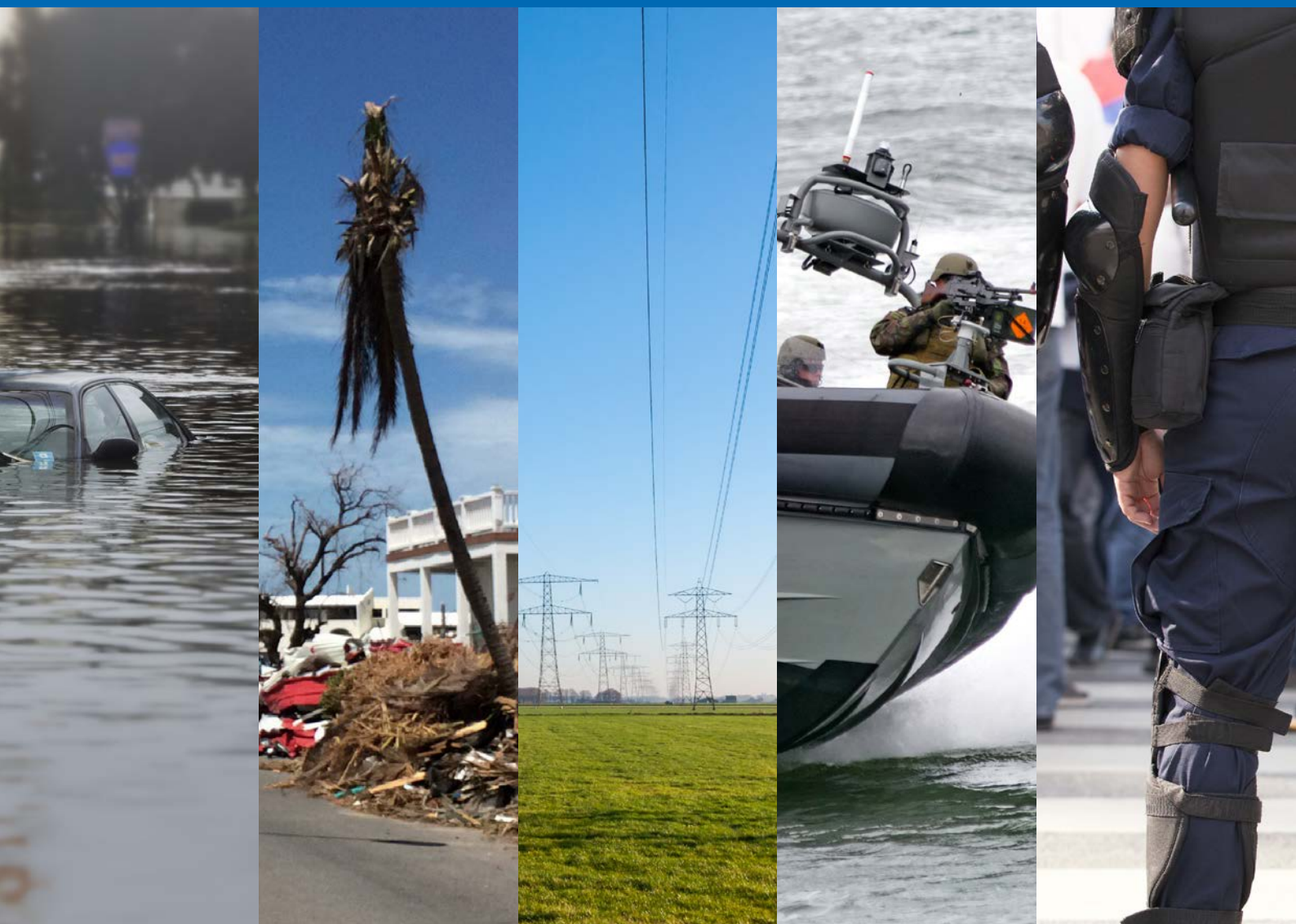
Trendanalyse Nationale Veiligheid 2024

Verdieping op de Trendanalyse

Analistennetwerk Nationale Veiligheid



Trendanalyse Nationale Veiligheid 2024

Verdieping op de Trendanalyse

Analistennetwerk Nationale Veiligheid

Colofon

Deze Trendanalyse is gemaakt door het Analistennetwerk Nationale Veiligheid in opdracht van de NCTV.

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

Contact: *anv@rivm.nl*

Inhoudsopgave

Inleiding

Voor u ligt de Verdieping op de Trendanalyse Nationale Veiligheid 2024. Dit document is opgesteld door het Analistennetwerk Nationale Veiligheid (ANV) op verzoek van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De Trendanalyse brengt de belangrijkste ontwikkelingen voor de nationale veiligheid in kaart en dient daarmee als onderbouwing voor het actualiseren van de implemantatie van Veiligheidsstrategie voor het Koninkrijk der Nederlanden. De Trendanalyse zelf bouwt voort op de bevindingen uit de in 2022 door het ANV opgestelde Rijksbrede Risicoanalyse Nationale Veiligheid (RbRa; ANV, 2022).

De Trendanalyse nationale veiligheid bestaat uit twee delen:
- Het Hoofdrapport;
- De Verdieping op de Trendanalyse.

Deze Verdieping op de Trendanalyse bevat voor elk van de tien dreigingsthema's uit de RbRa een overzicht van ontwikkelingen (onderdeel A). Dit wordt aangevuld met een overzicht van ontwikkelingen op acht verschillende technologiegebieden met mogelijke implicaties voor de nationale veiligheid (onderdeel B). Dit rapport bevat ook een nadere toelichting van de gehanteerde methode (onderdeel C) en een korte introductie tot het ANV (onderdeel D).

