische aanslag met een biologisch wapen	• Uiteenspatten van de OVSE	• Innovatie nucleaire overbrengings-middelen	
Beperkt					

De oplopende geopolitieke spanningen tussen de diverse grootmachten bedreigen onze omgeving en onze nationale veiligheid. De Russische inval in Oekraïne van begin 2022 is een illustratie van de toenemende militaire dreiging, waardoor de grenzen in Europa opnieuw bedreigd worden met gewapend optreden. Maar ook verder weg van Europa nemen de internationale spanningen toe, zoals in Zuidoost- en Oost-Azië, waar China zich steeds meer profileert als de economische, politieke én militaire grootmacht van de toekomst. De jaarlijks stijgende mondiale militaire uitgaven illustreren dit geopolitieke spanningsveld. Ook al is een rechtstreekse bedreiging van de landsgrenzen van het Koninkrijk onwaarschijnlijk, toch groeit het risico op internationale en militaire crisissituaties die Nederland kunnen meeslepen, mede door onze verdrags-verplichtingen, bijvoorbeeld via artikel 5 van het NAVO-verdrag en artikel 42.7 van het EU-verdrag.

Daarbovenop is er een wedloop gestart voor de controle over onontgonnen regio's met het risico op nieuwe conflicthaarden: het Arctische gebied, de zeeën en de ruimte. Conflicten en fragiliteit in onze periferie creëren bovendien een machtsvacuüm waarin extremisten, terroristische groeperingen en de georganiseerde misdaad vrij spel krijgen, druk zetten op de betreffende regio's en een bedreiging vormen voor onze nationale veiligheid en onze handelsroutes. Wanneer dit bijdraagt tot hoge, ongecontroleerde en onregelmatige migratie, kan dit invloed uitoefenen op onze publieke ruimte en forse druk zetten op de maatschappelijke stabiliteit. Statelijke actoren die invloed hebben op migratiestromen, deinzen er bovendien niet voor terug om dit als drukmiddel tegen ons te gebruiken.

Dit alles luidt een nieuw tijdperk van internationale en militaire dreigingen in, waarin statelijke maar ook niet-statelijke actoren zich steeds meer wenden tot hybride methodes en technieken. Dit omvat het gecombineerde gebruik van economische, politieke, militaire en andere instrumenten waarbij de grens tussen oorlog en vrede steeds meer vervaagt, variërend van de beïnvloeding van de publieke opinie door desinformatie en propaganda, van cyberaanvallen en spionage, tot chantage, sabotage en aanvallen met CBRN-middelen. Dergelijke hybride aanvallen richten zich op de kwetsbaarheden van de tegenstander, zijn ambigu van aard en trachten doelbewust onder de drempels van detectie te blijven, wat attributie moeilijk maakt. Hybride aanvallen beogen bovendien om onze democratische rechtsorde te verzwakken en de cohesie en solidariteit binnen onze samenleving, de EU en NAVO te ondermijnen en zo onze slagkracht aan te tasten.

Een op regels gebaseerde, functionerende internationale rechtsorde is essentieel voor onze nationale veiligheids-belangen. Het multilaterale kader ervan helpt bovendien de onvoorspelbaarheid van het veranderende karakter van de internationale betrekkingen te verminderen en conflict en instabiliteit te voorkomen. De toenemende geopolitieke spanningen tussen de grootmachten zetten echter zware druk op dit multilaterale systeem. Dit kan verschillende vormen aannemen, van het gebruik van het vetorecht binnen de VN-Veiligheidsraad tot de terugtrekking uit internationale overeenkomsten en verdragen.
De verstoring van de internationale samenwerking op gebieden als vrijhandel, veiligheid, non-proliferatie of klimaat, heeft rechtstreekse gevolgen voor onze economie en onze internationale positie, maar heeft ook een directe impact op ingezetenen van het Koninkrijk in het buitenland. In de huidige, gemondialiseerde wereld reikt ons Koninkrijk verder dan zijn fysieke grenzen. Ingezetenen van het Koninkrijk, ondernemingen en in het bijzonder onze diplomatieke en consulaire posten en uitgezonden militairen en civiele functionarissen lopen het risico op betrokkenheid bij gewelddadige acties en gevechtshandelingen.

De EU, NAVO, OVSE en de VN zijn niet immuun voor de druk op het internationale systeem. Enerzijds trachten bepaalde staten actief hun cohesie en slagkracht te ondermijnen door tal van hybride acties. Anderzijds keren sommige leden van deze organisaties zich af van het multilateralisme.
De specifieke invraagstelling door bepaalde EU-lidstaten van de fundamentele principes en waarden waarop het Europese integratieproject is gebaseerd, waaronder de democratische rechtsstaat, verzwakt niet alleen de internationale invloed van de EU, maar ook dezelfde fundamenten die essentieel zijn voor onze welvaart, voor het beschermen van onze veiligheid en voor het respect voor individuele en collectieve waarden. Georganiseerde en gecoördineerde strategieën voor het manipuleren van meningen, door de massale verspreiding van nepnieuws en door de exploitatie van algoritmes die inherent zijn aan de huidige werking en programmering van sociale media, hebben een toenemende invloed en kunnen samenlevingen uit evenwicht brengen door de beïnvloeding van de publieke opinie of van democratische processen zoals verkiezingen.

Massavernietigingswapens vormen een ander belangrijk risico. In de afgelopen jaren zijn de dreigingen met Chemische, Biologische, Radiologische en Nucleaire (CBRN) agentia toegenomen. In de context van toenemende geopolitieke spanningen doen er zich regionale wapenwedlopen voor en achten staten zich steeds minder gebonden door multilaterale wapenbeheersingsafspraken. Een bijkomende dreiging schuilt in de toepassing van technologische ontwikkelingen in wapensystemen, waardoor de reactietijd wordt verkleind en de onvoorspelbaarheid wordt vergroot. Ontwikkelingen in de biologische wetenschap brengen potentieel gevaarlijke toepassingen binnen handbereik, ook van niet-statelijke actoren. Een aanval met het gebruik van CBRN agentia vereist weliswaar specifieke kennis, maar de grotere toegang tot informatie (via internet) werkt drempelverlagend. Terroristische organisaties of extremisten roepen bovendien geregeld op om aanslagen te plegen met CBRN agentia.

Door de lens van de zes nationale veiligheidsbelangen bezien, scoren de dreigingen van het thema 'internationale en militaire dreigingen' relatief hoog op het belang van een goed functionerende internationale rechtsorde en stabiliteit. Overkoepelend moet daarbovenop worden geconstateerd dat deze internationale orde momenteel sterk aan het veranderen is. De naoorlogse periode waarin het internationale statensysteem en de onderlinge machtsverhoudingen werden gedomineerd door de Verenigde Staten lijkt definitief voorbij. We hebben inmiddels te maken met een opkomend China en een revisionistisch en revanchistisch Rusland die de VS meer en meer uitdagen. De aard van de internationale orde is bovendien erg complex doordat er op allerlei terreinen internationale samenwerking blijft bestaan, waardoor aspecten van de multilaterale wereldorde gehandhaafd blijven, en er tegelijkertijd aspecten van diezelfde wereldorde onder flinke druk staan. Op allerlei terreinen wordt in wisselende coalities samengewerkt én tegengewerkt. Deze internationale verhoudingen zorgen voor een grote mate van onzekerheid en dragen bij aan een verslechterende internationale en militaire veiligheidssituatie.

8. Economische dreigingen

Economische dreigingen komen in vele vormen en maten voor: van handelskrimp, financiële crises, tekorten aan strategische goederen als fossiele energie of essentiële grondstoffen, uitgebreide bedrijfsspionage of andere vormen van inmenging in het Nederlandse bedrijfsleven. De impact van deze scenario's is op korte termijn mogelijk (zeer) significant. Op langere termijn kunnen risico's zich opbouwen.

Binnen het thema '*Economische dreigingen*' staan vijf dreigingscategorieën centraal:

- Bedreigingen van de knooppuntfunctie van Nederland
- Handelskrimp of verstoring van de internationale handel
- Buitenlandse inmenging bij het bedrijfsleven
- Strategische afhankelijkheden
- Destabilisatie van het financiële systeem

De scenario's binnen elk van deze dreigingscategorieën raken de nationale veiligheid, maar wel op verschillende wijze, in verschillende mate, en met verschillende waarschijnlijkheid. Het risicodiagram vat dit samen.[13]

[13] Sommige scenariotitels in het diagram zijn afgekort.

Figuur 8 Risicodiagram economische dreigingen

	Zeer onwaarschijnlijk	Onwaarschijnlijk	Enigzins waarschijnlijk	Waarschijnlijk	Zeer waarschijnlijk
Catastrofaal					
Zeer ernstig			• Systeempartij in de financiële sector in zwaar weer	• Import van fossiele energie	
Ernstig		• Handelsoorlog waar Europa bij betrokken is • Verstoring van het betalingsverkeer • Statelijke verwerving van een minderheids-belang in een grote telecommunicatie-aanbieder			• Verstoring van handel door productie-problemen in het buitenland
Aanzienlijk		• Nieuwe Europese schuldencrisis	• Buitenlandse regulering techbedrijven	• Correctie op waardering finaciële activa doordat verwachtingen niet uitkomen	
Beperkt				• Tekorten essentiële grondstoffen • Overname onder de radar van niet-beursgenoteerd bedrijf dat o.a. dual-use goederen produceert	• Buitenlandse durfkapitaal-investeringen in health- en biotechstartups

Impact op het economische veiligheidsbelang
Impact op het economische veiligheidsbelang wordt afgemeten aan de mate waarin de scenario's voor private of publieke kosten zorgen en voor de mate waarin de vitaliteit van de Nederlandse economie in het geding is (afgemeten aan een toename van de werkloosheid en de staatsschuld).

De impact op het economisch veiligheidsbelang is relatief groot in scenario's die de economie 'midscheeps' raken. Dit komt in vrijwel alle dreigingscategorieën terug. Voor een kleine open economie als Nederland is een verstoring van de internationale handel of mondiale handelskrimp kostbaar en dat heeft gevolgen voor de werkgelegenheid en de overheidsfinanciën. Hetzelfde geldt voor grote macro-financiële schokken die vallen onder de categorie destabilisatie van het financiële systeem. Dit is vrij onafhankelijk van de oorsprong van de schok. Zowel een binnenlandse als een buitenlandse schok heeft impact op de economische veiligheid. Handel krimpt zowel bij productieverstoringen als bij handelsconflicten en de macro-economie voelt zowel de pijn van een schok bij systeempartijen op financiële marktpartijen als op markten voor staatschuld.

In scenario's die een bedreiging voor de knooppuntfunctie van Nederland beschrijven, is de economische schade meer of minder beperkt afhankelijk van de oorsprong van de verstoring. In algemene zin geldt dat de Nederlandse welvaart gevoelig is voor verstoringen van deze functie, maar niet elke verstoring heeft een even grote impact. Om recht te doen aan deze oorsprong van de verstoring zijn de scenario's over de knooppuntfunctie feitelijk ondergebracht in de themarapporten over internationale

en militaire dreigingen en natuurrampen. Een verstoring van de knooppuntfunctie die effectief een mondiale handelskrimp tot gevolg heeft (zoals bij de Chinese hereniging Taiwan, zie themarapport internationale en militaire dreigingen) heeft economisch grote kosten. Een tijdelijke en meer lokale verstoring als gevolg van verstoring van de binnenvaart bij extreem weer minder (zoals bij extreme hitte/droogte, zie themarapport klimaat- en natuurrampen).

Verhoudingsgewijs worden de economische veiligheidsbelangen overwegend minder scherp geraakt in de scenario's over buitenlandse inmenging bij het bedrijfsleven en strategische afhankelijkheden, met uitzondering van de afhankelijkheid van de import van fossiele energie. Buitenlandse inmenging bij het bedrijfsleven kán kosten hebben, maar dat is niet noodzakelijkerwijs zo. Deze kosten zijn ook kleiner dan bij grote macro-economische schokken. Ook is de vitaliteit van de Nederlandse economie zelden in het geding. Strategische afhankelijkheden hebben kosten, met name de afhankelijkheid van fossiele energie import indien deze verstoord raken, maar de gevolgen voor de vitaliteit van de economie zijn beperkter over een termijn van vijf jaar.

Impact op andere veiligheidsbelangen

Lage kosten of een beperkte impact op de vitaliteit van de Nederlandse economie zijn geen garantie voor het ontbreken van risico's voor de nationale veiligheid. In veel gevallen raken de scenario's namelijk ook aan andere veiligheidsbelangen. De kosten van een verstoring van het betalingsverkeer zijn weliswaar te overzien, maar de maatschappelijke gevolgen groot doordat de integriteit van de digitale ruimte wordt aangetast, het dagelijks leven wordt verstoord, en dit een sociaal-maatschappelijke impact heeft. In de staart kan een afhankelijkheid van fossiele energie ertoe leiden dat burgers een gebrek aan primaire behoefte aan (betaalbare) energie ervaren. Handelsoorlogen gaan gepaard met internationaal-politieke fall-out en schaden het internationaal op regels gebaseerde financieel-economisch bestel. Handelskrimp door productieproblemen in het buitenland kunnen zorgen voor tekorten van essentiële goederen zoals medicijnen. Spionage na een overname in de telecom-municatiesector is een schending van de integriteit van de Nederlandse digitale ruimte. In veel gevallen waar economische dreigingen het economisch veiligheidsbelang niet raken, is hiermee toch sprake van risico's voor de nationale veiligheid – zij het via een ander veiligheidsbelang.

De economie als endogeen systeem, de rol van beleid en de opbouw van sluimerende dreigingen

Een aantal scenario's hebben direct slechts een beperkte impact op het economisch veiligheidsbelang, zeker als het gaat om de graadmeter vitaliteit van de Nederlandse economie. Dit speelt met name binnen de dreigingscategorieën buitenlandse inmenging bij het bedrijfsleven en strategische afhankelijkheden. In het scenario over de buitenlandse verwerving van Nederlandse startups zijn bijvoorbeeld de economische effecten beperkt onder andere omdat het directe 'economisch verlies' over de middellange termijn nihil is. Startups zijn veelal klein, produceren nog weinig omzet, en hebben een onzeker toekomstperspectief. Daarmee zijn de kosten van verlies van Nederlands eigenaar- en zeggenschap beperkt, net zoals de gevolgen voor de vitaliteit van de Nederlandse economie van de eventuele verplaatsing van kennis, kapitaal en mensen naar het buitenland. Voor het scenario over de buitenlandse overname van een innovatieve batterijproducent gelden vergelijkbare overwegingen.

