



# Horizonscan *Nationale Veiligheid* 2020

Analistennetwerk Nationale Veiligheid



# Horizonscan Nationale Veiligheid 2020

**Analistennetwerk Nationale Veiligheid**

*Oktober 2020*



## Colofon

De Horizonscan Nationale Veiligheid 2020 is gemaakt door het Analistennetwerk Nationale Veiligheid in opdracht van de NCTV van het Ministerie van Justitie en Veiligheid.

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)  
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)  
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)  
Nederlandse Organisatie voor toegepast-natuur-wetenschappelijk onderzoek (TNO)  
Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael'  
Erasmus Universiteit Rotterdam, Institute of Social Studies (ISS)

© RIVM 2020

Uit deze publicatie mogen worden overgenomen op voorwaarde van bronvermelding.  
Analistennetwerk Nationale Veiligheid (ANV), Horizonscan Nationale Veiligheid 2020, 2020.

# Inhoudsopgave

<b>1. Inleiding</b>	<b>9</b>
1.1 Doel	9
1.2 Team en proces	9
1.3 COVID-19	10
1.4 Opzet en opbouw rapport	10
<b>2. Methodiek</b>	<b>11</b>
2.1 Scan	12
2.2 Koppeling	13
2.3 Duiding	13
<b>3. Internationale economie</b>	<b>15</b>
3.1 Politisering van de internationale markteconomie	15
3.2 Digitalisering van de economie	16
3.3 Klimaattransitie	17
3.4 Koppeling met risicocategorieën	17
<b>4. Internationale politiek</b>	<b>19</b>
4.1 Tanende multilaterale wereldorde	19
4.2 Instabiliteit brede randen van Europa	20
4.3 Polarisatie binnen de Europese samenlevingen	21
4.4 Koppeling met de risicocategorieën	21
<b>5. Demografisch-maatschappelijk</b>	<b>25</b>
5.1 Groeiende ongelijkheid en tegenstellingen tussen bevolkingsgroepen	25
5.2 Gevolgen van toenemende diversiteit in de samenleving	26
5.3 Fluctuering van mate van vertrouwen in samenleving, politiek en autoriteiten	28
5.4 Koppeling met de risicocategorieën	28
<b>6. Ecologie</b>	<b>31</b>
6.1 Klimaatverandering	31
6.2 Biodiversiteit	32
6.3 Milieudruk	32
6.4 Koppeling met de risicocategorieën	33
<b>7. Informatietechnologie</b>	<b>35</b>
7.1 Autonomie	35
7.2 Cognitie	36
7.3 Vernetting	36
7.4 Afhankelijkheid	36
7.5 Nadere uitwerking van enkele manifestaties	37
7.6 Koppeling trends en risicocategorieën	39



<b>8. COVID-19</b>	<b>41</b>
8.1 Economie	41
8.2 Internationaal	42
8.3 Maatschappelijk	43
8.4 Ecologie	43
8.5 Informatietechnologie	43
8.6 Koppeling met risicocategorieën	44
<b>9. Overzicht van de koppeling met de risicocategorieën</b>	<b>47</b>
<b>10. Resultaten en conclusie</b>	<b>53</b>
10.1 Overzicht van de resultaten van de scan	53
10.2 Koppeling met risicocategorieën	54
10.3 Vergelijking met de resultaten uit de GRA 2019 en de NVS 2019	55
<b>Bijlage 1. Bronnenlijst</b>	<b>59</b>
<b>Bijlage 2. Overzicht van dreigingsthema's en risicocategorieën</b>	<b>60</b>



# 1. Inleiding

In zowel 2018 als 2019 heeft het Analistennetwerk Nationale Veiligheid (ANV) een Horizonscan Nationale Veiligheid uitgebracht. Het doel van deze horizonscans is om periodiek een verkenning uit te voeren naar trends en ontwikkelingen die mogelijk relevant zijn voor de Nederlandse nationale veiligheid. Voor u ligt de nieuwste editie van de Horizonscan: de Horizonscan Nationale Veiligheid 2020.

## 1.1 Doel

De Horizonscan 2020 bouwt voort op de scans uit 2018 en 2019. Net als bij voorgaande edities bevat de Horizonscan 2020 een verkenning van trends en ontwikkelingen die mogelijk relevant zijn voor de nationale veiligheid. Voor het

ordenen en stroomlijnen van de Horizonscan, wordt deze verkenning aangevlogen vanuit vijf overkoepelende categorieën van 'autonome' ontwikkelingen: internationale economie, internationale politiek, demografisch-maatschappelijke ontwikkelingen, ecologie en informatietechnologie. Meer hierover in hoofdstuk twee.

Naast het in kaart brengen van trends en ontwikkelingen, heeft de Horizonscan 2020 nog een tweede functie waarmee het product zich onderscheidt van eerdere edities. Binnen deze scan worden de ontwikkelingen niet alleen in kaart gebracht, maar worden ze ook gekoppeld aan de risico's waar zij mogelijk invloed op hebben. Het gaat hier om risico's die de Nederlandse nationale veiligheid kunnen raken, zoals beschreven in de Geïntegreerde Risicoanalyse 2019 (GRA 2019, zie tekstkader).

### Geïntegreerde Risicoanalyse

Het ANV stelt periodiek een Geïntegreerde Risicoanalyse (GRA) op. Binnen de GRA worden een groot aantal verschillende scenario's (mogelijke gebeurtenissen) geanalyseerd op het gebied van gevolgen en waarschijnlijkheid. De scenario's zijn verdeeld over 9 uiteenlopende thema's zoals natuurrampen en bedreigingen voor de internationale vrede en veiligheid. Elk thema bestaat op zijn beurt uit enkele risicocategorieën waarbinnen de verschillende scenario's een plek hebben. Zo bestaat het thema natuurrampen uit de risicocategorieën extreem weer, natuurbrand, overstroming en aardbeving. De meest recente GRA is uitgebracht in 2019 (GRA 2019).

De Horizonscan 2020 kijkt dus niet alleen naar de ontwikkelingen die zich hebben voorgedaan sinds de Horizonscan 2019, maar ook naar hoe deze ontwikkelingen zich verhouden tot de (eigenschappen van de) risico's uit de GRA 2019. De reden voor het maken van deze koppeling is dat de Horizonscan 2020 dient als input voor een geplande 'mid-term' review van de in juni 2019 aangeboden Nationale Veiligheid Strategie (NVS 2019). Een belangrijke vraag bij deze review van de strategie is of er sinds het opstellen van de Geïntegreerde risicoanalyse Nationale Veiligheid 2019 (GRA 2019) nieuwe risico's en dreigingen naar voren zijn gekomen, dan wel bestaande risico's en dreigingen aan verandering onderhevig zijn geweest. De uiteindelijke actualisatie van de risico's zelf valt buiten de

scope van deze Horizonscan, maar zal worden uitgevoerd in een nieuwe risicoanalyse (voorzien voor 2021).

## 1.2 Team en proces

De Horizonscan 2020 is een product van het ANV. Voor het opstellen van het product is in de basis gebruikgemaakt van dezelfde horizonscanmethodiek als bij de voorgaande edities. Bij de uitwerking zijn wel aanpassingen gedaan (zie hoofdstuk 2). In toevoeging hierop is gewerkt aan een methode voor het koppelen van trends en ontwikkelingen aan veranderingen in de eigenschappen van een risico of het ontstaan van nieuwe varianten.



Vijf organisaties hebben gezamenlijk de Horizonscan uitgevoerd: Instituut Clingendael, SEO Economisch Onderzoek, het RIVM, TNO en het Verwey-Jonker Instituut. Elke organisatie heeft zich gericht op één van de in deze Horizonscan opgenomen autonome ontwikkelingen. Voor de koppeling van de trends en ontwikkelingen met de risico's uit de GRA 2019 zijn vervolgens alle vijf de organisaties betrokken geweest, samen met de methodici van het ANV. In tegenstelling tot eerdere edities, zijn er voor de Horizonscan 2020 geen sessies georganiseerd met externe deskundigen. Dit onder andere vanwege de COVID-19-crisis.

### 1.3 COVID-19

Zoals gemeld heeft de Horizonscan 2020 als focus de mogelijke beïnvloeding van de risico's uit de GRA 2019 door trends en ontwikkelingen. COVID-19 is een bepalende gebeurtenis die vanwege de reikwijdte van het virus en van de getroffen maatregelen structurele gevolgen heeft voor de nationale veiligheid. Hoofdstuk 8 gaat daarom apart in op de effecten van de COVID-19-crisis binnen de scope van deze Horizonscan.

### 1.4 Opzet en opbouw rapport

Het volgende hoofdstuk beschrijft de methodologische verantwoording van deze Horizonscan (hoofdstuk 2). Naast de wijze waarop de scan wordt uitgevoerd, is beschreven hoe de koppeling met de risico's uit de GRA 2019 gestalte krijgt.

Vervolgens bevatten de hoofdstukken 3 tot en met 7 de resultaten van de scan aan de hand van de vijf autonome ontwikkelingen: internationale economie, internationale politiek, demografisch-maatschappelijke ontwikkelingen, ecologie en informatietechnologie. Hoofdstuk 8 gaat in op de effecten van de COVID-19-crisis binnen de scope van deze Horizonscan.

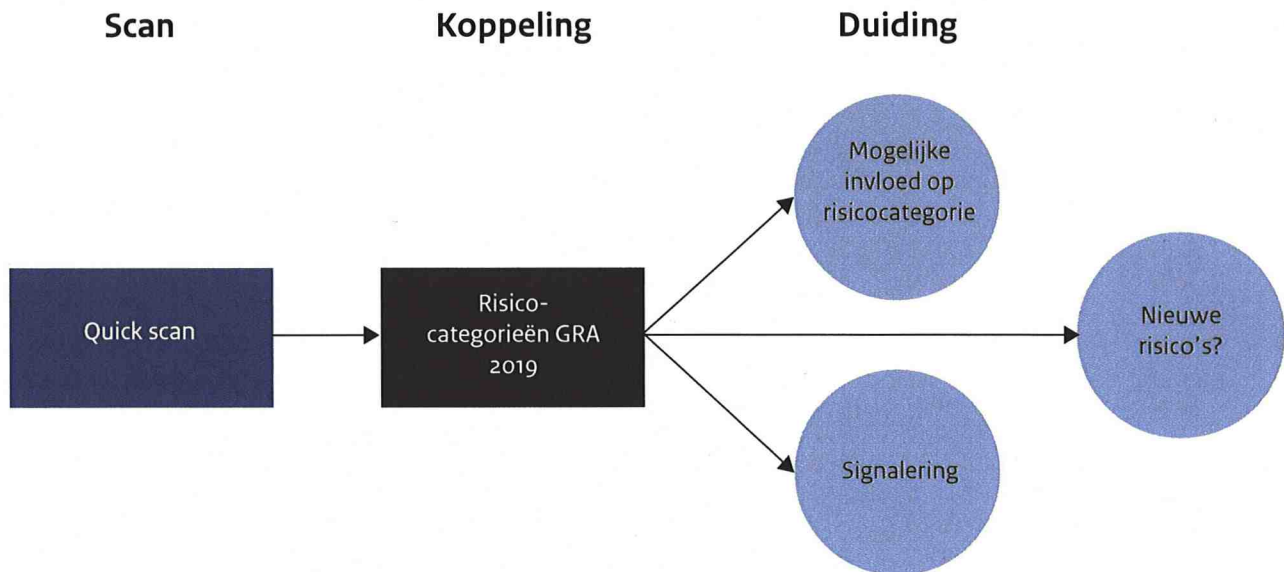
In hoofdstuk 9 wordt vervolgens het overzicht gegeven van de koppelingen die er zijn gelegd met de risico's uit de GRA 2019. In dit hoofdstuk vindt ook een beschouwing van deze koppelingen plaats. Het rapport sluit tenslotte af met de resultaten en conclusie, waarin kort de meest opvallende resultaten uit de Horizonscan 2020 en de koppeling met de risico's uit de GRA 2019 worden genoemd en een vergelijking met de GRA 2019 en NVS 2019 is gemaakt (hoofdstuk 10). In bijlage 1 staan de gebruikte bronnen voor de scans.

## 2. Methodiek

De Horizonscan 2020 bestaat uit drie elkaar opvolgende stappen: scan, koppeling en duiding (zie figuur 1). Binnen de eerste stap (scan) wordt in kaart gebracht welke nieuwe ontwikkelingen zich hebben voorgedaan sinds de uitgifte van de Horizonscan 2019 en of de reeds opgenomen trends nog actueel zijn. Dit gebeurt door middel van een 'quick-scan': een beknopte variant van de scan uitgevoerd in voorgaande horizonscans. Voor de quick-scan is uitgegaan

van dezelfde autonome ontwikkelingen en megatrends als in de Horizonscan 2019 (zie paragraaf 2.1). Binnen de tweede stap (koppeling) wordt vervolgens nagegaan voor welke risicocategorieën uit de GRA 2019 de in kaart gebrachte ontwikkelingen mogelijk van belang zijn. Binnen de laatste stap (duiding) wordt deze koppeling nader geanalyseerd en op hoofdlijnen geduid.

**Figuur 1.** Schematische weergave werkwijze



De methodiek van de Horizonscan 2020, zoals hierboven op hoofdlijnen beschreven, wijkt enigszins af van de vorige Horizonscans. Om te beginnen bevat de Horizonscan 2020 een zogeheten 'quick-scan' op basis van de in de Horizonscan 2019 opgenomen autonome ontwikkelingen en megatrends. Dit in tegenstelling tot een volledige scan waarbij ook de indeling van deze autonome ontwikkelingen en megatrends onder de loep wordt genomen. Hier is voor gekozen omdat de Horizonscan 2020 relatief kort volgt op

de Horizonscan 2019 (oktober 2019), waardoor het uitvoeren van een volledig nieuwe horizonscan niet opportuun is (peildatum van de quick-scan is april 2020). Een tweede punt waarop de Horizonscan 2020 afwijkt is de aanwezigheid van de laatste twee stappen: koppeling en duiding. De koppeling van ontwikkelingen met risico's is gemaakt, omdat deze Horizonscan als input voor de 'mid-term' review van de NVS 2019 zal dienen. De paragrafen hieronder gaan nader in op de stappen van deze Horizonscan.



## 2.1 Scan

Het startpunt van de quick-scan zijn vijf categorieën van autonome ontwikkelingen: internationale economie, internationale politiek, demografisch-maatschappelijk, informatietechnologie en ecologie. Deze autonome ontwikkelingen vormden ook de basis van de eerdere horizon-scans en gezamenlijk beslaan ze een groot deel van de potentiële trends en ontwikkelingen die mogelijk relevant zijn voor de nationale veiligheid.<sup>1</sup> Elke autonome ontwikkeling kan op zijn beurt worden uitgewerkt in een aantal 'megatrends'. Dit zijn brede ontwikkelingen die zich kunnen uitstrekken over decennia. Megatrends kunnen mondiaal, maar evengoed regionaal in oorsprong en reikwijdte zijn. Het zijn trends die zich gestaag ontwikkelen, maar een langdurig effect hebben. Binnen elke megatrend kunnen zich verschillende ontwikkelingen of manifestaties voordoen.

Er is voor gekozen om in de Horizonscan 2020 dezelfde set megatrends te hanteren als in de Horizonscan 2019, omdat die naar verwachting het meeste effect hebben op de nationale veiligheid. Tabel 1 bevat een overzicht van deze megatrends. De quick-scan richt zich nadrukkelijk op de vraag of er zich binnen de megatrends nieuwe manifestaties voordoen dan wel of de reeds opgenomen manifestaties nog actueel zijn. De keuze om uit te gaan van de autonome ontwikkelingen en megatrends uit de Horizonscan 2019 betekent uiteraard een inperking van de scope van de quick-scan, omdat niet alle mogelijk relevante megatrends zijn beschouwd en deze horizonscan dan ook niet volledig zal zijn.

**Tabel 1.** Megatrends

Autonome ontwikkeling	Megatrend
<i>Internationale economie</i>	Politisering van de internationale markteconomie Digitalisering van de economie Klimaattransitie
<i>Internationale politiek</i>	Tanende naoorlogse multilaterale wereldorde Instabiliteit aan de brede randen van Europa Polarisatie binnen de Europese samenleving
<i>Demografisch-maatschappelijk</i>	Groeiende ongelijkheid en tegenstellingen tussen bevolkingsgroepen Gevolgen van toenemende diversiteit in de samenleving Fluctuering van vertrouwen in samenleving, politiek en autoriteiten
<i>Ecologie</i>	Klimaatverandering Biodiversiteit Milieudruk
<i>Informatietechnologie</i>	Autonomie van informatietechnologie Cognitie van informatietechnologie Verbondenheid en verwevenheid van informatietechnologie Afhankelijkheid van informatietechnologie

<sup>1</sup> In de scan van 2019 is de autonome ontwikkeling informatietechnologie niet als zelfstandig thema opgenomen, maar als overkoepelende factor vermeld binnen de overige thema's.



Binnen de quick-scan is voor elk van de megatrends nagegaan of de manifestaties die opgenomen zijn in de Horizonscan 2019 nog relevant zijn, en of er mogelijk nieuwe manifestaties zijn waar te nemen.

Qua uitvoering is enerzijds gekeken of uit de bronnen van de Horizonscan 2019 nieuwe publicaties zijn verschenen. Anderzijds is verkend of er nieuwe publicaties zijn uitgekomen van instanties als planbureaus en denktanks. Het resultaat is een lijst met manifestaties per megatrend (peildatum april 2020).

## 2.2 Koppeling

De volgende stap betreft het maken van koppelingen tussen de geïdentificeerde manifestaties en de risico's uit de Geïntegreerde risicoanalyse (GRA) 2019. Deze koppeling wordt gemaakt op het niveau van de risicocategorieën. Zo wordt bijvoorbeeld niet gekeken of er een koppeling mogelijk is met een specifiek scenario zoals het plaatsvinden van een terreuraanslag op een bepaalde plek en van een bepaalde omvang, maar met de bredere risicocategorie 'terrorisme'. Bijlage 2 bevat het overzicht van de risicocategorieën uit de GRA 2019. Om de relatie tussen manifestaties en de risicocategorieën inzichtelijk te maken is gezocht naar zowel directe als indirecte relaties.

De volgende voorwaarden zijn gehanteerd voor het wel of niet opnemen van een koppeling met de risicocategorieën:

- Er is een directe relatie tussen de manifestatie en de betreffende risicocategorie. Die directe relatie heeft mogelijk al op korte termijn invloed op de risicocategorie;
- De relatie tussen manifestatie en risicocategorie is relevant voor de langere termijn, dan wel voor de context van een risicocategorie. Deze koppelingen zijn 'indirect' en dienen binnen deze scan als signaleringen.

Op basis van hun expertise hebben de scanteams eerst zelf de mogelijke koppelingen gelegd tussen manifestaties en risico-categorieën. Vervolgens zijn de koppelingen in een gezamenlijke sessie door vertegenwoordigers van alle scanteams en de taakgroep van het ANV besproken en gevalideerd.

In elk hoofdstuk zijn de koppelingen samengevat in een tabel met aan de ene kant de trends en aan de andere kant de relevante risicocategorieën. Het verschil tussen een koppeling met een directe relatie en een indirecte koppeling (signalering) is in deze tabellen met blauwtinten aangegeven (zie het voorbeeld in tabel 2). Tot slot heeft elke koppeling een nummer gekregen. Bij het corresponderende nummer onder de tabel wordt een korte verklaring voor of extra uitleg over de koppeling gegeven.

## 2.3 Duiding

Na het vaststellen van een koppeling wordt deze vervolgens nader geduid. In deze stap wordt niet meer vanuit de manifestaties gekeken, maar vanuit de risicocategorieën. In de analyse wordt aangegeven of een risicocategorie mogelijk kan worden beïnvloed door de relevante trends. Daarnaast worden eventueel nieuw geïdentificeerde dreigingen en risico's benoemd. Het is belangrijk om te vermelden is dat een eventuele uitwerking van veranderende risico's (in de vorm van waarschijnlijkheid en impact) niet plaatsvindt binnen deze Horizonscan. Als er naar aanleiding van deze Horizonscan reden is om bijvoorbeeld de ingeschatte waarschijnlijkheid van een risico te verhogen, dan zal dit plaatsvinden binnen de volgende geïntegreerde risicoanalyse.

De volgende vijf hoofdstukken beschrijven per autonome ontwikkeling de resultaten van de quick-scan.

Tabel 2. Voorbeeld van koppelingen

Thema	Natuurrampen	
Risicocategorie → Megatrend ↓	Overstroming	Extreem weer
Klimaatverandering	1 Signalering	2 Directe koppeling

1 & 2: Korte verklaring voor of extra uitleg over koppeling of signalering



# 3. Internationale economie

De Horizonscan 2019 identificeerde drie megatrends binnen het thema internationale economie, die ook in deze scan als uitgangspunt zijn gehanteerd.

Deze megatrends en de onderliggende manifestaties zijn in 2020 onverminderd relevant. Wel zijn er enkele relevante ontwikkelingen geconstateerd. Deze hebben onder andere betrekking op de manifestatie 'cybersecurity', bij de megatrend 'Digitalisering van de economie'. Ook hebben de ontwikkelingen en wereldwijde maatregelen rondom de COVID-19-crisis een significante impact op de internationale economie (zie ook hoofdstuk 8).

Autonome ontwikkeling	Megatrend
Internationale economie	Politisering van de internationale markteconomie
	Digitalisering van de economie
	Klimaattransitie

## 3.1 Politisering van de internationale markteconomie

De afgelopen jaren is sprake geweest van openlijk protectionisme. Internationale handelsconflicten hebben ook vaak een bredere diplomatieke context gekregen en raken steeds vaker ook andere beleidsterreinen als veiligheid en milieu. Deze ontwikkelingen in de laatste jaren hebben de oude scheiding tussen economie en geopolitiek tenietgedaan. De toenemende verwevenheid van handelsbeleid en geopolitiek bedreigen nu het multilaterale systeem dat de wereld na de Tweede Wereldoorlog heeft gekenschetst. Een belangrijke ontwikkeling in deze politisering van het handelssysteem is het vleugellam maken van de Beroepsinstantie (*Appellate Body*) van de World Trade Organization (WTO). Er zijn sinds december 2019 te weinig rechters om een uitspraak te doen in geschillen tussen handelspartners. Dit omdat de Verenigde Staten weigeren in te stemmen met de benoeming van iedere rechter. De Beroepsinstantie is echter een cruciale

spil in het *rule-based* handelssysteem. Zonder de Beroepsinstantie is er meer onzekerheid rondom internationale handel, wat kan leiden tot een (verdere) afname van deze handel. Dit heeft voor Nederland negatieve gevolgen, met name vanwege de doorvoerfunctie van Nederland. Ook is de Nederlandse economie kwetsbaar voor handelsconflicten tussen landen die via Nederland goederen of diensten transporteren.

De aanhoudende handelsoorlog tussen de Verenigde Staten en China onderging tijdelijk een positieve ontwikkeling in december 2019, toen fase één van een **handelsakkoord** werd ondertekend door beide landen. Inmiddels zijn de banden tussen de Verenigde Staten en China wederom verslechterd, met name omdat de Verenigde Staten China direct verantwoordelijk houden voor de uitbraak van het coronavirus (zie verder hoofdstuk 8). Deze geopolitieke spanningen en de handelsbeperkingen die het virus met zich meebrengt, leiden tot minder internationale samenwerking op het gebied van handel. Dit kan eerdere toenaderingen in de handelsoorlog weer tenietdoen.

Echter, het bilaterale handelsakkoord tussen de VS en China staat in scherp contrast met het multilaterale karakter van internationale handelsverdragen. Het akkoord is mogelijk een manifestatie van de overgang van een multilateraal *rule-based* systeem naar een **bilateraal power-based systeem**. Dit past goed bij de toenemende politisering, nu handelsverdragen als een machtsstrijd worden gezien. Een dergelijk bilateraal systeem kan mogelijk voordelig zijn voor landen met de middelen om ze tot stand te brengen, maar niet voor landen met minder middelen, die zijn gebaat bij een multilateraal systeem gebaseerd op algemene regels. Voor Nederland – een kleine open economie – ontstaat hier een risico op welvaartsverlies. Dit hangt onder meer af van de verhouding van de EU ten opzichte van zowel de VS als China.

Op het gebied van **industriepolitiek** meldt China zich steeds nadrukkelijker op de Europese markt (althans tot de uitbraak van COVID-19). In combinatie met de hernieuwde opmars van Chinees staatskapitalisme, kan dit een bedreiging vormen voor de concurrentiepositie van



Europese bedrijven. Europese landen, inclusief Nederland, zijn de laatste jaren kritischer geworden op Chinese invloed via investeringen. Concurrentiebevordering en bescherming van de nationale veiligheid kunnen hiermee op gespannen voet staan. Als buitenlandse bedrijven (mogelijk ondersteund door hun overheid) willen toetreden in strategische sectoren op de Europese interne markt, kan de nationale veiligheid in het geding komen. In reactie hierop stellen veel landen (ook Nederland) wetgeving in om bedrijven in strategische sectoren te beschermen tegen buitenlandse overnames. Europese voorbeelden van beleid zijn dat buitenlandse overnames in strategische sectoren moeten worden goedgekeurd door de regering, er is meer *investment screening* en op Europees niveau wordt informatie gedeeld over Chinese investeringen. Hoewel zulke wetgeving risico's op ongewenste inmenging verkleint, ontstaan er ook nieuwe risico's door. Bescherming tegen overnames kan bijvoorbeeld competitieve prikkels verminderen, wat markten minder efficiënt kan maken. Ook ontstaan mogelijk politiek-economische risico's omdat overheden moeten bepalen welke bedrijven in welke sectoren nu 'strategisch' zijn en welke niet. Overheidsfalen ligt hier op de loer.

De **economische banden tussen China en Rusland** worden sterker, waardoor China in toenemende mate concurreert met de EU op de Russische markt. De EU en Rusland zijn van oudsher sterk met elkaar verbonden. China's snel groeiende economie brengt hier verandering in, alsmede nieuwe Chinese initiatieven zoals de *Ice Silk Road*: de ontwikkeling van nieuwe handelsroutes die mogelijk worden via het Noordpoolgebied. Nederland en de EU kunnen ook baat hebben bij dergelijke nieuwe handelsroutes, maar Rusland blijft voornamelijk een van de belangrijkste machten in het Noordpoolgebied. De EU en Rusland hebben sterke banden op het gebied van gas en olie, maar ook daar treedt China toe. Bij een grotere afhankelijkheid van Russisch gas en een grotere rol voor China op die markt, kunnen in de toekomst echter risico's omtrent de energielevering ontstaan. Gezien de sterke daling in de olie- en gasprijzen begin 2020, komt de Russische economie onder grote druk te staan. In combinatie met de coronamaatregelen zal dit tot een substantiële krimp van de Russische economie leiden.

China mengt zich ook steeds nadrukkelijker in de strijd om **standaardsetting**. Het *Belt and Road Initiative* (BRI) blijft zich uitbreiden, met name richting instabiele ontwikkelingslanden. Met de BRI verstevigt China ook haar invloed op het wereldtoneel en bij de BRI-partners is China ook leidend bij het bepalen van de standaardsetting, op technologisch gebied maar ook op het gebied van economische relaties. De BRI biedt kansen voor Nederland als logistieke hub, omdat het Euraziatische (handels)netwerk sterk is uitgebreid, maar met

de BRI neemt ook de geopolitieke machtspositie van China in Europa toe. Risico's zijn ook dat China de eenheid tussen EU-landen in gevaar brengt. Ook op het gebied van digitalisering en automatisering eist China een belangrijkere rol op om haar internationale machtspositie te verstevigen. Recentelijk is er wel toenemende weerstand tegen het uitrollen van 5G-netwerken met Chinese technologie.

Door de uitbraak van het coronavirus loopt de BRI vertraging op, aangezien de meeste BRI-projecten afhankelijk zijn van Chinese bedrijven, Chinese materialen en Chinese werknemers. Door de internationale beperkingen wordt een zwak punt van de BRI blootgelegd, namelijk de grote afhankelijkheid van China. Het is mogelijk dat dit overheden tot nadenken zet over de wenselijkheid van BRI-projecten in hun land.

### 3.2 Digitalisering van de economie

**Automatisering** heeft een transformerend effect op de arbeidsmarkt, waaraan zowel kansen als risico's zijn verbonden. Banen zullen verdwijnen, nieuwe banen zullen ontstaan, maar veel banen zullen vooral veranderen. De positie van werknemers op de arbeidsmarkt wordt daarmee steeds meer afhankelijk van hun vermogen om hun menselijk kapitaal op peil te houden of aan te passen. Het risico is dat er een groep achterblijvers ontstaat op de arbeidsmarkt van de toekomst die hier te beperkt in slaagt. Dit kan zorgen voor groeiende ongelijkheid en sociaaleconomische polarisering. Voor bedrijven bestaat het risico dat zij te weinig arbeidskrachten met de juiste vaardigheden kunnen aantrekken. Dit kan de welvaarts-groei drukken. Op korte termijn vallen deze risico's echter waarschijnlijk in het niet bij de COVID-19-crisis, met het risico op hoge werkloosheid is (zie hoofdstuk 8).