Een meer samenvattend en integraal beeld van ontwikkelingen kan worden gevonden in het hoofdrapport. Het Hoofdrapport bevat ook de thema-overstijgende, strategische inzichten die naar voren zijn gekomen uit de Trendanalyse en staat tevens stil bij de mogelijke implicaties voor verdere strategievorming.

Onderdeel A
Overzicht van ontwikkelingen per dreigingsthema uit de RbRa

Dit onderdeel bevat per dreigingsthema uit de Rijkrede Risicoanalyse (RbRa) een overzicht van de belangrijkste ontwikkelingen.[1] Afhankelijk van de indeling en inhoud van het dreigingsthema in kwestie wordt of voor het thema als geheel of voor de onderliggende dreigingscategorieën ingegaan op:

- De belangrijkste bevindingen en conclusies uit de Trendanalyse
- Een algemeen overzicht van bevindingen en de stand van zaken ten opzichte van de RbRa
- Nadere toelichting op het dreigingsbeeld naar aanleiding van mogelijke ontwikkelingen

[1] Noot: het onderwerp georganiseerde criminaliteit is niet een eigen dreigingsthema in de RbRa, maar is hier wel apart opgenomen als thema om aan te sluiten bij de indeling gehanteerd in de veiligheidsstrategie

A.1 Klimaat- en natuurrampen

Belangrijkste bevindingen en conclusies
Binnen het thema Klimaat- en natuurrampen zijn in de Rijksbrede Risicoanalyse vier typen dreigingen in kaart gebracht die de nationale veiligheid kunnen raken. Het gaat hierbij om overstromingen, extreem weer, natuurbranden en aardbevingen. Er is reeds in de RbRa gesignaleerd dat klimaatverandering van grote invloed is op deze dreigingen. Ten opzichte van de inzichten in de RbRa blijft klimaatverandering versnellen en kunnen de effecten groter worden dan tot dan toe werd gedacht. Zowel de impact als de waarschijnlijkheid van extreem weer, overstromingen en natuurbranden neemt hierdoor toe.

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

Extreem weer
Uit de KNMI klimaatscenario's (KNMI, 2023) blijkt dat de gemiddelde temperatuur in Nederland verder is toegenomen en zal blijven stijgen, sneller dan eerder werd verwacht. Hogere temperaturen vertalen zich in meer en zwaardere weersextremen, zoals extreme hitte, droogte en neerslag. Vooral de verwachtingen voor Nederlandse zomers vallen op. De zomers worden een stuk heter en er zal sprake zijn van meer en intensere hittegolven (PBL, 2024). In een 2 graden warmere wereld kan de zomerhitte in Nederland rond 2100 tot 45 graden Celsius reiken. Door het hitte-eilandeffect liggen de temperaturen in steden, vooral 's nachts, gemiddeld 5 graden hoger dan in het buitengebied (KNMI, 2023; Nu.nl, 2023). De negatieve effecten van de opwarming zullen dan ook het eerst in de steden gevoeld worden (EEA, 2022; Academische Werkplaats Gezonde Leefomgeving, 2023).

Hittegolven zijn nu wereldwijd al de dodelijkste natuurrampen en dit zal de komende jaren alleen maar toenemen (VN, 2023). Van de sterfgevallen door hitte in Nederland kan al 31% worden toegeschreven aan klimaatverandering. Dat komt neer op bijna 250 sterfgevallen per jaar (RIVM, 2021). Vooral de hogere nachttemperaturen zijn gevaarlijk omdat het lichaam niet kan herstellen van de hitte.

Naast dat de temperatuur toeneemt kan het ook aanzienlijk droger worden dan eerder werd gedacht. In het droogste KNMI-scenario kan het gemiddelde neerslagtekort in 2100 79 procent groter zijn dan in de afgelopen dertig jaar (KNMI, 2023). In dit droogste scenario is een gemiddelde zomer in de toekomst (in 2100) ongeveer even droog als een extreem droge zomer nu. Tegelijkertijd neemt ook het aantal zware buien met veel neerslag toe (KNMI, 2023). Het aantal stortbuien per jaar is in Nederland in een eeuw tijd al bijna in aantal verdubbeld. Er vindt een verschuiving

plaats van lichte naar zwaardere (er valt meer regen uit de bui) en intensere (er valt meer regen in een bepaalde tijd) buien (KNMI, 2023). Daarbij komt dat windstoten bij buien sterker kunnen worden, de kans op valwinden toeneemt en de grootste hagelstenen vermoedelijk nog groter worden.

Ook in het Caribisch deel van het Koninkrijk neemt de temperatuur toe. Hierdoor kunnen extreem hoge temperaturen worden bereikt. Zo was de zomer van 2023 het warmste ooit met temperaturen tussen de 40 en 50 graden Celsius (Stamper, 2023). Dergelijke hoge temperaturen kunnen zorgen voor gezondheidsschade. Ook kan verlies aan biodiversiteit ontstaan. Dit is te zien aan verblekende koralen. Daarnaast is er juist een toename in Sargassum (verstikkend zeewier) dat de stranden vervuilt (Centrale Bank Curaçao & Sint Maarten, 2023). Naast hogere temperaturen gaat het harder waaien en neemt de totale hoeveelheid regen naar verwachting af (KNMI, 2023). Al zullen er ook momenten zijn met extreme neerslag, zoals in november 2022 toen Bonaire last had van enorme regenval, waardoor delen van het eiland onder water stonden (NOS, 2023). Op de bovenwindse eilanden neemt de kans op zware orkanen met veel regen toe. Voor orkanen van de zwaarste categorie neemt de herhalingstijd toe van eens in de 20 tot 34 jaar in de toekomst (tot 2050), tegenover eens in de 39 jaar nu (KNMI, 2023). Voor de benedenwindse eilanden geldt dat zij niet direct worden getroffen door deze orkanen omdat deze veelal een noordelijkere route volgen. Wel zijn er signalen dat deze route zich geleidelijk verplaatst richting het zuiden, waardoor de benedenwindse eilanden vaker te maken zullen krijgen met de effecten van (op een afstand) langstrekkende orkanen, waaronder zware regenval. Een toename in zware regenval kan op zijn beurt leiden tot (een versnelling van) erosie. De extremere temperaturen, verblekend koraal en vervuilde stranden kunnen een bedreiging vormen voor de bewoners en voor het toerisme. De Caribische economie draait op toerisme. Wegvallen hiervan heeft daardoor grote economische gevolgen. Daarnaast kan het afsterven van koraal ook gevolgen hebben voor de visserij, omdat gezond koraal belangrijke schuil- en broedplaatsen zijn voor vissen. Daarnaast kunnen klimaat gerelateerde natuurrampen, zoals orkanen, grote financiële verliezen met zich meebrengen en vitale processen, de samenleving en economie ontwrichten (Centrale Bank Curaçao & Sint Maarten, 2023).