Deze beperkte uitslag op de impactindicatoren hoeft niet te betekenen dat dit type dreigingen geen relevantie hebben voor een langetermijnstrategie voor de Nederlandse (economische) nationale veiligheid. Over een langere termijn kán een aanhoudend 'lek' van hoogwaardige economische activiteit naar het buitenland na buitenlandse overnames gevolgen hebben voor de vitaliteit van de Nederlandse economie, maar dit is geen noodzakelijk gegeven en de taxatie van de potentiële aantasting van de vitaliteit van de economie op de lange termijn is complex. Ook kan een 'lek' van kennis naar het buitenland of de opbouw van strategische afhankelijkheden in de toekomst de randvoorwaarden scheppen voor gebeurtenissen die schadelijk zijn voor de nationale veiligheid, bijvoorbeeld doordat de opbouw van politiek, economisch of militair strategische positie door een buitenlandse actor hiermee gefaciliteerd wordt. De uitwerking van een dergelijk 'lek' is echter onzeker en ontvouwt zich over een lange termijn. Daarmee zijn zowel de impact als de kans moeilijk op waarde te schatten.

Voor economische risico's is een aanvullend aandachtspunt hierbij dat de economie vaak fungeert als een endogeen systeem. Gegeven door beleid geschapen kaders bewegen actoren zich onder druk van economische prikkels vaak naar efficiënte uitkomsten. Onvoorziene gevolgen hiervan kunnen bijdragen aan de opbouw van risico's binnen het financiële systeem, oplopende druk op het multilaterale stelsel van op regels gebaseerde internationale handel, de opbouw van afhankelijkheden, of het anderszins faciliteren van de strategische positie van buitenlandse actoren. De nadruk is hier 'onvoorzien' in de zin dat het oorspronkelijke doel van het beleid vaak baten beoogde, maar kosten of risico's sluipenderwijs ontstaan. Economisch gezien efficiënte transacties vinden plaats omdat de private baten de kosten overstijgen, maar in deze beslissing zijn vaak externe effecten niet meegenomen, zoals nationale veiligheidsrisico's. Dit komt doordat elke individuele transactie geen of nauwelijks effect heeft op de

nationale veiligheid, maar de cumulatie van veel transacties maakt uiteindelijk het veiligheidsrisico wel reëel. Zogeheten *no-regret* beleidsopties zijn hiermee waarschijnlijk schaars. Waar het bijvoorbeeld gaat om afhankelijkheden geldt dat elke 'afhankelijkheid' zowel kosten als baten heeft – in mondiale waardeketens is 'afhankelijk' immers de kostenkant van de baat 'efficiënt'.

9. Cyberdreigingen

Binnen het thema cyberdreigingen zijn voor vijf scenario's de gevolgen en waarschijnlijkheid in kaart gebracht. Daarnaast zijn er enkele scenario's uit andere thema's die nauwe raakvlakken met het thema cyberdreigingen kennen, zoals de ransomware aanval op een telecom provider (thema bedreiging vitale infrastructuur) en het scenario cyberspionage overheid (thema ongewenste inmenging en beïnvloeding democratische rechtstaat). In onderstaande figuur worden deze scenario's in vergelijkend perspectief weergegeven.

Figuur 9 Risicodiagram cyberdreigingen

	Zeer onwaarschijnlijk	Onwaarschijnlijk	Enigszins waarschijnlijk	Waarschijnlijk	Zeer waarschijnlijk
Catastrofaal					
Zeer ernstig				• Aanval Cloud Service Provider	
Ernstig	• Ransomware telecom				
Aanzienlijk		• Cyberaanval ICS - chemische sector • Ransomware zorgsector		• Cyberspionage overheid • Misconfiguratie grote internet-dienstverlener	• Collateral damage
Beperkt					

Het valt op dat de waarschijnlijkheid van de scenario's sterk uiteenloopt en dat de impact over het algemeen relatief beperkt blijft. Hierbij is het belangrijk om te benadrukken dat die impactbeoordeling beïnvloed wordt doordat het in veel gevallen erg moeilijk te voorspellen is wat de gevolgen zijn van verstoringen van digitale systemen, netwerken en diensten. Zoals ook al in de ANV Horizonscan Nationale Veiligheid 2020 werd geconstateerd zorgt de vernetting en digitalisering van de samenleving er voor dat "we niet goed kunnen overzien wat de impact van een digitale verstoring is. In alle sectoren van de samenleving worden databronnen en informatiesystemen aan elkaar gekoppeld,

maar vaak met onvoldoende inzicht in cascade-effecten bij uitval of nieuwe aanvalsroutes die daarmee gecreëerd worden" (ANV, 2020). Daar komt nog bij dat de digitale ruimte (het complexe samenspel van IT netwerken en informatiesystemen) continu in beweging is en dat zorgt ook weer voor nieuwe, onverwachte afhankelijkheidsrelaties en effecten. De 'sluimerende dreigingen' die kunnen voortkomen uit technologische ontwikkelingen zoals AI (geavanceerde AI gebaseerde cyberaanvallen) en Quantum (kwetsbare cryptografie, waardoor protocollen en gevoelige gegevens niet meer veilig zijn én meer rekenkracht voor kwaadwillenden om geautomatiseerde aanvallen uit te voeren) laten zien dat het ook niet te verwachten is dat deze dynamiek in de toekomst zal verminderen.

Een andere oorzaak voor de relatief lage impact lijkt te zijn dat de maatschappelijke impact van de verstoringen in veel gevallen een beperkte duur kent. Door het belang van digitale systemen is er ook een (commerciële) drive bij aanbieders om problemen snel te verhelpen. In andere gevallen kunnen de maatschappelijke gevolgen na verloop van tijd opgevangen worden met alternatieven of back-up systemen terwijl de daadwerkelijke herstelwerkzaamheden nog doorgaan. Tenslotte zorgt de decentrale architectuur van het Internet en Internetdiensten ervoor dat veel verstoringen beperkt blijven tot een specifieke groep gebruikers of diensten. Die kunnen weliswaar wijdverspreid zijn (wereldwijd), maar de effecten zijn relatief geconcentreerd.

De impact die ontstaat vanuit cyberdreigingen is divers en verspreid over alle veiligheidsbelangen en impactcriteria. Dit is ook logisch want binnen dit thema worden ook zeer uiteenlopende typen dreigingen geadresseerd waardoor ook verschillende veiligheidsbelangen worden bedreigd. Door deze breedte van het thema en de dreigingscategorieën is het moeilijk om generaliserende conclusies te trekken over de omvang en aard van de impact van de onderliggende fenomenen in relatie tot specifieke veiligheidsbelangen of criteria.

Vanuit deze analyse wordt opnieuw bevestigd dat de digitalisering van de samenleving (en economie) niet alleen zorgt voor nieuwe mogelijkheden én kwetsbaarheden, maar dat het ook steeds meer een onderwerp van strategisch, (geo)politiek belang is. De dominante rol van grote techbedrijven en de manier waarop staten zich op uiteenlopende manieren manifesteren in het digitale domein zorgen ervoor dat er spanningsvelden ontstaan tussen verschillende belangen en perspectieven op de digitale ruimte, bijvoorbeeld als het gaat om het streven naar digitale soevereiniteit of autonomie van landen en het effect daarvan op de technische ontwikkelingen/innovaties. Ook zijn er ontwikkelingen die de governance en waarden van het Internet en de digitale ruimte onder druk zetten, waardoor op termijn onze Nederlandse belangen van een open en digitale economie in het geding kunnen komen.

10. Bedreiging vitale infrastructuur

Vitale infrastructuur is nauw verbonden met veel verschillende dreigingen voor de nationale veiligheid. De vitale processen die gezamenlijk de Nederlandse vitale infrastructuur vormen zijn vitaal omdat uitval of verstoring ervan al gauw leidt tot maatschappelijke ontwrichting. Het is dan ook logisch dat de impact van veel verschillende dreigingstypen voor een deel ontstaat door verstoringen van vitale infrastructuur. De scenario's die binnen dit thema worden behandeld laten zien dat hier een grote verscheidenheid van dreigingen is. Zo wordt ingegaan op terroristische- en cyberaanvallen, maar ook op natuurlijke verstoringen als overstromingen en natuurbranden, technisch of menselijk falen en een fenomeen als ruimteweer. Ook in veel andere dreigingsthema's wordt impact op vitale infrastructuur geadresseerd (bijvoorbeeld in de thema's klimaat- en natuurrampen, cyberdreigingen, ongewenste inmenging en ondermijning democratische rechtsstaat, en economische bedreigingen). In onderstaande figuur staat het risicodiagram voor het thema bedreiging vitale infrastructuur.

Figuur 10 Risicodiagram bedreiging vitale infrastructuur

	Zeer onwaarschijnlijk	Onwaarschijnlijk	Enigszins waarschijnlijk	Waarschijnlijk	Zeer waarschijnlijk
Catastrofaal					
Zeer ernstig		• Keteneffecten elektriciteitsuitval	• Overstroming rivier		
Ernstig	• Ransomware telecom			• Landelijke black-out	• Natuurbranden
Aanzienlijk					
Beperkt					

De analyse bevestigt opnieuw het beeld dat we als samenleving sterk afhankelijk zijn van vitale processen, waarbij vitale processen in de energiesector en telecomsector eruit springen vanwege de vele afhankelijkheden hiervan in de samenleving. Net als vrijwel alle delen van de samenleving wordt ook de vitale infrastructuur steeds afhankelijker van digitale systemen. Tegelijkertijd is het belangrijk om te realiseren dat deze afhankelijkheden niet statisch zijn, maar kunnen veranderen. De complexiteit van systemen en afhankelijkheden tussen systemen en processen nemen steeds verder toe waardoor het moeilijk is om een goede inschatting te maken van de gevolgen van gebeurtenissen zoals beschreven in de scenario's, aangezien er veel onderlinge, verborgen afhankelijkheden binnen en tussen processen bestaan. Bovendien zorgen de veranderlijkheid in het gebruik en de constante technologische ontwikkeling en vernieuwing van systemen en infrastructuur ervoor dat het een uitdaging is om constant zicht te blijven houden op deze afhankelijkheden.

Op de langere termijn kunnen schaarste op de arbeidsmarkt en in het bijzonder gebrek aan technisch geschoold personeel, bijvoorbeeld op het gebied van cybersecurity of benodigde kennis en expertise om de energietransitie vorm te geven, ervoor zorgen dat er onvoldoende capaciteit is om de weerbaarheid van vitale infrastructuur op peil te houden. Dit wordt dan ook gezien als een sluimerende dreiging.

Kijkend naar de dreigingen met betrekking tot de vitale infrastructuur voor de komende vijf jaar komt naar voren komt dat zowel statelijke actoren als cybercriminelen een steeds grotere bedreiging vormen voor de continuïteit van vitale processen. Vanwege de belangrijke maatschappelijke rol van vitale processen zijn ze een aantrekkelijk doelwit van kwaadwillende actoren. Om die reden wordt de bescherming van de continuïteit van de vitale infrastructuur ook steeds meer onderdeel van discussies over strategische autonomie en economische veiligheid.

De waarschijnlijkheid van moedwillige aanvallen op de Nederlandse vitale infrastructuur, zoals uitgewerkt in deze analyse, wordt op dit moment relatief laag ingeschat. Dit heeft deels te maken met de preventieve en mitigerende maatregelen van de vitale aanbieders en deels met de capaciteit en motivatie van actoren die nodig is om doelbewust en doelgericht een dergelijke aanval uit te voeren.

Als het gaat om niet-moedwillige bedreigingen vormen vooral de effecten van klimaatverandering en de energietransitie een bedreiging voor vitale infrastructuur, wat in de komende jaren steeds reëler zal worden en meer impact zal hebben. Door klimaatverandering zullen steeds vaker extreme weersomstandigheden ontstaan, zoals extreme regenval, overstromingen en droogte. De waarschijnlijkheid van verstoring van vitale infrastructuur door een natuurlijke oorzaak zal dan ook steeds verder toenemen.

De energietransitie, in combinatie met geopolitieke ontwikkelingen, zorgt er voor dat er meer en meer ingezet wordt op elektrificatie, maar ook dat er veranderingen plaatsvinden in de manier waarop elektriciteit wordt geproduceerd en gedistribueerd. Met name in de transitiefase kan dit ervoor zorgen dat er onverwachte effecten optreden omdat de ontwikkeling van de infrastructuur continu in beweging is.

Tenslotte is digitalisering een belangrijke ontwikkeling die ervoor zorgt dat de digitale infrastructuur ook continu aan verandering onderhevig is en dat verbindingen en afhankelijkheden tussen systemen ook dynamisch zijn. Niet alleen de infrastructuur zelf verandert, maar ook het gebruik (en dus de maatschappelijke afhankelijkheid). De COVID-19-pandemie heeft er bijvoorbeeld voor gezorgd dat we massaal zijn gaan thuiswerken, waardoor de Internettoegang voor huishoudens een veel belangrijkere rol kreeg en de datastromen veranderden. Deze dynamieken zorgen ervoor dat de directe impact en keteneffecten van uitval of verstoring van een vitaal proces lastig in te schatten is. Bij de voorbereiding op dit type gebeurtenissen is het dan ook van belang om ook altijd rekening te houden met onverwachte effecten.

11. Risico's in het Caribisch deel van het Koninkrijk

Zoals gemeld is een aparte risicoanalyse uitgevoerd om dreigingen die zich kunnen manifesteren in het Caribisch deel van het Koninkrijk inzichtelijk te maken. Dit hoofdstuk bevat de belangrijkste resultaten.