Voor de bescherming van de interne Europese markt is het van belang dat de digitale **monopolisten** zich houden aan de regels van de markt en geen te grote machtspositie verwerven (bijvoorbeeld door het bezit en verhandelen van data). Monopolievorming kan ertoe leiden dat consumenten en bedrijven te veel betalen voor goederen en diensten. Ook kan een rem op innovatie en marktdynamiek ontstaan als potentiële toetreders door bijvoorbeeld schaal- en netwerk-effecten in datagebruik te hoge barrières ondervinden voor daadwerkelijke toetreding. Voor zover gebruik wordt gemaakt van persoonsgegevens is het risico dat het publieke belang van privacy onvoldoende geborgd blijft. Passende wet- en regelgeving met betrekking tot privacy en eigenaarschap en de handhaving daarvan spelen hier dan ook een belangrijke rol in. Zie verder hoofdstuk 7.

**Cybersecurity** is een onderwerp dat ook in de economie steeds meer onder de aandacht komt. Door toenemende digitalisering neemt het veiligheidsrisico ook toe. Zo kan een cyberaanval financiële instellingen of zelfs hele markten in gevaar brengen. Bedrijven blijken nog niet voldoende beschermd tegen mogelijke cyberaanvallen, wat ze kwetsbaar maakt. Daarnaast is cybersecurity van groot belang voor e-commerce. Huidige handelsakkoorden bevatten niet de nodige clausules tegen cybersecurity incidenten, wat internationale e-commerce hindert. In tijden dat veel mensen thuis werken en de afhankelijkheid van digitalisering toeneemt, is de rol van cybersecurity des te belangrijker. Zie verder hoofdstuk 7.

### 3.3 Klimaattransitie

De klimaattransitie leidt tot **internationaal-economische politieke machtsverschuivingen**. Zo neemt de Europese Commissie met haar *European Green Deal* een grotere rol op zich in de klimaattransitie en de transformatie van de economie. Dit is voor Nederland waarschijnlijk een positieve ontwikkeling vergeleken met een grotere rol van de Verenigde Staten of China op het gebied van de klimaattransitie. Deze landen hanteren een geheel andere visie op het gebied van klimaatbeleid dan Nederland. Ook handelsakkoorden moeten worden aangepast op de klimaattransitie, om ook in de 21<sup>e</sup> eeuw relevant te blijven. Zo is het aantal clausules omtrent milieu wel in opmars, maar nog beperkt.

De klimaattransitie raakt ook het **bedrijfsleven** en kan extra **kosten** met zich meebrengen. De aangekondigde CO<sub>2</sub>-belasting wordt over het algemeen gezien als een effectief instrument om CO<sub>2</sub>-uitstoot te verminderen volgens het principe 'de vervuiler betaalt'. Echter, Europese afstemming is hierbij wenselijk zodat een level *playing field* gewaarborgd blijft. Bij een relatief hoge Nederlandse klimaatambitie, en dus een relatief hoge CO<sub>2</sub>-belasting, bestaat het risico dat het Nederlandse bedrijfsleven met

hogere kosten te maken krijgt dan bedrijven in andere Europese landen. Arbitrage in CO<sub>2</sub>-belasting door verschuiving van productie naar laag-belastende landen moet worden voorkomen, maar de effectiviteit van een zogenaamd *carbon border adjustment mechanism* is nog niet bewezen. Daarnaast lijkt door de COVID-19-crisis het draagvlak voor een CO<sub>2</sub>-heffing te zijn afgenomen, hetgeen weer kan leiden tot toenemende klimaat-gerelateerde risico's op langere termijn. Aan de andere kant wordt de roep om klimaatinvesteringen via het noodfonds van de Europese Commissie groter, wat de klimaattransitie zou kunnen versnellen.

### 3.4 Koppeling met risicocategorieën

Er zijn koppelingen te maken met een aantal risicocategorieën uit de GRA 2019. Deze behoren bij de dreigings-thema's Financieel-economische bedreigingen en cyberdreigingen. Voor cyberdreigingen gaat over cyberspionage en digitale sabotage, terwijl voor financieel-economische bedreigingen alle vier de risicocategorieën relevant zijn. Onderstaande tabel geeft de koppelingen weer.

Tenslotte zijn er enkele risico's die minder goed bij de risico-indeling van de GRA passen, maar wel relevant zijn voor de context van de risico-afweging. Zo kan bescherming van bedrijven tegen buitenlandse overnames vanuit het oogpunt van nationale veiligheid onder andere tot concurrentievermindering leiden, met welvaartsverliezen tot gevolg. Daarnaast heeft de transformatie van de arbeidsmarkt door digitalisering invloed op het verdien- en productievermogen van Nederland. Ook monopolievorming vormt een bedreiging voor economische groei, ook zonder een specifiek internationaal-economisch aspect.



**Tabel 3.** Koppeling met risicocategorieën vanuit internationale economie

Dreigingsthema → Megatrend ↓	Cyberdreigingen		Financieel-economische bedreigingen			
	Cyber- spionage	Digitale sabotage	Criminele inmenging	Bedreigingen van de knooppuntfunctie en de aan- en afvoerlijnen van Nederland (flow security)	Handelskrimp/ verstoring internationale handel	Destabilisatie financieel systeem
Politisering van de internationale markteconomie	1			2	3	
Digitalisering van de economie	4	4	5		6	7
Klimaattransitie					8	

- (Groeiende) invloed van China in strategische sectoren kan cyberspionage faciliteren.*
- China investeert in infrastructuur via BRI, maar geopolitieke factoren kunnen risico vormen voor bijvoorbeeld de Rotterdamse haven.*
- De handelsoorlog brengt onzekerheid met zich mee, dit terwijl Nederland als open economie sterk afhankelijk is van handel.*
- Cybersecurity wordt steeds belangrijker, risico's zijn groot. Dat gaat het zowel om cyberspionage als om digitale sabotage.*
- Door digitalisering kunnen criminele activiteiten ook online plaatsvinden.*
- Huidige regels zijn niet voldoende voor e-commerce, dit kan een belemmering vormen.*
- Cyberaanval op financiële instelling of markt kan heel systeem platleggen.*
- Door CO<sub>2</sub>-belasting hogere transportkosten, kan tot arbitrage leiden en Nederland benadelen.*



# 4. Internationale politiek

Op het gebied van internationale politiek is in de Horizonscan 2019 ingezoomd op drie megatrends die de meeste impact hebben op de Europese veiligheid en bij extensie op die van Nederland. Deze megatrends zijn ook in de Horizonscan 2020 als uitgangspunt genomen.

Autonome ontwikkeling	Megatrend
Internationale politiek	Tanende naoorlogse multilaterale wereldorde
	Instabiliteit aan de brede randen van Europa
	Polarisatie binnen de Europese samenleving

## 4.1 Tanende multilaterale wereldorde

De tanende naoorlogse multilaterale wereldorde manifesteert zich op drie manieren: spanningen tussen grote mogendheden, afbrokkelende internationale regimes en verslechterende trans-Atlantische betrekkingen. Deze manifestaties zijn sinds de publicatie van de Horizonscan 2019 nog steeds relevant en hebben zich in het algemeen versterkt.

Er is nog steeds sprake van **spanningen tussen de grote mogendheden**. Dit uit zich onder andere in wapenwedlopen die zich verder hebben ontwikkeld. Op het gebied van hypersonische wapens is duidelijk dat de trend van groeiende competitie is versterkt. Eind 2019 lanceerde Rusland een nieuwe hypermoderne intercontinentale raket 'Avangard', waarna zowel de VS als China bekend maken ook in hun hypersonische wapenarsenaal te investeren. Daarnaast hebben bijvoorbeeld Iran en India de afgelopen maanden ook relevante ontwikkelingen doorgemaakt op dit terrein. De groeiende wapenwedloop manifesteert zich dan ook op het gebied van offensieve ruimtecapaciteiten en de ruimte is door de NAVO officieel als vijfde domein erkend. Naast de ontwikkelingen binnen dit vijfde domein ligt een nucleaire wapenwedloop op de loer. China heeft nieuwe wapens onthuld, waaronder (nucleaire) raketten die de VS kunnen bereiken.

De Chinees-Amerikaanse relatie is aanzienlijk verslechterd sinds de Horizonscan 2019. Alhoewel er in januari 2020 een akkoord is gesloten om de handelsoorlog gefaseerd tot stilstand te brengen, blijven de spanningen oplopen. Dit komt met name door de beschuldigingen over de oorzaak, verspreiding en de aanpak van het coronavirus. Tegelijkertijd zoeken Rusland en China op zowel militair als economisch vlak nadrukkelijk toenadering tot elkaar. Terwijl de VS Huawei de toegang tot de Amerikaanse markt ontzegt omdat Huawei een dreiging voor de nationale veiligheid zou zijn, ontvangt Rusland het Chinese telecombedrijf met open armen. Dit zorgt voor een versterkte spanning tegenover de VS en het Westen.

Er is ook nog steeds sprake van **afbrokkelende internationale regimes**. Het stelsel van nucleaire wapenbeheersing wankelt, nu het INF-verdrag in augustus 2019 is opgezegd en het New Start-verdrag – dat in principe in 2021 afloopt – samen met het kernstopverdrag nog ter discussie staat. In november 2019 heeft Rusland een formeel voorstel gedaan om het New Start-verdrag met vijf jaar te verlengen, maar de VS stelt zich kritisch op. Tevens dreigde Iran in januari 2020 uit het Non-proliferatieverdrag te stappen als Frankrijk, het Verenigd Koninkrijk en Duitsland naar de VN stappen met de Iraanse overtredingen van het atoomakkoord uit 2015 (het JCPOA). Een voorgesteld resolutiemechanisme waar ook de VS weer deel van uit zou maken, wordt door Iran afgewezen. Door de maatregelen rond de COVID-19-crisis is bovendien de toetsingsconferentie van het NPV in april 2020 niet doorgegaan. Dit zou een belangrijk ijkmoment voor het mondiale stelsel van de nucleaire wapenbeheersing zijn geweest. De ontwikkelingen lijken erop te wijzen dat er wordt bewogen richting een wereld zonder wapenbeheersing regimes. Ook heeft de VS aangegeven na te denken om zich terug te trekken uit het Open Skies verdrag, waardoor andere landen geen militaire verkenningsvluchten boven Amerikaans grondgebied kunnen maken, en vice versa. Dit zou reeds bestaande spanningen tussen met name de VS en Rusland verergeren.

Daarnaast werd er in de voorgaande Horizonscan geconstateerd dat het draagvlak voor het internationale handelssysteem steeds verder afbrokkelt. De crisis rondom de WTO heeft zich de afgelopen zes maanden verder



ontwikkeld (zie ook paragraaf 3.1). In reactie hierop kondigde de Eurocommissaris voor Handel een wetsvoorstel aan waarmee de EU importtarieven en andere sancties kan treffen zonder goedkeuring van de WTO. Een belangrijke pijler van vrije wereldhandel valt hiermee weg. De ontwikkelingen binnen deze manifestatie zijn daarmee in redelijke mate versterkt sinds de Horizonscan 2019.

Ten slotte zijn de **trans-Atlantische betrekkingen verder verslechterd**. De huidige opstelling van de VS ten opzichte van de multilaterale wereldorde, zet de relaties met Europa en Nederland op scherp. Het handelsconflict tussen de EU en de VS is een aantal keer geëscaleerd, onder andere door het invoeren van Amerikaanse importheffingen op Europese producten, het verhogen van de vennootschapsbelasting op grote Amerikaanse techbedrijven en Amerikaanse sancties tegen (Europese) bedrijven die meebouwen aan de Nordstream 2 pijplijn. Daarnaast is de discussie over het bestaan en functioneren van de NAVO opnieuw aangewakkerd door een reeks gebeurtenissen. Turkije heeft aangegeven Russische luchtafweerraketten te willen kopen, waarop Amerika heeft gedreigd geen F-35 gevechtsvliegtuigen meer te zullen leveren. In oktober 2019 kondigde de VS aan zich te willen terugtrekken uit Syrië en zette daarmee het bondgenootschap met de Koerden op losse schroeven. Turkije viel vervolgens onaangekondigd het land binnen. Zowel het eenzijdige Amerikaanse besluit als de Turkse inval zorgde voor discussie over de betrouwbaarheid en loyaliteit van beide landen. De toenadering van Turkije tot Rusland leidt tot versterkte spanningen tussen Turkije en zijn NAVO bondgenoten. Maar ook leiders van West-Europese landen, zoals president Macron en bondskanselier Merkel, hebben kritische opmerkingen geplaatst bij het functioneren van de NAVO en de betrouwbaarheid van de VS in dit kader. De veiligheidsgarantie van de militaire alliantie, en de belangrijke rol van de VS in het bondgenootschap lijken niet meer als vanzelfsprekend te worden gezien.

## 4.2 Instabiliteit brede randen van Europa

Wat betreft de instabiliteit rondom Europa zijn de manifestaties uit de Horizonscan 2019 (conflicten en fragiliteit ten zuiden, ten oosten en ten noorden van Europa) nog steeds relevant. Sommige ontwikkelingen binnen de manifestaties hebben zich de afgelopen maanden versterkt.

De regio die de laatste jaren de belangrijkste dreiging voor de Nederlandse veiligheid heeft gevormd ligt **ten zuiden van Europa**. Conflicten, (burger)oorlogen en politieke opstanden in diverse landen in het Midden-Oosten en Noord Afrika hebben geleid tot toenemende instabiliteit aan de zuidflank van Europa. Dit is de afgelopen maanden niet veranderd. In Irak is de onrust de afgelopen maanden

sterk toegenomen. Verschillende factoren spelen hierbij een rol. Zo is Irak in toenemende mate 'slachtoffer' geworden van de geïntensiveerde spanningen tussen de VS en Iran. De liquidatie van de belangrijkste Iraanse generaal door de VS en in reactie daarop de Iraanse aanval op de Amerikaanse ambassade in Bagdad is hiervan een voorbeeld. Bovendien ondergaan terreurorganisaties, waaronder IS, een heropleving op Iraaks grondgebied. Ook de instabiliteit in Libië is verder toegenomen. Dit onder andere wegens de toegenomen buitenlandse inmenging, waaronder het Turkse besluit om troepen te sturen naar Libië. Verder duurt de Syrische burgeroorlog nog steeds voort. In dit opzicht kan er gesproken worden van continuïteit. Echter, het onverwacht (gedeeltelijk) terugtrekken van de Amerikaanse troepen en de vrijbrief aan het adres van de Turkse president Erdogan om het noordoosten van Syrië binnen te vallen in zijn strijd tegen de Koerden, heeft tot groeiende instabiliteit in het land geleid.

In de Horizonscan 2019 is al geconstateerd dat het **Poolgebied** onder invloed van klimaatverandering in toenemende mate een arena is geworden van geopolitieke wedijver. Deze manifestatie heeft zich gestaag voortgezet, met name door aankondigingen van Russische en Chinese zijde over toenemende (militaire) investeringen. Een reactie van de VS is dan ook niet uitgebleven; recentelijk heeft het aangekondigd het consulaat in Groenland te heropenen. Toenemende spanningen tussen de grote mogendheden elders in de wereld kan bovendien een spill-over effect hebben in het Arctisch gebied en daarmee leiden tot een vergrote kans op conflicten. De spanningen zijn de laatste maanden niet geïntensiveerd of geëscaleerd, waarmee ook de ontwikkelingen binnen deze manifestatie stabiel zijn gebleven.

Wat betreft **conflicten en fragiliteit ten oosten en zuidoosten van Europa** is de situatie over het algemeen onveranderd. Een assertief Rusland blijft tot fragiliteit ten oosten van Europa leiden. Ook blijft de instabiliteit op de Westerse Balkan voortbestaan. Een lichtpuntje in dit verband zijn de toetredingsonderhandelingen die hebben plaatsgevonden tussen de EU enerzijds en Albanië en Noord-Macedonië anderzijds. Laatstgenoemde is bovendien sinds maart 2020 officieel lid van de NAVO.

Een regio die in de Horizonscan 2019 buiten beschouwing werd gelaten is het **Caribisch gebied**. De afgelopen maanden is de situatie in landen als Venezuela en Colombia relatief stabiel gebleven. Echter, het gevaar ligt hier voornamelijk in een mogelijke escalatie van de reeds bestaande interne conflicten en crises. Een verergering van de Venezolaanse vluchtelingen crisis is daarbij voorstelbaar waarvan de gevolgen gevoeld kunnen worden binnen het Caribisch deel van het Koninkrijk (waaronder Aruba, Bonaire en Curaçao).

### 4.3 Polarisatie binnen de Europese samenlevingen

De huidige trend richting verdere polarisatie binnen de Europese samenleving manifesteert zich op verschillende manieren: ongewenste buitenlandse inmenging, verminderde cohesie in de Europese samenlevingen en de afbrokkeling van het principe rechtsstatelijkheid. Deze ontwikkelingen hebben zich in het afgelopen jaar versterkt.

**Ongewenste buitenlandse inmenging** blijft een belangrijke dreiging voor Europese staten. Dankzij de continue ontwikkeling van nieuwe technologieën wordt de verspreiding van desinformatie steeds complexer. De dreiging van 'deepfakes' blijft om die reden reëel (zie ook hoofdstuk 7). De AIVD meldt dat Nederland in 2019 een belangrijk spionagedoelwit voor Rusland was. Beïnvloeding van de berichtgeving rondom het MH-17-proces via sociale media speelde hierbij een aanzienlijke rol. Met betrekking tot de voortzetting van het MH-17 proces wordt verwacht dat Russische inmenging niet zal afnemen. Daarnaast is het de verwachting dat Russische desinformatiecampagnes in Europa rondom verkiezingen, referenda en grootschalige protestacties zullen toenemen, met als doel om polarisatie binnen Europese samenlevingen aan te wakkeren.

Naast de dreiging van desinformatie zetten China, en in mindere mate Iran, zich actief in op het gebied van digitale economische spionage in de Nederlandse technologische sector. Zorgen rondom deze vorm van inmenging worden versterkt door onenigheid over de mogelijke bouw van 5G-netwerken door het Chinees telecombedrijf Huawei. Uiteenlopend beleid tussen EU-lidstaten over de Huawei-kwestie en de daaruit voortvloeiende dreiging valt eveneens niet uit te sluiten.

Ontwikkelingen omtrent de beïnvloeding van onder andere de Turkse, Chinese en Iraanse diaspora's in Nederland zijn voornamelijk stabiel gebleven. De dreiging van deze vorm van beïnvloeding is dat het identificeren en soms ook intimideren van critici bestaande spanningen binnen (diasporagroepen in) de Nederlandse samenleving kan vergroten.

Ongewenste buitenlandse inmenging draagt dus bij aan **verminderde cohesie in de Europese samenlevingen**. Het AIVD-jaarverslag van 2019 berichtte bijvoorbeeld dat financiële steun voor salafistische aanjagers in Nederland

geregeld uit het buitenland komt. Deze aanjagers hebben volgens de AIVD een disproportioneel grote invloed. De polariserende retoriek die deze aanjagers verspreiden via regulier en buitenschools onderwijs is problematisch voor zowel integratie als het veiligheidsperspectief.

Ook zorgen rond het verband tussen sociale media, geweld en snelle radicalisering zijn in 2020 nog altijd aanwezig. Zo maakten acties van *Extinction Rebellion* in oktober 2019 duidelijk dat klimaatactivisten en links-extremisten steeds vaker de wet overtreden. Verder wordt ook verwacht dat polarisatie rond de Zwarte Piet-discussie elke winter weer zal oplaaien. De AIVD noemde daarnaast 2019 het "jaar van rechts-extremistische aanslagplegers wereldwijd"; in Nederland blijft deze ontwikkeling vooralsnog slechts zichtbaar online. Het gevaar voor kopieergedrag dat gefaciliteerd wordt door het internet blijft echter reëel.

Tenslotte zijn er signalen rondom de **afbrokkeling van het principe rechtsstatelijkheid**. Dit is vooral zichtbaar in Centraal- en Oost-Europa. Manifestaties van deze trend betreffen: verminderde persvrijheid en bescherming van mensenrechten, angst om de regering te bekritisieren en wantrouwen jegens informatie afkomstig van de overheid en media. Liberale normen en waarden staan vooral onder druk in Polen en Hongarije. In april 2020 heeft de Europese Commissie een vierde inbreukprocedure tegen Polen gelanceerd, wegens grootschalige juridische veranderingen die in strijd zijn met EU wetgeving. In Hongarije spelen vergelijkbare processen zich af. Sinds de uitbraak van COVID-19 heeft minister-president Orbán zijn overheid onbeperkte macht gegeven, door het regeren per decreet mogelijk te maken en de noodtoestand voor onbepaalde duur te laten voortzetten. Verder is in Rusland de macht van president Poetin door enkele wijzigingen aan de grondwet verder vergroot. Poetins constitutionele staatsgreep en het toenemende gebruik van repressie verkleinen de kans op een ordelijke machtsoverdracht en vergroten het risico op geweld in Rusland.

### 4.4 Koppeling met de risicocategorieën

De hierboven beschreven megatrends kunnen (via concrete manifestaties) een invloed hebben op risicocategorieën uit de GRA 2019. Een overzicht van mogelijke koppelingen is opgenomen in onderstaande tabel.



**Tabel 4.** Koppeling met risicocategorieën vanuit internationale politiek (donkerblauw=directe koppeling; lichtblauw en cursief=signalering (langetermijn of relevant voor de context))

Dreigings-thema →	Gewelddadig extremisme en terrorisme	Financieel-economische bedreigingen		Bedreigingen internationale vrede en veiligheid			
Risico-categorie →	Terrorisme	Bedreigingen van de knooppunt-functie (flow security)	Handelskrimp/verstoring internationale handel Handelskrimp/verstoring internationale handel	Instabiliteit rondom Europa	Militaire dreigingen (NAVO-lidstaat)	CBRN-proliferatie	Veiligheidsarrangementen onder druk (NAVO, EU)
Megatrend ↓							
Tanende multilaterale wereldorde			1	2		3	4
Instabiliteit brede randen van Europa	5	6	7	8	9	10	11
Polarisatie binnen de Europese samenlevingen			12				

Dreigings-thema →	Cyberdreigingen		Ondermijning democratische rechtsstaat en open samenleving	
Risico-categorie →	Digitale sabotage	Cyberspionage	Niet-gewelddadig extremisme	Ongewenste buitenlandse inmenging en beïnvloeding
Megatrend ↓				
Tanende multilaterale wereldorde	13	13		13
Polarisatie binnen de Europese samenlevingen		14	15	16

- Groeiende competitie tussen grote mogendheden en druk op het draagvlak voor internationale handelssystemen heeft geleid tot verder verstoorde handelsbetrekkingen. Ook de koers van de VS heeft geleid tot ondermijning van het internationaal vrijhandelssysteem.
- De onvoorspelbare (diplomatiek, militair) en unilaterale acties van de VS in landen rondom Europa leiden tot meer instabiliteit aan de grenzen van Europa.
- Onzekerheid rondom stabiliseringsmechanismen zoals het NPT en START (manifestatie: spanningen tussen grote mogendheden & afbrokkelende internationale regimes).
- Toenemende spanningen tussen grote mogendheden leidt tot ondermijning van veiligheidsarrangementen. Wat betreft de NAVO ondermijnt de houding van de VS ten opzichte van rivaliserende mogendheden en NAVO bondgenoten het vertrouwen in het bondgenootschap.
- Indien conflicten en fragiliteit ten zuiden van Europa zorgen voor een heropleving van terreurorganisaties, kan de waarschijnlijkheid van terroristische aanslagen in Europa toenemen.
- Het conflict in Venezuela vormt een bedreiging van de aan- en afvoerlijnen van Caribisch Nederland.
- Conflicten tussen staten over de grondstoffen in het Arctische gebied kunnen spill-over effecten hebben op andere terreinen, en daarmee de internationale handel verstoren. Deze kan ook worden geraakt als de stabiliteit ten oosten van Europa afneemt.
- Als concrete voorbeelden gelden de groeiende instabiliteit in Syrië, Libië en Irak. Verder is de laatste jaren ook het Noordpoolgebied uitgegroeid tot een regio met groeiend conflict-potentieel. Instabiliteit rondom Europa kan uiteindelijk leiden tot conflicten met gevolgen voor Europa en ook tot polarisatie binnen Nederland.
- Militarisering van het Arctische gebied zorgt voor een verhoogd risico op militaire escalatie. Ook vanuit Rusland blijft een militaire dreiging uitgaan (manifestatie: conflicten en fragiliteit ten noorden & (zuid-)oosten van Europa).
- China en Rusland hebben aangegeven ijsbrekers met nucleaire capaciteiten te ontwikkelen die in het Arctische gebied kunnen varen. Daarnaast geldt dat ook aan de oostflank van Europa moet rekening worden gehouden met CBRN proliferatie.
- Rusland poogt verdeeldheid te creëren onder lidstaten van zowel de EU als de NAVO.
- In (Europese) landen zoals Hongarije, Polen en Rusland hebben regeringsleiders gebruik gemaakt van verminderde cohesie en verergerde polarisatie om verregaande maatregelen door te voeren die ingaan tegen het principe van een democratische rechtstaat.
- Om hun macht te tonen kunnen grootmachten digitale sabotage of cyberspionage bewust inzetten. Dit kan tevens onderdeel zijn van hybride operaties om zo een land te beïnvloeden.
- De dreiging van digitale (economische) spionage is toegenomen, onder andere door de verdeeldheid rondom de aanleg van 5G netwerken (manifestatie: ongewenste buitenlandse inmenging).
- Door de wijdverbreide desinformatie is er verminderde sociale cohesie. De publieke opinie is in toenemende mate verdeeld in minder, maar extremere kampen, die elkaar steeds minder weten te vinden. Dit kan leiden tot steeds "extremer" politiekgedragenvolgensweertotmaatschappelijke instabiliteit (manifestatie: verminderde cohesie in de Europese samenlevingen).
- Verspreiding van desinformatie door externe partijen (met als doel polarisatie) kan leiden tot verminderd vertrouwen in zowel de politiek als de rechterlijke macht. Vooral populistische partijen hebben hier voordeel bij. Ook buitenlandse inmenging in de vorm van beïnvloeding van diaspora's kan leiden tot ondermijning van de democratische rechtstaat.

Tenslotte noemen we twee toekomstige gebeurtenissen die van belang zijn voor de wijze waarop de internationale politiek en ook de internationale en Nederlandse economie zich de komende jaren ontwikkelen. Het gaat om de Brexit

en om de verkiezingen in de VS. Beide zijn losse gebeurtenissen die in deze scan niet apart zijn beschouwd, maar die wel ineen volgende risicoanalyse meegenomen dienen te worden.<sup>2</sup>

---

<sup>2</sup> In de GRA 2019 is een scenario uitgewerkt waarbij is uitgegaan van onder meer een chaotische Brexit, met onder andere problemen rondom import en export van goederen, gevolgen met betrekking tot data-uitwisseling en grote financiële impact (GRA, 2019).





# 5. Demografisch- maatschappelijk

In de Horizonscan 2019 zijn binnen het thema demografisch-maatschappelijk drie megatrends geïdentificeerd, die met name op het maatschappelijke vlak liggen.

Autonome ontwikkeling	Megatrend
Demografisch-maatschappelijk	Groeiende ongelijkheid en tegenstellingen tussen bevolkingsgroepen
	Gevolgen van toenemende diversiteit in de samenleving
	Fluctuering van vertrouwen in samenleving, politiek en autoriteiten

Deze megatrends en bijbehorende manifestaties zijn ook in 2020 onverminderd relevant. Wel blijken er bij verschillende manifestaties versterkingen van de trends. Het belang van primaire identiteiten neemt steeds meer toe, zowel bij groepen zonder- als met een migratieachtergrond. Ook constateren we dat diverse tendensen in samenhang met elkaar (zoals toenemende complexiteit, internationalisering, immigratie, digitalisering) de maatschappelijke polarisatie verder versterken. De verspreiding van nepnieuws neemt verder toe en verbreedt zich. Verder is er sprake van een opkomende eenzijdige en polariserende mediasfeer die concurreert met de mainstream. Tevens zijn er in het afgelopen jaar meer voorbeelden bijgekomen van extremisme die niet past in het klassieke onderscheid van links- en rechts maar zich richten op specifieke onderwerpen.

In de periode dat Horizonscan 2020 wordt afgerond vinden ook in Nederland grootscheepse demonstraties en debat plaats naar aanleiding van de dood van George Floyd. De demonstratiebereid en het Black Lives Matter debat laten zien dat er bij groepen sprake is van veel onvrede en frustraties over hun positie in de samenleving, welke nu aan de oppervlakte komen. De verdere ontwikkelingen en impact hiervan zijn echter nog niet te overzien.

## 5.1 Groeiende ongelijkheid en tegenstellingen tussen bevolkingsgroepen

Tegenstellingen tussen bevolkingsgroepen manifesteren zich langs zowel sociaal-culturele als sociaaleconomische scheidslijnen. Op **sociaal-cultureel vlak** is er sprake van verharding en etnificering van het (online) maatschappelijk debat, maar uit bevolkingsenquêtes blijkt niet dat de polarisatie over de hele linie toeneemt. Wel maken Nederlanders, net zoals in 2019, zich grote zorgen dat de polarisatie in de samenleving verder zal toenemen, en wijten dit grotendeels aan de (nieuwe) media. Denk hierbij aan verharding (ook door sociale media), verhuftering, intolerantie, gebrek aan respect, onverdraagzaamheid, polarisatie en discriminatie. Ook de toenemende diversiteit lijkt nog steeds bij te dragen aan een vermindering van de sociale cohesie.

Ongeveer een kwart van de Nederlanders geeft aan discriminatie te ervaren. Deze cijfers zijn vergelijkbaar met voorgaande jaren. Echter, er is een opvallende groei in de mate van ervaren discriminatie in het onderwijs. Het gaat hier bovendien relatief vaker om ernstige vormen van discriminatie, zoals geweld, bedreiging of seksueel lastigvallen.