Overstromingen

Zoals hierboven is beschreven zorgen hogere temperaturen ervoor dat de kans op en intensiteit van weersextremen toenemen. Uit de KNMI-klimaatscenario's volgt dat de weersextremen zo extreem kunnen worden dat het watersysteem dit waarschijnlijk niet meer op kan vangen (KNMI, 2023).

Aan de ene kant neemt het aantal zware buien met veel neerslag in korte tijd toe. Hierdoor neemt ook de kans op wateroverlast en overstromingen toe. Aan de andere kant wordt het aanzienlijk droger in Nederland, vooral tijdens de zomers. Hierdoor kan, sneller dan tot nu toe werd gedacht, een zoetwatertekort ontstaan voor drinkwaterproductie, natuur, landbouw, industrie en overige watervragers. De verwachting is dat de huidige zoetwaterbuffer van het IJsselmeer, vanaf 2050 vaker dan eens per 5 jaar ontoereikend zal zijn (KKNMI, 2023). Nederland krijgt dus te maken met twee tegengestelde problemen.

Naast extreem weer heeft ook de zeespiegelstijging effect op het watersysteem. De zeespiegelstijging zet door en blijft versnellen (PBL, 2024). Nu met enkele millimeters per jaar, maar dit loopt naar verwachting op tot enkele decimeters per jaar (16 tot 37 cm) in 2050. Hierdoor neemt de kans op overstromingen en daarmee het risico voor mens, omgeving en milieu toe (KNMI, 2023). Voor het Caribisch deel van het Koninkrijk vormt de zeespiegelstijging vooral een bedreiging voor de laaggelegen delen van de benedenwindse eilanden. Overigens zijn overstromingen (en de kwetsbaarheid hiervoor) hier niet alleen te wijten aan klimaatverandering, maar ook aan het weghalen van natuurlijke barrières zoals mangroves, ontbossing en grootschalig bouwen in kustgebieden.

Natuurbranden

Naast problemen in het watersysteem zorgen hogere temperaturen ook voor een vergrote kans op natuurbranden (PBL, 2024). Het aantal natuurbranden en de intensiteit hiervan neemt wereldwijd toe. Daarbij is de duur van het natuurbrandseizoen sinds 1979 met 27% toegenomen (OECD, 2023). Door de effecten van klimaatverandering zal ook Nederland vaker te maken krijgen met natuurbranden (KNMI, 2023). Doordat droogte en warmte elkaar versterken, neemt het natuurbrandrisico sneller toe dan dat het klimaat verandert (NIPV, 2023). Ook worden natuurbranden steeds vaker intense branden die niet meer te blussen zijn en neemt de kans op de gelijktijdigheid van zulke branden toe. Dit kan zorgen voor een zodanig toenemende druk op het brandweersysteem dat de grenzen van brandbestrijding worden bereikt (NIPV, 2023).

Aardbevingen

Aardbevingen worden niet beïnvloed door klimaatverandering. Voor geïnduceerde aardbevingen is de belangrijkste ontwikkeling dat de gaswinning in Groningen per oktober 2023 is gestopt. Per 19 april 2024 is het Groningenveld definitief gesloten, zodat ook opstarten in noodgevallen niet meer mogelijk is (Rijksoverheid, 2024). Het stoppen van de gaswinning zorgt ervoor dat zowel de waarschijnlijkheid als de kracht van de aardbevingen afneemt. In de afgelopen jaren is er een daling in het totaal aantal aardbevingen in

Groningen zichtbaar. Het grootste aantal bevingen met een magnitude groter dan 1,5 is geregistreerd in 2013 (30). In 2018 (15), 2019 (11), 2020 (16), 2021 (12), 2022 (12) en in 2023 (9) was dit aantal een stuk lager (KNMI, 2024). Er zal echter nog lange tijd kans op aardbevingen blijven vanwege de drukverschillen die door de gaswinning in de bodem zijn opgebouwd. Voor natuurlijke aardbevingen zijn er geen ontwikkelingen bekend die van invloed zijn op de dreiging.

Toelichting dreigingsbeeld

De almaar versnellende klimaatverandering heeft gevolgen voor het dreigingsbeeld van de dreigingscategorieën extreem weer, overstromingen en natuurbranden. De waarschijnlijkheid en de impact hiervan nemen toe.