Impact op de nationale veiligheid
Uit de analyse volgt dat bij de thema's klimaat- en natuurrampen en internationale en militaire dreigingen enkele risico's zijn geïnventariseerd waarvan de impact op de nationale veiligheid groot kan zijn. Bij natuurrampen komt daarbij een orkaan als het grootste risico naar voren (zowel de waarschijnlijkheid als de impact). Zoals orkaan Irma (2017) heeft laten zien, heeft een orkaan gevolgen voor alle facetten van de samenleving op een getroffen eiland, waarbij vooral het dagelijks leven verstoord raakt en de economische schade groot is. In het thema klimaat- en natuurrampen is het scenario orkaan verder uitgewerkt.

Bij het thema internationale en militaire dreigingen is ingezoomd op de situatie in Venezuela en een eventuele escalatie. Binnen dit thema is een scenario hierover ontwikkeld. Een escalatie zoals beschreven in het scenario kan leiden tot onder meer een vergrote vluchtelingenstroom naar het Caribisch deel van het Koninkrijk.

Beide scenario's hebben een grote impact. Ook bij de andere thema's die geanalyseerd zijn zullen er in geval van het manifesteren van de dreigingen zeker op het (ei)land waar het plaatsvindt grote gevolgen naar voren kunnen komen. Bij veel van de thema's (zoals zware ongevallen, terrorisme en openbare orde verstoringen) zijn mogelijke gevolgen voor het toerisme, de economie en het dagelijkse leven op de eilanden benoemd, zeker als de infrastructuur inclusief het vervoer van en naar de eilanden wordt geraakt. Bij enkele andere thema's (zoals georganiseerde criminaliteit) geldt daarnaast dat er aantasting van de sociale en politieke stabiliteit (ondermijning van de democratische rechtsstaat) plaats kan vinden.

Lokale impact en beperkte capaciteit
Een andere constatering is dat de impact op de nationale veiligheid conform de gehanteerde methodiek soms minder relevant zal zijn voor het Koninkrijk als geheel, maar dat de lokale impact vanwege de kleinschalige context van de eilanden wel groot kan zijn. Als voorbeeld noemen we een natuurramp of infectieziekte waarbij grote aantallen mensen medische hulp nodig hebben. Als het om tientallen mensen gaat, is dat qua impact conform de methodiek niet groot, maar raakt dat wel het betreffende eiland, onder meer vanwege de beperkte (medische) capaciteit aan de kant van de hulpverlening. Datzelfde geldt als het gaat om de opvang van grote groepen mensen, bijvoorbeeld van een nabijgelegen (ei)land als gevolg van natuurgeweld of bij een ongeval van een cruiseschip. De beschikbare opvangcapaciteit zal al snel overvraagd worden.

Afhankelijkheid en kwetsbaarheid
Een laatste en hieraan verbonden constatering gaat over de afhankelijkheid en kwetsbaarheid van het Caribisch deel van het Koninkrijk. In de eerste plaats is de afhankelijkheid een gegeven met het feit dat de eilanden voor bevoorrading van voedsel en goederen aangewezen zijn op transport via zee en lucht, zodat de havens en luchthaven essentieel zijn. Als die niet toegankelijk of bruikbaar zijn heeft dat grote gevolgen.

Verder is de economie in het Caribisch gebied voor een aanzienlijk deel afhankelijk van het toerisme. Uit de analyse volgt dat er verschillende dreigingen kunnen optreden waardoor het toerisme kan worden geraakt. Dit maakt dat deze afhankelijkheid ook een kwetsbaarheid inhoudt. De coronapandemie heeft dat duidelijk laten zien.

Tenslotte is het Caribisch deel van het Koninkrijk (net als Europees Nederland) sterk afhankelijk van de (vitale) infrastructuur. Een verstoring kan een grote impact hebben op de eilanden, zeker als meerdere infrastructuren tegelijk geraakt worden. Daarbij komt dat de infrastructuur kwetsbaar is voor natuurgeweld en is gesignaleerd dat de processen kwetsbaar zijn voor cyberdreigingen.

DEEL 2: Overkoepelende resultaten Rijksbrede Risicoanalyse

Deel twee van dit rapport gaat in op de resultaten van de Rijksbrede Risicoanalyse als geheel, alsmede enkele dwarsverbanden tussen de verschillende dreigingsthema's, enkele overkoepelende onderwerpen die uit de analyse naar voren zijn gekomen en het bredere dreigingslandschap nationale veiligheid.

12. Algemene resultaten: risicodiagram

Binnen de RbRa zijn meer dan zestig scenario's beoordeeld langs de assen waarschijnlijkheid en impact op de nationale veiligheid. De resultaten van deze beoordeling, samen met het identificeren van relevante ontwikkelingen, dwarsverbanden en overkoepelende inzichten, vormen de belangrijkste resultaten van deze analyse. In dit hoofdstuk wordt ingegaan op de resultaten van de risicobeoordeling.

12.1 Resultaten risicobeoordeling

Doordat alle in de RbRa opgenomen scenario's met behulp van dezelfde methodiek zijn opgesteld en beoordeeld, biedt de RbRa de mogelijkheid om de verschillende dreigingen die onze samenleving kunnen ontwrichten in vergelijkend perspectief te plaatsen. De hieruit voortkomende inzichten kunnen assisteren bij het toekennen van prioriteiten in onder andere de Rijksbrede Veiligheidsstrategie. Om niet alleen de afzonderlijke beoordelingen van de scenario's weer te geven, maar ook deze onderlinge vergelijking te faciliteren, zijn de resultaten weergegeven in een risicodiagram (figuur 11).

Het diagram in kwestie betreft een uitvergrote versie van de diagrammen uit de voorgaande themahoofdstukken, met hierin opgenomen alle van de meer dan zestig uitgewerkte scenario's. De verticale as van het diagram laat de totale impact van het betreffende scenario op de nationale veiligheid zien. Deze is berekend op basis van de impactscores op de zes veiligheidsbelangen (zie methodiek bijlage) en is opgedeeld in zes klassen: van beperkt tot catastrofaal. De horizontale as laat de waarschijnlijkheid zien van een scenario. Ook deze is onderverdeeld in vijf klassen, van zeer onwaarschijnlijk tot zeer waarschijnlijk.

Figuur 11 Totale risicodiagram

	Zeer onwaarschijnlijk	Onwaarschijnlijk	Enigszins waarschijnlijk	Waarschijnlijk	Zeer waarschijnlijk
Catastrofaal		• Overstroming zee	• Pandemie door een mens overdraagbaar virus		
Zeer ernstig	• IS grijpt de macht in Marokko • Inzet van kernwapens Saoedi-Arabië – Iran • Geïnduceerde aardbeving	• Keteneffecten elektriciteitsuitval • Chinese hereniging Taiwan • Tijdelijke bezetting van een EU-lidstaat	• Overstroming rivier • Griep pandemie • Instorten van de Venezolaanse staat • Uiteenvallen van de NAVO • Systeempartij in de fin. sector in zwaar weer	• Orkaan • Hitte/droogte • Import van fossiele energie • Aanval Cloud Service Provider	
Ernstig	• Kerncentrale Borssele • Treinramp met gaswolkbrand • Ransomware telecom	• Handelsoorlog waar Europa bij betrokken is • Meervoudige terroristische aanslag • Verstoring van het betalingsverkeer • Statelijke verwerving van een belang in grote telecom-aanbieder • Infiltratie openbaar bestuur	• Sneeuwstorm • Crisis in de Zuid-Chinese Zee • Tweespalt in de EU • Crimineel geweld richting media en overheid • Ongewenste buitenlandse inmenging in diasporagemeenschappen • Bestorming en gijzeling Tweede Kamer	• Landelijke black-out • (Heimelijke) beïnvloeding door China • Polarisatie rond complottheorieën • Desintegratie van Bosnië-Herzegovina	• Hybride operaties – aangrijpen op maatschappelijk debat • Griep epidemie • Verstoring van handel door productieproblemen buitenland • Natuurbranden
Aanzienlijk	• Stralingsongeval in Europa • Falen opslagtank ammoniak	• Europese schuldencrisis • Cyberaanval ICS - Chemische sector • Ransomware zorgsector • Terroristische aanslag met een bio-wapen	• Uiteenspatten van de OVSE • Aanval op pride evenement • Natuurlijke aardbeving • Geweldsescalatie rechtsextremisten • Anarcho-extremisme • Buitenlandse regulering techbedrijven • Ondermijnende enclaves	• Cyberspionage overheid • Georganiseerde criminaliteit door heel Nederland • Uitbraak MKZ onder koeien • Klassieke statelijke spionage • Innovatie nucleaire overbrengingsmiddelen • Correctie op waardering financiële activa • Misconfiguratie Internetdienstverlener • Criminele inmenging bedrijfsleven • Anti-overheidsextremisme	• Collateral damage
Beperkt			• Uitbraak zoönotische variant vogelgriep	• Tekorten essentiële grondstoffen • Overname van bedrijf dat o.a. dual-use goederen produceert	• Alleenhandelende dader • Buitenlandse durfkapitaalinvesteringen in startups

Bij het doornemen van het bovenstaande diagram is het goed om een aantal zaken in gedachten te houden. Ten eerste dienen de scenario's in bovenstaande diagram primair als illustratie van een bredere dreigingscategorie. Zo geven bijvoorbeeld de scenario's die zijn uitgewerkt binnen de dreigingscategorie terrorisme een indicatie van de verschillende wijzen waarop deze dreiging zich kan manifesteren, maar zijn ze tegelijkertijd niet uitputtend. Voor een meer compleet van de verschillende dreigingen en de opbouw van de in het diagram opgenomen scenario's wordt verwezen naar de in dit rapport opgenomen themahoofdstukken en de onderliggende, afzonderlijke themarapportages.

Ten tweede is de vraag welke typen risico's de grootste dreiging voor de nationale veiligheid vormen niet zondermeer te beantwoorden. Gaat het bijvoorbeeld om de dreiging met de grootste impact, los van de waarschijnlijkheid van optreden? Of ligt de focus juist op de dreigingen die zeer waarschijnlijk zijn, terwijl de impact relatief beperkt is? Het kan ook zijn dat de behoefte juist is om in te gaan op de risico's met zowel een relatief hoge impact als waarschijnlijkheid.

Omdat het antwoord op deze vraag sterk afhangt van het gehanteerde perspectief, bespreken we hieronder de resultaten uit het risicodiagram vanuit verschillende invalshoeken. In de eerste plaats kijken we vanuit de waarschijnlijkheid van optreden. Vervolgens leggen we de focus op de impact op de nationale veiligheid, waarna we tenslotte aandacht geven aan de combinatie van waarschijnlijkheid en impact. Dat laatste doen we niet op een rekenkundige wijze (in de zin van risico is waarschijnlijkheid maal impact), maar kwalitatief op basis van de type risico's die zowel een relatieve hoge impact als waarschijnlijkheid hebben.

12.2 Gezien vanuit waarschijnlijkheid

Uit het risicodiagram volgen enkele algemene constateringen wat betreft waarschijnlijkheid. Allereerst is duidelijk dat de scenario's zijn verdeeld over de verschillende klassen en dat dus alle waarschijnlijkheidsklassen naar voren komen. Van de scenario's met een zeer lage waarschijnlijkheid (aan de linkerzijde van het diagram) zijn de meeste een 'fysiek' risico (safety), zoals zware ongevallen in de vorm van een ongeval bij kerncentrales of de chemische industrie en een natuurramp in de vorm van een geïnduceerde aardbeving. Daarnaast zijn er ook moedwillige risico's (security) met een lage waarschijnlijkheid, zoals een scenario rond ransomware in de telecomsector en scenario's met een internationaal karakter (zoals de inzet van kernwapens buiten het Koninkrijk).

De scenario's met een hoge waarschijnlijkheid staan aan de rechterzijde van het diagram. Wat opvalt is dat zich daar veel scenario's bevinden. Er zijn onder meer relatief veel scenario's met de hoogste waarschijnlijkheid (zeer waarschijnlijk). Ook hier gaat het om scenario's die verdeeld zijn over de verschillende thema's. Het betreft zowel safety (natuurbranden, griepepidemie) als security dreigingen (hybride operaties, verstoringen internationale handel, collateral damage cyberaanvallen).

Als we de hoge scores op waarschijnlijkheid leggen naast het risicodiagram uit het NVP 2016 (ANV, 2016) is er een duidelijk verschil te zien en zijn er in deze nieuwe analyse meer scenario's met een hoge waarschijnlijk (zeer waarschijnlijk). Daaruit zou kunnen worden afgeleid dat volgens de verschillende experts de kans van optreden van verschillende dreigingen de laatste jaren is toegenomen. Uiteraard dient dit genuanceerd te worden, omdat het onder meer afhangt van de onderliggende keuzes en het aantal uitgewerkte scenario's (het aantal scenario's is bijvoorbeeld beduidend hoger dan in 2016) en de constatering geldt ook niet voor elk type dreiging. Dat de waarschijnlijkheid is toegenomen geldt in ieder geval wel voor het dreigingstype 'natuurbranden', waarbij is gemeld dat het niet gaat om *of* maar *wanneer* er een brand optreedt die de nationale veiligheid zal raken.

Een algemene constatering uit bovenstaande is dat de kans dat er de komende jaren gebeurtenissen optreden die de nationale veiligheid raken relatief groot is. Op basis van dit inzicht kan nader ingezoomd worden op de weerbaarheid tegen de type dreigingen met een hoge waarschijnlijkheid.

12.3 Gezien vanuit impact

Er zijn veel scenario's waarvan de impact 'ernstig' of hoger is. Dit betekent dat in al deze gevallen er sprake is van aantasting van de nationale veiligheid. Als we inzoomen op de dreigingen met de hoogste impact (zeer ernstig en catastrofaal) blijkt dat daarin wederom de verschillende dreigingsthema's zijn vertegenwoordigd. Ook hier is een mix van zowel safety en security als interne en externe dreigingen te zien.