Groeiende tegenstellingen langs sociaal-culturele scheidslijnen zijn vooral een risico wanneer dit zich ontwikkelt samen met sociaal-economische scheidslijnen, en vice versa. Er lijkt sprake te zijn van een **groeiende kloof tussen bevolkingsgroepen op basis van sociaal-economische scheidslijnen**. De koopkracht in Nederland is toegenomen (sinds 2013), maar deze stijging is gepaard gegaan met een lichte stijging in inkomensongelijkheid. Vergeleken met andere welvarende landen ligt de inkomensongelijkheid in Nederland wel onder het gemiddelde. Desalniettemin geven veel Nederlanders aan dat ze zich zorgen maken over toenemende tegenstellingen in Nederland tussen arm en rijk. Veel Nederlanders vinden bovendien dat de verschillen tussen inkomensgroepen te



groot zijn en dat de mensen in hoge en lage sociaal-economische klassen in parallelle werelden leven. Dit kan voor spanning zorgen. Een combinatie met dat er een verhoogd risico is op langdurige armoede bij eerste generatie niet-westerse migranten of vluchtelingen zorgt ervoor dat de spanning op sociaal-cultureel vlak en op sociaaleconomisch vlak vaak langs dezelfde scheidslijnen lopen.

Er zijn significante verschillen tussen sociaaleconomische groepen met betrekking tot hun kwaliteit van leven, gepercipieerde kansen in de samenleving en oordeel over deze samenleving. De Nederlandse samenleving wordt door mensen met hogere inkomens en opleidingsniveaus structureel beter beoordeeld dan door mensen met lage en middeninkomens. Het maatschappelijk onbehagen, verminderd vertrouwen in bedrijfsleven, overheid, Ngo's en media, is juist aanzienlijk hoger bij de lagere sociaaleconomische klasse. Ook het vertrouwen in autoriteiten verschilt per bevolkingsgroep. Er zijn grote verschillen tussen de waardering van politici door mensen met een laag inkomen/lage opleiding en mensen met een hoog inkomen/hoge opleiding, al zijn deze verschillen al wel meerdere jaren stabiel.

## 5.2 Gevolgen van toenemende diversiteit in de samenleving

**Immigratie en integratie** staat in het nationaal probleembesef op de tweede plaats als belangrijk maatschappelijk probleem. Er zijn veel zorgen en onvrede in de maatschappij over omvang en gevolgen van migratie. Ongeveer een vijfde van de Nederlanders ervaart grote spanningen tussen autochtone en allochtone groepen. Het grootste deel van de Nederlanders ervaart dit minder sterk, maar ziet tegelijkertijd de groepsspanningen en polarisatie wel. Dit weerklinkt ook in de groepsgesprekken, waarbij vooral moslims polarisatie ervaren.

Een groot deel van de migranten die zich vestigen in Nederland (zowel regulier als via een asielpcedure) zal zich vestigen in één van de grote steden. Dit betekent een toenemende druk op steden en voorzieningen, door de versnelde groei van deze gebieden en dus hogere eisen op het gebied van infrastructuur en huisvesting.

Er is sprake van een **toenemend belang van primaire identiteit bij jongeren met een migratieachtergrond**. Per context kan het verschillen of iemand zich sterker identificeert met de etnische achtergrond, het Nederlands-zijn of juist met de religieuze achtergrond.

**Buitenlandse mogendheden oefenen druk uit op de relaties tussen groepen.** Landen ondernemen pogingen tot beïnvloeding van geëmigreerde (ex-)landgenoten en/of hen onder druk te zetten; dit zijn onder andere China, Iran, Rusland, en Turkije. Deskundigen tijdens de parlementaire ondervraging over beïnvloeding in Nederland vanuit onvrije landen en naar moskeeën zijn het erover eens dat deze beïnvloeding plaatsvindt. Er is ook buitenlandse financiering aan radicaal-salafisten, zoals investeringen in en de bouw van moskeeën, het financieren van studiebeurzen voor islamstudies aan universiteiten in het buitenland en het leveren van lesmateriaal voor buitenschools onderwijs. Dergelijke steun kan gepaard gaan met inmenging op ideologisch gebied. Deze financiering zorgt er voor dat radicaal-salafistische aanjagers, ondanks dat zij in absolute termen een minderheid vormen, disproportioneel vertegenwoordigd zijn in Nederland. Dit geldt vooral voor hun aanwezigheid online en hun onderwijsactiviteiten. Dit kan ervoor zorgen dat individuen die informatie opzoeken over de islam sneller in aanraking kunnen komen met extremistisch gedachtegoed dat op gespannen orde kan staan met de democratische rechtstaat.

Er lijkt een hogere mate van maatschappelijke tolerantie te ontstaan ten opzichte van extreemrechtse organisaties, aldus experts van het extreemrechtse veld. Dat wil niet zeggen dat deze ideeën meer aanhang of sympathie hebben gekregen, maar vooral dat **extreemrechtse ideeën en activiteiten steeds meer gezien worden als politieke meningen, gelijk elke ander**. Ook verweving van alt-right met 'gewone' politiek is vaker zichtbaar.

We zien een **verschuiving bij extreemrechts van een focus op ras naar een focus op cultuur en identiteit**. Aan de ene kant wordt de eigen identiteit (het 'wij') benadrukt. De eigen culturele waarden worden beschermd, onder andere met het felle verdedigen van het uiterlijk van Zwarte Piet, of het eigen blanke ras. Tegelijkertijd wordt het duale vijandsbeeld (de 'zij') van extreemrechts steeds duidelijker waarneembaar. Aan de ene kant de 'volksvreemde' vijanden (moslims, vluchtelingen, migranten), waarnaast aan de andere kant ook de 'volksvijandige groepen' (de overheid, de 'elite', (extreem)linkse tegenstanders, linkse politici, voorstanders van vluchtelingenopvang en autoriteiten) steeds meer aandacht krijgen van extreemrechtse groepen. Het aantal acties van **identitaire groepen** lijkt toe te nemen in Nederland (en in andere Europese landen). 'Identitaire formaties' streven naar een ideaal van een homogeen Nederlands volk binnen het gebied waar dit volk historisch gezien is gevestigd. De aanhang van verschillende identitaire groepen in Nederland is lastig in te schatten. De groepen zelf bestaan uit maar kleine aantallen actieve leden. De invloed is echter groter via 'slimme communicatie' op sociale media en het internet. Kleine rechts-extremistische groeperingen zijn actief met



intimiderende en radicale acties waarmee ze voor onrust zorgen binnen moslimgemeenschappen.

Opgemerkt moet worden dat er juist in recente jaren een toenemende invloed is van (internationale) bewegingen zoals alt-right waarin ras wel een rol speelt. Het is onzeker of en hoe deze trend zal doorzetten. Door de populariteit van de omvolkingstheorie van de alt-right is er ook juist weer meer nadruk op ras gaan liggen. De vaak uitgesproken racistische en antisemitische ('white supremacy') ideeën van de Alt-Right hebben ook voet aan grond in Nederland gekregen, vooral bij de organisatie Erkenbrand en daaraan gelieerde organisaties. Maar ook sommige andere extreemrechtse organisaties lijken zich veiliger te voelen om binnen het huidige publieke debat antisemitische of racistische onderwerpen aan te snijden.

Naast langer bestaande extreemrechtse organisaties is een toename te zien van los-vaste verbanden van rechts-extremistische activisten. Deze activisten zijn aanwezig bij acties van verschillende organisaties of organiseren zelf acties door een eenvoudige oproep te doen op sociale media. Naast acties op straat, worden er vanuit deze fluïde netwerken ook rechtsextremistische activiteiten ontplooid op internet.

Het jaar 2019 was het jaar van rechts-extremistische aanslagplegers wereldwijd. Vooral de aanslag in Christchurch heeft mensen aangezet tot copycat-gedrag. Copycat-gedrag wordt versterkt doordat aanslagplegers en hun sympathisanten elkaar vinden op rechts-extremistische websites. Van daaruit worden uitnodigingen verzonden naar besloten groepen, waar nog extremere uitlatingen worden gedaan dan op de websites. Extreme content kan mensen aanzetten tot radicalisering of zelfs tot geweld. Het gebruik van sociale media speelt daarbij een rol. Ook Nederlanders zijn lid van dergelijke internationale onlinegroepen. De traditionele extreemrechtse 'offline' scene in Nederland is klein, fragmentarisch en vrijwel geweldloos. Wel bestaat het risico dat extreemrechtse eenlingen geïnspireerd worden of copycat gedrag vertonen naar aanleiding van aanslagen. Verder reageren sommige traditionele rechts-extremisten sterk op de acties van vooral de antiracismeactivisten en zoeken daarbij aansluiting bij lokaal protesterende burgers. Dit heeft al verschillende malen tot (dreiging met) geweld geleid waarbij huisadressen van antiracisme-activisten worden gepubliceerd en bezocht. In de aanloop naar het Sinterklaasfeest van 2019 vonden meerdere gewelddadige escalaties plaats. Zoals geweld tegen leden van Kickout Zwarte Piet. Desalniettemin bleef het in 2019 rustiger dan de jaren daarvoor. Dat komt door de uitgebreide preventieve aanpak van veel lokale autoriteiten.

Tegenover het rechtsextremisme, is er ook een **opkomst van extreemlinkse groeperingen**. Een deel van extreem-links lijkt voorstander van een verharding van de protestacties. Daar staat tegenover dat anderen oproepen om met een alternatief te komen en geen geweld te gebruiken of bedreigingen te uiten. Het is echter nog onduidelijk welke modus operandi links-extremisten bij acties zullen gaan gebruiken; daarvoor is de scene nog onderling te verdeeld. In 2019 zijn bij 'linkse' groeperingen gewelddadigheden uitgebleven. Zij concentreerden zich op activisme in de vorm van demonstraties en burgerlijke ongehoorzaamheid. De acties zijn, mede ten gevolge daarvan, minder persoonsgericht. Op deze manier wordt een grotere groep belangstellenden bereikt, voor wie extremisme een brug te ver is.

Volgens de AIVD gaat thans van het **jihadistisch terrorisme nog steeds de grootste extremistische dreiging** uit. Het jihadistisch-terroristisch dreigingsbeeld wordt nog steeds gekenmerkt door het gevaar van aanslagen in het Westen door enkele mondiaal actieve jihadistische organisaties, lokale netwerken en personen. De NCTV stelt dat in Nederland nog steeds een jihadistische beweging bestaat waarbinnen personen of groepjes een terroristische dreiging vormen. De dreiging is in de afgelopen jaren wel verminderd, wat met name blijkt uit de sterke afname van het aantal aanslagen in Europa. Desondanks heeft Europa, waaronder Nederland, te maken met relatief veel aanhoudingen, het voorkomen van aanslagen en incidenten die aan jihadistisch terrorisme kunnen worden gerelateerd. De dreiging is dus wel verminderd, maar nog steeds aanzienlijk. Naast jhadisme bestaan er andere vormen van extremisme waarbij aanhangers ondermijnende activiteiten rechtvaardigen vanuit hun religieuze overtuiging. Dit is het geval bij salafistische aanjagers die problematische gedragingen vertonen die weliswaar niet strafbaar zijn, maar die haaks staan op onze democratische rechtsorde en deze dreigen te ondermijnen. Op korte of langere termijn kunnen hun activiteiten een ondermijnende werking hebben op het democratisch bestel. Daarnaast kunnen gedragingen van salafistische aanjagers een voedingsbodem zijn voor verdere radicalisering naar het (gewelddadige) jhadistisch gedachtegoed.

Er zijn vormen van **extremisme** die niet passen in het klassieke onderscheid tussen links- en rechtsextremisme, maar **die zich richten op één specifiek onderwerp**. Dat is bijvoorbeeld het geval met de acties tegen windturbines in sommige delen van Nederland, die het laatste jaar zijn geradicaliseerd. Hoewel een klassieke ideologie bij het Nederlandse buitenwettelijke verzet tegen windturbines ontbreekt, is het gelet op de politieke doelen, wel degelijk als extremisme te omschrijven. Een recentelijk voorbeeld is de oploeiende polarisatie tussen boeren en de milieubeweging. Daarnaast is er sprake van vormen van soms



sterke anti-overheidssentimenten, bijvoorbeeld met betrekking tot de stikstofmaatregelen, 5G en het COVID-19-beleid van de overheid. De vraag is in hoeverre deze sterke **anti-overheidssentimenten** op termijn kunnen leiden tot vormen van extremisme (die verder gaan dan activistisch protest dat binnen de kaders van de wet blijft).

### 5.3 Fluctuering van mate van vertrouwen in samenleving, politiek en autoriteiten

Het vertrouwen onder Nederlanders in media fluctueert in de tijd, en staat momenteel onder druk. Er is sprake van een **toename van desinformatie of nepnieuws**, dat vaak gratis is en makkelijk te verkrijgen. Een groot aantal Nederlanders maakt zich zorgen over wat echt en nep is op het internet.

Desalniettemin wordt mainstream nieuws op alle online platforms meer gecirculeerd en verkrijgt meer gebruiksinteractie dan desinformatie of nepnieuws, maar dit geldt niet voor alle specifieke kwesties. Thema's zoals Zwarte Piet en MH17 krijgen aanzienlijke hoeveelheden berichten die eenzijdig of nepnieuws zijn. Dit is ook te zien rond de COVID-19-crisis (zie hoofdstuk 8). Met betrekking tot sociale mediamanipulatie, zijn trol-achtige gebruikers actief rondom meerdere politieke kwesties op sociale media en is er waarschijnlijk sprake van artificiële versterking (nepvolgers). Er is een opkomende eenzijdige en polariserende mediasfeer, die concurreert met de mainstream, in de zin dat ze niet alleen door trol-achtige sociale mediagebruikers, maar ook door reguliere sociale mediagebruikers worden verspreid. Facebook en Twitter zijn platforms met een relatief grote hoeveelheid nep/junknieuws. YouTube is een belangrijke debat-arena voor desinformatie en nepnieuws over maatschappelijke kwesties. Wel nemen grote sociale media bedrijven als Facebook en Twitter steeds meer actie om nepnieuws en desinformatie tegen te gaan. Zie verder paragraaf 7.5.

Zorgwekkend is dat samen met desinformatie en nepnieuws steeds vaker ook achterliggende complottheorieën worden verspreid over thema's zoals migratie, opwarming van de aarde, 5G, vaccinatie, en recent de oorsprong van het coronavirus en kwaadwillende intenties daaromtrent (zie hoofdstuk 8). Vaak wordt daarbij ook twijfel gezaaid over het democratisch gehalte van ons politieke bestel en de overheid en de democratische waarden van onze samenleving. Er is in dit verband sprake van tendensen die op termijn zouden kunnen leiden tot vormen van 'complot-extremisme'.

Het **publieke vertrouwen in de wetenschap in Nederland is relatief hoog, maar verschilt per onderwerp**. Maar bij onderwerpen als klimaat, vaccinaties en recent ook de stikstofuitstoot en COVID-19, zien we groepen met veel wantrouwen in de wetenschap. De redenen waarom groepen wantrouwig zijn verschillend, bijvoorbeeld door politieke, religieuze of juist spirituele overtuigingen.

De overheid draagt zelf soms bij aan polarisatie. Bijna de helft van de ondervraagde Nederlanders zegt zich wel eens gediscrimineerd te voelen door een overheidsinstantie (op grond van leeftijd, geslacht en etnische achtergrond). Dat zet het vertrouwen in de overheid onder druk.

**Georganiseerde, ondermijnende misdaad heeft impact op de samenleving**. Georganiseerde criminaliteit is breed maatschappelijk vertakt en verankerd, met als effect dat een ontwrichtende invloed wordt uitgeoefend op de samenleving als geheel. De echt grote ondermijnende effecten van de georganiseerde misdaad zijn te vinden op een niveau dat de onderwereld allang is ontstegen en zich daarbij probleemloos heeft gemengd met de 'bovenwereld'. Deze menging van onderwereld en bovenwereld is een groot maatschappelijk probleem. De effecten van ondermijnende criminaliteit worden ingedeeld in drie niveaus: slachtoffers, sociale schade en systeem schade. Het is van groot belang dat de overheid op alle niveaus effectief kan ingrijpen en dit ook doet. Wanneer dit niet lukt loopt het vertrouwen van de burger in de overheid schade op.

### 5.4 Koppeling met de risicocategorieën

Eén van de dreigingsthema's, zoals beschreven in de Geïntegreerde Risicoanalyse (GRA) is **Ondermijning democratische rechtsstaat en open samenleving**. Onder dit thema zijn drie risicocategorieën geïdentificeerd die voor de koppeling relevant zijn:

- Niet-gewelddadig extremisme,
- Ondermijnende criminaliteit (enclavevorming),
- Ongewenste buitenlandse inmenging (en beïnvloeding).

Daarnaast is het dreigingsthema **Gewelddadig extremisme en terrorisme** relevant, met de risicocategorieën **Gewelddadig extremisme en Terrorismen**.

**Tabel 5.** Koppeling met risicocategorieën vanuit internationale politiek (donkerblauw=directe koppeling; lichtblauw en cursief=signalering (langetermijn of relevant voor de context))

Dreigings-thema →	Ondermijning democratische rechtsstaat en open samenleving			Gewelddadig extremisme en terrorisme	
	Niet-gewelddadig extremisme	Ondermijnende criminaliteit (enclavevorming)	Ongewenste buitenlandse inmenging	Gewelddadig extremisme	Terrorisme
Risico-categorie →					
Megatrend ↓					
Groeiende ongelijkheid en tegenstellingen tussen bevolkingsgroepen	1			1	
Gevolgen van toenemende diversiteit in de samenleving	2a; 2b; 2c; 2d		3a; 3b	4a; 4b	4a; 4b
Fluctuering van vertrouwen in samenleving, politiek en autoriteiten	5	6	7	5	

1. Toename tegenstelling in de samenleving (sociaal-economisch én sociaal cultureel) i.c.m. ervaren achterstelling van groepen vergroot risico op extremisme. Hier wordt een link gelegd met niet-gewelddadig extremisme, maar door (verdere) escalatie kan dat mogelijk ook leiden tot gewelddadig extremisme.

2. 2a: Toename van (niet-gewelddadig) extremisme dat zich richt op specifieke onderwerpen  
2b: Salafistische aanjagers vergroten onverdraagzaamheid en de voedingsbodem voor (niet-gewelddadig) extremisme.  
2c: Toename belang van primaire identiteit bij migrantengroepen én autochtone groepen vergroot ontvankelijkheid voor (niet-gewelddadig) extremisme.  
2d: Toename van verspreiden van nepnieuws en complottheorieën kunnen leiden tot vormen van 'complotextremisme'.

3. 3a: Pogingen van landen tot beïnvloeding van geëmigreerde (ex-) landgenoten, o.a. China, Iran, Rusland, en Turkije.  
3b: Buitenlandse financiering van salafistische groeperingen.  
4. 4a: Hoewel bronnen vooral aanwijzingen geven voor toename van risico's op niet-gewelddadig extremisme, wordt hierdoor ook het risico vergroot op (verdere) radicalisering tot mogelijk gewelddadig extremisme of terrorisme.  
4b: Extreme content die wordt verspreid op internet en sociale media kan aanzetten tot radicalisering en geweld.

5. Toename van desinformatie nepnieuws kan leiden tot meer wantrouwen in de samenleving, politiek en instanties en op termijn de kans op extremisme bij bepaalde groepen vergroten.  
6. Ondermijnende criminaliteit is breed vertakt en verankerd in de samenleving  
7. Toename nepnieuws op specifieke thema's (bv MH17) door buitenlandse krachten.

Tenslotte zijn er enkele aspecten die minder goed bij de risico-indeling van de GRA passen. Toename van desinformatie en nepnieuws met achterliggende complottheorieën vormt een risico voor het vertrouwen in de democratische instituties en processen en de onafhankelijke media. Daarnaast wordt het waarheidsgehalte van uitspraken van wetenschap en kennisinstituten vaker in

twijfel getrokken (ook door groeperingen die niet als extremistisch te kenschetsen zijn). Het publieke vertrouwen in wetenschappers en kennisinstituten (bijvoorbeeld klimaatwetenschappers of het RIVM) staat onder druk. Dit kan gevolgen hebben voor draagvlak en het gedrag van burgers en leiden tot verzet tegen overheidsbeleid en sociale spanningen.





# 6. Ecologie

De Horizonscan 2019 identificeerde drie megatrends binnen het thema ecologie, die ook het uitgangspunt voor de Horizonscan 2020.

Autonome ontwikkeling	Megatrend
Ecologie	Klimaatverandering
	Biodiversiteit
	Milieudruk

De in 2019 geïdentificeerde megatrends en manifestaties zijn in 2020 onverminderd relevant. In dit hoofdstuk worden de veranderingen in impact en waarschijnlijkheid van de megatrends ten opzichte van de Horizonscan uit 2019 besproken.

## 6.1 Klimaatverandering

In de Horizonscan uit 2019 is aangegeven dat de **opwarming van het klimaat sneller** gaat dan verwacht. Deze versnelling is nog steeds zichtbaar. De versnelling van klimaatverandering wordt veroorzaakt door een toename van de concentraties broeikasgassen in de atmosfeer. De afgelopen vijf jaar was de jaarlijkse stijging voor de belangrijkste broeikasgassen (CO<sub>2</sub>, CH<sub>4</sub> en N<sub>2</sub>O) ongeveer 20 procent hoger dan in de vijf jaar ervoor. Daarbij ligt de Europese Unie (EU) wel op schema om de gestelde emissiereductiedoelstelling voor broeikasgassen van 20% voor 2020 te halen. De doelstelling om voor 2030 tot een vermindering van de uitstoot met 40% te komen, zal volgens de huidige beleidsscenario's naar verwachting niet gehaald worden. De klimaatverandering wordt steeds duidelijker zichtbaar in het dagelijkse weer. Zo was het afgelopen decennium (2010-2019) wereldwijd het warmste decennium ooit. Het jaar 2019 was voor Nederland het zesde warme jaar op een rij, met zowel de warmste winter- als zomerdag sinds het begin van de metingen. Van 23 tot en met 27 juli gold er in het hele land code oranje voor extreme hitte. Ook voor het jaar 2020 wordt een top vijf-positie van warmste jaren ooit verwacht.

De opwarming van het klimaat vergroot de kans op **extrem weer**. Het gaat hierbij bijvoorbeeld om extreme temperaturen en hittegolven. De kans op hittegolven is in Nederland rond de honderd keer waarschijnlijker geworden dan in 1900. Ook de intensiteit neemt toe. Hittegolven zijn door klimaatverandering

tussen de 1,5 en 3 graden warmer geworden. Hitte en droogte zijn de belangrijkste factoren achter natuurbranden, dus ook hierop neemt de kans toe<sup>3</sup>. Daarnaast is een toename in de kans op extreme neerslag en zware stormen te verwachten. Als gevolg daarvan kunnen wateroverlast, overstromingen vanuit de rivieren en schade door hagel of storm ontstaan.

In de Horizonscan 2019 is vooral aandacht besteed aan de gevolgen van hetere, drogere zomers door klimaatverandering, zoals vervroegd overlijden en tegenvallende oogsten. De winters worden echter ook steeds warmer en ook dit heeft belangrijke gevolgen. Door aanhoudend zachte winters neemt de overwinteringskans in de Nederlandse natuur mogelijk toe voor bijvoorbeeld vectoren (ziekteverwekker overdragende teken en muggen), en (insecten)plagen (bijvoorbeeld de eikenprocessierups). Ook het pollenseizoen wordt langer, waardoor hooikoortsklachten langer kunnen gaan duren. Het langdurig uitblijven van een aaneengesloten periode van kou is daarom mogelijk nog belangrijker voor de natuur en volksgezondheid dan de toenemende hitte in de zomer.

Klimaatverandering is daarnaast, voornamelijk in ontwikkelingslanden, in toenemende mate een factor in het veroorzaken, versterken en versnellen van gewapende conflicten. Klimaatverandering heeft in deze landen onder andere impact op de landbouwproductie, aanbod van drinkwater, de economie in het algemeen en op ongelijkheden tussen groepen. Deze factoren kunnen op hun beurt andere conflictfactoren beïnvloeden en op die manier het risico op geweld laten toenemen. Toenemende (gewapende) conflicten in ontwikkelingslanden kunnen de **instabiliteit rondom Europa** versterken.

Wanneer wereldwijd klimaatbeleid faalt, wordt de kans groter dat landen **geo-engineering** gaan inzetten om de gevolgen van klimaatverandering te bestrijden. Dit brengt het risico op verdere verstoring van ecosystemen met zich mee. Ook kan geo-engineering zorgen voor **geopolitieke spanningen**.

In de Horizonscan uit 2019 is genoemd dat de **energielevering afhankelijker** wordt van het weer. Dit wordt versterkt door de

<sup>3</sup> In april 2020 heeft de grootste natuurbrand in Nederland ooit gewoed in de Deurnsche Peel. 800 hectare natuurgebied is hierbij verwoest.



verdere verduurzaming van de energievoorziening (wind- en zonne-energie). Op middellange termijn (vanaf 2025) kunnen hierdoor leveringszekerheidsrisico's ontstaan, waardoor Nederland voor elektriciteit afhankelijker wordt van import. Op de lange termijn (vanaf 2030) wordt verwacht dat bij extreme weersituaties niet aan de norm voor energielevering, als vitale infrastructuur, voldaan kan worden.

Een bijkomend aspect van de energietransitie is de weerstand die het bij delen van de bevolking kan oproepen. Ook afgelopen periode waren er voorbeelden van protesten tegen de komst van windturbines. Dit kan leiden tot confrontaties tussen voor- en tegenstanders en bijdragen aan polarisatie.

Voor de risico's op de lange termijn is verder de **zeespiegelstijging** van belang. De zeespiegel stijgt de laatste jaren twee keer zo snel als in de twintigste eeuw. De versnelling wordt veroorzaakt door het smelten van de ijskappen in Groenland en Antarctica. In oktober 2019 bereikte het wereldwijde gemiddelde zeeniveau zijn hoogste waarde sinds het begin van de metingen in 1993. De stijging van de zeespiegel vergroot de kans op overstromingen uit zee. In Nederland zijn de gevolgen van de zeespiegelstijging tot nu toe beperkt. Dit heeft onder andere te maken met de investeringen die in het verleden gedaan zijn om de Nederlandse kust te beschermen tegen overstromingen, bijvoorbeeld vanuit het Deltaprogramma. Wel zijn er signalen dat de druk op het watersysteem toeneemt. Een voorbeeld hiervan is dat door de zeespiegelstijging het verschil in waterpeil tussen de Waddenzee en het IJsselmeer afneemt. Hierdoor kan minder water op de Waddenzee worden geloosd, terwijl een hogere aanvoer uit de IJssel te verwachten is door toenemende neerslag. Dit zorgt mogelijk voor overstromingsrisico's stroomopwaarts in de IJssel. Vooralsnog valt deze ontwikkeling binnen de veiligheidsmarges van het huidige watersysteem.

## 6.2 Biodiversiteit

In de Horizonscan 2019 zijn twee belangrijke manifestaties benoemd onder de megatrend biodiversiteit, namelijk de afname in biodiversiteit en de toename in blootstelling aan nieuwe ziekteverwekkers.

De wereldwijde afname van biodiversiteit is nog steeds actueel. De Nederlandse Living Planet Index (LPI) beschrijft biodiversiteitstrends in Nederland. Wanneer deze worden opgedeeld naar ecosystemen blijkt dat de toename in biodiversiteit vooral plaatsvond in zoet water en moeras, maar in agrarische gebieden en in open natuurgebieden (hei, duin en half natuurlijk grasland samen) is juist sprake van afname. Het huidige natuurbeleid dringt de afname van biodiversiteit terug, maar is onvoldoende om een absolute afname tegen te houden. In de GRA 2019 wordt de afname van biodiversiteit genoemd als een mogelijke bedreiging voor de **voedselvoorziening** op langere termijn. Een voorbeeld hiervan is de mogelijke afname in bestuiving door de toename in bijensterfte en mogelijke verslechtering van de insectenpopulaties. Dit is nog steeds actueel.

In november 2019 is een tweede geval van Tekenencefalitis (hersenvlies)ontsteking vastgesteld in Nederland. Deze vector overdraagbare aandoening wordt veroorzaakt door het TBE, tick-borne encephalitis-virus, wat wordt overgebracht via tekenbeten. Het lijkt er op dat de kans op vestiging van nieuwe vectoren, die dergelijke nieuwe ziekteverwekkers kunnen overdragen, is toegenomen. Maar of deze trend zich doorzet en zich zal vertalen in een toename van het aantal en grootte van uitbraken van zoönosen (ziekteverwekkers afkomstig van dieren en overdraagbaar op mensen) is nog moeilijk te voorspellen. Daarnaast heeft het aantal gevallen van de Papegaaizenziekte (psittacose), gesignaleerd gedurende de winterperiode 2019/2020, zich doorgezet in de eerste maanden van 2020. Deze infectieziekte uit zich in een vorm van longontsteking en wordt veroorzaakt door een bacterie (Chlamydia psittaci) die bij vogels kan voorkomen.