Hogere temperaturen vertalen zich in meer weersextremen, zoals extreme hitte, droogte en neerslag. Daarentegen neemt het aantal ijsdagen af. De waarschijnlijkheid van een sneeuwstorm neemt daardoor af. De hogere temperaturen zorgen er ook voor dat de weersextremen zwaarder kunnen worden en daardoor de impact kan toenemen. Het aantal doden als gevolg van hitte zal de komende jaren bijvoorbeeld toenemen. Daarnaast neemt de blootstelling aan uv-straling toe, waardoor de kans op een chronische ziekte als huidkanker stijgt (PBL, 2024). Ook kunnen extreem hoge temperaturen zorgen voor een gebrek aan primaire levensbehoeften. Door de stijgende temperaturen ontstaat er sneller dan tot nu toe werd gedacht een zoetwatertekort voor drinkwaterproductie, natuur, landbouw, industrie en overige watervragers. Hierdoor kunnen de beschikbaarheid van drinkwater en mogelijkheden voor persoonlijke hygiëne onder druk komen te staan. Ook kan bijna de helft van de mensen weinig verkoeling vinden in huis als het aanhoudend warm is. Dit raakt de beschikbaarheid van een veilige woon- en leefomgeving. Daarbij komt dat het door het hitte-eilandeffect in steden tot wel 5 graden warmer kan worden dan in het buitengebied en juist hier veel kwetsbare groepen mensen aanwezig zijn in bijvoorbeeld scholen en ziekenhuizen. Ook hierdoor kan de beschikbaarheid van een veilige woon- en leefomgeving worden aangetast, evenals de continuïteit van essentiële gezondheidszorg. Als de temperatuur dusdanig hoog wordt dat het tijdelijk niet verantwoord is om naar buiten te gaan, raken mensen in hun dagelijks leven verstoord. Voor korte tijd kan het daardoor niet mogelijk zijn om naar school, werk en maatschappelijke voorzieningen te gaan, of noodzakelijke aankopen te doen.

Voor het watersysteem is vooral de verwachting opvallend dat het enerzijds extreem droog kan worden en anderzijds ook in korte tijd zeer veel regen kan vallen. Het Nederlandse watersysteem moet dus voorbereid zijn op de impact van twee uiterste dreigingen. Bij natuurbranden speelt dat de grote kans van optreden, in combinatie met een verdere verdichting van Nederland kan leiden tot grotere impact. Mensen zullen vaker moeten vluchten, er zal vaker directe en indirecte schade en uitval van vitale infrastructuur zijn en er zal vaker onherstelbare schade aan flora en fauna ontstaan. Daarnaast zal de gezondheid van mensen vaker bedreigd worden (NIPV, 2023).

A.2 Infectieziekten

Belangrijkste bevindingen en conclusies
Voor alle ontwikkelingen die al zijn beschreven in de RbRa geldt dat de situatie in de tussentijd grotendeels onveranderd is. Er zijn geen veranderingen geweest die invloed hebben op de nationale veiligheid. Wel geldt dat nieuwe technologische ontwikkelingen binnen de bioinformatica en AI nu en in de toekomst invloed zullen hebben op risico's door infectieziekten. Ook kan een dalende vaccinatiegraad implicaties hebben voor de immuniteit van de bevolking tegen een groot aantal infectieziekten.

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa
Door de COVID-19-pandemie is duidelijk geworden dat een pandemie met een dergelijke omvang impact heeft op een groot aantal nationale veiligheidsbelangen. Sinds de pandemie is er wereldwijd een toename in onderzoek naar hoog risico pathogenen. Daardoor neemt het risico op het bedoeld of onbedoeld vrijkomen van één van deze pathogenen uit een laboratorium toe (Kaiser, 2023). Verder blijven uitbraken van het aviaire influenzavirus (vogelgriep) relevant. Omdat een toenemend aantal diersoorten geïnfecteerd kan raken door het influenzavirus, heeft dit mogelijk gevolgen voor het ontstaan van varianten die over kunnen gaan op de mens.

Uit een recente rapportage van het RIVM (over de vaccinatiegraad in 2022) blijkt dat het percentage kinderen dat binnen het Rijksvaccinatieprogramma is gevaccineerd is gedaald. De vaccinatiegraad is bovendien voor het eerst in een lange periode onder de 90% uitgekomen (NOS, 2024). Dat betekent dat er een kans bestaat dat verschillende besmettelijke ziekten weer terugkomen.[2] De afname van de vaccinatiegraad lijkt te verklaren doordat tegenwoordig meer ouders negatief tegenover vaccineren staan. Het vertrouwen in vaccins is afgenomen, bijvoorbeeld door de COVID-19-pandemie. De afnemende vaccinatiegraad is reden tot zorg, omdat wanneer de minimale vaccinatie-graad niet bereikt wordt, de kans op een uitbraak van ernstige besmettelijke ziekten toeneemt. Daarnaast is de afnemende vaccinatiegraad een trend die zichtbaar is over de laatste twee jaar. Vanzelfsprekend is dat als de vaccinatiegraad verder daalt, de kans op uitbraken van besmettelijke ziekten verder toeneemt. Hoewel, als gevolg van de maatregelen die zijn getroffen tijdens de COVID-19-pandemie, het aantal meldingen van verschillende

[2] Een belangrijke kanttekening is dat het sinds 1 januari 2022 niet meer mogelijk is om zonder toestemming persoonlijke gegevens te delen. Daarom wordt een deel van de vaccinaties anoniem gemeld. Deze anonieme meldingen worden niet meegeteld voor de vaccinatiegraad, waardoor er sprake is van onderrapportage.

infectieziekten fors gedaald is, is er sindsdien voor veel infectieziekten weer een voorzichtige toename van het aantal meldingen zichtbaar (RIVM, 2023a; RIVM, 2023b).