De grootste impact ('catastrofaal') is te verwachten bij fysieke dreigingen, namelijk bij een overstroming vanuit zee en een nieuwe pandemie vergelijkbaar met COVID-19. In beide gevallen is de impact zeer groot en worden meerdere veiligheidsbelangen catastrofaal geraakt. Beide dreigingen stonden ook in eerdere analyses (ANV, 2016; 2019a) bovenaan wat de impact betreft. Toch zijn er ook verschillen ten opzichte van deze eerdere analyses. Voor de overstroming geldt dat een ander scenario is gekozen. Het gaat niet om een overstroming van de Randstad (dijkring

14), maar om Flevoland en een deel van Noord-Nederland. Nog steeds leidt dit tot catastrofale gevolgen, maar tegelijkertijd is de waarschijnlijkheid een categorie hoger (onwaarschijnlijk). Voor het pandemiescenario geldt dat dit scenario is gebaseerd op de COVID-19-pandemie, met dien verstande dat het uitgewerkte scenario nog iets ernstiger is, bijvoorbeeld als het gaat om de beschikbaarheid van vaccins. Deze variant heeft een grotere totale impact (catastrofaal) dan het scenario grieppandemie (impact zeer ernstig) en is als enigszins waarschijnlijk beoordeeld.

Op de vraag in hoeverre de samenleving op de verschillende dreigingen met een grote impact op de nationale veiligheid is voorbereid kan in de weerbaarheidsinschatting dieper worden ingegaan. Daarbij kan nader inzicht op de soort impact (welke belangen of achterliggende criteria worden geraakt) helpen bij de focus op de weerbaarheid en de crisisbeheersing. De informatie op scenarioniveau (opgenomen in de themarapportages) en samenvattende overzichten uit deze analyse kunnen hiervoor worden gebruikt.

12.4 Combinatie van impact en waarschijnlijkheid

Bij de vraag welke dreigingen zowel een relatieve grote impact als waarschijnlijkheid hebben ligt de focus op de scenario's rechtsboven in het risicodiagram. De eerste constatering is dat de cellen helemaal rechtsboven in het diagram geen scenario's bevatten. In de overige donkerblauwe cellen staan de volgende scenario's:

- Hitte/droogte;
- Orkaan;
- Natuurbranden;
- Import van fossiele energie;
- Verstoring van handel door productieproblemen in het buitenland;
- Aanval Cloud Service Provider;
- Hybride operaties Rusland;
- Griep epidemie;
- Pandemie door een mens overdraagbaar respiratoir virus.

De opsomming betreft geen rangorde, maar de scenario's zijn geclusterd naar dreigingsthema.

De scenario's hitte/droogte en natuurbrand vallen binnen het dreigingsthema klimaat- en natuurrampen en zijn logischerwijs ook onderling met elkaar verbonden wat betreft waarschijnlijkheid. Klimaatverandering is een belangrijke driver van een toenemende waarschijnlijkheid van langdurige hitte en droogte, met als gevolg ook een toenemend risico van natuurbranden. Dit laat zien dat het zowel van belang is om in het vervolg in te gaan op de weerbaarheid tegen deze specifieke risico's zoals natuurbranden en hitte en droogte, als dat het relevant is om het onderwerp klimaatverandering te blijven agenderen. In het volgende hoofdstuk wordt hierop verder ingegaan. Het scenario orkaan is één van de grootste risico's voor het Caribisch deel van het Koninkrijk. Het scenario is gebaseerd op orkaan Irma. Ook bij dit onderwerp is klimaatverandering van belang, omdat door klimaatverandering orkanen in de toekomst krachtiger zullen worden.

De scenario's met betrekking tot fossiele energie en verstoring van de handel door productieproblemen in het buitenland horen bij het thema economische dreigingen. Bij de import van fossiele energie gaat het om afhankelijkheid van buitenlandse leveranciers en het mogelijk ontstaan van hoge kosten voor producten als olie en gas, met onder andere potentiële 'energiearmoede' als gevolg. De verstoring van de handel door productieproblemen ontstaat op zijn beurt doordat landen in een situatie van schaarste eerst voor zichzelf kiezen, wat kan zorgen voor grote schade aan onze open economie. Uit deze scenario's komen de risico's van afhankelijkheid naar voren welke zich mogelijk kunnen manifesteren zodra er schaarste dreigt of als er spanningen tussen betrokken actoren zijn.

De aanval op een cloud service provider valt onder het thema cyberdreigingen binnen de categorie verstoring van het internet. Het bijzondere van dit scenario is dat de integriteit van de digitale ruimte maximaal wordt aangetast, maar dat er verder weinig effecten merkbaar zijn. Verder volgt uit het scenario dat het niet goed in te schatten is welke vitale processen zouden kunnen worden verstoord, waaruit een bepaalde mate van onvoorspelbaarheid qua gevolgen naar voren komt.

Bij het scenario hybride operaties voedt Rusland een bestaand maatschappelijk debat om zo de spanningen in de samenleving toe te laten nemen. Dit valt onder het thema ongewenste inmenging en beïnvloeding van de democratische rechtsstaat. In het scenario worden maatschappelijke discussies rondom vluchtelingen en Corona aangewakkerd via onder andere de inzet van *deepfakes*, terwijl tegelijkertijd internationale spanningen toenemen door push-backs en militair vertoon door Rusland richting de NAVO.

De laatste twee scenario's betreffen een epidemie en een pandemie die onder het thema Infectieziekten vallen, waarbij de griepepidemie een scenario is wat zich regelmatig voltrekt, terwijl het pandemiescenario is gebaseerd op COVID-19. Naast grote aantallen doden en zieken (met als gevolg ernstige druk op de medische sector)

kunnen er (afhankelijk van de situatie en de genomen maatregelen) grote gevolgen voor de economie en de samenleving optreden.

Vanuit het perspectief van de combinatie van waarschijnlijkheid en impact kan deze informatie helpen bij de prioritering van risico's en de nadere beschouwing van de weerbaarheid en crisisbeheersing op de betreffende thema's. Daarbij is het goed om niet blind te staren op de negen genoemde scenario's. Ook de scenario's die in het diagram in de iets minder donkere cellen staan hebben een relatief hoog risico als je kijkt vanuit de combinatie van impact en waarschijnlijkheid. Daarbij komen internationale dreigingen gekoppeld aan China (beïnvloeding), de NAVO (uiteenvallen), Europa (Bosnië) en Venezuela (met directe impact op het Caribisch deel van het Koninkrijk) naar voren. Hieruit volgt dat de internationale situatie onrustig is en dat de oplopende geopolitieke spanningen onze nationale veiligheid bedreigen.

Verder gaat het om de elektriciteitsvoorziening (black out), polarisatie (complottheorieën), een bankencrisis en een overstroming van een rivier (zoals in Limburg). Deze opsomming laat tenslotte zien dat ook vanuit dit perspectief (van impact en waarschijnlijkheid) een scala aan typen dreigingen naar voren komt, waar rekening mee gehouden dient te worden. Ook de impact van deze verschillende dreigingen is divers. Waar een bankencrisis vooral de economie raakt, tast polarisatie met name de sociale en politieke stabiliteit aan. Bij een overstroming zijn de gevolgen meer verspreid over verschillende criteria (grondgebied, slachtoffers, kosten, verstoring dagelijks leven), terwijl een verstoring van de elektriciteitsvoorziening naast directe gevolgen voor onder meer het dagelijks leven ook keteneffecten omvat vanwege de grote afhankelijkheid van elektriciteit.

Dit laat zien dat het niet alleen gaat om verschillende typen dreigingen, maar ook om verschillen in de impact op de maatschappij. In de weerbaarheidsinschatting en bij de versterking van de crisisbeheersing kan hiermee rekening worden gehouden.

12.5 Dwarsverbanden en verwevenheid

Een ander element waar bij een weerbaarheidsinschatting rekening dient te worden gehouden, zijn de diverse dwarsverbanden tussen de dreigingsthema's. Zo hebben klimaat- en natuurrampen, maar ook cyberdreigingen potentieel een groot effect op het functioneren van voor de maatschappij vitale infrastructuur. Een natuurramp of een cyberaanval kan bijvoorbeeld leiden tot een verstoring van vitale infrastructuur. Daarnaast is er verbondenheid tussen verschillende vitale processen onderling en is er de afhankelijkheid van digitale systemen. Zo zijn veel vitale processen, net als de maatschappij, afhankelijk van elektriciteits- en telecomvoorzieningen, zodat een verstoring kan leiden tot keteneffecten. Door de verschillende afhankelijkheden is het tegelijkertijd lastig in te schatten welke effecten er precies kunnen optreden. Hiervoor zouden verdiepende analyses uitgevoerd dienen te worden.

Ook bij andere thema's zijn er dwarsverbanden en verwevenheid. Zo kunnen internationale en militaire dreigingen een effect hebben op dreigingen opgenomen in het thema economische dreigingen. Oplopende spanningen tussen grootmachten kunnen bijvoorbeeld potentieel een effect hebben op economische afhankelijkheden, zoals opgenomen in het laatstgenoemde thema.

De dwarsverbanden en afhankelijkheden die we hier aanstippen staan niet op zichzelf en laten zien dat er sprake is van complexiteit en een bepaalde mate van onvoorspelbaarheid. Dat is de reden dat we in hoofdstuk 14 nationale veiligheid als complex systeem benaderen als een aanvulling op de werkwijze waarbij per thema wordt ingezoomd op de risico's.

13. Overkoepelende onderwerpen

In het vorige hoofdstuk zijn de resultaten zoals samengevat in het risicodiagram vanuit een drietal perspectieven bekeken. In aanvulling hierop is het goed om stil te staan bij enkele onderwerpen die bij meerdere thema's naar voren zijn gekomen. In dit hoofdstuk gaan we in op de overkoepelende onderwerpen hybride dreigingen, klimaatverandering, energietransitie en spanningen in de samenleving.

13.1 Hybride dreigingen

Hybride dreigingen zijn vaak onderdeel van een lange termijn campagne. Hoewel individuele hybride activiteiten op zichzelf al een impact kunnen hebben op de nationale veiligheid (denk aan cyberaanvallen), is het noodzakelijk om ook het grote plaatje te blijven zien, omdat de combinatie van individuele activiteiten tot een grotere impact kan leiden dan de som der delen. Bij de bespreking van dit onderwerp in hoofdstuk 6 is al gemeld dat het van cruciaal belang is om altijd een integraal perspectief toe te passsen op specifieke dreigingen en het grote plaatje niet uit het oog te verliezen. Dat werken we in deze paragraaf verder uit aan de hand van een voorbeeld.

In deze Rijksbrede Risicoanalyse zijn binnen verschillende thema's scenario's besproken die ook onderdeel kunnen zijn van een hybride campagne. Het is nuttig om vanuit de verschillende perspectieven naar dreigingen als economische spionage, cyberaanvallen, desinformatie-campagnes of militaire invallen te kijken, maar het is cruciaal om dergelijke fenomenen ook met elkaar in samenhang te bekijken, omdat deze dreigingen ook onderdeel kunnen zijn van een hybride campagne. Onderstaand voorbeeld illustreert deze dreigingsthema-overstijgende aard van hybride dreigingen.

Uitgangspunt van dit scenariovoorbeeld is dat Rusland op allerlei mogelijke manieren wil voorkomen dat Finland toe zal treden tot de NAVO. Enerzijds probeert Rusland Finland te beïnvloeden, maar anderzijds ook andere NAVO landen, waaronder Nederland. Hierbij worden beïnvloedings-campagnes ingezet om de Nederlandse (en Europese) bevolking overwegend negatief te laten staan tegenover toetreding van Finland tot de NAVO. Wanneer de gesprekken tussen Finland en de NAVO steeds concreter worden over de toetreding en de spanningen tussen Rusland en Finland toenemen, probeert Rusland de aandacht van de individuele NAVO landen (inclusief Nederland) af te leiden van de mogelijke toetreding van Finland tot de NAVO. Het doel is om de Finse toetreding lager op de agenda te zetten van de NAVO landen. Rusland probeert daartoe in verschillende landen de binnenlandse spanningen te laten toenemen, door middel van (in Nederland) het *aanwakkeren van maatschappelijk debat* en een *grootschalige cyberaanval*. Doel is om Europese landen dusdanig af te leiden van de spanningen tussen Finland en Rusland, waardoor Rusland uiteindelijk langer vrij spel heeft om een *vliegbasis in Finland te bezetten*. Dit vertaalt zich in een aantal scenario's die los van elkaar lijken te staan, maar eigenlijk onderdeel zijn van een groter campagneplan vanuit Rusland. Deze structuur is weg te zetten op een zogenoemde 'escalatieladder': naarmate de tijd vordert zal Rusland telkens een stapje verder gaan in het escalatie-niveau. Zie figuur 12 voor een visuele representatie van de escalatieladder met de drie scenario's die onderdeel uitmaken van de hybride operatie van Rusland, die uiteindelijk leidt tot escalatie (de 'drempel' van gewapend conflict wordt overtreden) in Finland.

Figuur 12 Escalatieladder met de drie 'hybride' Rusland scenario's in drie verschillende dreigingsthema's

Te midden van spanningen tussen Rusland en Finland, waarbij Rusland middels verschillende kanalen de Europese bevolking ervan probeert te overtuigen dat Finse toetreding tot de NAVO een slecht idee is, wordt het maatschappelijke debat rondom vluchtelingen opnieuw aangewakkerd. In dit scenario faciliteert Rusland een grote vluchtelingenstroom richting de EU, waarbij push-backs aan zowel de zuidelijke als de oostelijke grenzen van Europa op grote schaal worden uitgelicht in de media. Het belangrijkste narratief dat Rusland poogt te laten aanslaan bij de bevolking van EU- en NAVO- lidstaten is dat de EU een incompetente en hypocriete institutie is, zonder enig bestaansrecht. Bovendien wordt een gestage troepenopbouw aan de westelijke grenzen van Rusland gesignaleerd. Er is onenigheid binnen de EU of dergelijke troepenopbouw een militaire reactie van de EU vereist (omdat Finland dus nog geen lid is van de NAVO), waarbij sommige lidstaten zelfs zover willen gaan artikel 42.7 in te roepen. Het belangrijkste effect dat Rusland in dit scenario zal beogen is het verdelen van de EU (en daarmee een groot deel van de lidstaten van de NAVO) en besluitvorming te beïnvloeden. Het is echter maar de vraag in hoeverre dergelijke verdeeldheid een structurele impact heeft op de besluitvorming van de EU (en de NAVO). Uiteindelijk leidt de troepenopbouw niet tot militaire acties van Rusland op EU/NAVO grondgebied, en lijkt de toegenomen spanning met een sisser af te lopen.