De voornaamste gebeurtenis met betrekking tot de toename in blootstelling aan nieuwe ziekteverwekkers binnen deze manifestatie is de wereldwijde verspreiding (pandemie) van het virus SARS-CoV-2, een mens overdraagbaar coronavirus dat de infectieziekte COVID-19 veroorzaakt. Dit heeft al geleid tot meer dan 18 miljoen ziektegevallen en 700.000 doden wereldwijd (peildatum 1 augustus 2020). In Nederland zijn er in dezelfde periode rond de 55.000 ziektegevallen en ruim 6.000 doden gemeld, als gevolg van COVID-19. Hoewel de uitbraak van COVID-19 vermoedelijk een zoönotische oorsprong heeft, met als vermoedelijke eerste bron een markt in China, zijn mensen momenteel de primaire bron van verspreiding. In hoofdstuk 8 wordt verder ingegaan op COVID-19 binnen de scope van deze Horizonscan.

## 6.3 Milieudruk

Zoals in de Horizonscan 2019 is genoemd neemt de milieudruk de laatste decennia af, maar kunnen activiteiten met kortetermijn voordelen leiden tot schade op lange termijn.

De eerste manifestatie onder milieudruk betreft de luchtkwaliteit. Er wordt al langere tijd op ingezet om de luchtkwaliteit te verbeteren. Voor Nederland geldt dat in 2018 in vrijwel heel het land de berekende concentraties stikstofdioxide en fijnstof onder de Europese grenswaarden lagen. De verwachting is dat de gemiddelde concentratie waar mensen aan blootgesteld worden voor beide stoffen de komende jaren nog verder afneemt. Lagere concentraties stikstofdioxide en fijnstof verbeteren de volksgezondheid. Op dit moment is het nog steeds zo dat Nederlanders gemiddeld negen maanden korter leven door luchtverontreiniging en overlijden jaarlijst circa 11.000 mensen vroegtijdig.

Luchtverontreiniging heeft ook nadelige gevolgen voor biodiversiteit en ecosystemen. Ongeveer 62% van het ecosysteem van Europa wordt blootgesteld aan te hoge stikstofconcentraties,



wat tot eutrofiëring leidt.<sup>4</sup> In de Horizonscan 2019 is reeds vermeld dat door de uitspraak van de Raad van State op basis van de Nederlandse Programmatische Aanpak Stikstof geen vergunningen meer mogen worden verleend die extra neerslag van stikstof in Natura 2000-gebieden tot gevolg hebben. De situatie heeft uiteindelijk geleid tot een 'stikstofcrisis'. Door de uitspraak zijn 18.000 projecten in meer of mindere mate geraakt en een deel hiervan kan geen doorgang vinden. Het gaat hierbij onder andere om vergunningaanvragen voor veehouderijen, bedrijventerreinen, woningbouw of nieuwe wegen. Eind 2019 is een spoedwet aangenomen om de bouw van woningen voor 2020 weer op gang te krijgen. De voorgenomen plannen vanuit het kabinet om de stikstof-uitstoot van onder andere de landbouw- en bouwsector te verminderen, hebben geleid tot meerdere protesten. De protesten zorgden voor verkeersoverlast in vrijwel heel Nederland. Daarnaast leidt het tot polarisatie tussen voor- en tegenstanders. De protesten hebben ervoor gezorgd dat een aantal provincies de nieuwe stikstofregels hebben ingetrokken.

De tweede manifestatie is **waterkwaliteit**. Zoals reeds in de Horizonscan 2019 is aangegeven, geldt voor Nederland dat niet alle wateren een goede ecologische en chemische toestand hebben. Dit beeld is niet veranderd. Dit komt onder andere door belasting van het oppervlakte- en grondwater

door landbouwactiviteiten (stikstof, fosfaat, gewasbeschermingsmiddelen), infrastructuur (PAK, zware metalen) en nutriënten in rioolwater zuiveringsinstallaties.

Ook de **kwaliteit van de drinkwaterbronnen staat onder druk**. Grondwater dat voor drinkwater wordt gebruikt raakt op steeds grotere diepten en met steeds meer stoffen verontreinigd. Het gaat hierbij vooral om vervuiling met nitraat, bestrijdingsmiddelen, oude bodemverontreinigingen en verzilting. Ook het oppervlaktewater dat als drinkwaterbron wordt gebruikt heeft te maken met meerdere bedreigingen. Hierbij gaat het om bestrijdingsmiddelen, verzilting, medicijnresten en opkomende stoffen. Ook microplastics en nanomaterialen kunnen een bedreiging vormen. Klimaatverandering zal de waterkwaliteit waarschijnlijk negatief beïnvloeden door meer verzilting en minder verdunning van verontreiniging door lagere rivierafvoeren. De verwachting is dat de drinkwaterkwaliteit in de toekomst verder zal afnemen.

## 6.4 Koppeling met de risicocategorieën

Onder het thema ecologie zijn een aantal specifieke trends te zien die verschillende risico's kunnen beïnvloeden. Deze zijn opgenomen in de volgende tabel.

**Tabel 6.** Koppeling met risicocategorieën vanuit ecologie (donkerblauw=directe koppeling; lichtblauw en cursief=signalering (langetermijn of relevant voor de context))

Thema	Bedreigingen voor gezondheid en milieu		Natuurrampen		
	Infectieziekten humaan	Dierziekten en zoönose	Extreem weer	overstroming	natuurbrand
Risico-categorie →					
Megatrend ↓					
Klimaatverandering	1	1	2	3	4
Biodiversiteit		5			
Milieudruk	6				

Thema	Verstoring vitale infrastructuur	Ondermijning democratische rechtsstaat en open samenleving	Bedreigingen internationale vrede en veiligheid	
			Instabiliteit rondom Europa	Veiligheidsarrangementen onder druk (NAVO, EU)
Risico-categorie →	Verstoring vitale infrastructuur	Niet-gewelddadig extremisme		
Megatrend ↓				
Klimaatverandering	7	8	9	10
Biodiversiteit	11			
Milieudruk	12	13		

<sup>4</sup> Eutrofiëring is 'verrijking' van oppervlaktewater met nutriënten (vaak via de bodem). Dit gaat vaak met zulke enorme hoeveelheden dat er te veel nutriënten in het oppervlaktewater terecht komen.



1. Aanhoudende zachte winters verlengen pollenseizoenen waardoor hooikoortsklachten langer duren. Ook neemt de overwinteringskans voor vectoren en plagen mogelijk toe. Dit zijn vooral relevante signalen en geen directe koppeling.
2. Opwarming van het klimaat vergroot de kans op extreem weer. Het gaat hier specifiek om een toename in waarschijnlijkheid. Het is wel de verwachting dat intensiteit en daarmee ook de impact van hittegolven toeneemt.<sup>5</sup>
3. Zeespiegelstijging als gevolg van klimaatverandering versnelt, met druk op het watersysteem tot gevolg: rivieren wateren minder makkelijk af, waardoor landinwaarts het overstromingsrisico vergroot. Het gaat wederom vooral om ene toename van waarschijnlijkheid.
4. Hitte en droogte zijn de belangrijkste factoren achter natuurbranden. Door het opwarmende klimaat neemt de kans hierop ook toe.
5. Toegenomen overwinteringskans van vectoren hebben mogelijk gevolgen voor de volksgezondheid. Er is een lichte toename in het aantal ziektegevallen door blootstelling aan nieuwe ziekteverwekkers, zoals TBEV en Chlamydia psittaci. Dit is onderdeel van een sluimerend proces.
6. Luchtkwaliteit verbetert. Voor zowel stikstofdioxide als voor fijnstof is de verwachting dat de gemiddelde concentratie waar mensen aan blootgesteld worden de komende jaren afneemt. Dit heeft positieve gevolgen volksgezondheid. Nog wel vroegtijdig overlijden.
7. Energielevering wordt door verdere verduurzaming afhankelijker van het weer met kans op leveringszekerheidsrisico's.
8. Klimaatbeleid en energietransitie kunnen leiden tot protesten en confrontaties van voor- en tegenstanders.
9. Klimaatverandering vormt in toenemende mate een factor in het versterken van gewapende conflicten. Toenemende (gewapende) conflicten in ontwikkelingslanden kunnen de instabiliteit rondom Europa versterken.
10. Als klimaatbeleid faalt, wordt de kans groter dat landen geo-engineering gaan inzetten met risico op geopolitieke spanningen. Hierdoor komen ook mogelijk veiligheids-arrangementen zoals de NAVO onder druk te staan waardoor
11. Afname van biodiversiteit nog steeds actueel. Toename in bijensterfte vormt mogelijk een bedreiging voor voedselvoorziening.
12. Kwaliteit van drinkwaterbronnen staat onder druk door vervuiling grond- en oppervlaktewater. De beschikbaarheid van drinkwater kan in het geding komen. Dit is met name het geval in combinatie met extreme droogte waardoor vervuiling minder kan verdunnen in het water.
13. Milieubeleid (zoals beleid met betrekking tot stikstof) leiden tot protesten en demonstraties.

Tenslotte merken we op dat we bij ecologie te maken hebben met sluimerende processen die pas op langere termijn effect zullen hebben. Deze sluimerende processen worden gekenmerkt door niet-stabiele evenwichten. Dat wil zeggen dat wanneer het proces een kritisch punt heeft bereikt, dit onomkeerbaar wordt en niet of nauwelijks meer veranderd

kan worden. Denk hierbij aan de onomkeerbaarheid van de verstoring van ecosystemen door het wegvallen van specifieke elementen door de afname in biodiversiteit, of het smelten van de poolkappen en de invloed hiervan op stromingen in de oceanen en temperaturen op aarde.

<sup>5</sup> Gezien de opwarming van het klimaat, die ook in Nederland steeds zichtbaarder wordt in het dagelijks leven wordt een scenario van hevige sneeuwval en ijzel, zoals deze in de geïntegreerde risicoanalyse is opgenomen, steeds minder waarschijnlijk. Dit scenario wordt in een komende analyse dan ook geactualiseerd.

# 7. Informatietechnologie

Het domein 'Informatietechnologie' (IT) omvat technologieën en producten die data en informatie verspreiden, verwerken, opslaan en aanbieden. In de praktijk vallen hier voornamelijk digitale diensten en producten onder, en de netwerken en systemen die een digitale samenleving mogelijk maken.

Het is niet altijd even makkelijk om aan te geven welke technologieën of producten wel of niet onder de noemer Informatietechnologie vallen. Steeds meer systemen hebben een digitaal component aan boord, van keukenapparatuur tot grootschalige industriële systemen. Dit maakt potentieel elk product dat een online verbinding heeft een informatietechnologisch product. Autonome systemen zijn bijvoorbeeld geen typisch IT-product, maar kunnen alleen bestaan bij gratie van IT, en zijn daarom een onderwerp van belang. Daarnaast wordt Kunstmatige Intelligentie (*Artificial Intelligence*, AI) meestal niet gezien als een Informatietechnologie, maar algoritmes uit de AI zijn in hoge mate verantwoordelijk voor veel van de huidige IT-ontwikkelingen en derhalve van belang voor toekomstverkenningen.

Voor de Horizonscan 2020 kijken we naar actuele ontwikkelingen in het digitale domein, zoals online diensten, mediaplatformen en trends. Ook wordt gekeken naar fysieke productgroepen die een sterk IT-component hebben, zoals onbemande luchtvaartuigen ('drones') en *Internet of Things* (IoT) producten. Daarbij kijken we breed naar technologische ontwikkelingen die bijdragen aan deze producten (zoals AI) en het gebruik van deze producten door actoren in de samenleving.

Hieronder worden de resultaten van de Horizonscan 2020 toegelicht, in vergelijking met de resultaten van de Horizonscan 2019. Binnen het domein informatietechnologie zijn er vier megatrends meegenomen.

Autonome ontwikkeling	Megatrend
Informatietechnologie	Autonomie van informatietechnologie
	Cognitie van informatietechnologie
	Verbondenheid en verwevenheid van informatietechnologie (vernetting)
	Afhankelijkheid van informatietechnologie

Omdat deze trends veelal gezamenlijk optreden is er (in tegenstelling tot de voorgaande hoofdstukken) voor gekozen om in een aparte paragraaf (paragraaf 7.5) in te gaan op enkele relevante manifestaties voor de nationale veiligheid. Tenslotte is, waar relevant, de koppeling gemaakt met risicocategorieën zoals die in de Geïntegreerde risicoanalyse zijn geïdentificeerd.

## 7.1 Autonomie

Met de megatrend autonomie bedoelen we dat IT-systemen steeds onafhankelijker van de mens kunnen opereren en beslissingen nemen. Waar we in de Horizonscan 2019 hebben gezien dat er in de samenleving steeds meer een debat ontstaat over de grenzen van autonome systemen, zien we dat er nu ook op het gebied van aankomende wet- en regelgeving en beleid steeds meer aandacht wordt besteed aan de mate van autonomie van systemen. Doordat steeds meer autonoom functionerende IT-systemen in de praktijk worden toegepast, worden de implicaties duidelijker voor een breder publiek. Deze toepassingen worden gevoed door de doorgaande ontwikkelingen op het gebied van AI-technologie, internet-diensten en rekenkracht.

Naast dat de discussie doorlopend wordt gevoerd over de grenzen van autonome systemen en wat 'betekenisvolle menselijke controle' betekent, zien we ook vragen ontstaan op het gebied van verantwoordelijkheid, aansprakelijkheid, ethiek en privacy. Dit laatste manifesteert zich duidelijk ten tijde van de COVID-19-crisis: in hoeverre willen burgers persoonlijke informatie zoals locatiegegevens prijsgeven aan een app voor



het kunnen monitoren van de verspreiding van het corona-virus? De discussie rondom IT en privacy wordt steeds breder in de maatschappij gevoerd omdat burgers de implicaties van IT beter gaan begrijpen door concrete toepassingen zoals de voorgestelde corona-app.

## 7.2 Cognitie

Onder de megatrend cognitie binnen IT verstaan we het gegeven dat IT-systemen in toenemende mate zelflerend worden en patronen kunnen herkennen in grote hoeveelheden data. Ook hier zien we dat door het toegenomen dagelijks gebruik van cognitieve systemen, bepaalde kwetsbaarheden in systemen zichtbaar worden. Dit is een voortzetting van de trend zoals die ook in 2019 is toegelicht. Algoritmes in systemen kunnen bijvoorbeeld bepaalde *biases* in zich meedragen en bovendien fouten maken.

Virtuele assistenten of spraakassistenten (denk aan Google Assistant, Apple Siri) worden ook in Nederland steeds vaker gebruikt. De technologie omtrent spraakherkenning ontwikkelt zich doorlopend, onder andere op het gebied van het herkennen van intenties (wanneer een opdracht niet expliciet wordt benoemd, maar een virtuele assistent de opdracht wel begrijpt). Mede door dit toegenomen gebruik en de enorme hoeveelheid data die hierdoor wordt verkregen, komen ook ethische vraagstukken aan het licht: audio opgenomen door spraakassistenten wordt geanalyseerd om de algoritmes onder diezelfde *smart speakers* te verbeteren. De discussie over kwetsbaarheden in cognitieve systemen en dataverzameling voor het verbeteren van lerende systemen is niet nieuw, maar door de toepassingen in de praktijk worden de vraagstukken concreter. We zien dan ook een toenemend belang van 'explainable AI': we willen weten wat de achterliggende beweegredenen zijn (geweest) dat een systeem een bepaalde beslissing heeft genomen, mede om bias in een beslissysteem te voorkomen. Men wil weten wat er in de 'black box' van systemen zoals SyRI (voor het detecteren van uitkeringsfraude) gebeurt.

## 7.3 Vernetting

De vernetting van systemen in onze samenleving blijft een relevante trend. In de Horizonscan 2019 was al geconstateerd dat digitalisering van onze samenleving leidt tot waardevolle nieuwe diensten, maar ook tot vragen over beheersbaarheid, bestuurbaarheid en kwetsbaarheid. Deze vragen blijven ook in 2020 onverminderd belangrijk.

De vernetting en digitalisering van de samenleving maakt dat we kwetsbaarder worden voor digitale verstoringen en 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.

Digitalisering zorgt voor de nodige vragen rondom beheersbaarheid van systemen, het voorkomen van het lekken van persoonlijke data en het zorgdragen voor transparantie over bij beslissingen gehanteerde afwegingen en databronnen. De Autoriteit Persoonsgegevens waarschuwt steeds nadrukkelijker voor gevaarlijke situaties als persoonsdata in verkeerde handen komt, bijvoorbeeld door mobiele apps die persoonlijke data zonder toestemming versturen. Niet alleen buitenlandse apps zoals TikTok maken zich schuldig aan het ongeoorloofd gebruiken van persoonsgegevens. Ook grote platformen zoals Google en apps van Nederlandse origine maken zich nog steeds te weinig sterk voor het beschermen van privacy en persoonsgegevens, met potentieel grote risico's voor individuen en groepen. Ook kennen veel IT-systemen nog steeds ingebouwde 'achterdeurtjes' ten behoeve van systeembeheer, maar die zorgen ook voor inherente kwetsbaarheden in het systeem.

## 7.4 Afhankelijkheid

In eerdere horizonscans is al geconstateerd dat digitalisering een gestaag proces is: de samenleving maakt in steeds grotere mate gebruik van digitale diensten en IT, en wordt daar steeds afhankelijker van. Ook bedrijven en vitale infrastructuren maken steeds meer gebruik van diensten van derden, zoals *cloud* opslag, *virtual private networking* systemen en data-analyse systemen. Hiermee creëren ze een afhankelijkheid van derde partijen.

Eenzijds manifesteert de trend afhankelijkheid zich in de macht van enkele grote technologiebedrijven, waardoor samenlevingen afhankelijk zijn van de producten en diensten van een select aantal aanbieders. Hierdoor bezitten staten geen volledige digitale autonomie en zijn ze in zekere mate afhankelijk van de grillen van grote technologiebedrijven. Wanneer dominante technologiebedrijven wel onder controle van een staat komen, dan heeft dat als implicatie dat IT-producten potentieel tot machtsinstrument verworden. Zie ook paragraaf 3.2.

Anderzijds manifesteert afhankelijkheid zich in de gedigitaliseerde samenleving. De hedendaagse maatschappij kan eigenlijk niet meer zonder IT-systemen functioneren, wat wederom werd benadrukt gedurende de COVID-19-crisis, met name door het thuiswerken (zie verder hoofdstuk 8).

Als reactie op de steeds verdergaande afhankelijkheid van digitale diensten (en dus het internet), zien we dat staten pogen een 'nationaal internet' op te zetten, een fenomeen dat ook wel wordt geduid middels de term 'splinternets'. Het 'segmenteren' van het internet geeft staten zoals Rusland en China een grote



macht over het binnenlands internetgebruik. Dit kan middels het afschermen van bepaalde sites of *content* (denk aan de *Great Firewall* in China), maar ook door het technisch omleiden van het dataverkeer (Rusland). Om een daadwerkelijk nationaal internet te hebben, moet een land zich ontkoppelen van het wereldwijde domeinnaamsysteem (DNS). Dit is absoluut geen gemakkelijke opgave, maar ook niet onmogelijk. De impact van het fenomeen splinternets is op dit moment nog niet volledig bekend, maar de gevolgen van mondiale technologiestrijd kunnen door de vergaande afhankelijkheid van IT-systemen verstrekkend zijn voor de nationale veiligheid.

## 7.5 Nadere uitwerking van enkele manifestaties

Uit de beschrijving van de vier trends in de voorgaande paragrafen volgt een algemeen beeld van ontwikkelingen op het terrein van IT. Naast vragen rondom de grenzen van autonome systemen, aansprakelijkheid en ethiek zijn ook aspecten als toenemende kwetsbaarheden, onvoorziene cascade-effecten, nieuwe aanvalsroutes en werkwijzen en afhankelijkheid van derde partijen naar voren gekomen. In deze paragraaf wordt een concretisering hiervan gemaakt door in te gaan op enkele manifestaties die relevant zijn voor de nationale veiligheid. Hierbij wordt een link gelegd met de dreigingsthema's uit de GRA 2019.

### Afhankelijkheden en cascade-effecten bij vitale infrastructuur

De vitale infrastructuur van Nederland is in steeds hogere mate afhankelijk van informatie- en communicatie technologie. Het toenemend gebruik van IT technologie in systemen zoals gebruikt in de vitale processen is in de basis gericht op het verbeteren van het functioneren van deze systemen. Hierbij gaat het niet alleen om IT, maar ook om Operationele Technologie (ten behoeve van bedrijfsvoering en de kantooromgeving). Trends op het gebied van IT hebben daarom impact op de risicocategorie **verstoring vitale infrastructuur**. Dreigingen of risico's die samenhangen met de IT-innovaties in vitale processen leiden niet automatisch tot een groter risico op verstoring van vitale infrastructuur, omdat andere kwetsbaarheden juist worden weggenomen door deze innovaties. Doordat het voor een bedrijf efficiënter is om met één type systeem te werken en het bovendien niet gemakkelijk is om snel een alternatief systeem uit te rollen in het geval van een incident, zitten ook sommige vitale infrastructuren in een afhankelijkheidspositie.

Verder zorgt vernetting van systemen ervoor dat er risico's zijn op cascade-effecten. Door systemische afhankelijkheden kan verstoring van één systeem leiden tot een kettingreactie van verstoring in andere systemen. Deze kwetsbaarheid kan benut worden door kwaadwillenden met gecoördineerde cyberaanvallen. Er is wel steeds meer bewustwording van

risico's door vernetting en er worden ook redundante alternatieven ingebouwd in sommige sectoren. Desondanks zijn er vervolgens alsnog functionele afhankelijkheden waardoor de impact toch doorwerkt. In theorie betekent dit dat er een kwetsbaarheid ontstaat die kan worden uitgebuit door kwaadwillenden.

Naast het inbouwen van redundantie in systemen, zien we ook dat er meer aandacht is voor herstelvermogen, in het geval dat een incident zich voordoet. Het is niet alleen belangrijk om incidenten te voorkomen, maar ook de weerbaarheid en veerkracht van systemen (en sectoren) om een incident te boven te komen te verhogen.

Tenslotte worden er door de toenemende cognitie, autonomie en complexiteit in IT-systemen ook nieuwe typen kwetsbaarheden geïntroduceerd die kunnen leiden tot technisch falen. Bovendien is het niet altijd duidelijk op welke manier het beste ingegrepen kan worden bij uitval, omdat de gevolgen, mede door vernetting, niet goed te overzien zijn. De complexiteit van IT-netwerken maakt het voorkomen van dreigingen en effectief reageren op verstoringen een grote uitdaging.

### Nieuwe aanvalsmogelijkheden, middelen en werkwijzen

De trends van autonomie en cognitie zorgen (in combinatie met vernetting en afhankelijkheid van IT-systemen) voor andere aanvalsmogelijkheden, middelen en werkwijzen (zie ook paragraaf 3.2). Malware wordt steeds geavanceerder, maar deze ontwikkeling gaat gestaag en is op zichzelf niet nieuw. Kwaadwillenden innoveren als de perceptie bestaat dat ontwikkeling van nieuwe aanvalssystemen lonend is. Er is bijvoorbeeld een ontwikkeling gaande richting het geautomatiseerd zoeken naar kwetsbaarheden in systemen. Als het voor kwaadwillenden lonend is om met nieuwe, geavanceerdere middelen (zoals zelflerende aanvalssystemen, of autonome malware) een aanval te plegen, of via een andere aanvalsroute (gefaciliteerd door vernetting) een aanval te plegen, zullen zij investeren in deze ontwikkelingen. Het is lonend op het moment dat maatregelen die tegen bekende aanvalsmiddelen zijn genomen kunnen worden omzeild, of wanneer het bijvoorbeeld goedkoper of gemakkelijker is.

Informatietechnologische ontwikkelingen hebben uiteraard ook effect op de verdediging tegen **cyberdreigingen**, maar de vraag is of die gelijk oplopen. Cybersecurity maatregelen zijn vaak reactief en het beeld is dat kwaadwillenden telkens weer nieuwe manieren vinden om kwetsbaarheden uit te buiten. De wendbaarheid van kwaadwillenden is in die zin sneller dan de tegenmaatregelen. Bovendien hoeft een kwaadwillende maar één keer een kwetsbaarheid te vinden die gemakkelijk is uit te buiten, waar cybersecurity professionals continu bezig moeten zijn met het afdekken van allerlei typen mogelijke risico's. Daarmee heeft deze situatie alle kenmerken van een digitale wapenwedloop.

De steeds verdere digitalisering van de samenleving heeft impact op de risicocategorie **digitale sabotage**. Door vergaande vernetting hoeft een systeem of aanbieder van een dienst niet meer zelf gesaboteerd te worden, maar kan verstoord raken doordat gekoppelde systemen of diensten verstoord zijn (*supply chain risico's*). Kwaadwillenden gaan op zoek naar de zwakke schakel in de keten en door vernetting zijn er feitelijk meer mogelijkheden tot het vinden en misbruiken van die zwakke schakel. Echter, het via een ander systeem of bedrijf binnenkomen in het gewenste systeem zal alleen gebeuren wanneer het lonend is om dat te doen. Als er een gemakkelijkere aanvalsroute is, zal die route de voorkeur krijgen. We zien een steeds verdergaande professionalisering bij cybercriminelen, wat het volwassen worden van het *cybercrime-as-a-service* model, waarbij kwaadwillenden derden betalen om cyberaanvallen uit te voeren, in de hand werkt.

Ook voor wat betreft de risicocategorie **aantasting van het functioneren van het internet** zorgen IT-ontwikkelingen voor zowel nieuwe bedreigingen, als nieuwe beschermingen. Kwaadwillenden maken steeds vaker gebruik van autonoom opererende programma's om grootschalige aanvallen uit te voeren op internetdiensten. Bij DDoS (*Distributed Denial of Service*) aanvallen worden zeer grote hoeveelheden met het Internet verbonden apparaten ingezet om diensten te overbelasten met dataverkeer en deze diensten hierdoor uit te schakelen. Hoewel er steeds meer aandacht is voor *security by design* in IoT apparaten, zien we dat DDoS aanvallen niet in complexiteit zijn toegenomen. Deze aanvallen richten zich ook steeds vaker op de basisstructuren van het internet, zoals DNS servers, routing netwerken en dataopslag faciliteiten.

We zien daarnaast een toenemend gebruik van clouddiensten, waarbij een groot deel van de diensten in kleine handen is. Bedrijven die dergelijke diensten aanbieden, hebben beveiliging van de cloud als topprioriteit, waardoor de informatie die in de cloud opgeslagen is, vaak veiliger is dan op de systemen van het bedrijf dat gebruik maakt van de clouddiensten. Aan de andere kant, door homogenisering van de cloud-based pakketten, is het rendabel voor kwaadwillenden om op zoek te gaan naar de kwetsbaarheden in de systemen van de aanbieders (Windows, IOS) en gemakkelijker omdat er maar weinig verschillende software bestaat.

### **Autonome onbemande systemen**

Ontwikkelingen op het gebied van IT drijven in belangrijke mate de ontwikkeling richting autonome onbemande systemen, onder andere binnen het militaire domein, en beïnvloeden dus de risicocategorie **militaire dreigingen**. Deze trend richting autonomie in het militaire domein is al jaren te zien en is dus niet nieuw. Onbemande systemen zoals onbemande luchtvaartuigen worden al toegepast ten behoeve van bijvoorbeeld *Command, Control, Communications, Computers, Intelligence, Surveillance en Reconnaissance* (C4ISR) activiteiten, maar ook om vanaf een afstand een doel uit te schakelen (waarbij een militair

letterlijk en figuurlijk 'aan de knoppen' zit). Er gebeurt veel op het gebied van autonomie binnen het militaire domein en hoewel gestaag, kan juist de combinatie van verschillende doorgaande technologische ontwikkelingen tot onverwachte uitkomsten leiden.

Ook het debat over onbemande wapensystemen ("killer robots") en de ethiek rondom het toepassen van AI in militaire systemen is al langer gaande. We zien dat er steeds meer autonome systemen operationeel worden ingezet, waarbij enkele systemen (zoals 'kamikaze drones' waarbij het onbemande systeem zichzelf detoneert op het doelwit) ook daadwerkelijk als autonome wapensystemen worden ingezet. Hierbij moet opgemerkt worden dat onbemande (wapen) systemen vaak wel autonoom (zonder menselijke inmenging) kunnen opereren, maar niet intelligent (cognitief) zijn. Belangrijk is dat cognitie in systemen (zoals zelflerend vermogen) niet hoeft te betekenen dat systemen zelf beslissingen maken. In militaire context is nog steeds de heersende opvatting dat het noodzakelijk is dat de mens bepaalt wat de uitkomsten zijn van het opereren van het systeem (de doelen, het 'wat'), maar dat een systeem zelf kan bepalen op welke manier dat gebeurt (de beste manier, het 'hoe').

### **Des- en misinformatie**

Diverse toepassingen van IT worden gebruikt om snel, gericht en in grote hoeveelheden informatie te verspreiden. Dat betekent ook dat dergelijke technologie kan worden misbruikt ten behoeve van het verspreiden van des-/misinformatie, propaganda en extremistisch gedachtegoed. Dergelijke beïnvloeding middels online (sociale) media wordt van toenemend belang en raakt de dreigingsthema's **Ondermijning van de democratische rechtstaat en Extremisme/terrorisme**. Berichten kunnen steeds sneller en breder gedeeld worden, waarmee groeperingen steeds meer kans krijgen om propaganda te verspreiden, of gelijkdenkenden aan te trekken. Niet alleen kan online een bepaald gedachtegoed worden gedeeld, ook het verspreiden van des-/misinformatie is een tactiek van onder meer hybride actoren om verdeeldheid en onrust te zaaien op onderwerpen waar al sociale polarisatie over bestaat (denk aan het uitbuiten van de vluchtelingencrisis). Ook complottheorieën zijn, hoewel het fenomeen zeker niet nieuw is, gemakkelijker en sneller te verspreiden. Een goed voorbeeld hiervan is de complottheorie dat er een verband is tussen 5G en de verspreiding van het coronavirus (zie hoofdstuk 8).