Er zijn verschillende manieren waarop technologie van invloed kan zijn op het risico dat infectieziekten vormen voor de nationale veiligheid. Met dank aan ontwikkelingen in de bioinformatica kunnen infectieziekten en zoönosen steeds sneller worden gediagnosticeerd. Verdere ontwikkeling van kunstmatige intelligentie zou hier mogelijk in de toekomst aan bij kunnen dragen, door bijvoorbeeld razendsnelle DNA-analyse van potentiële pathogenen of controle van afvalwater of ziekteverwekkers. Een mogelijke keerzijde van dergelijke ontwikkelingen is dat informatie over schadelijke agentia en de productie ervan voor mensen met kwade bedoelingen mogelijk wel toegankelijker wordt (zie ook onderdeel B.7 over biotechnologie). Beperkingen aan de productie, zoals financiering, infrastructuur en materialen, blijven echter wel bestaan (Carter, 2023). Daarnaast wordt het door verbetering van surveillance op uitbraken en moderne technieken makkelijker om bronnen van voedselverontreiniging vroegtijdig op te sporen, waardoor het risico op een crisis door een uitbraak kleiner wordt. Daar staat tegenover dat voedsel en vee vaker internationaal getransporteerd en op grotere schaal geproduceerd wordt, waardoor een dergelijk risico mogelijk juist toeneemt.

Tot slot is er nog een aantal overige ontwikkelingen die mogelijk de nationale veiligheid beïnvloeden. Zo vindt monitoring naar de aanwezigheid van plantenziekten bij bijvoorbeeld sier- en voedselgewassen continu plaats. Wanneer door een zeer schadelijke variant, zoals Tomato brown rugose fruit virus (ToBRFV) of Xylella fastidiosa, de voedselproductie in gevaar komt, zou dit effect kunnen hebben op de nationale veiligheid. Daarnaast is een bijeffect van de COVID-19-pandemie de verminderde verspreiding en daarmee afname van het aantal aangetroffen resistente bacteriën. De situatie lijkt echter weer te normaliseren en in 2023 is er een 'inhaalslag' geobserveerd Klimaatverandering leidt mogelijk ook tot een verhoogd risico op infectieziekten in Nederland, doordat bijvoorbeeld nieuwe vectoren zich makkelijker kunnen vestigen, virussen sneller delen of door de aanwezigheid van besmet water. Op dit moment spelen echter andere sociale, biologische en economische factoren nog een belangrijkere rol (RIVM, 2024).

Toelichting dreigingsbeeld

Het dreigingsbeeld rondom infectieziekten is niet significant veranderd ten opzichte van het beeld dat geschetst is in de RbRa, wel is er een aantal factoren die mogelijk het risico op een uitbraak verhogen, zoals het aantal laboratoria waar onderzoek gedaan wordt naar hoog risico pathogenen en het toenemende aantal diersoorten dat geïnfecteerd kan raken met het influenzavirus. De invloed van de ontwikkelingen van technologie, zoals in de bioinformatica en kunstmatige intelligentiekunnen zowel een positief als negatief effect hebben op de impact van infectieziekten voor de nationale veiligheid. De gevolgen van een uitbraak zijn afhankelijk van het type infectie en de maatregelen die getroffen (kunnen) worden. Het is daarbij van belang om op te merken dat in het Caribische deel van het Koninkrijk de gevolgen waarschijnlijk ernstiger zouden zijn, omdat de maatregelen die getroffen kunnen worden beperkter zijn. Men is voor bijna 100% van levensmiddelen en medicatie afhankelijk van import, en bovendien is er een gebrek aan eigen middelen en (medische) capaciteit.

A.3 Zware ongevallen

Belangrijkste bevindingen & conclusies

Het merendeel van de reeds in de RbRa omschreven stand van zaken ten aanzien van het dreigingsthema zware ongevallen blijft actueel. Wel zijn er enkele verschuivingen ten aanzien van stralingsongevallen in het kader van de oorlog in Oekraïne. De kans op stralingsongevallen in het kader van de oorlog in Oekraïne is aan het begin van de oorlog door andere partijen dan het ANV beschouwd (RIVM, 2024). Ten opzichte van deze beschouwing aan het begin van oorlog zijn de risico's momenteel in het algemeen lager, maar dit is uiteraard sterk afhankelijk van het verloop van de oorlog en de locatie en intensiteit van gevechten dan wel beschietingen (ANVS, 2023).

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

Afgelopen jaren zijn er, zoals reeds vastgesteld in de RbRa, relatief weinig ontwikkelingen op het gebied van stralingsongevallen. Zo zijn er betreffende ongevalsscenario's voor de kerncentrale Borssele geen recente onderzoeken gepubliceerd. Wel wordt er gewerkt aan een nieuwe invulling van de ongevalsscenario's, deze wordt eind 2024 verwacht. Hiermee wijzigen ook de brontermen en uitgangspunten. Wanneer besloten zou worden tot de bouw van (een) nieuwe kerncentrale(s), zal het nog een groot aantal jaar duren voordat deze daadwerkelijk operationeel zijn.

Wat betreft mogelijke ongevallen met chemische stoffen, is er sprake van een verwachte toename in het transport van waterstofrijke energiedragers en CO_2. Plannen voor waterstof en CO_2 zijn vergevorderd en worden momenteel uitgevoerd (Gasunie waterstof netwerk en Porthos CO_2 (Gasunie, 2024; Porthos, 2024)).[3] Een andere ontwikkeling, één die al langer gaande is, betreft de veroudering van chemische installaties. Met de verdere veroudering van de installaties zal de kans op een incident enkel verder toenemen. De incidenten laten zien dat dit inderdaad een relevant onderwerp blijft, al blijft de impact, op de schaal van nationale veiligheid, beperkt. Tot slot bleek in het verleden uit monitoring dat rondom het transport van vooral brandbare vloeistoffen en gassen over het spoor er overschrijdingen plaatsvinden op de Brabantroute Tegelijkertijd hebben diverse steden aan de Brabantroute ambities wat betreft ruimtelijke ontwikkelingen rond het spoor. Uit de monitoringsrapportage spoor van 2022 blijkt dat de overschrijding van het risicoplafond gelijk is aan de voorgaande jaren (AVIV, 2023). Ook ruimtelijke ontwikkelingen rondom het spoor blijven een toename in het groepsrisico veroorzaken. De impact van een ongeval kan hierdoor mogelijk toenemen.