Een treetje hoger op de escalatieladder zet Rusland in dit scenariovoorbeeld een cyberaanval in, met het doel om de Nederlandse focus te verleggen naar de binnenlandse problematiek rondom de cyberaanval in plaats van op het internationale toneel. Rusland kan hierbij gebruikmaken van een 'proxy' zoals een criminele organisatie. Hierdoor kan Rusland betrokkenheid ontkennen ('plausible deniability') en dus attributie trachten te voorkomen.[14]

Een aanval op een vitaal proces kan leiden tot een groot (maatschappelijk) effect, maar ook een aanval op een niet-vitale sector (zoals een chemieconcern) kan (relatief) grote impact hebben, omdat er doden en gewonden vallen.[15] Een dergelijke 'directe' aanval waarbij slachtoffers te betreuren zijn zal een hybride actor op een lager escalatieniveau niet riskeren, omdat een sluimerend hybride conflict dan direct kan escaleren naar een openlijk militair conflict. Een vitaal proces wat voor een hybride actor als Rusland 'interessanter' is om te verstoren, is de elektriciteitsvoorziening. De impact kan groot zijn, blijkend uit de twee elektriciteitsuitvalscenario's in het thema bedreiging vitale infrastructuur[16], en de hybride actor hoeft zelf niet veel 'last' te hebben van deze aanval. Hoewel de scenario's over elektriciteitsuitval uit het thema verstoring vitale infrastructuur geen digitale component kennen, zal de impact grotendeels hetzelfde zijn (ongeacht de oorzaak). Ook kan een verstoring van de elektriciteitsvoorziening door heel Europa effecten hebben door de koppelingen in het Europese elektriciteitsnet.

Het moment dat Nederland (en wellicht ook andere lidstaten) afgeleid is door de cyberaanval, grijpt Rusland aan om de aanval in te zetten richting Finland. Wanneer de eerste bewegingen van deze aanval worden gesignaleerd reageren EU-lidstaten erg afwachtend ('het zal wel weer niets zijn'), waardoor Rusland nog meer ruimte wordt gegund in de eerste aanvalsfase. Omdat in een eerdere fase in de hier geschetste situatie van oplopende spanningen

[14] Zie bijvoorbeeld het scenario 'ransomware aanval telecomprovider' binnen het thema bedreiging vitale infrastructuur, dreigingscategorie moedwillige bedreiging vitale processen of het scenario 'ransomware aanval op ziekenhuizen' binnen het thema cyberdreigingen, dreigingscategorie cybercrime.

[15] Zie bijvoorbeeld het scenario 'Cyberaanval ICS – Chemische sector' binnen het thema cyberdreigingen, dreigingscategorie verstoring cyber-fysieke systemen.

[16] Zie thema bedreiging vitale infrastructuur, dreigingscategorie moedwillige bedreiging vitale processen en verstoring vitale processen als gevolg van technisch of menselijk falen.

troepenopbouw uiteindelijk tot niets had geleid, wordt aangenomen dat de militaire dreiging vanuit Rusland opnieuw niet zo groot zou zijn. Om niet verder te escaleren, doet de EU in eerste instantie niets, wat Rusland de ruimte gunt om de vliegbasis in Finland te bezetten.

13.2 Klimaatverandering

Als gevolg van de uitstoot van broeikasgassen verandert het klimaat; het wordt wereldwijd steeds warmer. Volgens het KNMI verandert het klimaat sneller dan eerder werd gedacht en merken we dat in Nederland steeds meer. Klimaatverandering is een belangrijke driver voor het versterken van verschillende dreigingen, niet alleen binnen het thema klimaat- en natuurrampen, maar ook binnen de andere thema's zoals economische dreigingen.

Door klimaatverandering neemt de kans op weersextremen toe. Weersextremen op zich zijn een dreiging voor de nationale veiligheid, maar kunnen ook andere dreigingen triggeren. Extreme neerslag kan bijvoorbeeld leiden tot overstromingen en extreme hitte en droogte kunnen leiden tot onbeheersbare natuurbranden. Extreme droogte, wateroverlast en overstromingen hebben op hun beurt als gevolg dat de vitale infrastructuur, zoals de drinkwater-, elektriciteits- en telecomvoorziening, verstoord kan raken. Daarnaast kunnen te hoge of te lage waterstanden, als gevolg van extreem weer, leiden tot verstoring van de handelsverbindingen en daarmee de knooppuntfunctie van Nederland bedreigen.

Ook de steeds hogere temperaturen kunnen dreigingen versterken. Door hogere temperaturen stijgt de zeespiegel, waardoor de kans op overstromingen toeneemt. Ook is de verwachting dat door hogere temperaturen in Nederland andere infectieziekten kunnen gaan voorkomen. Daarnaast kan het leiden tot een afname van de kwaliteit, veiligheid en kwantiteit (schaarste) van voedsel wereldwijd, met als gevolg hogere voedselprijzen en toename van migratiebewegingen.

Vraagstukken rond klimaatverandering zijn daarnaast vatbaar voor polarisatie of het ontstaan van anti-overheidssentiment, bijvoorbeeld rondom maatregelen die genomen worden, zoals het plaatsen van windturbines, maar ook datacentra, die grootverbruikers zijn van energie, kunnen zorgen voor weerstand en spanningsvelden tussen verschillende belangen. Tevens kunnen mensen rond dit onderwerp radicaliseren vanuit een links gedachtegoed, bijvoorbeeld vanuit de gedachte dat er te weinig wordt gedaan om klimaatverandering te beperken. Ook kan klimaatverandering internationaal voor spanningen zorgen, bijvoorbeeld doordat internationaal geen consensus gevonden wordt over benodigde maatregelen, maar ook doordat de discussies rondom klimaatveranderingen kunnen worden misbruikt om spanningen tussen landen op te bouwen en buitenlandse politieke agenda's te propageren. Daarnaast ontstaat door klimaatverandering een economisch risico door structurelere schade. Door te weinig te investeren in gevolgbeperking en preventie (klimaatadaptatie) bestaat het risico dat internationale kredietbeoordelaars de kredietwaardigheid van Nederland naar beneden bijstellen. Ook zal verzekerbaarheid van schade onder druk komen te staan.

Klimaatverandering is dus, als driver voor het versterken van verschillende dreigingen, een sluimerende dreiging, die leidt tot een toenemende kwetsbaarheid van de nationale veiligheid. Het zorgt ervoor dat het steeds reëler wordt dat de nationale veiligheid wordt geraakt door de aan klimaatverandering gerelateerde dreigingen en dat de potentiële impact toeneemt. Daarbij komt dat de gevolgen en risico's van klimaatverandering steeds complexer worden en moeilijker te beheersen. Het IPCC-rapport van eind februari 2022 waarschuwt voor domino-effecten, waarbij verschillende klimaatgevolgen elkaar triggeren en onderling versterken. Een voorbeeld is een hittegolf die droogte veroorzaakt, gevolgd door biodiversiteitsverlies, hogere voedselprijzen en honger, waardoor de kwetsbaarheid van mensen en natuur voor nieuwe weersextremen toeneemt en migratiebewegingen op gang komen. Er zullen meerdere klimaatrisico's tegelijkertijd gaan optreden en meerdere klimatologische en niet-klimatologische risico's gaan op elkaar inwerken.

13.3 Energietransitie

De energietransitie is een ingrijpende verandering waar veel facetten aan zitten die relevant zijn voor de nationale veiligheid. Zo zal het gebruik van bepaalde technieken en stoffen risico's met zich meebrengen, zoals het gebruik van waterstof. Deze risico's heeft het ANV eerder in een studie in kaart gebracht (ANV, 2019b). Daaruit volgde onder andere dat de risico's gekoppeld aan het gebruik van gevaarlijke stoffen voor de nationale veiligheid door de energietransitie niet wezenlijk anders zullen zijn dan in de huidige situatie, alhoewel er op onderdelen zoals het gebruik van waterstof in de woonomgeving expliciet aandacht nodig is. Ook komt naar voren dat met name de transitiefase waarin oude en nieuwe technieken naast elkaar bestaan en steeds meer met elkaar geïntegreerd gaan worden tot (onverwachte) knelpunten kan leiden.
Qua technieken zijn onder meer windenergie en kernenergie relevant, met als optie de ontwikkeling van nieuwe kerncentrales. De risico's hiervan zijn in het thema zware ongevallen in kaart gebracht, waaruit volgt dat de waarschijnlijkheid van ongevallen extreem klein is. Los van

de vraag naar de risico's van een centrale an sich, zal een besluit om een nieuwe centrale tot maatschappelijke ophef kunnen leiden. Voor windenergie geldt dat er ingezet wordt op windparken in de Noordzee. Het aantal windparken op zee zal toenemen, waardoor ook de kans op ongevallen van scheepvaart op de windparken toeneemt, zodat er nagedacht wordt over de beveiliging van deze parken. Naast ongevallen op de Noordzee die via de windparken de energievoorziening kunnen raken, kan er sprake zijn van moedwillige dreigingen. Zo kunnen componenten van de vitale infrastructuur, waaronder windparken op zee, doelwit kunnen zijn van o.a. cyberaanvallen en sabotage.

Elektrificatie is één van de pijlers van de energietransitie. Er zal steeds meer gebruik worden gemaakt van elektriciteit in plaats van bijvoorbeeld gas of olie, denk bijvoorbeeld elektrisch vervoer. Dit leidt tot een grotere afhankelijkheid van en druk op het elektriciteitsnet. Dit kan op sommige plaatsen tot capaciteitsproblemen leiden en kan de kans op verstoringen vergroten.

Omdat onze maatschappij sterk afhankelijk is van de elektriciteitsvoorziening zijn vragen rondom betrouwbaarheid en leveringszekerheid relevant. Een verstoring kan grote impact hebben op de nationale veiligheid (zoals ook blijkt uit de twee scenario's die binnen het thema bedreiging vitale infrastructuur zijn uitgewerkt met betrekking tot de elektriciteitsvoorziening). Met het oog op de energietransitie zijn technische aspecten van belang zoals het omgaan met verschillen tussen vraag en aanbod (van verschillende bronnen op verschillende momenten) en de beschikbare netwerkcapaciteit, zeker gezien de genoemde elektrificatie. Voor de aansturing en optimalisatie zal technologie als smart grids en AI een belangrijke rol kunnen vervullen, waardoor aandacht moet zijn voor potentiële kwetsbaarheden gerelateerd aan cyberaanvallen.

Tenslotte zijn vraagstukken rondom afhankelijkheid, kosten en draagvlak van belang. Dit raakt onder andere de economische veiligheid. Zo is het verstandig om in een vroeg stadium stil te staan bij de vraag over de afhankelijkheid van bronnen, materialen, technologie en (buitenlandse) actoren, waarvan de afhankelijkheid van Russisch gas een actueel voorbeeld is. De betaalbaarheid en de kosten van de energietransitie met daaraan gerelateerde vragen over de verdeling hiervan zijn onderwerpen die raken aan de haalbaarheid van en het draagvlak voor de energietransitie in de maatschappij. Discussies rondom de plaatsing van windturbines laten zien dat draagvlak een belangrijk issue is en dat de energietransitie ook voeding kan zijn voor spanningen in de samenleving, wat vervolgens kan leiden tot polarisatie en extremisme. Ook de haalbaarheid van de transitie zelf, met de beschikbaarheid van voldoende materialen en technisch personeel is een aandachtspunt.

Samenvattend betekent bovenstaande dat bij de energietransitie veel vraagstukken naar voren komen die vanuit het perspectief van de nationale veiligheid relevant zijn en integraal aandacht behoeven. Juist in de fase waarin keuzen worden gemaakt over de energietransitie kan invulling worden gegeven aan '*safe and secure by design*'.

13.4 Spanningen in de maatschappij

Het ontstaan van maatschappelijke spanningen is niet alleen verbonden aan dreigingen die vallen binnen het thema polarisatie, extremisme en terrorisme, maar kan plaatsvinden in het kader van praktisch elke binnen de RbRa dreigingen. Deze spanningen kunnen zich onder andere uiten in de vorm van buitensluiting, demonstraties, bedreigingen en zelfs fysiek geweld in de vorm van mishandelingen of vernielingen. Deze uitingen kunnen gericht zijn op zowel (groepen) burgers als de overheid en kunnen potentieel een groot effect hebben op hun functioneren alsmede het goed functioneren van de maatschappij in bredere zin. Het is dan ook belangrijk om rekening te houden met het ontstaan van deze spanningen. Uit de voor de RbRa uitgevoerde analyses blijkt dat een breed spectrum aan dreigingen kan leiden tot spanningen in de maatschappij, ook bij typen dreigingen die hier op het eerste gezicht niet altijd mee worden geassocieerd.

Enerzijds zijn er veelal moedwillige dreigingen waarbij het bewust creëren van angst, spanningen en verdeeldheid een middel is van de betrokken statelijke of extremistische actoren om de eigen doelen te bereiken. Voorbeelden hiervan zijn het verspreiden van desinformatie als onderdeel van hybride operaties, het plegen van een terreuraanslag of het opzettelijk zaaien van angst en verdeeldheid binnen diasporagemeenschappen of de bredere maatschappij.

Anderzijds zijn er dreigingen waarbij het ontstaan van maatschappelijke spanningen niet het resultaat is van een bewust streven hiertoe. Bij gebeurtenissen zoals een overstroming, aardbeving of een zwaar ongeval met chemische stoffen kan veel boosheid ontstaan rond de vraag hoe een dergelijke ramp heeft kunnen gebeuren en wie er verantwoordelijk dient te worden gehouden voor de gevolgen. In dit geval zullen de spanningen zich niet per se manifesteren in de verhoudingen tussen verschillende groepen burgers onderling, maar bijvoorbeeld wel in de relatie tussen burger en overheid. Ook voor het onderwerp georganiseerde criminaliteit geldt dat de aanwezigheid hiervan de verhoudingen tussen burger en overheid op scherp kan zetten, vooral wanneer er weinig vertrouwen is in het vermogen van de overheid voor het effectief bestrijden van criminele activiteiten. Dit geldt ook voor het op grote schaal plaatsvinden van cybercrime, bijvoorbeeld

in de vorm van ransomware aanvallen op ziekenhuizen of nutsvoorzieningen.