Zoals ook in de Horizonscan 2019 is geconstateerd, zijn zogenoemde *deepfakes* in opkomst (zie ook paragraaf 4.3). Levensachte beelden kunnen worden verspreid en middels *deep learning* technieken kunnen kwaadwillende actoren het laten lijken alsof bijvoorbeeld wereldleiders dingen zeggen of doen die ze in werkelijkheid niet hebben gezegd of gedaan. De verwachting is dat "synthetische media" technologieën snel gecommercialiseerd en breed verkrijgbaar zullen zijn.



Aan de andere kant zien we dat grote sociale media bedrijven als Facebook en Twitter steeds meer actie ondernemen om nepnieuws tegen te gaan. Zeker gedurende de 'infodemic' (de enorm snelle verspreiding van des- en misinformatie) tijdens de COVID-19 epidemie zien we dat platformen steeds vaker onjuiste berichten of advertenties verwijderen, of waarschuwen dat de inhoud van een bericht mogelijk misleidend of onjuist is. Dit betekent ook dat dergelijke bedrijven opnieuw meer macht krijgen.

## 7.6 Koppeling trends en risicocategorieën

Het toenemende gebruik van informatietechnologie in allerlei aspecten van het dagelijks leven en in de processen en

systemen die we dagelijks gebruiken, zorgt ervoor dat IT in veel potentiële risico's en dreigingen voor de nationale veiligheid een rol speelt. IT is nergens de primaire drijvende kracht achter (nieuwe) risico's en dreigingen, maar ontwikkelingen binnen IT hebben vaak wel directe impact op (nieuwe) risico's en dreigingen.

Deze zijn opgenomen in de tabel hieronder en betreffen:

- Verstoring vitale infrastructuur
- Cyberdreigingen
- Bedreigingen internationale vrede en veiligheid (militaire dreiging)
- Ondernijning democratische rechtsstaat en open samenleving.

**Tabel 7.** Koppeling met risicocategorieën vanuit informatietechnologie (donkerblauw=directe koppeling; lichtblauw en cursief=signalering (langetermijn of relevant voor de context))

Dreigingsthema	Verstoring vitale infrastructuur	Cyberdreigingen			
Risico-categorie →	Verstoring vitale infrastructuur	Digitale sabotage	Aantasting functioneren internet	Cyberspionage	
Megatrend ↓					
Autonomie	1.	2.	2.	2.	2.
Cognitie					
Vernetting	3.	4.	4.	4.	4.
Afhankelijkheid	5.	6.	6.	6.	6.

Dreigingsthema	Ondernijning democratische rechtsstaat en open samenleving	Gewelddadig extremisme en terrorisme	Bedreigingen internationale vrede en veiligheid
Risico-categorie →	Alle	Alle	Militaire dreigingen
Megatrend ↓			
Autonomie			8.
Cognitie	7.	7.	
Vernetting			
Afhankelijkheid	6.	6.	

1. Vernieuwde aanvalsmiddelen en -werkwijzen en technisch falen. Naast moedwillige dreigingen (zie 2) worden er door de toenemende cognitie, autonomie en complexiteit in IT-systemen nieuwe typen kwetsbaarheden geïntroduceerd die kunnen leiden tot technisch falen.
2. Bij cyberdreigingen zijn er vernieuwde aanvalsmiddelen en -werkwijzen. Er is bijvoorbeeld een ontwikkeling gaande richting het geautomatiseerd zoeken naar kwetsbaarheden in systemen met behulp van nieuwe, geavanceerdere middelen (zoals zelflerende aanvalssystemen, of autonome malware).

3. Risico op cascade-effecten. Door de koppeling van databronnen en informatiesystemen is onvoldoende inzicht in cascade-effecten bij uitval. Zo kan een systeem verstoord raken doordat gekoppelde systemen of diensten verstoord zijn (supply chain risico's).
4. Nieuwe routes voor sabotage en cyberaanvallen. Als voorbeeld: kwaadwillenden maken steeds vaker gebruik van autonoom opererende programma's om grootschalige DDoS (Distributed Denial of Service) aanvallen uit te voeren op internetdiensten. Bovendien is er professionalisering bij cybercriminelen te zien inclusief het cybercrime-as-a-service model, waarbij

- kwaadwillenden derden betalen om cyberaanvallen uit te voeren.
5. Vitale infrastructuur is in grote mate afhankelijk van IT. Het toenemend gebruik van IT technologie in systemen zoals gebruikt in de vitale processen is in de basis gericht op het verbeteren van het functioneren van deze systemen. Hierbij gaat het niet alleen om IT, maar ook om Operationele Technologie (ten behoeve van bedrijfsvoering en de kantooromgeving).

6. Samenleving is afhankelijk van IT. Voorbeeld is het toenemend gebruik van clouddiensten, waarbij een groot deel van de diensten in handen van enkele aanbieders is.
7. Snellere en bredere verspreiding informatie (propaganda, complottheorieën, desinformatie).
8. Autonome onbemande systemen worden steeds vaker ingezet.



De tabel is gericht op de mogelijke beïnvloeding van de risico's binnen de categorieën. Een belangrijk aspect wat niet in bovenstaande tabel tot uiting komt, is de aandacht voor de kant van de beveiliging van IT-systemen. De nuancering is dat IT-ontwikkelingen niet automatisch tot

een groter risico leiden, omdat kwetsbaarheden soms juist verminderen en daarnaast ingezet wordt op het vergroten van de weerbaarheid (redundantie, herstelveermogen) van de systemen.

# 8. COVID-19

In dit hoofdstuk wordt ingegaan op de mogelijke implicaties van de uitbraak van COVID-19 en de respons hierop. COVID-19 is een bepalende gebeurtenis die zich ontvouwt met dusdanige gevolgen dat deze thuishoort in de Horizonscan. In deze Horizonscan gaat het niet zozeer om de directe impact van de COVID-19-crisis op de nationale veiligheid, maar gaat het erom dat de COVID-19-crisis tot structurele veranderingen kan leiden die relevant zijn voor de context van de nationale veiligheid en de risicocategorieën. Dat is in dit hoofdstuk de focus.

Op de achtergrond spelen verschillende ontwikkelingen een rol bij de huidige pandemie, die in het Nationale Veiligheidsprofiel (NVP, 2016) al kort zijn genoemd. Zo maken globalisering en verstedelijking een snelle verspreiding van ziekten mogelijk. Verder geldt dat door vergrijzing de groep kwetsbaren toeneemt, wat bij deze pandemie gevolgen kan hebben voor het aantal ziekenhuisopnames en sterfgevallen. Dit is bij COVID-19 terug te zien. Daarbij geldt ook dat na COVID-19 de dreiging niet weg zal zijn, maar een nieuwe infectieziekte zich op een bepaald moment zal aandienen. Daarom is het nodig dat de analyse van COVID-19 in een volgende risicoanalyse een plek zal krijgen.<sup>6</sup> Daarbij kan het pandemiscenario dat in de GRA 2019 is opgenomen, worden geactualiseerd. Dat scenario gaat uit van een griepandemie met miljoenen besmettingen, een groot aantal doden en ziekenhuisopnames. Dat leidt tot grote druk op de medische sector en op de IC-capaciteit en veroorzaakt grote verstoring van het dagelijks leven.

Voor deze Horizonscan 2020 is vooral de respons op de uitbraak van COVID-19-crisis van belang. De ingrijpende maatregelen hebben maatschappelijke en economische effecten op langere termijn. Vanuit de nationale veiligheid

gezien is het daarbij opvallend dat instrumenten zijn ingezet om het aantal slachtoffers te beperken die tegelijkertijd andere veiligheidsbelangen raken, namelijk verstoring van het dagelijks leven en aantasting van de economie.

Qua opbouw is in dit hoofdstuk aangesloten bij de thema's uit de scan. Hieronder wordt voor de autonome ontwikkelingen internationale economie, internationale politiek, demografisch-maatschappelijk, ecologie en informatietechnologie aangegeven wat de mogelijk implicaties zijn van de COVID-19 uitbraak. Hierbij hoort de kanttekening dat ten tijde van deze Horizonscan (peildatum 1 augustus 2020) er geen (totaal)overzicht te geven is van de verschillende gevolgen van de COVID-19 uitbraak en respons. Onderstaande betreft dan ook een eerste indicatie. Daarbij geldt dat er bijvoorbeeld ontwikkelingen denkbaar zijn die op hun beurt weer leiden tot onvoorziene gevolgen of vervolgebeurtenissen. Inmiddels lopen er diverse onderzoeken naar de impact van de COVID-19-crisis, zodat de verwachting is dat er voor een volgende analyse meer informatie beschikbaar zal zijn.

## 8.1 Economie

De COVID-19-crisis raakt de Nederlandse economie en de internationale economische orde. Op korte termijn zal sprake zijn van een recessie en een toenemende werkloosheid. De eerste tekenen daarvan hebben zich reeds in de cijfers over het eerste kwartaal van 2020 afgetekend. De vooruitzichten voor de komende periode zijn onzeker en hangen onder andere af van de vraag hoe het aantal besmettingen zich ontwikkelt en hoe de respons hierop wordt vormgegeven.

Overheidsbeleid heeft de eerste klap van de crisis verzacht en na de eerste terugval was er ook een sterk herstel op de beurs. Passend beleid kan daarnaast helpen om het herstel te bespoedigen. Naar mate de crisis langer duurt krimpt de financiële speelruimte voor de overheid. Dit kan de mate waarin de overheid nieuw (crisis)beleid kan voeren raken.

<sup>6</sup> In de volgende risicoanalyse (GRA 2021) zal nader worden ingegaan op het pandemiscenario n.a.v. de COVID-19-crisis. Daar zal het o.a. gaan over de impact die we nu al zien, zoals fysieke veiligheid (doden, ziekenhuisopnames) met daarbij de druk op het zorgsysteem (IC-capaciteit), de economie (werkloosheid) en de sociaal-politieke stabiliteit (verstoring van het dagelijks leven door de genomen maatregelen (lock-down, sluiten van o.a. scholen, verpleeg/verzorgingsinstellingen en horeca, etc)).



In het geval van een langdurige recessie en een traag herstel hiervan kan welvaart blijvend verloren gaan. Bepaalde bedrijfsmodellen of sectoren zullen blijvend beschadigd blijken en niet langer houdbaar zijn, terwijl andere sectoren juist profiteren. Dit betekent een herstructurering van de economie, waarin gevestigde bedrijven failliet gaan en nieuwe ontstaan. De fricties die dit met zich meebrengt kunnen pijnlijk en kostbaar zijn voor bedrijven, maar ook voor werknemers die zich van sector naar sector moeten gaan bewegen. Oplopende werkloosheid is te verwachten. Een factor van belang voor de duur van de recessie is het aanpassingsvermogen van de economie. Een dynamische economie waarin burgers en ondernemers snel (kunnen) inspelen op veranderende omstandigheden heeft een grotere kans om sneller uit de crisis te komen.

Nederland is een kleine open economie en dus gevoelig voor het herstel in andere landen. Achterblijvende vraag in andere landen, kan de duur en diepte van de recessie in Nederland beïnvloeden. Het instorten van de wereldhandel heeft Nederland tijdens de vorige crisis hard geraakt. Ook in deze crisis krimpt de handel in zowel goederen- als diensten. De inperkende werking van coronamaatregelen op het vrije verkeer van personen zorgt ervoor dat met name sectoren die zeer afhankelijk zijn van personenverkeer (zoals toerisme) hard geraakt worden.

Aan deze internationale gevoeligheid zit ook een politiek component. Zo drukt het conflict tussen de Verenigde Staten en China rondom de bron van het coronavirus steeds meer zijn stempel op handelsonderhandelingen. Verdere escalatie van politieke tegenstellingen vormen een risico voor de Europese en de wereldeconomie. Binnen Europa zijn door de COVID-19-crisis economische en politieke tegenstellingen vergroot. Dit blijkt onder andere bij discussies over een economisch steunpakket. Voor een stabiele Europese economie is goede samenwerking essentieel. Interne tegenstellingen verhogen onzekerheid op financiële markten. Voor Europa geldt dat dit het risico op een hernieuwde euro- of schuldencrisis met zich kan meebrengen. Financiële markten zijn vooralsnog maar beperkt geraakt door de crisis, maar naarmate de crisis langer duurt kan ook hier de stress op het systeem toenemen.

Een diepe crisis heeft ook langetermijn gevolgen. Mogelijk ontstaat een herbezinning van de inrichting van internationale waardeketens. Bedrijven zullen bijvoorbeeld al dan niet mede onder druk van overheden (een deel van) hun activiteiten terugverplaatsen naar hun 'thuisland'. Aan zulke *re-sourcing* zitten plussen en minnen. Enerzijds maken kortere aanvoerlijnen bedrijven minder gevoelig voor schokken in andere landen. Anderzijds wordt de productie door terugverplaatsing minder efficiënt, duurder voor de consument en juist gevoeliger voor schokken in het thuisland. Qua risicocategorieën raakt dit aan de

knooppuntfunctie, de *flow security* van Nederland, en aan handelskrimp in den brede, niet alleen op de korte maar ook op de lange termijn. Een ander voorbeeld is dat het risico bestaat dat er sprake kan zijn van interactie-effecten met andere risico's. Als overheden hun middelen vooral inzetten om de economische crisis het hoofd te bieden, bestaat de kans dat andere beleidsdoelen uit het zicht raken. Dit kan bijvoorbeeld de klimaattransitie vertragen doordat er minder publiek geld beschikbaar komt en bedrijven geen middelen hebben om zelf te investeren. Het uitstellen van de klimaattransitie kan toekomstige klimaatrisico's vergroten.

## 8.2 Internationaal

Internationaal zijn de spanningen tussen onder andere de grootmachten China en de VS tijdens de COVID-19-crisis toegenomen. Zo houdt de VS China verantwoordelijk voor de uitbraak van het virus. Deze toegenomen spanningen kunnen weerslag hebben op de handelsoorlog tussen beide landen. In zijn algemeen staat de huidige wereldorde onder druk door COVID-19 en wordt de koppeling van politieke en economische systemen versneld. Het verder wegvallen van Amerikaans leiderschap binnen de bestaande wereldorde vormt een groot probleem voor de EU, dat hiermee een traditionele bondgenoot verliest in internationale gremia. Dit is te merken in bijvoorbeeld de World Health Organization (WHO) waar Amerika dreigt haar bijdrage te bevrozen omdat de organisatie zich door Chinese desinformatie over het virus zou laten beïnvloeden.

Verder kan de respons op het virus de cohesie tussen Europese staten beïnvloeden. De COVID-19-crisis kan als stresstest voor veel Europese overheden fungeren, ook omdat het virus nieuw leven in populistische partijen kan blazen. Steun voor autoritair leiderschap, xenofobie, racisme en de populariteit van complottheorieën lijken potentiële consequenties van de COVID-19-crisis te zijn. Daarnaast heeft het virus niet alleen polarisatie tussen Noord- en Zuid-Europa vergroot, vanwege onenigheid over financieel-economische maatregelen, maar ook tussen Oost- en West-Europa, wegens controverses over de beperking van burgervrijheden. Deze landen lijken de crisis te gebruiken om bepaalde doelen te bereiken.

Het is ook waarschijnlijk dat, gezien de verspreiding van het virus, ook de instabiliteit van regio's grenzend aan de randen van Europa verder zal toenemen. In het geval van het Midden-Oosten en Noord-Afrika zal dit voornamelijk veroorzaakt worden door groeiende economische moeilijkheden en groeiende onrust onder de bevolking. Hierdoor is de regio ook vatbaarder voor een heropleving van terreurorganisaties als Islamitische Staat. Echter, de COVID-19-crisis biedt theoretisch ook kansen voor de instabiele regio.

Door het afgekondigde staakt-het-vuren ontstaat een gelegenheid voor conflictresolutie. Zo kunnen Saudi-Arabië en Jemen, als ook Iran en de VS pogingen doen om nader tot elkaar te komen.

Tegelijkertijd is er een desinformatiestrijd aan de gang, waarbij China, Rusland en de VS elkaar beschuldigen van het creëren en verspreiden van het coronavirus. De verspreiding van desinformatie lijkt te zijn toegenomen door de uitbraak van de COVID-19 pandemie. Deze toename wordt voornamelijk gefaciliteerd door sociale media. Ook in Nederland zijn de effecten van desinformatie duidelijk merkbaar, zoals bij recente brandstichtingen van zendmasten die via 5G het virus zouden verspreiden. Verder biedt het virus voor Rusland en China een mogelijkheid om "soft power" te gebruiken, bijvoorbeeld door medische steun te bieden aan Europese landen die het zwaarst getroffen worden door de pandemie en zich in de steek gelaten voelen door de EU. De kans is aanwezig dat deze liefdadigheid echter verbonden is aan bredere geopolitieke ambities die, in combinatie met (cyber)spionage en sabotage en de verspreiding van desinformatie, het doel hebben om reeds bestaande polarisatie te vergroten.

### 8.3 Maatschappelijk

Het is op moment van schrijven nog niet duidelijk wat precies de impact van de COVID-19-crisis op de sociale cohesie, sociaal vertrouwen en sociale stabiliteit in Nederland zal zijn. Wel ontstaat steeds meer consensus dat deze groot en langdurig zal zijn. Na de 'intelligente' lockdown is Nederland voor een groot deel weer op gang gekomen. Het midden zal moeten worden gevonden tussen publieke acceptatie, de ziektelast binnen de perken houden en de verspreiding van het virus tegengaan. Veel aandacht gaat uit naar de economische gevolgen van de crisis, maar minstens zo urgent is de vraag welk blijvende maatschappelijke effecten de COVID-19-crisis zal hebben.

De eerste onderzoeken naar de verwachte impact laten zien dat sommige (kwetsbare) groepen bovengemiddeld worden getroffen, waardoor de ongelijkheid toeneemt. Naast werkloosheid gaat het om sociaal isolement en afnemend vertrouwen in de toekomst. Daarnaast speelt het vertrouwen in de overheid een rol, waarbij de duur en de gevolgen van de maatregelen van belang zijn. Het is duidelijk dat dit kan leiden tot spanningen en tot het ontstaan van extremistisch gedachtegoed en polarisatie.

De COVID-19-crisis kan tenslotte gezien worden als een politieke stresstest. Hoe kan tegemoet worden gekomen aan de roep om meer veiligheid, gemeenschapszin en collectieve bescherming, zonder hiervoor burgerlijke vrijheden op te offeren? Het is de vraag naar de verhouding

tussen bescherming, gezondheid, veiligheid én economie én persoonlijke vrijheden.

### 8.4 Ecologie

De uitbraak van COVID-19 en de getroffen maatregelen leiden tot enkele neveneffecten op het terrein van de ecologie. Voor de korte termijn zijn door de crisis in 2020 mogelijk positieve effecten voor de luchtkwaliteit te verwachten. Sinds 16 maart golden er in Nederland maatregelen om het coronavirus te beheersen. Door deze maatregelen was er een sterke vermindering van weg- en vliegverkeer, waardoor er tijdelijk minder uitstoot was van schadelijke stoffen, zoals koolstofdioxide en stikstofdioxide. Het gaat hierbij voor Nederland om een afname van tussen de 20 en 60 procent. Ook boven China, Noord-Italië en verschillende Europese steden, zoals Parijs, Rome en Madrid is een sterke afname in luchtvervuiling gemeten. De verbetering van de luchtkwaliteit die hierdoor ontstaat heeft positieve gevolgen voor de volksgezondheid. Daarnaast zorgt de afname van de uitstoot van stikstof en broeikasgassen voor tijdwinst in de stikstofcrisis en voor het klimaatbeleid. De kans bestaat echter dat er een inhaaleffect ontstaat wanneer maatregelen worden opgeheven en de economie weer aantrekt. Tenslotte kan deze crisis leiden tot verandering in bepaalde beleidskeuzen. Zo is gesuggereerd dat het klimaatbeleid en de energietransitie door de COVID-19-crisis wellicht uitgesteld zullen worden.

### 8.5 Informatietechnologie

Gedurende de uitbraak van COVID-19 is er sprake van zowel een groot gebruik als een grote afhankelijkheid van toepassingen van informatietechnologie. Een belangrijk deel van de samenleving en de economie ging tijdens de 'intelligente' lockdown, door vanwege de digitale mogelijkheden. Dit maakt de gedigitaliseerde samenleving tegelijk kwetsbaar en gevoelig voor cyberdreigingen. Doordat mensen veelal thuis zijn gaan werken, werd er bovendien een groot beslag gelegd op netwerkcapaciteit en moesten er maatregelen getroffen worden door telecomproviders om te kunnen voorzien in de toegenomen vraag naar netwerkcapaciteit.

Verder maakt de discussie over een corona-app de vraagstukken over het toepassen van IT en privacy concreet. Het privacy-vraagstuk kwam ook naar voren doordat er tijdens de crisis veel gebruik gemaakt werd van applicaties die onveilig of niet goed doorontwikkeld waren. Bijvoorbeeld diverse videobeldiensten waarbij end-to-end versleuteling niet werd ondersteund of apps die naast hun primaire functie ook veel (meta)data verzamelden voor onder meer advertentiedoelinden.



Tot slot speelt het fenomeen van 'infodemic', wat gaat over de enorm snelle verspreiding van desinformatie, nepnieuws en complottheorieën (zoals de gesuggereerde link tussen COVID-19 en 5G of de desinformatiecampagnes door o.a. China en de VS). Verspreiding van desinformatie is een fenomeen dat binnen meerdere thema's binnen deze Horizonscan naar voren komt in het kader van de COVID-19-crisis.

## 8.6 Koppeling met risicocategorieën

Op basis van bovenstaande is duidelijk dat de uitbraak van en respons op COVID-19 implicaties kan hebben voor de context waarbinnen risico's voor de nationale veiligheid zich afspelen en uit voort komen. In onderstaand overzicht is aangegeven welke risicocategorieën door ontwikkelingen als gevolg van de COVID-19-crisis mogelijk beïnvloed kunnen worden.

**Tabel 8.** Koppeling met risicocategorieën vanuit COVID-19

Dreigingsthema GRA	Risicocategorie GRA	COVID-19
dreigingen voor gezondheid en milieu	Infectieziekten humaan	COVID-19 zal als input dienen voor actualisatie pandemie-scenario)
Natuurrampen	Extreem weer	
	Overstroming	
	Natuurbrand	
	Aardbeving	
Verstoring vitale infrastructuur	Verstoring vitale infrastructuur	Afhankelijkheid (internet, ICT) is toegenomen en de druk op netwerkcapaciteit vergroot
Zware ongevallen	Stralingsongevallen	
	Chemische incidenten	
Cyberdreigingen	Digitale sabotage	Door verdergaande digitalisering (thuiswerken, digitaal vergaderen) is kwetsbaarheid toegenomen
	Aantasting functioneren internet	
	Cyberspionage	Door verdergaande digitalisering (thuiswerken, digitaal vergaderen) is kwetsbaarheid toegenomen
	Cybercriminaliteit	
Ondermijning democratische rechtsstaat en open samenleving	Niet-gewelddadig extremisme	Demonstraties, polarisatie, Infodemics, afname van vertrouwen in de overheid
	Ondermijnende criminaliteit (enclavevorming)	
	Ongewenste buitenlandse inmenging	
	Ongewenste buitenlandse beïnvloeding (via hybride operaties)	Infodemics (statelijke actoren)
Gewelddadig extremisme en terrorisme	Gewelddadig extremisme	
	Terrorisme	



Dreigingsthema GRA	Risicocategorie GRA	COVID-19
Financieel-economische bedreigingen	Criminele inmenging	
	Bedreigingen van de knooppuntfunctie en de aan- en afvoerlijnen van Nederland	
	Handelskrimp/verstoring internationale handel	Internationale handel is geraakt door de COVID-19 maatregelen
	Destabilisatie financieel systeem	Indirect: Als uitkomst van een recessie en discussie over financiële maatregelen is een euro- of financiële crisis denkbaar
Bedreigingen internationale vrede en veiligheid	Instabiliteit rondom Europa	Indirect: COVID-19 kan instabiliteit in het Midden Oosten en Noord-Afrika vergroten en ook partijen als IS versterken
	Militaire dreigingen (NAVO-lidstaat)	
	CBRN-proliferatie	
	Veiligheidsarrangementen onder druk (NAVO, EU)	Spanningen binnen EU en WHO zijn zichtbaar geworden.

Wat uit de tabel naar voren komt, is dat bij de meerderheid van de koppelingen de (toegenomen) afhankelijkheid als gevolg van het virus een belangrijke rol speelt. Zo geldt bij de dreigingsthema's **verstoring vitale infrastructuur** en **cyberdreigingen** dat afhankelijkheid en gebruik van digitale systemen is toegenomen. Dit onder andere door het op grote schaal thuiswerken. Hierdoor is er tegelijkertijd echter ook sprake van een toegenomen risico als deze systemen niet goed meer zouden functioneren of als onbevoegden toegang krijgen tot digitaal opgeslagen informatie. In die zin is er ook een sterke koppeling met de risicocategorieën cyberspionage en digitale sabotage. Als gevolg van de COVID-19-crisis zijn er ook andere afhankelijkheden blootgelegd, zoals de afhankelijkheid van buitenlandse leveranciers voor onder andere medische hulpmiddelen.

Tot slot valt ook op dat een pandemie zoals COVID-19 kan leiden tot destabilisatie en conflict. De uitbraak van het coronavirus en de daaruit volgende maatregelen kunnen aanleiding zijn voor het ontstaan van extremistisch gedachtengoed en polarisatie omtrent de vraag hoe met het virus om te gaan. Ook kan het leiden tot spanningen binnen internationale organisaties en veiligheidsarrangementen over de aanpak van de crisis, toenemende instabiliteit in al kwetsbare landen rond Europa en discussie op internationaal vlak over financiële maatregelen (en de verdeling van de lasten hiervan). In deze hoedanigheid kan de COVID-19-crisis worden gekoppeld aan de dreigingsthema's **ondermijning democratische rechtsstaat en open samenleving**, **financieel-economische bedreigingen** en **bedreigingen internationale vrede en veiligheid**.





# 9. Overzicht van de koppeling met de risicocategorieën

De koppelingen van de trends en manifestaties met de risicocategorieën uit de GRA 2019 zijn in de voorgaande hoofdstukken al per onderwerp weergegeven. Dit hoofdstuk bevat een overzicht en beschouwing van deze koppelingen. De koppelingen zelf zijn weergegeven in tabel 9 op de volgende pagina. Net als bij de weergaves in elk hoofdstuk, zijn er twee typen koppelingen. Enerzijds zijn er directe koppelingen die al op de korte termijn relevant kunnen zijn. Anderzijds zijn er meer indirecte, maar wel degelijk relevante koppelingen. Deze spelen veelal op de langere termijn en dienen binnen deze Horizonscan voornamelijk als signalering. De twee typen koppelingen zijn in de figuur met blauwtinten aangegeven. Ten opzichte van de weergaves in voorgaande hoofdstukken is de figuur gekanteld. Bij deze beschouwing wordt er gekeken vanuit de dreigingsthema's en risicocategorieën uit de GRA 2019.

Op basis van het overzicht van koppelingen kunnen ten eerste enkele algemene constatering worden gemaakt. Om te beginnen is er een duidelijk verband tussen trends in een onderwerp (autonome ontwikkeling) met de risicocategorieën die gerelateerd zijn aan datzelfde onderwerp. Dat geldt voor alle vijf de thema's. Ontwikkelingen vanuit Ecologie raken de risicocategorieën onder natuurrampen en gezondheid en milieu. Bij Informatietechnologie is er duidelijk een koppeling met cyberveiligheid. Op dezelfde wijze is het onderwerp Internationale politiek verbonden met internationale vrede en veiligheid en het onderwerp internationale economie met financieel-economische bedreigingen. Bij demografisch-maatschappelijke ontwikkelingen is tenslotte een link met ondermijning van de democratische rechtsstaat te zien.

Daarnaast valt op dat een aantal autonome ontwikkelingen uit de quick-scan een veel breder bereik, een bredere invloed heeft dan anderen. Dit geldt met name voor de autonome ontwikkelingen informatietechnologie en internationale politiek. Informatietechnologie heeft niet alleen betrekking op cyberdreigingen, maar ook op de risicocategorieën ondermijning van de democratische rechtsstaat en open samenleving, verstoring vitale infrastructuur, gewelddadig extremisme en terrorisme en,

tot slot, bedreigingen internationale vrede en veiligheid. Dit laat onder andere de belangrijke rol en invloed van informatietechnologie zien op uiteenlopende terreinen. Hetzelfde geldt voor ontwikkelingen op het gebied van internationale politiek. Deze kunnen niet alleen worden gekoppeld met de gerelateerde risicocategorie, maar ook met de categorieën gewelddadig extremisme en terrorisme, financieel-economische bedreigingen, ondermijning democratische rechtsstaat en open samenleving en cyberdreigingen. Hieruit blijkt onder meer de sterke verbinding tussen ontwikkelingen die zich buiten Nederland afspelen en mogelijke gebeurtenissen in Nederland zelf. Dit wordt ook wel de 'nexus interne en externe veiligheid' genoemd.