[3] Zie ook onderdeel A.10 over vitale infrastructuur.

Naast de acute effecten van de blootstelling aan chemische stoffen, is er de afgelopen jaren steeds meer aandacht voor langdurige gezondheidseffecten op omwonenden van industriële bedrijven. In 2023 heeft het RIVM onderzoek gedaan naar de bijdrage van Tata Steel Nederland aan de gezondheidsrisico's van omwonenden (Geelen, 2023). "*Het onderzoek bevestigt dat de uitstoot van het Tata Steel-terrein bijdraagt aan de hoeveelheid fijnstof, stikstofdioxide, PAK(Polycyclische Aromatische Koolwaterstoffen) en metalen in de directe leefomgeving. Vooral de uitstoot van fijnstof, stikstofoxiden en de hinder door stof, stank en geluid vergroten de kans op gezondheidseffecten. Omwonenden hebben hierdoor een iets grotere kans op astma, longkanker en om eerder te overlijden.*" In navolging van het onderzoek naar Tata Steel Nederland is het RIVM in opdracht van het ministerie van Infrastructuur en Waterstaat een verkenning naar de gezondheidseffecten van Chemours en de Westerschelde op de omwonenden gestart (RIVM, 2024b). Alhoewel de langdurige gezondheidseffecten op omwonenden van industriële bedrijven momenteel niet direct een onderwerp is voor de nationale veiligheid, kan het wel invloed hebben op beslissingen en afwegingen rond de vestiging van (nieuwe) industrie en daarmee ook op (ongewenste) strategische afhankelijkheden.

Toelichting dreigingsbeeld

De risico's van zware ongevallen zijn niet fundamenteel anders dan voorzien in de RbRa, wel zetten de in de RbRA benoemde trends zich voort. Het dreigingsbeeld wijzigt dan ook niet.

A.4 Polarisatie, extremisme & terrorisme

Voor het dreigingsthema polarisatie, extremisme en terrorisme zullen we de volgende twee dreigingscategorieën apart van elkaar beschouwen: maatschappelijke polarisatie en (niet)-gewelddadig extremisme en terrorisme. Extremisme en terrorisme worden hier gezamenlijk beschouwd omdat er veel overlap is in relevante ontwikkelingen.

Dreigingscategorie maatschappelijke polarisatie

Belangrijkste bevindingen en conclusies
Het dreigingsbeeld is momenteel niet wezenlijk veranderd. Het is wel waarschijnlijk dat gezien het toenemende belang van de thema's klimaat en migratie ook het risico van verdere polarisatie rond deze thema's toe zal nemen in de toekomst. Er is tevens sprake van een toegenomen risico dat bestaande polarisatie wordt verergerd door beïnvloedings- en desinformatiecampagnes van kwaadwillende actoren, mede geholpen door de steeds bredere toegankelijkheid van generatieve AI (zie ook onderdeel B, technologieverkenning).

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa
Politieke en maatschappelijke polarisatie blijft een aanzienlijke uitdaging in het kader van de nationale veiligheid. Nederlanders geven aan het gevoel te hebben dat maatschappelijke tegenstellingen en onverdraagzaamheid toenemen (ANV, 2022). Opvattingen rondom cultuur en identiteit vormen één van de scheidslijnen waarlangs polarisatie zichtbaar is. Daarnaast zijn de afgelopen jaren vooral de beleidsthema's klimaat en migratie in veel gevallen bepalend geweest voor (politieke) identiteit, en is de polarisatie vooral gegroeid rondom deze thema's. Sinds oktober 2023 heeft ook de oorlog in Gaza zich ontwikkeld tot een politieke en ideologische splijtzwam, waarbij er sprake is van maatschappelijke verdeeldheid met betrekking tot de gewenste reactie van de Nederlandse overheid op de crisis (Movisie, 2023).

Opinievorming over beleidskwesties en over de overheid in het algemeen wordt in grote mate beïnvloed door het soort media dat wordt geconsumeerd. Een meerderheid van Nederlanders gebruikt nog meerdere nieuwbronnen en zit niet in een zogenaamde filterbubbel. De variatie in het gebruik van mediamerken en nieuwsbronnen is in 2023 wel gedaald ten opzichte van 2022 (Commissariaat voor de Media, 2023). De daling komt met name voor rekening van merken met een oorsprong in traditionele media, radio of televisie en print en met name onder de jongere leeftijdsgroepen (18-45-jarigen). Deze jongere leeftijdsgroepen halen hun nieuwsvoorziening in

toenemende mate op digitale platforms als X en TikTok (Mulder, 2023).

Als gevolg van strenger optreden door grote mediaplatforms om verspreiding van nepnieuws tegen te gaan is er een verschuiving zichtbaar van desinformatie van openbare sociale media naar besloten socialemediakanalen zoals bijvoorbeeld Telegram groepen. Dit kan het risico op zogenaamde "echokamers" verder toe doen laten nemen, die bovendien moeilijker te controleren zijn.

Naast de mogelijkheden die gesloten kanalen bieden voor de verspreiding van nepnieuws zien we ook ontwikkelingen aan de *productiekant* van desinformatie. De mogelijkheden voor het laagdrempelig produceren van desinformatie hebben dankzij generatieve AI sinds 2022 een vlucht genomen.[4] Niet alleen kan men op grotere schaal, en meer *microtargeted* nepnieuws produceren, ook worden deze apps en systemen steeds toegankelijker voor de gewone gebruiker en wordt daarmee de drempel tot gebruik lager. Het aantal potentiële dreigingsactoren is hiermee toegenomen. Bij het opstellen van de RbRA in 2022 is deze laagdrempeligheid ook al gesignaleerd als ontwikkeling.