Ook dreigingen die zich oorspronkelijk buiten de grenzen van het Koninkrijk manifesteren, kunnen binnen deze grenzen tot maatschappelijke spanningen leiden. Internationale conflicten en instabiliteit kunnen zich vertalen tot vijandigheden tussen of binnen verschillende in Nederland woonachtige diasporagemeenschappen, tot de stigmatisering van groepen mensen met een bepaalde nationaliteit en tot toenemende aantallen vluchtelingen alsmede meningsverschillen over hoe hiermee om te gaan. Verstoringen in de internationale handel of levering van energie in de vorm van bijvoorbeeld aardgas kunnen op hun beurt leiden tot het ontstaan van tekorten of een grote prijsstijging van bepaalde goederen. Wanneer mensen hierdoor financieel in de knel komen, kan ook dit resulteren in maatschappelijk onrust en spanningen. Te meer wanneer het gevoel heerst dat de lasten van de situatie ongelijk zijn verdeeld over de bevolking of dat de overheid onvoldoende doet om de situatie te verbeteren.

Om het effect van maatschappelijke spanningen beter weer te geven binnen de RbRa, is er niet alleen aandacht voor geweest binnen de analyse van bovenstaande dreigingen, maar is ook het onderwerp maatschappelijke polarisatie opgenomen als eigen en aparte dreigingscategorie. Dit in tegenstelling tot eerdere door het ANV uitgevoerde analyses zoals het Nationaal veiligheidsprofiel 2016 en de Geïntegreerde Risicoanalyse 2019. Polarisatie is iets dat zich kan voordoen langs een breed spectrum aan onderwerpen en ontwikkelingen. Zo kan polarisatie ontstaan rond de opvang van asielzoekers, maar ook de afhandeling van een uitbraak van infectieziekten zoals de COVID-19-pandemie of zelfs geopolitieke gebeurtenissen zoals de oorlog in Oekraïne. In het kader van de RbRa zijn drie ontwikkelingen naar voren gekomen die hier expliciet dienen te worden vermeld: klimaatverandering, energietransitie en de verspreiding van desinformatie.

Het veranderende klimaat brengt een grote verscheidenheid aan complexe maatschappelijke vraagstukken met zich mee. Van hoe om te gaan met toenemende weersextremen tot de mogelijke komst van steeds meer klimaatvluchtelingen en de vraag hoe de baten en lasten van klimaatadaptatie te verdelen over de maatschappij. Stuk voor stuk zijn dit vragen waar fundamenteel verschillende zienswijzen over bestaan en er een potentieel is voor polarisatie. Te meer wanneer deze zienswijzen almaar worden uitvergroot en tegenover elkaar worden gezet in het publieke debat. Nauw verbonden aan klimaatverandering is de energietransitie. Waar sommige mensen het gebruik van duurzame energiebronnen als windmolens en zonnepanelen verwelkomen en zien als noodzaak, maken anderen zich zorgen over het bouwen van grote wind- en zonneparken en wat dit doet met de uitstraling van het landschap. Ook zal in het kader van de energietransitie de discussie rondom het gebruik van kernenergie weer verder toenemen.

Tegelijkertijd nemen de mogelijkheden voor het aanwakkeren van polarisatie en maatschappelijke spanningen door middel van desinformatie toe. Het is de verwachting dat het produceren van overtuigende deepfakes de komende jaren steeds laagdrempeliger zal worden. Waar er momenteel nog een zeker niveau van kennis nodig is voor het werken met de achterliggende software, zal deze barrière binnenkort wegvallen waardoor ook mensen zonder deze kennis steeds beter in staat zullen zijn deepfakes te produceren. Met deze technologie kan het publieke debat worden beïnvloed, en kan polarisatie in de hand worden gewerkt.

14. Dreigingslandschap nationale veiligheid als complex systeem

14.1 Inleiding

Net als in de Geïntegreerde Risicoanalyse Nationale Veiligheid (ANV, 2019) laat de RbRa analyse opnieuw zien dat er veel **samenhang** is tussen de verschillende dreigingen voor de nationale veiligheid. Zo zijn er specifieke fenomenen die op zichzelf een bedreiging vormen voor de nationale veiligheid, maar die mogelijk ook als onderdeel van een ander fenomeen optreden. Een verstoring van een vitaal proces zoals de elektriciteitsvoorziening kan bijvoorbeeld eigenstandig optreden vanuit een technische oorzaak maar ook als gevolg van een natuurramp. En een chemisch ongeval kan ook ontstaan vanuit een verstoring of sabotage van digitale systemen. Tevens toont het fenomeen hybride dreigingen hoe verschillende fenomenen bewust gecombineerd kunnen worden om de kwetsbaarheden in een samenleving te misbruiken.

Daarnaast geldt dat er sluimerende dreigingen zijn die niet direct van grote impact op de nationale veiligheid zijn, maar die op de **lange termijn** wel degelijk kunnen zorgen voor aanzienlijke impact. Het gaat hierbij enerzijds om lange termijn ontwikkelingen die gaandeweg tot problematische situaties kunnen leiden. Anderzijds gaat het om een reeks relatief kleine gebeurtenissen die individueel niet van grote betekenis lijken te zijn, maar waarbij de optelsom over een langere tijd wel degelijk een ernstig gevolg heeft voor de nationale veiligheid. Kenmerkend van sluimerende dreigingen is dat er vaak een kantelpunt optreedt waarna het heel moeilijk is om de problemen tegen te gaan. In veel gevallen kan hierbij achteraf worden herleid dat er iets is opgetreden dat onomkeerbaar is gebleken en voor problemen zorgt. Dergelijke risico's kunnen zich gestaag onder de radar opbouwen. Zo'n gestage opbouw van risico's kan bijvoorbeeld spelen bij economische afhankelijkheden. Waar bedrijven en overheden vanuit (bedrijfs)economische logica 'als vanzelf' kiezen voor een bepaalde productiestructuur, bestaat het risico dat er over tijd 'als vanzelf' een ongewenste afhankelijkheid ontstaat waar sprake is van geconcentreerd aanbod.

Binnen de verschillende dreigingsthema's zijn concrete voorbeelden van **sluimerende dreigingen** belicht die soms direct gekoppeld zijn aan een specifiek dreigingsthema (bijvoorbeeld de opkomst van AI-gedreven cyberaanvallen). Veelal zijn sluimerende dreigingen juist ook relevant voor de ontwikkeling van het dreigingslandschap van meerdere thema's, zoals de overkoepelende onderwerpen klimaatverandering, de energietransitie, de toename van spanningen in de samenleving en hybride dreigingen. Daarmee wordt opnieuw de samenhang en verbondenheid tussen fenomenen bevestigd.

Deze verbondenheid, gecombineerd met de grotere impact van de cumulatie van fenomenen op de langere termijn, zorgt voor een complexere dimensie van het dreigings-landschap voor de nationale veiligheid. Om die reden beschouwen we in dit hoofdstuk de nationale veiligheid als complex systeem, waarbij we kort ingaan op een aantal kenmerken van deze complexiteit.

14.2 Kenmerken van nationale veiligheid als complex systeem

Technologische systemen die van groot belang zijn voor processen in de samenleving (waaronder vitale processen) worden steeds complexer door digitalisering, verbondenheid van netwerken en automatisering. Hierdoor zijn effecten van verstoringen of uitval op voorhand niet goed te voorspellen. Bovendien is er sprake van een **dynamisch** systeem, waardoor afhankelijkheden tussen

fenomenen ook niet stabiel zijn. Maatschappelijke transities, zoals bijvoorbeeld de energietransitie, maar ook de snelheid waarmee technologische vernieuwingen worden geïmplementeerd, zorgen ervoor dat verbindingen en afhankelijkheden continu veranderen. Deze complexiteit van systemen of ketens maakt het moeilijk om 'diep' in systemen of ketens te kijken en de doorwerkeffecten van een enkel radartje in de systemen of ketens te doorgronden.

Hierbij is het ook belangrijk om er rekening mee te houden dat de Nederlandse maatschappij niet in een vacuüm functioneert maar in **een internationaal-economisch systeem**. Hierin hebben verschuivende verhoudingen en verschillende belangen een belangrijke invloed op de keuzevrijheid van Nederland als het gaat om het beschermen van de nationale veiligheidsbelangen.

Digitalisering is bijvoorbeeld belangrijk voor de economie en vooruitgang van de samenleving, maar zorgt ook voor **afhankelijkheden** van grote buitenlandse techbedrijven en internationale leverancierskетens. Hetzelfde geldt voor (economische) afhankelijkheid van specifieke producten of diensten, waarvoor geldt dat leverings- of productie-schokken in een mondiale waardeketen via doorwerkings-effecten elders onverwachte en onvoorspelbare uitkomsten kunnen hebben.

Vanuit internationaal politiek perspectief bezien speelt **globalisering** een essentiële rol. Door het proces van globalisering vervaagt de scheidslijn tussen interne en externe veiligheid steeds sneller, aangejaagd door technologische en digitale ontwikkelingen. Globalisering zorgt voor de mondiale spreiding van de connecties tussen mensen en zelfs voor het verdwijnen van obstakels in de stroom van goederen en diensten tussen landen (supra-territorialiteit). Met betrekking tot de nationale veiligheid geldt dat de nexus tussen interne en externe veiligheid niet alleen wordt gekenmerkt door het grensoverschrijdende karakter in strikte zin (intern versus extern), maar ook door het overstijgen van de traditionele grenzen tussen verschillende (beleids)sectoren en domeinen (justitie-, defensie-, economisch, financieel, industrieel, technologisch, politie-, sociaal, culturele, maatschappelijke, ecologische en politieke domeinen) (Drent, Pronk & Meijnders, 2020).

Tenslotte speelt de **politisering** van onderwerpen zoals het klimaat, gezondheid, en de economie een rol in de toenemende complexiteit van de samenleving. Rondom deze onderwerpen ontstaan politieke en maatschappelijke debatten waarbij steeds meer de tegenstellingen tussen verschillende belangen worden benadrukt. Hierbij wordt ook in toenemende mate het belang van veiligheid betrokken (*securitization*). Dit is merkbaar aan spanningen in samenleving rondom die onderwerpen, maar ook in de beleidsvorming met betrekking tot deze onderwerpen zoals de energietransitie of strategische autonomie.

14.3 Omgaan met complexiteit en onvoorspelbaarheid

Al deze kenmerken maken het dreigingslandschap divers en complex. Dit leidt tot een zekere mate van **onvoorspelbaarheid** van de gevolgen van een manifestatie van één of meerdere dreigingen. Dit geldt niet alleen op technisch vlak vanwege de verwevenheid en afhankelijkheid binnen en tussen (vitale) processen, maar bijvoorbeeld ook op economisch en internationaal politiek vlak vanwege het dynamische karakter, (wederzijdse) afhankelijkheden en de verbondenheid op allerlei terreinen. Zelfs wanneer we voor specifieke (combinaties van) fenomenen een goede inschatting kunnen maken van de denkbare gevolgen, blijft er een mate van onzekerheid vanwege de invloed van samenhangende ontwikkelingen en aanpalende gebeurtenissen.

Deze complexiteit en de daaruit voortkomende onvoorspelbaarheid vergen een andere manier van voorbereiding en het opbouwen van weerbaarheid. Zo vragen sluimerende dreigingen dat er wordt nagedacht over monitoring en signalering en is het belangrijk om het vermogen op te bouwen om adaptief te zijn om adequaat in te kunnen spelen op onverwachte gebeurtenissen.

Vanuit een bestuurlijke invalshoek bekeken moeten nationale veiligheidsvraagstukken als zogenoemde '***wicked problems***' worden gezien. Om dergelijke problemen aan te pakken, zijn meerdere actoren nodig. Daarnaast is coördinatie tussen die actoren noodzakelijk om overlap, duplicatie, lacunes en tegenwerking bij de ontwikkeling en uitvoering van beleid te voorkomen en samenhang te bereiken. Dit betekent onder andere dat bestuurlijke coördinatie nodig is voor de samenwerking en samenhang van de diverse overheidsorganisaties. Aangezien de veiligheidsvraagstukken veelal multi-sectoraal zijn geworden, zal een succesvolle voorkoming, afschrikking en bestrijding vaak ook multi-sectoraal moeten worden aangepakt. Het zal daarom niet alleen op een '*whole-of-government*' manier moeten worden vormgegeven, maar veeleer op een '*whole-of-society*' manier. Daarbij is het belangrijk om aandacht te geven aan de verschillende belangen en spanningen in de samenleving rondom de vraagstukken die een rol spelen bij nationale veiligheid (en daarbuiten). De veiligheidsbeleving onder verschillende segmenten van de samenleving kan sterk verschillen, waarbij ook andere belangen dan veiligheid een grote rol spelen. Dit vraagt om sensitiviteit bij de aanpak van dreigingen.

DEEL 3: Slotbeschouwing

Hoe kunnen de resultaten van de Rijksbrede risicoanalyse worden gebruikt voor het formuleren van onderbouwde beleidskeuzes?

15. Slotbeschouwing

Deze Rijksbrede Risicoanalyse nationale veiligheid biedt de mogelijkheid om de verschillende dreigingen die onze samenleving kunnen ontwrichten in vergelijkend perspectief te plaatsen. De hieruit voortkomende inzichten kunnen assisteren bij het toekennen van prioriteiten in onder andere de Rijksbrede Veiligheidsstrategie. Daarnaast geven de themarapportages inzicht in de relevante ontwikkelingen, risico's en sluimerende dreigingen op themaniveau. Deze inzichten kunnen op hun beurt gebruikt worden om in te schatten of we als samenleving afdoende weerbaar zijn tegen de dreigingen in kwestie of dat er verbeteringen nodig zijn, bijvoorbeeld via versterking van de crisisbeheersing. De themarapportages geven een schat van informatie waarop verder gebouwd kan worden om de veiligheid binnen ons Koninkrijk te versterken.