## **Dreigingsthema's**

Als we vervolgens vanuit de **dreigingsthema's** naar de koppelingen kijken, vallen verschillende zaken op. Wat betreft de verdeling van directe (donkerblauw) en indirecte (lichtblauw) koppelingen, blijkt dat er vooral rond de dreigingsthema's bedreigingen voor **gezondheid en milieu** en **natuurrampen** veel indirecte koppelingen zijn. Dit komt met name doordat er voor deze thema's alleen koppelingen zijn met de autonome ontwikkeling ecologie. Deze autonome ontwikkeling bevat hoofdzakelijk trends of processen waarvan de mogelijke effecten zich voordoen op de langere termijn, dan wel langzaam toenemen in ernst over tijd. Het gaat om sluimerende processen die worden gekenmerkt door 'tipping points' en niet-stabiele evenwichten. Dat betekent dat wanneer een kritisch punt wordt bereikt, het onomkeerbaar wordt en niet of nauwelijks meer veranderd kan worden. Dit sluimerende karakter neemt uiteraard niet weg dat als deze effecten zich uiteindelijk wel voordoen of een dusdanige omvang bereiken dat ze vaker merkbaar zijn, de gevolgen ervan en de effecten op de risicocategorieën groot kunnen zijn. Vandaar dat de indirecte koppelingen zijn meegenomen als signalering. Voor het dreigingsthema natuurrampen geldt overigens dat er ook één directe koppeling is gelegd, voor de risicocategorie extreem weer.

Het dreigingsthema **cyberdreigingen** heeft als enige alleen maar directe koppelingen, waarbij het gaat om mogelijke beïnvloeding van de risicocategorieën door de trends op



een relatief korte termijn. De koppelingen hangen nauw samen met de toenemende mogelijkheden én afhankelijkheden van informatietechnologie en internet. Bij **Verstoring van vitale infrastructuur** zien we diezelfde afhankelijkheid van IT duidelijk terugkomen. Daarnaast spelen bij dit dreigingsthema de trends vanuit ecologie een rol. Deze kunnen op termijn van invloed zijn op de leveringszekerheid van primaire levensbehoeften (voedsel, water, energie). Vanwege de langere termijn is deze koppeling als signalering opgenomen.

Bij het thema **ondermijning democratische rechtsstaat** houden de indirecte koppelingen verband met de mogelijke invloed van zaken als desinformatie, complottheorieën en propaganda. Dit zijn indirecte koppelingen, omdat hierdoor actoren (onbewust) kunnen worden beïnvloed door kwaadwillende actoren. Dat kan op zijn beurt bijvoorbeeld een voedingsbodem zijn voor niet-gewelddadig extremisme. Verder valt ook hier de afhankelijkheid van IT op en komt de al eerder genoemde nexus interne en externe veiligheid naar voren. Tenslotte springt het absolute aantal koppelingen bij niet-gewelddadig extremisme eruit (zie verder onder 'risicocategorieën').

De mogelijke gevolgen van desinformatie, complottheorieën, propaganda én de afhankelijkheid van IT zien we ook bij het dreigingsthema **terrorisme en extremisme**. Daarnaast geldt dat ook internationale politieke spanningen en spanningen binnen de Nederlandse samenleving relevante drijfveren zijn bij dit thema.

Uit het overzicht kan verder duidelijk de **koppeling tussen politieke en economische systemen** afgeleid worden. Zowel **financieel-economische bedreigingen** als het **thema bedreigingen internationale vrede en veiligheid** worden namelijk beïnvloed door de trends op het vlak van internationale politiek. Op dit onderwerp is er veel in beweging dat van invloed is op de risicocategorieën. Tenslotte merken we op dat klimaatverandering relevant is voor de **internationale vrede en veiligheid**, omdat het een mogelijke factor vormt voor het ontstaan van (gewapende) conflicten en zo de instabiliteit rondom Europa kan vergroten. Daarnaast kan het falen van of onenigheid over klimaatbeleid zorgen voor internationale spanningen.

**Tabel 9.** Overzicht van koppelingen tussen risicocategorieën uit de GRA 2019 en megatrends uit de Horizonscan 2020 (donkerblauw=directe koppeling; lichtblauw signalering (langetermijn of relevant voor de context))

Dreigingsthema GRA ↓	Thema →  Risicocategorie GRA ↓	Internationale politiek			Internationale economie			Demografisch maatschappelijk			Informatie-technologie			Ecologie		
		Tanende naoorlogse multilaterale wereldorde	Instabiliteit aan de brede randen van Europa	Polarisatie binnen de Europese samenleving	Politisering van de internationale markteconomie	Digitalisering van de economie	Klimaattransitie	Groeiende ongelijkheid en tegenstellingen	Gevolgen van toenemende diversiteit	Fluctuering van vertrouwen	Autonomie en cognitie	Vernetting	Afhankelijkheid van IT	Klimaatverandering	Biodiversiteit	Milieudruk
Bedreigingen voor gezondheid en milieu	Infectieziekten humaan												X			
	Dierziekten en zoönose												X	X		
Natuurrampen	Extreem weer												X			
	Overstroming												X			
	Natuurbrand												X			
	Aardbeving															



Dreigingsthema GRA ↓	Thema →  Megatrend  Risicocategorie GRA ↓	Internationale politiek			Internationale economie			Demografisch maatschappelijk			Informatie-technologie			Ecologie		
		Tanende naoorlogse multilaterale wereldorde	Instabiliteit aan de brede randen van Europa	Polarisatie binnen de Europese samenleving	Polifisering van de internationale markteconomie	Digitalisering van de economie	Klimaattransitie	Groeiende ongelijkheid en tegenstellingen	Gevolgen van toenemende diversiteit	Fluctuering van vertrouwen	Autonomie en cognitie	Vernetting	Afhankelijkheid van IT	Klimaatverandering	Biodiversiteit	Milieudruk
Verstoring vitale infrastructuur	Verstoring vitale infrastructuur									X	X	X	X	X	X	
Zware ongevallen	Straling-ongevallen															
	Chemische incidenten															
Cyber-bedreigingen	Digitale sabotage	X				X				X	X	X				
	Aantasting functioneren internet									X	X	X				
	Cyberspionage	X		X	X	X				X	X	X				
	Cyber-criminaliteit					X				X	X	X				
Ondermijning democratische rechtsstaat en open samenleving	Niet-gewelddadig extremisme			X				X	X	X	X		X	X	X	
	Ondermijnende criminaliteit (enclavevorming)								X	X		X				
	Ongewenste buitenlandse inmenging			X					X	X	X		X			
	Ongewenste buitenlandse beïnvloeding (via hybride operaties)	X								X		X				



Dreigingsthema GRA ↓	Thema →  Megatrend  Risicocategorie GRA ↓	Internationale politiek			Internationale economie			Demografisch maatschappelijk			Informatie-technologie			Ecologie		
		Tanende naoorlogse multilaterale wereldorde	Instabiliteit aan de brede randen van Europa	Polarisatie binnen de Europese samenleving	Politisering van de internationale markteconomie	Digitalisering van de economie	Rijmatransitie	Groeiende ongelijkheid en tegenstellingen	Gevolgen van toenemende diversiteit	Fluctuering van vertrouwen	Autonomie en cognitie	Vernetting	Afhankelijkheid van IT	Klimaatverandering	Biodiversiteit	Milieudruk
Gewelddadig extremisme en terrorisme	Gewelddadig extremisme							X	X	X	X		X			
	Terrorisme		X								X		X			
Financieel-economische bedreigingen	Criminele inmenging															
	Bedreigingen van de knooppuntfunctie en de aan- en afvoerlijnen van Nederland		X		X											
	Handelskrimp/verstoring internationale handel	X	X		X	X	X									
	Destabilisatie financieel systeem					X										
Bedreigingen internationale vrede en veiligheid	Instabiliteit rondom Europa	X	X	X									X			
	Militaire dreigingen (NAVO-lidstaat)		X								X					
	CBRN-proliferatie	X	X													
	Veiligheidsarrangementen onder druk (NAVO, EU)	X	X										X			

### **Risicocategorieën**

Na de beschouwing vanuit de dreigingsthema's wordt ingezoomd op het niveau van de risicocategorieën. We beperken ons hier tot enkele constatering.

Wat opvalt is dat er bij sommige risicocategorieën helemaal geen koppelingen zijn gelegd, zoals bij stralingsongevallen en chemische incidenten. Voor deze risicocategorieën geldt bijvoorbeeld dat er simpelweg geen voor de invulling van de categorieën zelf relevante ontwikkelingen zijn geconstateerd.

Verder zijn er meerdere risicocategorieën waarmee slechts een of twee koppelingen zijn gelegd. De risicocategorieën extreem weer en overstroming zijn daar voorbeelden van. Het feit dat er slechts één koppeling is gelegd, wil echter niet zeggen dat de mogelijke invloed van een trend op de risicocategorie minder groot is dan wanneer er meer koppelingen zijn gemaakt. Als er veel koppelingen zijn gevonden houdt dit niet per definitie in dat de risico's van een bepaalde risicocategorie significant toenemen. In deze scan zijn de verschillende trends niet (onderling) gekwalificeerd. Wel is het zo dat meerdere koppelingen als indicatie kan worden gezien dat er vanuit meerdere hoeken beweging is die relevant kan zijn voor de betreffende categorie en deze kan beïnvloeden. Dat is de reden dat verder aandacht wordt gegeven aan risicocategorieën met meerdere koppelingen.

Zoals al is gemeld kunnen de meeste koppelingen worden gemaakt met de risicocategorie **niet-gewelddadig extremisme**. Dit onder andere doordat deze risicocategorie niet alleen kan worden beïnvloed door nieuwe technieken en methoden (informatietechnologie), maar ook door bredere maatschappelijke trends (demografisch maatschappelijk) en onderwerpen of gebeurtenissen die aanleiding kunnen geven tot extremistisch gedachtengoed (ecologie). Daarnaast zijn er ook bij de risicocategorieën **cyberspionage** en **verstoring van vitale infrastructuur** veel koppelingen met trends gelegd, waarbij het in beide gevallen onder andere om koppelingen met trends vanuit de autonome ontwikkeling informatietechnologie gaat.

Uit de tabel volgt tenslotte dat voor de categorieën die moedwillige risico's bevatten de meeste koppelingen kunnen worden gemaakt met de verschillende trends. Naast de al genoemde categorieën **niet-gewelddadig extremisme** en **cyberspionage**, gaat het om **handelskrimp**, **digitale sabotage**, **ongewenste buitenlandse inmenging**, **gewelddadig extremisme**, **terrorisme** en **instabiliteit rondom Europa**.





# 10. Resultaten en conclusie

Het Analistennetwerk Nationale Veiligheid (ANV) heeft in opdracht van de NCTV de voorliggende Horizonscan Nationale Veiligheid 2020 uitgevoerd. In de Horizonscan is gekeken naar trends en ontwikkelingen die de nationale veiligheid mogelijk kunnen raken. Hierbij ligt de focus op ontwikkelingen die zich hebben voorgedaan sinds het opstellen van de Horizonscan 2019. Binnen de scan is hiernaast apart ingegaan op de situatie rond de COVID-19-crisis.

In aanvulling op de verkenning van trends en ontwikkelingen is in deze scan ook expliciet een koppeling gemaakt tussen deze trends en de risicocategorieën uit de Geïntegreerde risicoanalyse 2019 (GRA 2019). Via de gemaakte koppelingen kan een indicatie worden gegeven of er sinds het opstellen van de GRA nieuwe risico's en dreigingen naar voren zijn gekomen, dan wel of bestaande risico's en dreigingen mogelijk in verandering zijn. De resultaten uit de Horizonscan 2020 dienen als input voor de 'mid-term' review van de in juni 2019 aangeboden Nationale Veiligheid Strategie (NVS 2019).

In dit hoofdstuk worden de resultaten van de scan en de koppeling met de risicocategorieën op hoofdlijnen samengevat en beschouwd. Tenslotte zijn enkele conclusies getrokken, waarbij de link met de resultaten uit de GRA en de NVS 2019 is gelegd.

## 10.1 Overzicht van de resultaten van de scan

Voor de verkenning van mogelijk relevante ontwikkelingen is aangesloten bij de autonome ontwikkelingen en bijbehorende megatrends uit de Horizonscan 2019 (tabel 1, hoofdstuk 2). Binnen deze scan is voor elk van de megatrends gekeken welke concrete ontwikkelingen (manifestaties) zich voordoen en of de megatrends zelf nog relevant zijn.

Uit de Horizonscan 2020 blijkt dat de megatrends uit de voorgaande Horizonscan nog steeds relevant zijn. Dit mede doordat de megatrends betrekking hebben op de langere termijn en de Horizonscan 2019 relatief kort geleden is uitgevoerd. De resultaten laten echter niet alleen een bevestiging van de megatrends zien, maar in veel gevallen is er ook sprake van een toename of versnelling van een trend. Voorbeelden zijn de versnelling van klimaatverandering en de

toenemende internationale spanningen tussen de VS en China. Daarbij komt dat maatregelen volgend op de COVID-19 uitbraak sommige trends hebben versterkt, zoals het gebruik en de afhankelijkheid van informatietechnologie. De COVID-19-crisis vormt overigens ook een katalysator of middel voor het verwezenlijken van andere zaken. Denk aan het fenomeen infodemics en daarmee de verspreiding van desinformatie, propaganda en complottheorieën. Een ander voorbeeld betreft de opstelling van de VS richting de WHO waarbij de COVID-19-crisis als aanleiding wordt gebruikt om de WHO te bekritisieren voor de houding tot China.

Als we het algehele beeld van de scan beschouwen, komt naar voren dat internationale spanningen en de verwevenheid van geopolitiek en financieel-economisch beleid zijn toegenomen. Dit uit zich met name in spanningen tussen China en de VS. Alhoewel de mate van spanning binnen deze relatie fluctueert, is er wel degelijk sprake van een algemene toename van onderlinge spanningen. Eenzelfde argument geldt voor de verhoudingen binnen internationale regimes (WHO, EU, NAVO). Uitingen van dergelijke spanningen zijn het vleugellam maken van de beroepsinstantie van de WTO, een toenemende wapenwedloop en de ontwikkelingen rondom het stelsel van wapen-beheersing. Ook discussies aangaande Huawei, de Nordstream-2 pijplijn en het handelsconflict tussen de EU en de VS passen in deze trend.

De mogelijkheden én afhankelijkheid van Informatietechnologie nemen toe. Dat is door COVID-19 (thuiswerken, thuisonderwijs) extra onderstreept en het is duidelijk dat de samenleving eigenlijk niet meer kan functioneren zonder IT-systemen. Hetzelfde geldt voor vitale infrastructuur, met als gevolg dat de onderwerpen afhankelijkheid en kwetsbaarheid duidelijke aandachtspunten zijn. Omdat innovaties leiden tot een betere beveiliging van systemen en een versterking van de weerbaarheid, kan niet zondermeer geconcludeerd worden dat de risico's van cyberdreigingen toenemen. Verder is het zo dat de maatschappelijke bewustwording met betrekking tot privacy toeneemt door de verdere toepassingen van IT.



De snelheid en hoeveelheid van de verspreiding van desinformatie, propaganda en complottheorieën nemen toe en door ontwikkelingen als de opkomst van *deep fakes* wordt het steeds lastiger om daar weerstand aan te bieden. De toename van nepnieuws leidt er onder andere toe dat het vertrouwen in de mainstream media onder druk staat. Door gebruik van (sociale) media kunnen bijvoorbeeld extreemrechtse ideeën breed worden gecommuniceerd. Deze ideeën worden steeds meer als reguliere politieke meningen naast andere gezien.

In de samenleving is er een toenemend belang van de eigen identiteit, zowel bij jongeren met een migratie achtergrond als bij mensen met extreemrechts gedachtengoed. Tegelijkertijd is er een opkomst van extreemlinkse groeperingen en zien we een opkomend extremisme gericht op specifieke onderwerpen, zoals verzet tegen windturbines en 5G. Verder zijn er (soms in gewelddadigheden uitlopende) demonstraties tegen de maatregelen die getroffen zijn in de bestrijding van de COVID-19-crisis en is er de polarisatie tussen boeren, de milieubeweging en de overheid rond de 'stikstofcrisis'.

Dat laatste is een uitvloeisel van de trends van afnemende biodiversiteit en toenemende milieudruk. In het algemeen geldt dat deze ecologische trends sluimerende processen zijn. Deze processen hebben op het moment nog maar een beperkte invloed op de nationale veiligheid, maar worden op termijn wel degelijk relevant. Een uitzondering betreft de toename van de kans op extreem weer door de (versnelde) klimaatverandering. Hierbij gaat het bijvoorbeeld om hittegolven (waarvan zowel de kans als de intensiteit toenemen) als extreme neerslag en zware stormen. Verder heeft klimaatverandering geopolitieke gevolgen en kan het de instabiliteit rondom Europa versterken. Tenslotte leidt de verduurzaming van de energievoorziening ertoe dat de energielevering afhankelijker wordt van het weer (zon, wind), waardoor de leveringszekerheidsrisico's kunnen toenemen.

Hierboven zijn de resultaten beschreven op basis van de toename, versterking en of versnelling van beschouwde trends. In dit kader lijken ontwikkelingen op het gebied van terrorisme een positieve uitzondering, aangezien de terroristische dreiging is afgenomen. Hierbij geldt wel de nuancering dat jihadistisch terrorisme nog steeds de grootste (gewelddadig) extremistische dreiging vormt.

## 10.2 Koppeling met risicocategorieën

### Signaleringsfunctie

In het vorige hoofdstuk is de koppeling van de trends met de risicocategorieën beschreven. Hier vatten we de resultaten samen. Er is onderscheid gemaakt tussen directe en indirecte koppelingen. Bij dit laatste gaat het om koppelingen die wel relevant zijn, maar niet direct of op korte termijn een risicocategorie beïnvloeden.

Deze indirecte koppelingen hebben voornamelijk een **signaleringsfunctie**. Enkele zijn al in de vorige paragraaf naar voren gekomen. Zo zijn klimaatverandering en de afname van biodiversiteit sluimerende processen die op termijn risico's op natuurrampen, maar ook de risicocategorieën zoönosen en humane infectieziekten zullen beïnvloeden. Op langere termijn kunnen klimaatverandering en afname van biodiversiteit ook van invloed zijn op de drinkwater- en voedselvoorziening (vitale infrastructuur).

Hetzelfde geldt voor de leveringszekerheid van energie (vitale infrastructuur) wegens de toenemende afhankelijkheid van duurzame energiebronnen in combinatie met een toenemende kans op extreem weer (hittegolven, zware stormen). Klimaatverandering is verder een van de factoren die van belang is voor de instabiliteit in de landen rondom Europa, waardoor deze kan toenemen en de Nederlandse nationale veiligheid kan raken. De instabiliteit rondom Europa kan op zijn beurt weer risico's beïnvloeden op het gebied van economie (handel) en internationale vrede en veiligheid (militaire dreiging, CBRN proliferatie).

Een ander voorbeeld van indirecte beïnvloeding van risicocategorieën is de toename van nepnieuws en desinformatie. Dit vormt een voedingsbodem voor bepaalde gedachtevorming op het gebied van bijvoorbeeld extremisme. Op deze wijze kan het vertrouwen in overheidsinstanties worden aangetast. Verder beïnvloedt het de risico's van ongewenste buitenlandse beïnvloeding en inmenging, ondermijnende criminaliteit en niet-gewelddadig extremisme. Ook gewelddadig extremisme en terrorisme worden hierdoor beïnvloed.

### Aantal koppelingen

Uit het overzicht van de koppelingen van de megatrends met de risicocategorieën (zie figuur 2 in hoofdstuk 9) blijkt dat er veel directe koppelingen zijn gelegd, waarbij de trends dus **direct van invloed** zijn op de risico's in de betreffende risicocategorie. Als een risicocategorie door meerdere trends kan worden beïnvloed, wordt dat gezien als indicatie dat er vanuit meerdere hoeken beweging is die relevant kan zijn voor de betreffende categorie.

Uit de resultaten volgt dat de risicocategorie **niet-gewelddadig extremisme** de categorie is met de meeste koppelingen (vanuit informatietechnologie, demografisch-maatschappelijk en ecologie). Ook bij de risicocategorieën **cyberspionage** en **verstoring van vitale infrastructuur** zijn er veel koppelingen met trends gelegd (onder andere vanuit informatietechnologie). Er is verder geconstateerd dat voor de categorieën die moedwillige risico's bevatten de meeste koppelingen kunnen worden gemaakt met de verschillende trends. Naast de al genoemde categorieën gaat het om **handelskrimp**, **digitale sabotage**, **ongewenste buitenlandse inmenging**, **gewelddadig extremisme**, **terrorisme** en **instabiliteit rondom Europa**.

Rondom deze risicocategorieën zijn er veel koppelingen en daarmee ook veel beweging. Dit kan betekenen dat deze risico's relatief gezien eerder onderhevig zijn aan verandering dan anderen. Deze indicatie betekent overigens niet per definitie dat de risico's in deze categorieën ook toenemen, maar wel dat de invulling ervan in risicoanalyses als de GRA periodiek moet worden geëvalueerd in het licht van de relevante ontwikkelingen.

Tenslotte is duidelijk dat de COVID-19-crisis de nationale veiligheid op meerdere manieren raakt. De directe impact op de veiligheidsbelangen (fysieke veiligheid, economische veiligheid) zullen in de actualisatie van het pandemie-scenario in de volgende GRA worden meegenomen. In deze Horizonscan ligt de focus op de invloed van de COVID-19-crisis op de verschillende risicocategorieën. De COVID-19-crisis laat duidelijk een toegenomen afhankelijkheid en kwetsbaarheid zien met koppelingen met **vitale infrastructuur** (IT) en **cyberdreigingen** (cyberspionage en digitale sabotage).

Daarnaast kan COVID-19 leiden tot verdere destabilisatie en conflict, zowel nationaal (bijvoorbeeld **polarisatie** rondom de maatregelen en de gevolgen voor de samenleving) als internationaal (met spanningen binnen **internationale organisaties en veiligheidsarrangementen**). Op deze wijze zijn er koppelingen met de dreigingsthema's **ondermijning democratische rechtsstaat en open samenleving, financieel-economische bedreigingen en bedreigingen internationale vrede en veiligheid**.

#### **Voorbeeld: uitwerking van verwevenheid en interacties van trends**

Bij de toelichting op de koppelingen die zijn gelegd tussen de trends en de risicocategorieën is niet ingegaan op de onderlinge verwevenheid van de verschillende trends. Ook de mogelijke koppeling met de nationale veiligheidsbelangen blijft buiten beschouwing aangezien dit eerst een aanvullende risicoanalyse vergt. Om echter een eerste idee te geven van de onderlinge verwevenheid tussen trends en de wijze waarop verschillende trends niet alleen met elkaar interacteren maar ook elkaar kunnen faciliteren, wordt hieronder een kort voorbeeld gegeven. Dit gebeurt aan de hand van de risicocategorie 'niet-gewelddadig extremisme'. Zoals eerder vermeld is dit de risicocategorie met de meeste koppelingen.

De risicocategorie in kwestie heeft koppelingen met trends op het gebied van ecologie, internationale politiek, informatietechnologie en demografisch maatschappelijke ontwikkelingen. Enkele van deze maatschappelijke ontwikkelingen, zoals de toename van tegenstellingen (sociaaleconomisch én sociaal-cultureel), het toenemende belang van primaire identiteit, en toename van complotdenken vormen een voedingsbodem voor niet-gewelddadig extremisme en polarisatie. Deze trends kunnen op

hun beurt weer worden gefaciliteerd door mogelijkheden en ontwikkelingen op het gebied van informatietechnologie. Met name de mogelijkheden voor een snelle verspreiding van des- en misinformatie vormen hierbij het ideale middel om denkbeelden en standpunten breed, dan wel gericht, te communiceren. Samen kan dit leiden tot complottheorieën, acties en/of demonstraties over bepaalde onderwerpen waarover de meningen binnen de samenleving (sterk) verdeeld zijn. Onderwerpen als 5G, windturbines en de maatregelen rondom COVID-19 zijn hier concrete voorbeelden van. Ook kunnen maatregelen rondom klimaat en milieu, zoals het terugdringen van de uitstoot van stikstof leiden tot maatschappelijke discussie en polarisatie. Daarbij geldt dat dit ook een internationale dimensie heeft en dezelfde onderwerpen leiden tot acties en demonstraties in andere (Europese) landen. Bovendien kunnen kwaadwillende buitenlandse actoren dergelijke polarisatie over specifieke onderwerpen uitbuiten in het kader van buitenlandse beïnvloeding (via hybride operaties). Zij kunnen middels gerichte informatiecampagnes angst en verdeeldheid zaaien en zo polarisatie van het publieke debat verder aanwakkeren.

Als we vervolgens de stap maken naar de mogelijke gevolgen van de bovengenoemde trends op risico's voor de nationale veiligheid, dan komen enkele aspecten naar voren. Ten eerste kan er vanuit een toename van polarisatie en niet-gewelddadig extremisme een lijn lopen naar gewelddadig extremisme. Verder geldt dat de geschetste ontwikkelingen en uitingen rondom niet-gewelddadig extremisme mogelijk de sociale cohesie aantasten, anti-overheidsstemmingen doen toenemen en kunnen zorgen voor het verminderen van het vertrouwen in de overheid en instituties. Dit kan vervolgens leiden tot het aantasten en ondermijnen van de principes van de democratische rechtsstaat en open samenleving. Wat dit precies betekent voor de nationale veiligheid en of de in de GRA 2019 opgenomen scenario's hierdoor dienen te worden bijgesteld, is het onderwerp van de volgende risicoanalyse.

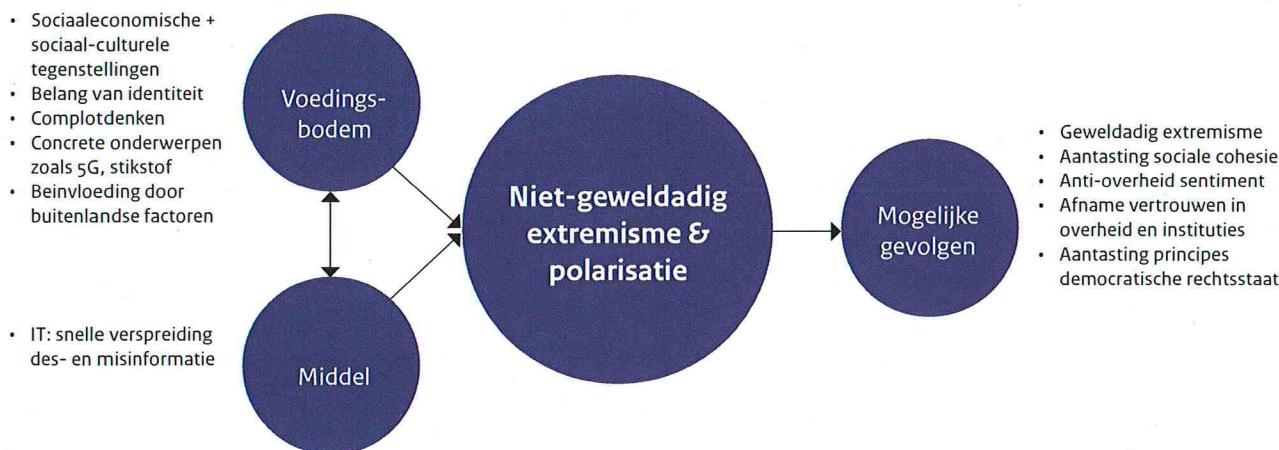
In figuur 2 is dit voorbeeld schematisch samengevat. Een dergelijke uitwerking kan ook voor andere risicocategorieën worden gedaan. Ook daarbij geldt dat dit onderdeel is van een volgende risicoanalyse.

### **10.3 Vergelijking met de resultaten uit de GRA 2019 en de NVS 2019**

In deze paragraaf maken we tenslotte een vergelijking van de resultaten uit de Horizonscan met de resultaten uit de GRA 2019 en de NVS 2019. In de vorige paragrafen zijn de risicocategorieën benoemd die uit de Horizonscan naar voren zijn gekomen waarbij mogelijk beweging is in de risico's.



**Figuur 2.** Schematische weergave van de uitwerking



Uit de vergelijking met de risicocategorieën die in de GRA 2019 als risico's met een hoge waarschijnlijkheid of juist met een hoog risico (qua combinatie van impact én waarschijnlijkheid) zijn benoemd, blijkt de grote overlap. Zo komen de risicocategorieën **verstoring vitale infrastructuur, cyberspionage, handelskrimp, digitale sabotage, ongewenste buitenlandse inmenging en instabiliteit rondom Europa**, zowel in deze verkenning als in de GRA 2019 naar voren.

De risicocategorie **niet-gewelddadig extremisme** vormt hierop de belangrijkste uitzondering. Deze categorie komt in deze verkenning duidelijk naar boven op grond van het aantal koppelingen met de trends, terwijl die niet in het overzicht van de meest relevante risicocategorieën in de GRA 2019 staat. Daaruit valt af te leiden dat deze categorie in beweging is en aandacht behoeft. Of de risico's in deze categorie ook werkelijk toegenomen zijn in waarschijnlijkheid of impact op de nationale veiligheid dient in de volgende risicoanalyse te worden onderzocht. Voor de risicocategorie **terrorisme** geldt het genuanceerde beeld dat het directe risico is afgenomen, maar dat internationale ontwikkelingen zoals instabiliteit in enkele landen in het Midden-Oosten de dreiging op terrorisme ook weer negatief kunnen beïnvloeden.

Er zijn ook enkele risicocategorieën die wel uit de GRA 2019 naar voren komen, maar waar weinig koppelingen vanuit de trends zijn gelegd in deze Horizonscan. Dat gaat met name om infectieziekten en extreem weer. Zoals eerder opgemerkt geldt dat een beperkt aantal koppelingen niet inhoudt dat de risico's binnen een categorie zijn afgenomen of niet relevant zouden zijn. De uitbraak van COVID-19 en de gevolgen laten dat duidelijk zien.