Dreigingscategorie (niet)-gewelddadig extremisme en terrorisme

Belangrijkste bevindingen en conclusies

De dreiging binnen dit dreigingsthema is gegroeid. Onder andere als gevolg van de oorlog in Gaza, koranvernielingen in Nederland en Scandinavië, en oproepen tot aanslagen door aanhangers van terroristische organisaties is de dreiging van extremisme en terrorisme vergoot, en het nationaal dreigingsniveau verhoogd. Daarnaast blijven anti-institutioneel extremisme, rechtsextremisme, en in mindere mate linksextremisme, op verschillende manieren een dreiging voor de nationale veiligheid.

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

Het lage vertrouwen in overheidsinstituten heeft zich sinds de coronapandemie onder meer geuit in *anti-institutioneel extremisme* en een toename van complotdenken, waarbij tussen beide groepen een overlap te zien is.[5] Ondanks dat COVID-19 als thema minder belangrijk is geworden, is de omvang van de anti-overheidsbeweging waarschijnlijk gegroeid, maar concentreert deze zich inmiddels ook op andere thema's (AIVD, 2023). Kenmerkend voor het narratief van anti-institutionele extremisten is het idee dat in Nederland de bevolking in oorlog is met een kwaadaardige, internationaal opererende elite, die de controle heeft over onder meer overheid, rechtspraak, media en wetenschap. Dit narratief ondermijnt de democratische rechtsstaat door het aantasten van het publieke vertrouwen in de instituties en het draagt bij aan een sfeer van bedreigingen, intimidatie en intolerantie. In beperkte mate leidt dit narratief tot een voorstelbare extremistische geweldsdreiging. Tot nu is toe aantal gewelddadige incidenten beperkt gebleven, maar de dreiging van geweld is de afgelopen jaren wel realistischer geworden (AIVD, 2023). De dreiging vanuit anti-institutioneel extremisme kan, naast het gebruik van intimidatie of geweld en het ondermijnen van de democratische rechtsstaat tevens worden gevonden in het bredere radicaliserende en maatschappelijk polariserende effect van het narratief.

Binnen de context van anti-institutioneel extremisme is er sprake van een groei van de soevereine beweging in Nederland. Alhoewel de precieze omvang lastig te duiden is, schat de AIVD in dat er ten minste momenteel enkele tienduizenden mensen zijn die zichzelf als soeverein identificeren (AIVD, 2024). Het is de verwachting dat deze aantallen verder toe zullen nemen de komende jaren. Deze personen geloven dat de Nederlandse wet- en regelgeving niet op hen van toepassing is, een geloof dat veelal voortkomt uit dezelfde overtuiging rond een kwaadwillende elite zoals hierboven reeds uiteengezet. Men streeft veelal naar een parallelle, alternatieve wereld, zonder onderdrukking van deze vermeende kwaadaardig elite. Het grootste deel van de soevereinen (soms ook autonomen genoemd) staan verandering voor binnen de grenzen van het huidige systeem van de democratische rechtsorde, in de zin van bijvoorbeeld het bereiken van een mate van zelfvoorziening. Een kleiner deel wijst het systeem en de legitimiteit hiervan echter fundamenteel af en houden zich bewust niet aan wet- en regelgeving, ondanks de soms grote persoonlijke gevolgen hiervan zoals huisuitzetting of oplopende schulden. Tot slot is er een zeer kleine subgroep die gelooft in de onvermijdelijkheid van een gewelddadige strijd met de overheid (AIVD, 2024).

Anti-institutioneel extremisme vertoont op enkele vlakken overlap met het rechtsextremisme, wat vooral zichtbaar is rondom onderwerpen als de omvolkingstheorie en het idee van een *"great reset"*. Binnen rechtsextremisme bestaat naast de nadruk op anti-Islam en anti-immigratieretoriek, een toegenomen aandacht voor rassenzuiverheid en de eerdergenoemde "omvormingstheorie". Antisemitisme staat ook centraal, maar wordt steeds vaker gekoppeld aan de ideeën over omvolking en rassenverzwakking (AIVD, 2024). De AIVD geeft aan dat grootste dreiging binnen het rechtsextremisme uitgaat van het zogenaamde accelerationisme, wat als grootste inspiratiebron dient voor mogelijke geweldplegers en een succesvolle werving

[4] Zie de technologieverkenning in onderdeel B voor meer informatie.

[5] Het vertrouwen in politieke instituties zoals de regering en de Tweede Kamer is lager is dan het vertrouwen in niet politieke instituties zoals de rechtspraak en politie. Zie: CBS, 2023.

van nieuwe aanhangers kent.[6] Het rechtsextremistisch discours in zijn algemeen is sinds de vluchtelingencrisis van 2015 steeds meer genormaliseerd. Tegelijkertijd wijken rechtsextremisten als gevolg van strengere moderatie op grote online platforms steeds vaker uit naar minder gangbare alternatieven en versleutelde chatdiensten, die moeilijker te controleren zijn door inlichtingendiensten.

Linksextremisme richt zich afgelopen jaren vooral op activisme via demonstraties en burgerlijke ongehoorzaamheid, en richt zich met name op klimaat en racisme. Men sluit zich daarbij aan bij bredere coalities. De dreiging van linksextremisme zit vooral in het uit de hand lopen van protesten, en het mogelijk de grens passeren van activisme naar extremisme als gevolg van maatschappelijke ontwikkelingen. Naast "langlopende" thema's als racisme en het klimaat heeft recentelijk de oorlog in Gaza veel links activisme gemobiliseerd, wat geresulteerd heeft in demonstraties in zowel Nederland als de rest van Europa, en de Verenigde Staten.

De oorlog in Gaza heeft naast links activisme ook een toename van antisemitisme veroorzaakt, waar rechtsextremistisch gedachtegoed van kan profiteren. Tegelijkertijd is er ook een toename in anti-Islamitisch sentiment waar te nemen. De dreiging voor deze beide groepen is toegenomen, en hebben geresulteerd in zowel beveiliging van Joodse instituties als van Islamitische instituties.