Vanwege de omvang van deze risicoanalyse en het aantal scenario's dat is beoordeeld, is het goed denkbaar dat het lastig is om te bepalen hoe hiermee verder te gaan. Dat zou zonde zijn, omdat de risicoanalyse juist bedoeld is voor het maken van onderbouwde beleidskeuzen. Bij de duiding van de scenario's in het risicodiagram (hoofdstuk 13) zijn daarom enkele perspectieven waarmee naar het diagram gekeken kan worden meegegeven. Die kunnen ook ondersteunen bij het vervolg:

- Voor de dreigingen die tot de grootste impact op de nationale veiligheid kunnen leiden ligt het voor de hand om de kans op voorkomen te minimaliseren. Daarbij is het uiteraard de vraag wat in onze eigen macht ligt om die kans zo klein mogelijk te maken of te houden en of extra investeringen wel in relatie staan tot de gerealiseerde veiligheidswinst.
- Voor het stellen van prioriteiten vanuit het risicoperspectief kunnen de dreigingen met een relatief *grote impact én hoge waarschijnlijkheid* worden gebruikt. Verdere analyse van de betreffende dreigingen kan inzicht geven of reductie van het risico eerder aan de kant van de waarschijnlijkheid of van de impact gezocht dient te worden.
- Door in te zoomen op de specifieke gevolgen van een bepaalde dreiging kan een weerbaarheidsanalyse worden geconcretiseerd en kunnen de resultaten gebruikt worden voor de versterking van de crisisbeheersing. Bij sommige dreigingen zal bijvoorbeeld het aantal slachtoffers groot kunnen zijn, waarbij de vraag kan worden gesteld of daar de benodigde hulp voor beschikbaar is dan wel hoe die beschikbaar gemaakt kan worden. Op deze manier kan een directe koppeling tussen risicoanalyse en weerbaarheidsinschatting worden gemaakt.
- Bij de dreigingen met een hoge waarschijnlijkheid lijkt het zinnig om daar als samenleving op voorbereid te zijn en na te gaan of de weerbaarheid op orde is. Denk bijvoorbeeld aan natuurbranden, aanslagen door een alleenhandelende dader of de nevenschade als gevolg van een cyberaanval.

Naast de mogelijkheid om vanuit deze risicoanalyse in te zoomen op specifieke risico's volgt uit de analyse de grote mate van onderlinge verbondenheid en verwevenheid tussen de verschillende risico's waar rekening mee moet worden gehouden. Denk hierbij aan de verwevenheid en afhankelijkheden tussen vitale processen en digitalisering en tussen economische en internationale ontwikkelingen. In aanvulling daarop zijn er in de analyse enkele overkoepelende onderwerpen naar voren gekomen, te weten klimaatverandering, energietransitie, spanningen in de samenleving en hybride dreigingen, waarbij verschillende ontwikkelingen samenkomen. De overkoepelende onderwerpen kunnen integraal geanalyseerd worden vanuit het perspectief van de weerbaarheid en crisisbeheersing.

De constateringen van onderlinge verbondenheid en afhankelijkheden kunnen leiden tot een zeker mate van onvoorspelbaarheid van gevolgen als een risico zich manifesteert. Dit vraagt een meer integrale benadering, waarbij in het vorige hoofdstuk het perspectief om dergelijke vraagstukken als complex systeem te benaderen kort is beschreven.

Binnen de RbRa is een groot aantal dreigingen en de bijbehorende risico's beschouwd. Waar voor sommige van deze dreigingen geldt dat deze al geruime tijd niet zijn voorgekomen in het Koninkrijk der Nederlanden of in de toekomst als (zeer) onwaarschijnlijk worden gezien, zijn anderen reeds werkelijkheid geworden of is de inschatting dat het waarschijnlijk is dat we hier als samenleving de

komende jaren (wederom) mee zullen worden geconfronteerd. Het in de RbRa geschetste dreigingsbeeld is nadrukkelijk niet statisch van aard, maar is onderhevig aan onder andere maatschappelijke, internationale en technologische ontwikkelingen. Het is van belang om als samenleving goed op de hoogte te zijn en te blijven van het set aan dreigingen dat de nationale veiligheid kan aantasten, onder meer door het uitvoeren van periodieke analyses zoals die in de RbRa. Aan de hand hiervan ontstaan handvaten voor het creëren van een weerbaar Koninkrijk der Nederlanden.

Nawoord

Het ANV is zich er terdege van bewust dat de huidige gebeurtenissen op het internationale toneel, en in het bijzonder de oorlog in Oekraïne, zich razendsnel ontwikkelen. Het is van belang om te beseffen dat de scenario's zoals weergegeven in dit hoofdrapport en de achterliggende themarapportages zijn ontwikkeld en getoetst nog voor de Russische inval in Oekraïne. Binnen het ANV wordt er dan ook naar gestreefd om in de risicoanalyse, maar ook in de onderliggende themarapportages, een goede balans te vinden tussen representatieve toekomstscenario's en scenario's die voldoende onderbouwing vinden in de actualiteit. Echter, het is een gegeven dat zodra de meest recente actualia worden meegenomen in de analyse, het risico bestaat dat op korte termijn die gebeurtenissen alweer achterhaald zijn. Daarom is er door het ANV gepoogd om scenario's op te stellen die zo toekomstbestendig mogelijk zijn.

Dit neemt echter niet weg dat de oorlog in Oekraïne een impact heeft op de analyse en, specifiek, op de waarschijnlijkheid van enkele van de in de RbRa beschouwde scenario's. Dit betreft bijvoorbeeld een aantal scenario's uit het thema 'internationale en militaire dreigingen', zoals het ontstaan van een tweespalt in de Europese Unie rondom de te varen beleidskoers (ten aanzien van Rusland), het uiteenspatten van de OVSE (nu Rusland is weggelopen bij de OVSE manifesteert dit scenario zich al) of een tijdelijke bezetting van een EU-lidstaat (na lidmaatschapsaanvraag van Finland en Zweden neemt het risico hierop toe). Ook op enkele dreigingen die worden beschouwd binnen het thema economische dreigingen worden mogelijk actueler, met name op het gebied van strategische afhankelijkheden betreffende grondstoffen als olie en gas.

Met het oog op de zuiverheid van de methodiek is er voor gekozen om scenario's inhoudelijk niet aan te passen of te updaten op basis van de actualiteit. Dit zou namelijk vereisen dat de scenario's opnieuw gevalideerd moeten worden door experts en vervolgens in nieuwe expertsessies gescoord moeten worden op hun waarschijnlijkheid en impact. Wat het ANV betreft is de uitgevoerde analyse voldoende robuust om de resultaten te gebruiken voor weerbaarheidsinschattingen en als input voor de Rijksbrede Veiligheidsstrategie.

Referenties

Analistennetwerk nationale veiligheid (ANV). (2016). Nationaal Veiligheidsprofiel 2016. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2019). Geïntegreerde Risicoanalyse Nationale Veiligheid 2019. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2019). Verkenning risico's van de energietransitie voor de nationale veiligheid. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2020). Horizonscan Nationale Veiligheid 2020. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk Nationale veiligheid (ANV). (2022a). Leidraad risicobeoordeling. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2022b). Rijksbrede Risicoanalyse Themarapportage Infectieziekten. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2022c). Rijksbrede Risicoanalyse Themarapportage Klimaat- & Natuurrampen. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2022d). Rijksbrede Risicoanalyse Themarapportage Bedreiging Vitale Infrastructuur. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2022e). Rijksbrede Risicoanalyse Themarapportage Cyberdreigingen. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2022f). Rijksbrede Risicoanalyse Themarapportage Zware Ongevallen. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2022g). Rijksbrede Risicoanalyse Themarapportage Polarisatie, Extremisme en Terrorisme. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2022h). Rijksbrede Risicoanalyse Themarapportage Ongewenste Inmenging en Beïnvloeding Democratische Rechtsstaat. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2022i). Rijksbrede Risicoanalyse Themarapportage Internationale en Militaire Dreigingen. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2022j). Rijksbrede Risicoanalyse Themarapportage Economische Dreigingen. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Analistennetwerk nationale veiligheid (ANV). (2022k). Rijksbrede Risicoanalyse Caribisch deel van het Koninkrijk der Nederlanden. Via: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Drent, M., Pronk, D. en Meijnders, M. (2020) Verbondenheid in veiligheid. *De contouren van een onderzoeksagenda voor drie ministeries*. Clingendael Rapport. Den Haag, Instituut Clingendael.

De referenties behorende tot de verschillende themahoofdstukken zijn opgenomen in de bijbehorende themarapporten.

Bijlage 1. Het Analistennetwerk Nationale Veiligheid

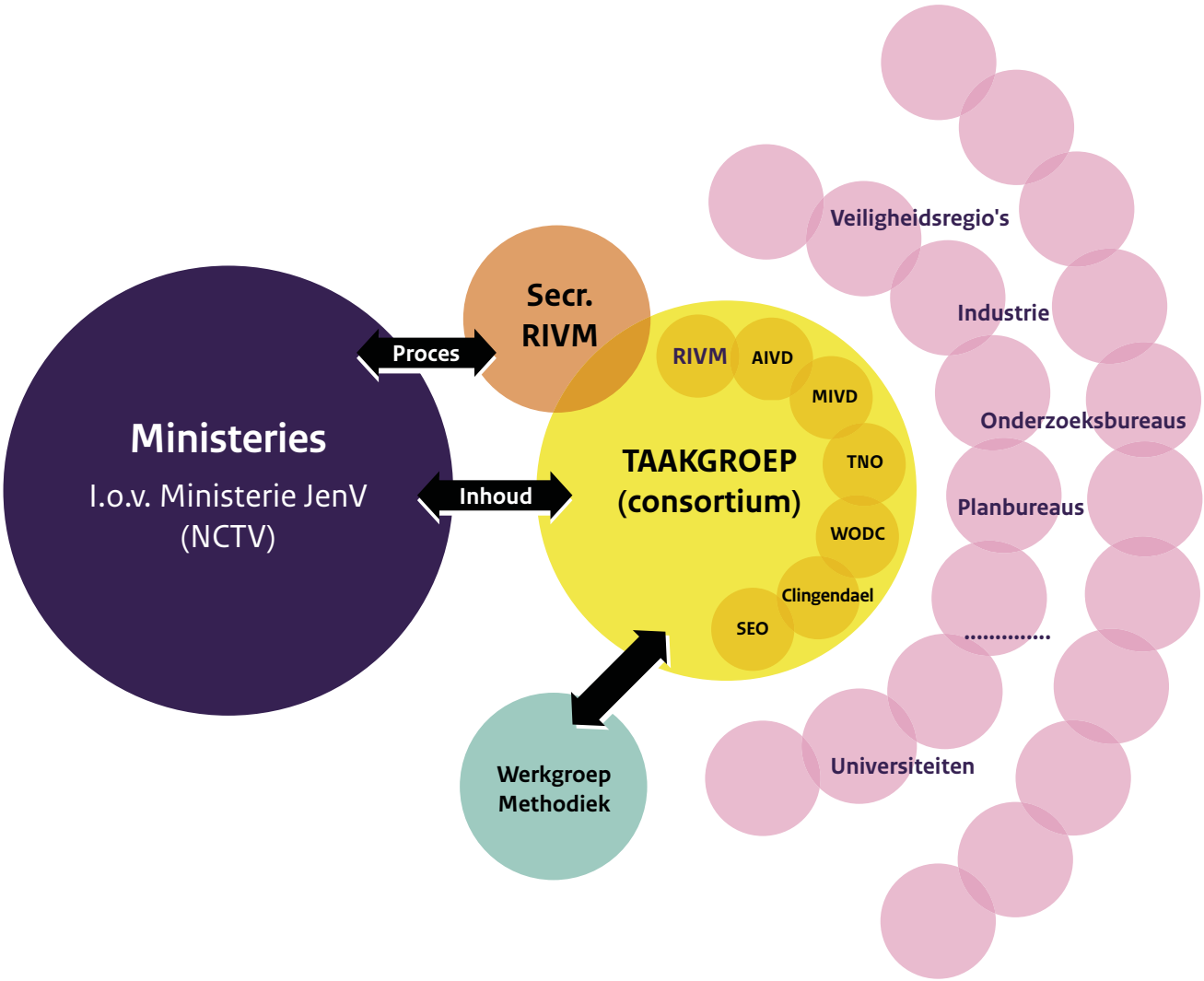
Het Analistennetwerk Nationale Veiligheid (ANV) is een kennisnetwerk dat in 2010 is opgericht. Sindsdien heeft het ANV periodiek een nationale risicoanalyse opgesteld en andere verdiepende analysestudies op het gebied van nationale veiligheid verricht. Dit in opdracht van het ministerie van Veiligheid en Justitie namens de toenmalige Stuurgroep Nationale Veiligheid (SNV). In 2016 heeft het ANV het Nationaal Veiligheidsprofiel (NVP) opgesteld en in 2019 de Geïntegreerde Risicoanalyse Nationale Veiligheid (GRA).

Het ANV bestaat uit een vaste kern van zeven organisaties met daaromheen een netwerk (de 'ring') van organisaties zoals kennisinstellingen, overheidsdiensten, veiligheidsregio's, (vitale) bedrijven en onderzoeksbureaus die afhankelijk van de kennisvraag worden ingeschakeld bij het uitvoeren van analyses en verdiepende studies. De vaste kern wordt gevormd door:

- Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
- De Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO
- De Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael'
- SEO Economisch Onderzoek
- Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
- Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
- Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Deze organisaties beschikken over brede, multidisciplinaire expertise en bestrijken gezamenlijk het werkveld van de Nationale Veiligheid. Op deze wijze is de *All Hazard benadering* gegarandeerd en is de eenheid in methodologie en overkoepelende analyses geborgd. Voor het bewaken en verder ontwikkelen van de door het ANV gehanteerde methodologie, is er een werkgroep methodiek opgericht. De zeven instellingen in de kern, verenigd in de Taakgroep, dragen gezamenlijk de verantwoordelijkheid voor de inhoudelijke kwaliteit van de producten van het ANV. Specifieke, aanvullende expertise wordt geleverd door de andere organisaties in het netwerk. De organisaties in de kern en de ring stellen experts en analisten ter beschikking, die in (in samenstelling steeds wisselende) werkgroepen inhoudelijke activiteiten uitvoeren. Een ondersteunend secretariaat (het ANV secretariaat) bestaande uit een algemeen secretaris en projectondersteuning, draagt zorg voor de processturing, voortgangsbewaking en ondersteuning van het tot stand brengen van de producten. Het ANV secretariaat is het vaste aanspreekpunt voor de opdrachtgever en is gevestigd bij het RIVM.
De organisatiestructuur van het Analistennetwerk Nationale Veiligheid is schematisch weergegeven in de volgende figuur.