Wanneer de resultaten uit de scan naast de NVS 2019 worden gelegd is het beeld iets anders. In de NVS 2019 zijn zeven dreigingen en thema's genoemd die extra inzet vergen. Dat zijn statelijke dreigingen, polarisatie, vitale infrastructuur, terrorisme en extremisme, militaire dreigingen, criminele ondermijning en digitale dreigingen. De meeste risicocategorieën die uit de scan naar boven zijn gekomen vallen binnen een van deze thema's. Voor de risicocategorieën **verstoring vitale infrastructuur, cyberspionage, digitale sabotage en terrorisme** is dat evident. De risicocategorie **niet-gewelddadig extremisme** past onder de thema's polarisatie en extremisme en de categorie **ongewenste buitenlandse inmenging** heeft een plek onder statelijke dreigingen.

De risicocategorieën **handelskrimp/verstoring internationale handel** en **Instabiliteit rondom Europa** komen niet direct naar voren bij een van de zeven thema's. Deze zouden wellicht extra aandacht behoeven, hoewel er aandacht is voor geopolitieke ontwikkelingen en economische veiligheid binnen de NVS 2019. De belangrijkste risicocategorieën die door de COVID-19-crisis kunnen worden beïnvloed (vitale infrastructuur, cyberdreigingen, niet-gewelddadig extremisme) vallen onder de genoemde thema's uit de NVS 2019. Wel is het vanwege de reikwijdte en impact van de COVID-19-crisis (o.a. op financieel-economisch gebied, de doorwerking in de samenleving en de internationale spanningen) duidelijk dat dit onderwerp niet beperkt is tot risicoanalyse, maar nu vooral gaat over crisisbeheersing<sup>7</sup> en infectieziektebestrijding.

<sup>7</sup> Ook bij de evaluatie van de Wet veiligheidsregio's wordt de crisisbeheersing van COVID-19 betrokken. Onder andere in dit kader wordt gekeken naar de doorontwikkeling van crisisbeheersing.

Dit laatste sluit aan bij het hoofdstuk uit de NVS 2019 waar ingegaan wordt op thema's waar 'onverminderde inzet op weerbaarheid' nodig is. Daar zijn multilaterale instituties, natuurrampen, CBRN-dreigingen en infectieziekten benoemd. Vanuit de geschetste internationale en geopolitieke trends en ontwikkelingen is duidelijk dat multilaterale instituties en CBRN-dreigingen blijvend relevant zijn voor de nationale veiligheid. Datzelfde geldt voor natuurrampen, waarbij klimaatverandering in deze scan als signalering fungeert. Voor infectieziekten geldt tenslotte dat dit door de COVID-19 uitbraak de komende tijd extra aandacht zal vragen.

Resumerend komen er uit de Horizonscan 2020 geen risico's naar voren die nog niet zijn opgenomen in de GRA 2019. Er is wel een versnelling of toename van een aantal trends geconstateerd. Dit heeft mogelijk impact op de waarschijnlijkheid of gevolgen van al in de GRA 2019 opgenomen risico's. Het is belangrijk om hier rekening mee te houden bij het opstellen van de volgende Geïntegreerde Risicoanalyse.



# Bijlage 1. Bronnenlijst

## Bronnenlijst Algemeen

- Analistennetwerk Nationale veiligheid (ANV). *Nationaal Veiligheidsprofiel*, 2016.
- Analistennetwerk Nationale veiligheid (ANV). *Horizonscan Nationale Veiligheid 2019*, 2019.
- Analistennetwerk Nationale veiligheid (ANV). *Leidraad Risicobeoordeling Geïntegreerde Risicoanalyse Nationale Veiligheid*, 2019.
- Analistennetwerk Nationale veiligheid (ANV). *Geïntegreerde Risicoanalyse Nationale Veiligheid*, 2019.
- Analistennetwerk Nationale veiligheid (ANV). *Horizonscan Nationale Veiligheid 2019*, 2019.
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). *Nationale Veiligheid Strategie 2019*, 2019.

## Bronnenlijst Internationale Economie

- Alden, E. (East Asia Forum). *Smaller countries lose in the US-China trade deal*, 2020.
- Baltensperger, M., & Dadusch, U. (Bruegel). *The European Union-Mercosur Free Trade Agreement: Prospects and risks*, 2019.
- Bebavly, M., Baiocco, S., Kilhoffer, Z., Akgüç, M., & Jacquot, M. (CEPS). *Index of readiness for digital lifelong learning*, 2019.
- Bessen, J., Goos, M., Salomons, A., & Berge, W. van den (Brookings). *Automation: a guide for policy makers*, 2020.
- Cameron, A., Claes, G., Midoes, C., & Tagliapietra, S. (Bruegel). *How good is the European Commission's Just Transition Fund Proposal?*, 2020.
- Catuti, M., Egenhofer, C., & Elkerbout, M. (CEPS). *The future of gas in Europe*, 2019.
- Centraal Planbureau (CPB). *Cyberincidenten, veiligheidsmaatregelen en financieel rendement: Een empirische studie van Nederlandse bedrijven*, 2020.
- Centraal Planbureau (CPB). *Een belasting op industriële luchtvervuiling veelbelovend*, 2019.
- Centraal Planbureau (CPB). *Een blik op de beveiligingsadviezen van het NCSC*, 2019.
- Centraal Planbureau (CPB). *Position paper digitalisering*, 2019.
- Centraal Planbureau (CPB). *Risicorapport cyberveiligheid economie 2019*, 2019.
- Centraal Planbureau (CPB). *Risicorapportage Financiële markten 2020*, 2020.

- Centraal Planbureau (CPB). *Scenario's coronacrisis (26 maart 2020)*, 2020.
- Chaziza, M. (Middle East Institute). *The impact of the coronavirus pandemic on China's Belt and Road Initiative in the Middle East*, 2020.
- Cheng, C. (East Asia Forum). *Trump's trade deal poses new dangers to Southeast Asia*, 2020.
- Claes, G., Tagliapietra, S., & Zachmann, G. (Bruegel). *How to make the European Green Deal work*, 2019.
- Control Risks (Control Risks). *Top 5 risks 2020*, 2019.
- Crawford, N. (IISS). *China and instability in developing countries*, 2019.
- Dadush, U., & Ait Ali, A. (Bruegel). *Manufacturing employment, international trade, and China*, 2019.
- Dadush, U., Domínguez-Jiménez, M., & Gao, T. (Bruegel). *The state of China-European Union relations*, 2019.
- Darvas, Z. (Bruegel). *Resisting deglobalisation: the case of Europe*, 2020.
- De Nederlandsche Bank (DNB). *Overzicht financiële stabiliteit: Najaar 2019*, 2019.
- De Nederlandsche Bank (DNB). *Position paper verduurzaming van de financiële sector*, 2019.
- Dechezleprêtre, A., Rivers, N., & Stadler, B. (OECD). *The economic cost of air pollution: Evidence from Europe*, 2019.
- Demertzis, M., & Wolff, G.B. (Bruegel). *Hybrid and cybersecurity threats and the European Union's financial system*, 2019.
- Demertzis, M., Sapir, A., Tagliapietra, S., & Wolff, G.B. (Bruegel). *An effective economic response to the Coronavirus in Europe*, 2020.
- Dröge, S., Neuhoff, K., Egenhofer, C., & Elkerbout, M. (CEPS). *How EU trade policy can enhance climate action*, 2019.
- Editorial Board (East Asia Forum). *Dealing in the brave new post-Trump trade world*, 2020.
- Elkerbout, M., Egenhofer, C., Núñez Ferrer, J., Catuti, M., Kustova, I., & Rizos, V. (CEPS). *The European Green Deal after Corona*, 2020.
- Findlay, C., Kimura, F., & Thangavelu, S. (East Asia Forum). *COVID-19 and the 'zoom' to new global value chains*, 2020.
- Gaidosch, T., Adelman, F., Morozova, A., & Wilson, C. (IMF). *Cybersecurity risk supervision*, 2019.

- Gao, H., & Zhou, W. (East Asia Forum). *China's developing country status brings it few benefits in the WTO*, 2019.
- García-Herrero, A. (Bruegel). *From globalization to deglobalization: Zooming into trade*, 2020.
- García-Herrero, A., & Xu, J. (Bruegel). *How does China fare on the Russian market? Implications for the European Union*, 2019.
- González, A., & Véron, N. (Bruegel). *EU trade policy amid the China-US clash: caught in the crossfire?*, 2019.
- Gordon, D. (IISS). *The looming economic impact of coronavirus*, 2020.
- Gordon, D., Tong, H., & Anderson, T. (IISS). *China's BRI: the development-finance dimension*, 2020.
- Heim, M. (Bruegel). *Can EU competition law address market distortions caused by state-controlled enterprises?*, 2019.
- Hillman, J.A. (Council on Foreign Relations). *A reset of the World Trade Organization's Appellate Body*, 2020.
- Hu, W. (CEPS). *China as developing WTO member, is it a problem?*, 2019.
- Hu, W. (CEPS). *Dinner for three: EU, China and the US around the geographical indications table*, 2020.
- International Monetary Fund (IMF). *Enhancing the emergency financing toolkit - Responding to the COVID-19 pandemic*, 2020.
- International Monetary Fund (IMF). *Global financial stability report, April 2020*, 2020.
- International Monetary Fund (IMF). *Policy steps to address the Corona crisis*, 2020.
- International Monetary Fund (IMF). *World Economic Outlook, April 2020: The great lockdown*, 2020.
- Kahn, M.E., Mohaddes, K., Ng, R.N.C., Pesaran, M.H., Raissi, M., & Yang, J.-C. (IMF). *Long-term macroeconomic effects of climate change: A cross-country analysis*, 2019.
- Kalff, D., Renda, A., Groen, W.P. de, Lannoo, K., Simonelli, F., Iacob, N., & Pelkmans, J. (CEPS). *Hidden treasures*, 2019.
- Kirchner, S. (USSC). *The 'reserve currency' myth: The US dollar's current and future role in the world economy*, 2019.
- Knake, R.A. (Council on Foreign Relations). *Preparing for the future: Assessment of emerging cybersecurity threats*, 2019.
- Knot, K. (DNB). *The impact of the energy transition on our economies and financial sectors: challenges and opportunities*, 2020.
- Kratz, A., Huotari, M., Hanemann, T., & Arcesatti, R. (MERICS). *Chinese FDI in Europe: 2019 update*, 2020.
- McWilliams, B., & Zachmann, G. (Bruegel). *A European carbon border tax: much pain, little gain*, 2020.
- Meltzer, J.P. (Brookings). *A WTO reform agenda*, 2019.
- Meltzer, J.P. (Brookings). *Cybersecurity and digital trade: What role for trade policy*, 2019.
- Meltzer, J.P., & Ferry, C.F. (Brookings). *Cybersecurity and digital trade: Getting it right*, 2019.
- Mittnik, S., Semmler, W., & Haider, A. (IMF). *Climate disaster risk - Empirics and a multi-phase dynamic model*, 2019.
- Nunn, R., O'Donnell, J., Shambaugh, J., Goulder, L.H., Kolstad, C.D., & Long, X. (Brookings). *Ten facts about the economics of climate change and climate policy*, 2019.
- Panezi, M. (Council on Foreign Relations). *Re-evaluating global trade governance structures to address climate change*, 2019.
- Pei, M. (Brookings). *International development cooperation in the age of US-China strategic rivalry*, 2019.
- Petropoulos, G., Marcs, J.S., Moës, N., & Bergamini, E. (Bruegel). *Digitalisation and European welfare states*, 2019.
- Pierri, N., & Timmer, Y. (IMF). *Tech in fin before fintech: blessing or curse for financial stability?*, 2020.
- Pisani-Ferry, J. (Bruegel). *Collective action in a fragmented world*, 2019.
- Pisani-Ferry, J., & Wolff, G.B. (Bruegel). *The threats to the European Union's economic sovereignty*, 2019.
- Prasad, E. (Brookings). *Has the dollar lost ground as the dominant international currency?*, 2019.
- Pupillo, L., Ferreira, A., & Fantin, S., (CEPS). *Artificial intelligence and cybersecurity*, 2020.
- Renda, A., & Laurer, M. (CEPS). *IoT 4 SDGs*, 2020.
- Rizos, V., Bryhn, J., Alessi, M., Campmas, A., & Zarra, A. (CEPS). *Identifying the impact of the circular economy on the fast-moving consumer goods industry*, 2019.
- Rizos, V., Elkerbout, M., & Egenhofer, C. (CEPS). *Circular economy for climate neutrality*, 2019.
- Seaman, J. (IFRI). *China and the new geopolitics of technical standardization*, 2020.
- Tagliapietra, S. (Bruegel). *The impact of the global energy transition on MENA oil and gas producers*, 2019.
- Tagliapietra, S., Zachmann, G., Edenhofer, O., Glachant, J.-M., Linares, P., & Loeschel, A. (Bruegel). *The European Union energy transition: key priorities for the next five years*, 2019.
- Ter Weel, B., Hers, J., Witteveen, J., Verheuvell, N. (SEO Economisch onderzoek). *Economisch beleid na de noodmaatregelen, (Post)coronabeleid op korte, middellange en lange termijn*, 2020.
- Todo, Y. (East Asia Forum). *The fallout from the Japan-Korea trade ruckus on global trade rules*, 2020.
- Triggs, A., & McKibbin, W.J. (Brookings). *Global implications of a US-led currency war*, 2020.
- United Nations Conference on Trade and Development (UNCTAD). *Global trade impact of the coronavirus (COVID-19) epidemic*, 2020.
- United Nations Conference on Trade and Development (UNCTAD). *Key statistics and trends in trade policy 2019*, 2020.
- Veugelers, R. (Bruegel). *Bridging the divide: new evidence about firms and digitalisation*, 2019.
- Ward, R. (IISS). *The global coronavirus crisis - an uneven recovery and rising political risk*, 2020.
- World Economic Forum (WEF). *Jobs of tomorrow: Mapping opportunity in the new economy*, 2020.



- World Economic Forum (WEF). *The Global Risks Report 2020*, 2020.
- Yang, Y. (East Asia Forum). *US-China trade rapprochement round one*, 2020.
- Zachmann, G. (Bruegel). *The European Union-Russia-China energy triangle*, 2019.
- Zenglein, M.J., & Holzmann, A. (MERICS). *Evolving Made in China 2025*, 2019.
- Zhou, W., Gao, H., & Bai, X. (East Asia Forum). *The resurrection of state capitalism in China*, 2019.
- Bronnenlijst Internationale Politiek**
- Algemene Inlichtingen- en Veiligheidsdienst. *AIVD-jaarverslag 2019*, 2020.
- Allahoum, R. (Al Jazeera). *How could coronavirus affect wars in the Arab world?*, 2020.
- Allison, G. (Foreign Affairs Magazine). *The New Spheres of Influence*, 2020.
- Angelo, P.J. (Foreign Affairs Magazine). *The Pandemic Could Bring Power to Latin America's Criminal Gangs*, 2020.
- Antilliaans Dagblad. *Venezuela-crisis kost burger veel*, 2019.
- Arnson, C.J. (Foreign Affairs Magazine). *The Venezuela Refugee Crisis Is Not Just a Regional Problem*, 2019.
- Balcer, A. (ECFR). *National populism at the heart of Europe: When will the clash come?*, 2019.
- Barber, T. (Financial Times). *The tides of illiberalism are beginning to ebb in eastern Europe*, 2019.
- Beemsterboer, T. (NRC). *'Turkije weigert NAVO-bondgenoten te steunen'*, 2019.
- Beemsterboer, T. & M. Kerres (NRC). *EU en Turkije: hard tegen hard*, 2020.
- Beunderman, M. & M. Schinkel (NRC). *Amerikaanse aanval maakt Wereldhandelsorganisatie vleugellam*, 2019.
- Beunderman, M. & M. Schinkel (NRC). *Niets is meer veilig in Trumps handelsoorlog*, 2019.
- Beunderman, M. & C. van de Wiel (NRC). *Ook Europa wil buiten WTO om klappen uitdelen*, 2019.
- Blackwill, R.D. & A.J. Tellis (Foreign Affairs Magazine). *The India Dividend*, 2019.
- Blanksma Çeta, A. & R. Cuperus (de Volkskrant). *Coronacrisis is stresstest voor het brede politieke midden*, 2020.
- Bond, I. (Centre for European Reform). *NATO at 70: Not 'brain dead', but needs shot in arm*, 2019.
- Bond, I. (Centre for European Reform). *The Covid-19 pandemic: The EU must think and act globally*, 2020.
- Bond, I. & A. Gostyńska-Jakubowska (Centre for European Reform). *Democracy and the rule of law: Failing partnership?*, 2020.
- Boon, F. (NRC). *Een Europees initiatief is nog geen Europees leger*, 2019.
- Borger, J. (The Guardian). *Trump re-election could sound death knell for Nato, allies fear*, 2019.
- Bouma, F. (NRC). *Kosovaarse regering valt te midden van coronacrisis*, 2020.
- Brouwers, A. (de Volkskrant). *De opmars van de megafoon-diplomatie: 'Dit mes wordt heel snel bot'*, 2020.
- Brouwers, A. (de Volkskrant). *Relatie tussen Europa en VS wordt steeds ongelijker, blijkt ook uit het Iran-beleid*, 2020.
- Brzozowski, A. (EURACTIV). *Russia significantly steps up Arctic engagement with new strategy*, 2020.
- Cafarella, J. (Foreign Affairs Magazine). *Time to Recommit to Syria*, 2020.
- Cambanis, T. (Foreign Affairs Magazine). *The Coming Emergency in Iraq*, 2019.
- Chun, Z. (The Maritime Executive). *China's "Arctic Silk Road"*, 2020.
- Colby, E.A. & A. Wess Mitchell (Foreign Affairs Magazine). *The Age of Great-Power Competition*, 2020.
- Conley, H.A. & M. Melino (CSIS). *North Macedonia: Issues to Consider for Senate Ratification of an Amended NATO Treaty*, 2019.
- Cordesman, A.H. (CSIS). *China's New 2019: Defense White Paper*, 2019.
- Cukier, E. (NRC). *Rusland ruikt kansen in Arctisch gebied*, 2019.
- De Gruyter, C. (NRC). *De WHO zit in de tang van Trump: 'wie betaalt die bepaalt'*, 2020.
- De Volkskrant. *China weigert oorlogsschepen VS toegang tot haven Hongkong*, 2019.
- De Volkskrant. *Hoge Iraanse legergeneraal gedood bij aanval VS op luchthaven Bagdad*, 2020.
- De Volkskrant. *Iran bestookt Amerikaans-Iraakse luchtmachtbases met raketten*, 2020.
- De Volkskrant. *Iran zet streep door nucleaire deal*, 2020.
- De Volkskrant. *Israël bestookt doelwitten in Syrië en Gaza na raketaanvallen*, 2020.
- De Volkskrant. *Parlement Venezuela roept oppositieleider Guaidó alsnog uit tot voorzitter na sabotagepoging Maduro*, 2020.
- De Volkskrant. *Poetin: 'Rusland op eenzame hoogte met nieuwe, hypersonische raket'*, 2019.
- De Volkskrant. *Premier Kosovo treedt af na oproep Kosovo-tribunaal in Den Haag om zich te melden als verdachte*, 2019.
- De Volkskrant. *VS gaan alle troepen terugtrekken uit noord-Syrië*, 2019.
- De Vries, J. (de Volkskrant). *Economische crisis raakt Venezuela harder dan het coronavirus zelf*, 2020.
- De Waal, M. (NRC). *FARC-afplitsing legt bom onder vrede*, 2019.
- De Waard, P. (de Volkskrant). *Einde van periode van eerlijke en vrije wereldhandel: WTO is vanaf nu tandeloos*, 2019.
- Dekker, B., et al. (Instituut Clingendael). *The multilateral system under stress: Charting Europe's path forward*, 2019.
- Dekker, P. & J. den Ridder (SCP). *Burgerperspectieven 2020* | 1, 2020.
- Dempsey, J. (Carnegie Europe). *Judy Asks: Is the Coronavirus Breeding Disinformation Across Europe?*, 2020.

- Den Ridder, J., et al. (SCP). *Burgerperspectieven 2019* 4, 2019.
- Derix, S. (NRC). 'Rusland probeert waarheidsvinding MH17 te verstoren', 2020.
- Devaux, A. (RAND Corporation). *How to Contain the Disinformation Virus*, 2020.
- Du Pré, R. (de Volkskrant). *Twijfel over de Amerikaanse motieven in de Perzische Golf noopt tot Nederlandse terughoudendheid*, 2019.
- Dunai, M. (Reuters). *Hungary's PM imposes lockdown, seeks more powers for govt to fight coronavirus*, 2020.
- Dupuy, L. (NRC). *De wedloop om de hypersonische raket*, 2020.
- Dupuy, L. (NRC). *Nieuw gevaar: kernkoppen op slagveld*, 2020.
- Dupuy, L. (NRC). *Rusland: hypersonische raket Avangard is in gebruik*, 2019.
- Duxbury, C. (Politico). *The 5 most important races for the Arctic*, 2020.
- Eavis, P., et al. (New York Times). *What's in (and Not in) the US-China Trade Deal*, 2020.
- Eijsvoogel, J. (NRC). *Duitsland wil geen missie onder Amerikaanse leiding*, 2019.
- Elshout, A. (de Volkskrant). *Een wereld zonder INF-raketverdrag is een wereld zonder houvast*, 2019.
- Elshout, A. (de Volkskrant). *Overspelige bondgenoot Turkije zet Navo-familie onder spanning*, 2019.
- Emmott, R. & A. Osborn (Reuters). *Russia aid to Italy leaves EU exposed*, 2020.
- Erlanger, S. (New York Times). *Coronavirus Tests Europe's Cohesion, Alliances and Even Democracy*, 2020.
- Fang, A. (Nikkei Asian Review). *US rejects China's 'near-Arctic state' claim in new cold war*, 2020.
- Fiedler, M. (EURACTIV). *Despite increased solidarity in the pandemic, authoritarianism threatens*, 2020.
- Graham, T. (Foreign Affairs Magazine). *Let Russia Be Russia*, 2019.
- Guo, L. & S.L. Wilson (The Diplomat). *China, Russia, and Arctic Geopolitics*, 2020.
- Hendriksen, K. (Caribisch Netwerk). *Illegaal met de boot vanuit Venezuela: 'Bij vertrek krijgt iedereen al een Curaçaose simkaart'*, 2020.
- Hoogerwaard, J. (NRC). *'China klopt al lang aan de deur bij het Noordpoolgebied'*, 2019.
- Humpert, M. (High North News). *Russia Activates Newest S-300 Air Defense Unit in the Arctic*, 2020.
- International Crisis Group. *CrisisWatch*, 2020.
- Jurna, N. (NRC). *Is corona het laatste zetje naar de afgrond, vragen Venezolanen zich af*, 2020.
- Katz, B. & M. Carpenter (Foreign Affairs Magazine). *ISIS Is Already Rising From the Ashes*, 2019.
- Kerres, M. (NRC). *Vertrouwen tussen NAVO en Turkije is nog niet hersteld*, 2019.
- Kester, S. (de Volkskrant). *Spanning Iran en Westen stijgt na drone-incident en ruzie om aangehouden tanker*, 2019.
- Koelé, T. (de Volkskrant). *Hevige beschietingen Israël en Gaza na dood 'aartsterrorist' Abu al-Ata*, 2019.
- Koelé, T. (de Volkskrant). *Verdeelde Navo richt blik naar de ruimte als mogelijk oorlogsgebied van de toekomst*, 2019.
- Koenis, C. (NRC). *AIVD: rechts-extremisme leeft op, ook in Nederland*, 2020.
- Kopra, S. (The Arctic Institute). *China and its Arctic Trajectories: The Arctic Institute's China Series 2020*, 2020.
- Kotkin, S. (Foreign Affairs Magazine). *American Hustle*, 2019.
- Kruijver, K. (Instituut Clingendael). *(Dis)unity on the NATO Agenda*, 2019.
- Lanting, B. (de Volkskrant). *Islamitische Staat steekt weer de kop op in Syrië, Irak en Afghanistan, waarschuwen veiligheidsdiensten*, 2019.
- Lanting, B. (de Volkskrant). *Rusland wil verdrag strategische kernwapens verlengen*, 2019.
- Le Goff, C. (World Economic Forum). *Yellow vests, rising violence – what's happening in France?*, 2020.
- Legucka, A. (PISM). *Disinformation from China and Russia during the COVID-19 Pandemic*, 2020.
- Legucka, A. (Carnegie Europe). *Russia's Long-Term Campaign of Disinformation in Europe*, 2020.
- Leijendekker, M. (NRC). *Stroom bootmigranten uit Libië zwelt weer aan*, 2020.
- Luckerhof, C. (de Volkskrant). *Krachtmeting in de ruimte: 'supermacht' India laat zich niet weerhouden door afgeblazen maanmissie*, 2019.
- Luckerhof, C. (de Volkskrant). *Macron noemt Navo 'hersendood' na terugtrekken Amerikanen uit Syrië*, 2019.
- Luckerhof, C. (de Volkskrant). *Noord-Korea waarschuwt voor nieuwe Koude Oorlog als de VS middellange-afstands raketten plaatsen in Azië*, 2019.
- Luttikhuis, P. (NRC). *Kiest Groenland voor roofzuchtig China of vriendelijke VS?*, 2020.
- Matthiesen, T. (Foreign Affairs Magazine). *The Coronavirus Is Exacerbating Sectarian Tensions in the Middle East*, 2020.
- McLeary, P. (Breaking Defense). *Battle For The Arctic: Russia Plans Nike Icebreaker, US counters China In Greenland*, 2020.
- Metselaar, D. (NRC). *Nieuwe raketaanvallen Israël en Gazastrook ondanks wapenstilstand*, 2019.
- Modderkolk, H. (de Volkskrant). *Met Stuxnet begon de digitale wapenwedloop*, 2019.
- Moniz, E.J. & S. Nunn (Foreign Affairs Magazine). *The Return of Doomsday*, 2019.
- Musch, S. (NRC). *Separatisten verbreken vredesakkoord met regering Jemen*, 2020.
- Mutsaers, I. & S. Van Pelt (de Volkskrant). *Oorlogstaal rondom coronacrisis vergroot angst en wantrouwen*, 2020.
- Nagtegaal, B. (NRC). *Iran lanceert militaire satelliet, VS waarschuwen voor acties op zee*, 2020.



- Nafm, M. & F. Toro (Foreign Affairs Magazine). *Venezuela's Problem Isn't Socialism*, 2020.
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). *Dreigingsbeeld Terrorisme Nederland 51*, 2019.
- NRC. *251 onbetrouwbare nieuwsberichten over corona via Twitter verspreid*, 2020.
- O'Hanlon, M. (Foreign Affairs Magazine). *Can America Still Protect Its Allies?*, 2019.
- Paauwe, C. (NRC). *Georgië: Russische inlichtingendienst achter grootschalige cyberaanval*, 2020.
- Paauwe, C. (NRC). *VS verlagen bijdrage NAVO-begroting substantieel*, 2019.
- Pelgrim, C. & C. van de Wiel (NRC). *Handelsconflict VS en EU bedreigt wereldeconomie*, 2019.
- Peritz, A. (Foreign Affairs Magazine). *The Coming ISIS Jailbreak*, 2019.
- Persson, M. (de Volkskrant). *Amerika bombardeert uit vergelding doelen in Irak, Syrië en Somalië*, 2019.
- Polyakova, A. & B. Haddad (Foreign Affairs Magazine). *Europe Alone*, 2019.
- Polyakova, A. & D. Fried (Brookings Institution). *Europe is starting to tackle disinformation. The US is lagging*, 2019.
- Przychodniak, M. & M. Makowska (PISM). *Guidelines for the Security of 5G Infrastructure in the European Union*, 2020.
- Pundy, D. (EURACTIV). *'New generation of disinformation' awaits next Commission, says rights group*, 2019.
- Ramdhari, S. (de Volkskrant). *VS hervatten militaire operaties in Irak, ondanks oproep Bagdad om te vertrekken*, 2020.
- Ramdhari, S. (de Volkskrant). *VS testen voor het eerst omstreden middellangeafstandsruket na opschorten INF-verdrag*, 2019.
- Rapp-Hooper, M. (Foreign Affairs Magazine). *Saving America's Alliances*, 2020.
- Rettman, A. (EUobserver). *Optimism and populism clash in central Europe*, 2019.
- Rijksoverheid. *Kamerbrief over de hoofdlijnen van het MIVD jaarplan 2020*, 2019.
- Rijksoverheid. *Kamerbrief tussenrapportage Geïntegreerde Buitenland- en Veiligheidsstrategie*, 2020.
- Rodrik, D. (Foreign Affairs Magazine). *Globalization's Wrong Turn*, 2019.
- Schinkel, M. (NRC). *VS en China: een gewapende vrede aan het handelsfront*, 2020.
- Shan, W. (Foreign Affairs Magazine). *The Unwinnable Trade War*, 2019.
- Sharifi, M.N. (NRC). *Extremisten winnen terrein in de Sahel, zoals eerder in Syrië en Irak*, 2019.
- Shikaki, K. (Foreign Affairs Magazine). *What Comes After the Middle East Peace Process?*, 2020.
- Skydsgaard, N., et al. (Reuters). *China mixing military and science in Arctic push: Denmark*, 2019.
- Stradner, I. & M. Frost (Foreign Policy). *NATO Has a New Weak Link for Russia to Exploit*, 2020.
- The Economist. *A crude attempt to stifle what's left of Venezuela's democracy*, 2020.
- The Economist. *A Saudi ceasefire provides some hope of ending the war in Yemen*, 2020.
- The Economist. *A tale of two crises in Colombia*, 2020.
- The Economist. *America heaps more sanctions on Venezuela*, 2019.
- The Economist. *America seeks faster ways to launch military satellites*, 2019.
- The Economist. *America wants the World Bank to stop making loans to China*, 2019.
- The Economist. *Amid the pandemic, Sino-American relations are worsening*, 2020.
- The Economist. *As Turkey pounds the Syrian army, Russia wants to talk*, 2020.
- The Economist. *China's nuclear arsenal was strikingly modest, but that is changing*, 2019.
- The Economist. *China's rulers see the coronavirus as a chance to tighten their grip*, 2020.
- The Economist. *Colombia's unquiet border with Venezuela*, 2019.
- The Economist. *Donald Trump gives Turkey the green light to invade northern Syria*, 2019.
- The Economist. *Donald Trump is set to rip up another arms-control treaty*, 2019.
- The Economist. *Donald Trump triggers a Turkish invasion and trashes the national interest*, 2019.
- The Economist. *Donald Trump wants to curb Iran. Has he gone about it the right way?*, 2020.
- The Economist. *Donald Trump's betrayal of the Kurds is a blow to America's credibility*, 2019.
- The Economist. *Emmanuel Macron on Europe's fragile place in a hostile world*, 2019.
- The Economist. *Foreign powers are piling into Libya*, 2019.
- The Economist. *Huawei is a cyber-security risk*, 2020.
- The Economist. *In the UN, China uses threats and cajolery to promote its worldview*, 2019.
- The Economist. *Iran's nuclear programme takes a dangerous step*, 2019.
- The Economist. *It's the end of the World Trade Organisation as we know it*, 2019.
- The Economist. *Johnson, Trump and the future of the Atlantic alliance*, 2020.
- The Economist. *Khalifa Haftar, the Libyan warlord, is not interested in compromise*, 2020.
- The Economist. *Missile-testing*, 2019.
- The Economist. *NATO marks its 70th anniversary in typically chaotic fashion*, 2019.
- The Economist. *Nuclear talks between North Korea and America break down, again*, 2019.
- The Economist. *Politics this week*, 2019.
- The Economist. *Politics this week*, 2020.

- The Economist. *Protesters in Iraq topple a prime minister but want more*, 2019.
- The Economist. *Protests in Iraq are met with violence*, 2019.
- The Economist. *Russia and Turkey agree to carve up northern Syria*, 2019.
- The Economist. *Saudi Arabia looks for an exit to the war in Yemen*, 2020.
- The Economist. *Tax our tech and we'll blacklist your bubbly*, 2019.
- The Economist. *The conflict between America and Iran intensifies in Iraq*, 2020.
- The Economist. *The corrupting of democracy*, 2019.
- The Economist. *The House votes to recognise the persecution of Armenians as genocide*, 2019.
- The Economist. *The search to find an alternative to the dollar*, 2020.
- The Economist. *The unintended consequences of indicting Nicolás Maduro*, 2020.
- The Economist. *The World Health Organisation is under fire from America's president*, 2020.
- The Economist. *The world this week*, 2020.
- The Economist. *To mark 70 years of Communist rule, China shows off new weapons*, 2019.
- The Economist. *Turkey is set to send troops to Libya*, 2020.
- The Economist. *Turkey launches an attack on northern Syria*, 2019.
- The Economist. *Turkey's invasion has thrown a once-stable corner of Syria into chaos*, 2019.
- The Economist. *Venezuela's political quarantine*, 2020.
- The Economist. *Why Vladimir Putin cannot retire*, 2020.
- The Economist. *Will an attack on Turkish troops in Syria change the course of the war?*, 2020.
- The Economist Intelligence Unit. *Democracy Index 2019*, 2020.
- The Guardian. *Venezuela: allies of Maduro and Guaidó hold secret talks over coronavirus fears*, 2020.
- The Moscow Times. *Russia Unveils Arctic Ambitions With 2035 Strategy*, 2020.
- Valášek, T. (Carnegie Europe). *Why Can't the EU's West and East Work as One?*, 2019.
- Van den Eerenbeemt, M. (de Volkskrant). *De handelsoorlog tussen de VS en China escaleert in hoog tempo: 'Dit kan nog lang doorgaan'*, 2019.
- Van der Meer, S., et al. (Instituut Clingendael). *Strategic Monitor 2019-2020. CBRN weapons: Where are we in averting Armageddon?*, 2020.
- Van Es, A. (de Volkskrant). *IS herrijst op de schouders van corona, en komt weer dicht bij bewoonde wereld*, 2020.
- Van Laarhoven, K. (NRC). *'Ondanks wapenstilstand vijftien doden bij gevechten in Idlib'*, 2020.
- Van Noort, W. (NRC). *Ian Bremmer: 'De grote vraag is of corona leidt tot een nieuwe Koude Oorlog'*, 2020.
- Van Outeren, E. (NRC). *Oppositie wint verkiezingen in Kosovo*, 2019.
- Van Outeren, E. (NRC). *Speciaal aanklager voor corruptie Noord-Macedonië zelf gearresteerd*, 2019.
- Van Pinxteren, G. (NRC). *China en VS: propagandaoorlog rond Covid-19 verhevigt*, 2020.
- Van Pinxteren, G. (NRC). *China en VS stevenen af op een Koude Oorlog*, 2019.
- Van Raaij, B. (de Volkskrant). *Rusland en Turkije komen staakt-het-vuren overeen in Noordwest-Syrië*, 2020.
- Van Raak, R. (Antilliaans Dagblad). *Schaduw van Venezuela over Curaçao*, 2020.
- Van Straaten, F. (NRC). *Het Afghaans vredesproces in zwaar weer door ruzie tussen president en Taliban*, 2020.
- Van Straaten, F. (NRC). *Pandemie of niet: VS en Iran blijven elkaar in de haren vliegen*, 2020.
- Van Straaten, F. (NRC). *VS weer door militie bestookt in Noord-Irak*, 2020.
- Van Unen, D. & B. Van der Spek (NRC). *Libische generaal Haftar kondigt staakt-het-vuren af*, 2020.
- Vennink, T. (de Volkskrant). *In het noordelijkste stadje van Rusland kunnen ze niet wachten tot de ijskappen smelten*, 2020.
- Verhagen, L. (de Volkskrant). *NCTV waarschuwt voor 'extremistische protestacties' door 5G-tegenstanders die vrezen voor coronavirus*, 2020.
- Vermaas, P. (NRC). *Macron: De NAVO is hersendood*, 2019.
- Vervaeke, L. (de Volkskrant). *Na 40 jaar toenadering ziet China nu vooral een kwaadwillende rivaal in Amerika*, 2019.
- Vervaeke, L. (de Volkskrant). *Wanhoopspoging Huawei: bedrijf sleept VS voor de rechter*, 2019.
- Vindino, L. (Foreign Policy). *Emmanuel Macron's War on Islamism Is Europe's Future*, 2020.
- Vlaskamp, M. (de Volkskrant). *Handelsakkoord is vooral een pas op de plaats tussen VS en China*, 2020.
- Vlaskamp, M. (de Volkskrant). *Vredesakkoord met Taliban bereidt weg voor militaire aftocht VS uit Afghanistan*, 2020.
- Vlaskamp, M. (de Volkskrant). *Wapenstilstand in Jemen biedt voor het eerst in jaren kans op vredesoverleg*, 2020.
- Vos, C. (de Volkskrant). *Jihadisten lijken uit op een nieuw kalifaat in de Sahel en het gaat hen voor de wind*, 2020.
- Vos, C. (de Volkskrant). *Strijd om Libië nadert eindfase na inname kuststad door leger van Haftar*, 2020.
- Vos, C. (de Volkskrant). *Terreuraanslag in Niger grootste ooit, de situatie in Sahel verslechtert snel*, 2019.
- Vos, C. (de Volkskrant). *Turkse inmenging in Libië vergroot spanningen op Middellandse Zee over toegang tot olie en gas*, 2020.
- Vreeken, R. (de Volkskrant). *Coronavirus bereikt Libië, burgeroorlog laait meteen op*, 2020.
- Vreeken, R. (de Volkskrant). *Turkije en Syrië heviger slaags dan ooit*, 2020.
- Vreeken, R. (de Volkskrant). *Turkse grondtroepen vallen Koerdisch gebied in noordoosten Syrië binnen*, 2019.
- Wanat, Z. (Politico). *Commission launches 4th infringement procedure over Poland's rule of law*, 2020.



- Wasilewski, K. (PISM). *Tensions in the Eastern Mediterranean: an Urgent Challenge for the EU*, 2019.
- Weiss, J.C. (Foreign Affairs Magazine). *A World Safe for Autocracy?*, 2019.
- Witteveen, J. & W. Dekker (de Volkskrant). *Wordt corona de nietsontziende vereffenaar van de ongelijkheid?*, 2020.
- Wyne, A. & S.W. Harold (RAND Corporation). *China's Footprint in Europe*, 2020.
- Yahye, E. (NRC). *Zeker drie doden bij protesten Colombia*, 2019.
- Yüksel, E., et al. (Instituut Clingendael). *Covid-19 and Conflict in the Middle East*, 2020.
- Zandee, D., et al. (Instituut Clingendael). *The Future of Arctic Security*, 2020.
- Zerka, P. (ECFR). *Ill will: Populism and the coronavirus*, 2020.
- Bronnenlijst Demografisch Maatschappelijk**  
Algemeen Inlichtingen – en veiligheidsdienst.  
*AIVD-jaarverslag 2019*, 2020.
- Andriessen, I., Hoegen Dijkhof, J., van der Torre, A., van den Berg, E., Pulles, I., Iedema, J. & de Voogd-Hamelink, M. (SCP). *Ervaren discriminatie in Nederland II*, 2020.
- Blanksma Ceta, A. & Cuperus, R. (De Volkskrant). *Coronacrisis is stresstest voor het brede politieke midden*, 30 maart 2020.
- Boeschoten, T. & van de Ven, C. (De Groene Amsterdammer). *'Je gaat me toch niet als genuanceerd wegzetten hè?'. Alt-light en alt-right domineren Nederlands Twitter*, 2019.
- Centraal Bureau voor de Statistiek. *Bevolking; geslacht, leeftijd, generatie en migratieachtergrond*, 1 januari, 2020.
- Centraal Bureau voor de Statistiek. *Randgemeenten bij grote steden groeiden in 2019 het meest*, 2020.
- Day, M. & Badou, M. (Kennissplatform Integratie en Samenleving). *Geboren en getogen: onderzoek naar de identiteitsbeleving en gevoelens van binding van jongeren met een migratieachtergrond*, 2019.
- De Nederlandsche Bank. (DNB). *De woningmarkt. Hollen of stilstaan*, 2019.
- Dekker, P. & Den Ridder, J. (Sociaal- en Cultureel Planbureau). *Burgerperspectieven 2020 |1*, 2020.
- De Volkskrant. *Zo werd het pro-Zwarte Piet-protest steeds gewelddadiger*, Achtergrond, 15 november, 2019.
- Druenen, van R. & Vastrick, E. (Trouw). *Met agrarische hulp je alle boeren*. 2019.
- Edelman. *Edelman Trust Barometer 2020*, 2020.
- Engbersen, G. & Wentink, T. (Erasmus Universiteit Rotterdam). *De bedreigde stad: De maatschappelijke impact van Covid-19 op Rotterdam*, 2020.
- Hulst, van, B., Hoff, S. & Wildeboer Schut, J. (Sociaal- en Cultureel Planbureau). *Armoede in kaart. Armen met en zonder migratieachtergrond*, 2019.
- Identitair Verzet NL. *ID Verzet Twitterpagina*, 2020
- Landelijk Informatie en Expertise Centrum. (LIEC). *Landelijk beeld ondermijnende criminaliteit*, 2019.
- Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Dreigingsbeeld Terrorisme Nederland 50*, 2019.
- Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Dreigingsbeeld Terrorisme Nederland 51*, 2019.
- Newman, N., Fletcher, R., Kalogeropoulos, A. & Kleis Nielsen, R. (Reuters). *Reuters Institute Digital News Report 2019*, 2019.
- Ridder, den, J., Miltenburg, E., Huijnk, W. & van Rijnberk, S. (Sociaal- en Cultureel Planbureau). *Burgerperspectieven 2019|4*, 2019.
- Rogers, R. & Niederer, S. (University of Amsterdam). *The Politics of Social Media Manipulation*, 2019.
- Rutjens, B. (University of Amsterdam). *Verklaart psychologische afstand wantrouwen in de wetenschap?*, 2019.
- Sterkenburg, N. (RAN Centre of Excellence). *A Practical Introduction To Far-Right Extremism*. 2019.
- Sterkenburg, N. (essay in Vrij Nederland.) *Hoe het extreem-rechtse geluid gewoon werd*, 22 januari 2020.
- Tweede Kamer der Staten-Generaal. *Parlementaire ondervragingscommissie ongewenste beïnvloeding uit onvrije landen*, 2019.
- Wagenaar, W. (Anne Frank Stichting). *Factsheet Extreemrechts in Nederlandse Gemeentes 11*, 2019.
- Wal, van der C. & van Mersbergen, C. (artikel in Het Parool). *Ook in Nederland wint extreemrechts terrein*. 2019.
- Wennekers, A., Boelhouwer, J., van Campen, C. & Kullberg, J. (Sociaal- en Cultureel Planbureau). *De sociale staat van Nederland 2019*, 2019.
- Wetenschappelijke Raad voor het Regeringsbeleid. *Project Migratiediversiteit*, 2020.
- Bronnenlijst Ecologie**  
Algemeen Dagblad (AD). *Grootste Nederlandse natuurbrand ooit onder controle, nablussen kan nog weken duren*, 23 april 2020.
- Analistennetwerk Nationale Veiligheid (ANV). *Horizonscan nationale veiligheid 2019*, 2019.
- Analistennetwerk Nationale Veiligheid (ANV). *Geïntegreerde risicoanalyse Nationale Veiligheid*, 2019.
- Bars, D. le. (KNMI). *Zeespiegelstijging nu en in de toekomst*, 14 november 2019.
- Dijkhuis, D. (NU.nl). *Te weinig oog voor ziektes door klimaatverandering*, 3 juni 2020.
- Haasnoot, M. & Hurk, B. van den, (KNMI). *Wat doet Nederland om de gevolgen te beperken?*, 2019.
- Hoekstra, A. (KNMI). *2019 mondiaal in top twee of drie warmste jaren*, 31 december 2019.
- Koninklijk Nederlands Meteorologisch Instituut (KNMI). *Broeikasgassen nemen versneld toe*, 25 september 2019.
- Koninklijk Nederlands Meteorologisch Instituut (KNMI). *Absolute temperatuurrecords door Saharahitte*, 2 augustus 2019.

- Koninklijk Nederlands Meteorologisch Instituut (KNMI). *Hittegolven zoals vorige week vroeger vrijwel onmogelijk*, 2 augustus 2019.
- Koninklijk Nederlands Meteorologisch Instituut (KNMI). *Als de kou uit de lucht is verdwenen*, 20 augustus 2019.
- Koninklijk Nederlands Meteorologisch Instituut (KNMI). *WMO: warmste decennium ooit*, 5 december 2019.
- Koninklijk Nederlands Meteorologisch Instituut (KNMI). *Afgelopen decennium warmste ooit*, 15 januari 2020.
- Koninklijk Nederlands Meteorologisch Instituut (KNMI). *Warm en zonnig 2019*, 3 januari 2020.
- Mach, K.J., Kraan, C.M., Adger, W.N. et al. *Climate as a risk factor for armed conflict*. *Nature* 571, 2019.
- Planbureau voor de leefomgeving (PBL). *Tracking climate policy progress*, 25 februari 2020.
- Tennet. *Monitoring leveringszekerheid 2019*, 1 december 2019.
- Tennet. *Europese samenwerking voorwaarde voor leveringszekerheid elektriciteit na 2025*, 17 januari 2020.
- University of East Anglia (via ScienceDaily). *Climate change increases the risk of wildfires confirms new review*, 14 januari 2020.
- World Economic Forum (WEF). *The global risk report 2020*, 15 januari 2020.
- World Meteorological Organization (WMO). *2019 concludes a decade of exceptional global heat and high-impact weather*, 3 december 2019.
- World Meteorological Organization (WMO). *WMO Statement on the state of the global climate in 2019*, 2020.
- Compendium voor de Leefomgeving (CLO). *Living Planet Index Nederland, 1990-2018*, 27 februari 2020.
- Interprovinciaal overleg (IPO) & Ministerie van Landbouw, Natuur en Voedselkwaliteit (LNV). *Vijfde Voortgangsrapportage Natuur. Natuur in Nederland: Stand van zaken eind 2018 en ontwikkelingen in 2019*, oktober 2019.
- Wereld Natuur Fonds (WNF). *Living Planet Report Nederland. Natuur en landbouw verbonden*, 2020.
- Rijksinstituut voor Volksgezondheid en Milieu (RIVM) *Infectieziekten Bulletin november 2019, Jaargang 30, nummer 6*, 2019.
- Klink, R. van, Bowler, D.E., Gongalsky, K.B., Swengel, A.B., Gentile, A. and Chase, J.M. *Meta-analysis reveals declines in terrestrial but increases in freshwater insect abundances*. *Science*, 368(6489), 2020.
- Rijksinstituut voor Volksgezondheid en Milieu (RIVM). *Atlasinfectieziekten, Psittacose (papegaaienziekte)*. Geraadpleegd op 30 april 2020.
- European Environment Agency (EEA). *SOER 2020*, 4 december 2019.
- Europees Milieu Agentschap. *Het klimaat, de natuur en de mensheid vragen onze aandacht*, 11 februari 2020.
- Informatiehuis Water. *Factsheets*. Geraadpleegd op 1 april 2020.
- Koninklijk Nederlands Meteorologisch Instituut (KNMI). *Afname luchtvervuiling boven Nederland*, 27 maart 2020.
- KWR. *De kwaliteit van bronnen van drinkwater in Nederland*, augustus 2019.
- Rijksoverheid. *Schone lucht akkoord: Gezondheidswinst voor iedereen in Nederland*, 13 januari 2020
- Rijksoverheid. *Vergunningverlening projecten komt weer op gang*, 13 september 2019
- Rijksinstituut voor Volksgezondheid en Milieu (RIVM). *Monitoringsrapportage NSL 2019. Stand van zaken Nationaal Samenwerkingsprogramma Luchtkwaliteit*, december 2019.
- Volkskrant. *De coronacrisis als generale repetitie voor klimaatcrisis die komt*, 20 maart 2020.

#### Bronnenlijst Informatietechnologie

- Algemene Rekenkamer. *Factsheets: Grip op digitalisering: rode draden uit tien jaar Rekenkameronderzoek*, 2020.
- Autoriteit Persoonsgegevens. *Privacy corona-apps niet aangetoond*, 20 april 2020.
- Autoriteit Persoonsgegevens. *Keuzehulp privacy bij videobel-apps*, 15 april 2020.
- Autoriteit Persoonsgegevens. *Focus AP 2020-2023. Dataproductie in een digitale samenleving*, 11 november 2019.
- Bittle, Jake. *Lie detectors have always been suspect. AI has made the problem worse*. *MIT Technology Review*, 13 maart 2020.
- Blauw, Sanne (De Correspondent). *Kun je van algoritmes verwachten dat ze onbevooroordeeld zijn?*, 13 februari 2020.
- Bullhorst, M. (Trouw). *Persoonsgegevens naar China sturen mag niet, maar bedrijven doen het toch*, 29 januari 2020.
- Chavannes, Esther en Arkhipov-Goyal, Amit (The Hague Centre for Strategic Studies). *Towards Responsible Autonomy. The Ethics of Robotic and Autonomous Systems in a Military Context*, september 2019.
- Comiter, Marcus (Harvard Kennedy School Belfer Center for Science and International Affairs). *Attacking Artificial Intelligence AI's Security Vulnerability and What Policymakers Can Do About It*, augustus 2019.
- Condliffe, J. (New York times). *The Week in Tech: Algorithmic Bias Is Bad. Uncovering It Is Good*, 15 november 2020.
- Daws, R. (IoT Tech News). *Bitdefender: New botnet is targeting millions of IoT devices*, 14 april 2020.
- Van den Dool, P. (NRC). *Kamer begint parlementair onderzoek naar gebrek aan grip op digitalisering*, 3 juni 2019.
- European Commission. *On Artificial Intelligence – A European approach to excellence and trust. White paper, COM(2020) 65 final*, 2020.
- European Commission. *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics. COM(2020) 64 final*, 2020.



- European Commission. *Reports on the status of internet capacity during coronavirus confinement measures*, 2020.
- Franke, Ulrike & Sartori, Paola (European Council on Foreign Relations). *Machine Politics: Europe and the AI revolution*, juli 2019.
- Future Today Institute. *2020 Tech Trends Report*, 2020.
- Gallagher R., & Bloomberg (Fortune). *Hackers 'without conscience' demand ransom from dozens of hospitals and labs working on coronavirus*, 2020.
- Gallagher, Ryan en Jona, Ludicova (The Intercept). *We Tested Europe's New Lie Detector for Travelers and Immediately Triggered a False Positive*, 26 juli 2019.
- De Groot, Natasja (Algemeen Dagblad). *Privacybaas Aleid Wolfsen: 'Het is levensgevaarlijk wat hier gebeurt'*, 6 april 2020.
- Hijink, M. (NRC). *Apple-klokkenluider: Elke dag hoorde ik 1.300 Siri gesprekken*, 19 mei 2020. Hofman, Lennart (De Correspondent). *Robotsoldaten zijn allang geen sciencefiction meer (en dus bouwt Nederland ze ook)*, 21 januari 2020.
- Van Iperen, R. (Vrij Nederland). *In de strijd tegen het coronavirus loopt onze privacy groot gevaar*, 1 april 2020.
- Kasapoğlu, C. en Kirdemir, B. (Carnegie Europe). *Artificial Intelligence and the Future of Conflict*, 2019.
- Kastelijjn, N. (NOS). *Chinese TikTok razend populair maar ook vragen over privacy en censuur*, 1 december 2019.
- Kayali, L. (Politico). *Apple whistleblower calls for European privacy probes into Big Tech voice assistants*, 20 mei 2020.
- De Lange, Rob en Leupen, Johan (Financieel Dagblad). *De wurggreep van de softwarereuzen*, 4 oktober 2019.
- Lelieveld, B. (Algemeen Dagblad). *We moeten maar vast wennen aan de drones*, 3 april 2020.
- Lewis, James Andrew (Center for Strategic and International Studies). *Big Company, Big Government, Big Brother? Privacy after Covid-19*, 17 april 2020.
- Mchangma, Jacob & McLaughlin, Sarah (Foreign Policy). *Coronavirus Has Started a Censorship Pandemic*, 1 april 2020.
- Meessen, R. Torossian, B., Bekkers, F. (TNO & HCSS). *A Horizon Scan of Trends and Developments in Hybrid Conflicts Set to Shape 2020 and Beyond*, 2020.
- Meserole, C. (Brookings). *COVID-19 and the future of techlash*, 27 april 2020.
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. *Beleidsbrief AI, publieke waarden en mensenrechten*, 2019.
- Ministerie van Economische Zaken en Klimaat. *Strategisch actieplan voor Artificiële Intelligentie*, 2019
- National Cyber Awareness System. *COVID-19 Exploited by Malicious Cyber Actors. US Department of Homeland Security, Alert (AA20-099A)*, 8 april 2020.
- Nationaal Coördinator Terrorismedebestrijding en Veiligheid (NCTV). *Reactie NCTV op sabotage en brandstichting zendmasten Nederland*, 10 april 2020.
- Nationaal Coördinator Terrorismedebestrijding en Veiligheid (NCTV). *Cybersecuritybeeld Nederland 2019*, 2019.
- Nationaal Coördinator Terrorismedebestrijding en Veiligheid (NCTV). *Cybersecuritybeeld Nederland 2020*, 2020.
- Nationaal Coördinator Terrorismedebestrijding en Veiligheid (NCTV). *Nationaal Crisisplan Digitaal*, 2020.
- Van Noort, Wouter (NRC). *Algoritmes en drones moeten het coronavirus in toom houden*, 4 maart 2020.
- NOS. *Meerderheid zou veilige corona-app installeren*, 30 april 2020.
- NOS. *Waarom worden door heel Nederland zendmasten in brand gestoken?*, 11 april 2020.
- Nurkin, Tate & Rodriguez, Stephen (Atlantic Council Scowcroft Center for Strategy and Security). *A Candle in the Dark: US National Security Strategy for Artificial Intelligence*, 2019.
- Petitjean, Frederic (Computable). *Duitsland wil minder afhankelijk worden van Microsoft*, 23 september 2019.
- Prins, J., Schrijvers, E. Passchier, R., De Visser, M. (Wetenschappelijke Raad voor Regeringsbeleid) *Voorbereiden op digitale ontworping (WRR-Rapport 101)*, 2019.
- Rechtbank Den Haag. *SyRI-wetgeving in strijd met het Europees Verdrag voor de Rechten voor de Mens*, 5 februari 2020.
- Rohmensen, G. J. (Trouw). *Ransomware is toenemend gevaar voor bedrijven en organisaties*, 3 januari 2020.
- Sanger, D. & Perloth, N. (New York Times). *U.S. Escalates Online Attacks on Russia's Power Grid*, 15 juni 2019.
- Taylor, M.P. et al. (Cappgemini Research Institute). *Smart Talk: How organizations and consumers are embracing voice and chat assistants*, 2019.
- Van Teeffelen, K. (Trouw). *Drones controleren of u zich aan de coronaregels houdt, maar mag dat eigenlijk wel?*, 1 april 2020.
- Van Teeffelen, K. (Trouw). *Nederland is wel erg afhankelijk van bedrijven als Google en Huawei en dat is gevaarlijk, zegt NCTV*, 12 juni 2019.
- UN Department of Global Communications (United Nations). *UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis*, 31 maart 2020.
- Ungerer, Christoph & Portugal, Alberto (Brookings). *Leveraging e-commerce in the fight against COVID-19*, 27 april 2020. Brookings.
- Vaughan, Adam (NewScientist). *Companies could be fined if they fail to explain decisions made by AI*, 2 december 2019.
- Verbruggen, M. (EU Non-Proliferation and Disarmament Consortium). *The Question of Swarms Control: Challenges to Ensuring Human Control over Military Swarms. Non-Proliferation and Disarmament Papers (no. 65)*, 2019.
- Verdict. *AI vs. AI: Artificial Intelligence and the DDoS Attack*, 2019.
- Vereniging van Nederlandse Gemeenten (VNG). *Principes voor de digitale samenleving*, 1 november 2019.

Verhagen, L., & Waarlo, N. (De Volkskrant). *Technologiebedrijven zijn wapen en speelbal geworden in geopolitieke strijd*, 7 januari 2020.

Wakefield, J. (BBC News). *Russia 'succesfully tests' its unplugged internet*, 24 december 2019.

Wassens, R. (NRC). *Groeiende kritiek op gehaaste selectieprocedure corona-app*, 17 april 2020.

White, G. (The Telegraph). *The internet's fracturing will change American capitalism forever*, 1 mei 2020.

Wolswinkel, J. *Betoog: Algoritmen niet blind volgen*. VNG Magazine, nummer 1, 2020.

Yeung, K. (Council of Europe). *Responsibility and AI*. Council of Europe study DGI(2019)05, 2019.



# Bijlage 2. Overzicht van dreigingsthema's en risicocategorieën

In onderstaande tabel is het overzicht van deze thema's en risicocategorieën uit de GRA 2019 opgenomen.

**Tabel 10.** Overzicht thema's en risicocategorieën

Thema	Risicocategorie
Bedreigingen voor gezondheid en milieu	Infectieziekten humaan
	Dierziekten en zoönose
Natuurrampen	Extreem weer
	Overstroming
	Natuurbrand
	Aardbeving
Verstoring vitale infrastructuur	Verstoring vitale infrastructuur
Zware ongevallen	Stralingsongevallen
	Chemische incidenten
Cyberdreigingen	Digitale sabotage
	Aantasting functioneren internet
	Cyberspionage
	Cybercriminaliteit
Ondermijning democratische rechtsstaat	Niet-gewelddadig extremisme
	Ondermijnende criminaliteit (enclavevorming)
	Ongewenste buitenlandse inmenging
	Ongewenste buitenlandse beïnvloeding (via hybride operaties)

<b>Thema</b>	<b>Risicocategorie</b>
<i>Gewelddadig extremisme en terrorisme</i>	Gewelddadig extremisme
	Terrorisme
<i>Financieel-economische bedreigingen</i>	Criminele inmenging
	Bedreigingen van de knooppuntfunctie en de aan- en afvoerlijnen van Nederland (flow security)
	Handelskrimp/verstoring internationale handel
	Destabilisatie financieel systeem
<i>Bedreigingen internationale vrede en veiligheid</i>	Instabiliteit rondom EU
	Militaire dreigingen (NAVO-lidstaat)
	CBRN-proliferatie
	Veiligheidsarrangementen onder druk (NAVO, EU)



## Analistennetwerk Nationale Veiligheid



Rijksoverheid

Dit is een uitgave van :

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)  
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)  
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)  
Nederlandse Organisatie voor toegepast-natuur-wetenschappelijk onderzoek (TNO)  
Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael'  
Erasmus Universiteit Rotterdam, Institute of Social Studies (ISS)

Oktober 2020