Figuur B1 Netwerkstructuur ANV



Bijlage 2. Werkwijze en methodische verantwoording

Deze bijlage bevat een toelichting op de werkwijze die is gebruikt voor deze risicoanalyse, waarbij tevens enkele aspecten van de methodiek op hoofdlijnen worden besproken.

2.1 Risico en dreiging

Deze risicoanalyse geeft een overzicht van dreigingen die onze samenleving kunnen ontwrichten en de bijbehorende risico's. Daarbij gaat het dus zowel om dreigingen als risico's. Voor beide begrippen bestaan verschillende definities, vandaar dat we kort stilstaan bij wat in deze analyse onder beide begrippen wordt verstaan. Een *dreiging* is "een aantoonbare ontwikkeling, gebeurtenis of fenomeen dat veiligheid of stabiliteit kan schaden." Een *risico* daarentegen is het samenspel van impact (het totaal van de gevolgen van een bepaalde dreiging) en de waarschijnlijkheid (de verwachting over het manifesteren van een dreiging). In het kort komt het erop neer dat in deze analyse dreigingen inzichtelijk worden gemaakt in de vorm van risico's.

Er vindt in deze risicoanalyse geen inschatting plaats van de weerbaarheid tegen de beschouwede dreigingen.[17]

2.2 Scenario's

Om het risico behorende tot een dreiging inzichtelijk te maken, wordt gebruik gemaakt van scenario's. Voor elk binnen de RbRa beschouwde type dreiging zijn één of meerdere scenario's (korte verhaallijnen of narratieven) opgesteld die vervolgens zijn beoordeeld op de impact op de nationale veiligheid en de waarschijnlijkheid van optreden. Zo wordt de meer abstracte dreiging die uitgaat van bijvoorbeeld terrorisme uitgewerkt in meerdere scenario's die onder andere ingaan op een relatief kleinschalige aanslag van een alleenhandelende dader en een grootschalige aanslag op meerdere locaties met gebruik van explosieven en vuurwapens.

De scenario's geven een concreet beeld van een bepaald type dreiging en bijbehorend risico. Ze zijn als het ware de illustratie hiervan en laten zien wat de mogelijke gevolgen kunnen zijn. Het streven is niet om volledig te zijn en alle mogelijke uitingen van een dreiging af te dekken met een scenario, maar nadrukkelijk om een dreigingsfenomeen en risico te illustreren.

2.3 Methodiek nationale veiligheid

Voor het beoordelen van de scenario's en het inschatten van zowel gevolgen als waarschijnlijkheid, maakt het ANV gebruik van de methodiek nationale veiligheid. Binnen deze methodiek wordt gekeken of en in welke mate een bepaalde gebeurtenis de zes nationale veiligheidsbelangen raakt. De nationale veiligheid is in het geding als één of meer van de zes nationale veiligheidsbelangen zodanig worden bedreigd dat er sprake is van (potentiële) maatschappelijke ontwrichting (ANV, 2022a). De zes belangen zijn elk opgesplitst in één of meerdere meetbare impactcriteria die helpen bij het in kaart brengen van een mogelijke aantasting. Onderstaande tabel geeft een kort overzicht van alle belangen en criteria. Een uitgebreide uitleg voor elk van deze onderdelen bevindt zich in de door het ANV opgestelde leidraad risicobeoordeling (ANV, 2022a).

[17] In de analyse wordt impliciet uitgegaan van de status quo wat betreft de weerbaarheid. Daar waar door experts opmerkingen zijn geplaats met betrekking tot de weerbaarheid zijn deze opgenomen als aanvullende informatie. Een specifieke weerbaarheidsanalyse ligt echter buiten de scope van deze risicoanalyse en zal mogelijk een plek krijgen in een vervolg.

Tabel 2 Belangen en impactcriteria behorende toe de methodiek nationale veiligheid

Belang	Impactcriteria
1. Territoriale veiligheid	1.1 Aantasting van de integriteit van het grondgebied van het Koninkrijk der Nederlanden
	1.2 Aantasting van de integriteit van de internationale positie van het Koninkrijk der Nederlanden
	1.3 Aantasting van de integriteit van de digitale ruimte
	1.4 Aantasting van de integriteit van het bondgenootschappelijk grondgebied
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 economie van het Koninkrijk der Nederlanden
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 en stabiliteit	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
	6.5 Instabiliteit van staten grenzend aan het Koninkrijk der Nederlanden en in de directe omgeving van de Europese Unie

Voor het geven van een oordeel over de precieze omvang van de gevolgen van een scenario, wordt aan elk van de criteria een impactscore toegekend, namelijk: niet van toepassing, beperkt (A), aanzienlijk (B), ernstig (C), zeer ernstig (D) of catastrofaal (E). Deze classificering is gebaseerd op een logaritmische schaal. Voor criterium 2.1 (aantal doden) betekent dit bijvoorbeeld dat een beperkte score staat voor 0-10 doden, een aanzienlijke score voor 10-100 doden, et cetera. Eenzelfde redenatie wordt gehanteerd voor criterium 3.1 (kosten). Er is sprake van maatschappelijke ontwrichting als één of meer van de belangen ernstig (klasse C) of hoger wordt aangetast.

Tabel 3 Voorbeeld van verschillende klassen van gevolg binnen de methodiek nationale veiligheid

Klasse van gevolgen	Voorbeeld criterium: Aantal doden (2.1)	Voorbeeld criterium: kosten (3.1)
A. Beperkt	Minder dan 10	< 50 miljoen euro
B. Aanzienlijk	10 tot 100	< 500 miljoen euro
C. Ernstig	100 tot 1000	< 5 miljard euro
D. Zeer ernstig	1000 tot 10.000	< 50 miljard euro
E. Catastrofaal	Meer dan 10.000	> 50 miljard euro

In tegenstelling tot de bovenstaande criteria 2.1 en 3.1, zijn sommige criteria niet uit te drukken in een absoluut aantal. Een voorbeeld hiervan is criterium 5.2, aantasting van de democratische rechtsstaat. Hier wordt de uiteindelijke score berekend door te kijken of, in welke mate en voor hoe lang verschillende onderdelen van de democratische rechtsstaat worden aangetast. Deze onderdelen zijn:

- Het functioneren van de politieke vertegenwoordiging;
- Het functioneren van het openbaar bestuur en daaraan verbonden ambtenaren;
- Het functioneren van het openbare orde en veiligheidssysteem;
- Het functioneren van een onafhankelijke rechtspraak;
- Vrijheden en rechten zoals vastgelegd in grondwet en wetgeving (vrijheid van godsdienst, meningsuiting, vereniging, kiesrecht, etc.).

Naarmate de aantasting groter is, voor meerdere onderdelen van toepassing blijkt en langer duurt, neemt de score toe.

Binnen de methodiek wordt niet alleen gekeken naar de gevolgen van gebeurtenissen, maar ook naar de waarschijnlijkheid van voorkomen. Voor het bepalen van de waarschijnlijkheid, wordt gekeken naar de kans van voorkomen binnen het moment van analyse (eerste kwartaal 2022) en vijf jaar. Deze kans wordt afhankelijk van het type gebeurtenis kwalitatief of kwantitatief weergegeven op een vijfpuntschaal van zeer onwaarschijnlijk tot zeer waarschijnlijk. Voor het bepalen van de gevolgen en waarschijnlijkheid van een scenario, wordt gebruik gemaakt van *expert judgement.*

Tabel 4 Waarschijnlijkheidsinschatting binnen de methodiek nationale veiligheid

Klasse van waarschijnlijkheid	Kwalitatieve omschrijving van de dreiging	Kwantitatieve benadering (% per 5 jaar)
A. Zeer onwaarschijnlijk	Geen concrete aanwijzingen en het scenario wordt niet voorstelbaar geacht	<0,05 %
B. Onwaarschijnlijk	Geen concrete aanwijzingen, maar het scenario wordt enigszins voorstelbaar geacht	0,05 - 0,5 %
C. Enigszins waarschijnlijk	Geen concrete aanwijzingen, maar het scenario is voorstelbaar	0,5 – 5 %
D. Waarschijnlijk	Het scenario wordt zeer voorstelbaar geacht; er zijn enige aanwijzingen dat het scenario zich daadwerkelijk zal voordoen,	5 – 50 %
E. Zeer waarschijnlijk	Concrete aanwijzingen dat het scenario geëffectueerd zou kunnen worden	50 – 100 %

2.4 Bouwstenen, sluimerende dreigingen en wild cards

Om te assisteren bij het identificeren en uitwerken van de scenario's is gebruik gemaakt van 'bouwstenen'. Bouwstenen zijn een overzicht van de voor een dreigingscategorie relevante factoren en actoren. Door de factoren en actoren te combineren kunnen meerdere situaties ofwel scenario's worden gecreëerd. Uiteraard zullen verschillende combinaties leiden tot verschillende scenario's met wisselende uitkomsten. De bouwstenen helpen om in één oogopslag duidelijk te maken wat wel en wat niet is meegenomen in het scenario en dienen als referentiekader voor de uiteindelijke verhaallijn.

Naast de op bouwstenen gebaseerde (reguliere) scenario's, worden er ook sluimerende dreigingen en wild cards beschouwd. Sluimerende dreigingen zijn dreigingen die niet direct van grote impact op de nationale veiligheid zijn, maar die op de **lange termijn** (10 tot 20 jaar) wel degelijk kunnen zorgen voor aanzienlijke impact op de nationale veiligheid. Het gaat hierbij enerzijds om lange termijn ontwikkelingen die gaandeweg tot problematische situaties kunnen leiden en anderzijds om een reeks relatief kleine gebeurtenissen die individueel niet van grote betekenis lijken te zijn, maar waarbij de optelsom over een langere tijd wel degelijk een ernstig gevolg heeft voor de nationale veiligheid.

Kenmerkend van sluimerende dreigingen is dat er vaak een kantelpunt optreedt waarna het heel moeilijk is om de problemen tegen te gaan. In veel gevallen kan hierbij achteraf worden herleid dat er iets is opgetreden dat onomkeerbaar is gebleken en voor problemen zorgt. Dergelijke risico's kunnen zich gestaag onder de radar opbouwen.

Wild cards zijn minder voor de hand liggende scenario's die ingaan op fenomenen die weliswaar denkbaar zijn maar toch minder voorstelbaar. Er is vaak nog een hoge mate van onzekerheid over de gevolgen van dit type gebeurtenissen, maar er wordt doorgaans wel verwacht dat het tot hoge impact kan leiden als het zich voordoet.

De sluimerende dreigingen en wild cards zijn alleen kwalitatief uitgewerkt en zijn aanvullend op de reguliere scenario's. Ook hierbij geldt dat ze niet uitputtend zijn, maar als verdere illustratie dienen.

2.5 Inventarisatie en selectie dreigingsthema's

Elk van de binnen de RbRa uitgewerkte scenario's kan worden geplaatst binnen een specifieke dreigingscategorie, welke op zijn beurt onderdeel is van een breder dreigingsthema. Zo bestaat het dreigingsthema klimaat- en natuurrampen onder andere uit de dreigingscategorieën extreem weer en overstromingen. Binnen de dreigingscategorie overstromingen zijn dan weer verschillende scenario's opgenomen ter illustratie van deze specifieke dreiging. Voor de risicoanalyse is een 'all hazard' benadering gehanteerd, waarbij naast safety én security ook interne én externe dreigingen zijn beschouwd.
De selectie van de dreigingen is gedaan op basis van een deskstudie van bestaande analyseproducten en input van experts uit het bredere netwerk van het ANV. Ook is gekeken welke rampen en crises in de afgelopen tijd zijn opgetreden en wat dat betekent voor deze risicoanalyse.

De verschillende dreigingen die zijn geselecteerd zijn ingedeeld in dreigingsthema's die verder zijn onderverdeeld in categorieën. Onderstaande tabel geeft hiervan het overzicht.

Tabel 5 Overzicht dreigingsthema en categorieën

Dreigingsthema	Categorie
Infectieziekten	Humane Infectieziekten en zoönosen
	Dierziekten en plantenziekten
Klimaat- & natuurrampen	Extreem weer
	Overstroming
	Natuurbrand
	Aardbeving
Bedreiging vitale infrastructuur	Moedwillige bedreiging vitale processen
	Verstoring vitale processen a.g.v. technisch of menselijk falen
	Natuurlijke verstoring vitale processen
Cyberdreigingen	Verstoring functioneren internet
	Verstoring cyber-fysieke systemen
	Cybercrime
Zware ongevallen	Stralingsongevallen
	Chemische ongevallen
	Transportongevallen
Polarisatie, extremisme en terrorisme	Maatschappelijke polarisatie
	Niet-gewelddadig extremisme
	Gewelddadig extremisme
	Terrorisme
Ongewenste inmenging en beïnvloeding democratische rechtsstaat	Spionage
	Ongewenste buitenlandse inmenging
	Ongewenste buitenlandse beïnvloeding (hybride operaties)
	Georganiseerde criminaliteit
Internationale en militaire dreigingen	Multilaterale veiligheidsinstituties onder druk
	Fragiliteit nabij het Koninkrijk en/of de EU
	Gewapend conflict tussen de machtsblokken
	Proliferatie van massavernietigingswapens
Economische dreigingen	Bedreigingen van de knooppuntfunctie van Nederland
	Buitenlandse inmenging bij het bedrijfsleven
	Handelskrimp/verstoring internationale handel
	Ongewenste strategische afhankelijkheden
	Destabilisatie financieel systeem

De resultaten van de analyse zijn per thema beschreven in de verschillende themarapportages. Binnen deze rapportages zijn onder andere de scores van de scenario's voor elk impactcriterium en de waarschijnlijkheid weergegeven in tabelvorm.

Rijksoverheid

Analistennetwerk Nationale Veiligheid

Dit is een uitgave van:

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)
Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael' (Clingendael)
SEO Economisch Onderzoek (SEO)
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Juli 2022

013966