Als gevolg van de oorlog in Gaza is tegelijkertijd ook de dreiging van Islamitisch extremisme en jihadisme toegenomen (NCTV, 2023a). Onder andere om deze reden heeft de NCTV in 2023 het dreigingsniveau verhoogd naar "substantieel". In Europa hebben sinds het begin van de oorlog meerdere aanslagen plaatsgevonden die waren geïnspireerd door de gebeurtenissen in Gaza (Reuters, 2023a). Daarnaast zijn er sinds oktober 2023 meerdere terroristische "cellen" opgerold, die mogelijk een aanslag hadden willen plegen op Europees grondgebied (Reuters, 2023b). Eerder werd door de NCTV ook al de dreiging vanuit de Afghaanse tak van ISIS *(Islamic State Khorasan Province)* aangestipt. Deze aangestuurde dreiging vanuit ISIS blijft voortduren, ook al worden veel aanslagplots verijdeld. De aanslag in Moskou in maart 2024 is illustratief voor deze dreiging (NCTV, 2023b).

[6] Accelarationisme is een rechtsextremistische ideologie. Aanhangers hebben als doel een rassenoorlog te ontketenen door middel van terroristisch geweld en op die manier een witte etnostaat te creëren.

A.5 Ongewenste inmenging en beïnvloeding democratische rechtsstaat

Het thema ongewenste inmenging en beïnvloeding van de democratische rechtsstaat bevat drie verschillende dreigingscategorieën die afzonderlijk worden beschouwd: Hybride dreigingen ongewenste buitenlandse beïnvloeding en spionage. Elk van deze drie categorieën komt hieronder aan bod. In de RbRa valt het onderwerp georganiseerde criminaliteit ook onder het dreigingsthema ongewenste inmenging en beïnvloeding democratische rechtsstaat. Voor de Trendanalyse is er echter voor gekozen om criminaliteit als apart thema op te nemen (A.6) om aan te sluiten bij de indeling gehanteerd in de veiligheidsstrategie.

Dreigingscategorie Hybride Dreigingen

Belangrijkste bevindingen en conclusies

Het dreigingsbeeld is niet veranderd van *aard*, maar we zien wel dat het dreigingsbeeld als gevolg van de toegenomen grootmachtcompetitie is verslechterd. De inzet van hybride middelen zelf is geen nieuw fenomeen. We zien de afgelopen jaren echter wel een uitbreiding van de manieren waarop middelen worden ingezet, en een uitbreiding van het type doelwitten dat wordt aangegrepen. Een van de meest in het oog springende voorbeelden van een vorm van hybride conflictvoering was al zichtbaar ten tijde van de vorige RbRa, in de vorm van de Europese afhankelijkheid van Russisch gas, en de beperkingen in de toevoer van gas door Poetin. Door middel van deze energiepolitiek zijn Europese samenlevingen onder druk gezet en is getracht de eensgezinde steun voor Oekraïne te doorbreken. Door de toegenomen spanningen in de wereld is er ook een groeiende dreiging dat actoren deze hybride instrumenten vaker en in ernstiger mate zullen inzetten.

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

De schaal en frequentie waarmee steeds assertiever en agressiever wordende staten gebruik maken van hybride instrumenten ten behoeve van ongewenste inmenging en beïnvloeding hebben de afgelopen twee jaar een verdere vlucht genomen. Dit wordt onder andere gefaciliteerd door technologische ontwikkelingen. Ook de steeds verdere integratie van digitale technologieën in alle aspecten van maatschappij creëert nieuwe kwetsbaarheden, onder andere in de vitale infrastructuur en digitale dienstverlening.

Dreigingscategorie Ongewenste buitenlandse beïnvloeding

Belangrijkste bevindingen en conclusies

Het dreigingsbeeld is niet veranderd van aard, maar we zien wel dat het dreigingsbeeld als gevolg van de toegenomen grootmachtcompetitie is verslechterd. Het meest in het oog springende voorbeeld hiervan zijn de beïnvloedings- en destabilisatieactiviteiten die Rusland in Europa heeft ontplooid sinds de aanvang van de oorlog in Oekraïne. Daarnaast blijven ook beïnvloedingspogingen van China en andere staten voortduren. Ongewenste beïnvloeding vindt in toenemende mate plaats door middel van desinformatiecampagnes rondom verkiezingen en grote internationale kwesties. Dit risico is de afgelopen twee jaar gegroeid als gevolg van de nieuwe mogelijkheden die de snelle ontwikkelingen rondom generatieve AI bieden voor informatiemanipulatie, en de ontwikkeling en verspreiding van misleidende informatie. Dit In het licht van de verslechterde geopolitieke verhoudingen

zorgt ervoor dat het risico van desinformatiecampagnes rondom bijvoorbeeld de Europese verkiezingen in 2024 is toegenomen (Ramdharie, 2024).

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

Ongewenste buitenlandse beïnvloeding en ongewenste inmenging vormen een blijvende dreiging. Het gaat hierbij zowel om beïnvloeding van diasporagemeenschappen als van invloedrijke personen of politici. De AIVD signaleert dat ook de afgelopen twee jaar landen als China, Rusland, Iran, Turkije en Marokko pogingen ondernamen om diasporagemeenschappen te beïnvloeden met als doel de (afhankelijkheids)relatie met het thuisland te versterken, of om via deze gemeenschappen invloed uit te oefenen op de Nederlandse democratische samenleving (AIVD, 2023). In sommige gevallen zien we een verandering in de wijze of frequentie van de ongewenste buitenlandse beïnvloeding en inmenging. Zo was er in het begin van de oorlog in Oekraïne sprake van een intensivering van de pogingen van Rusland om haar eigen diaspora in het buitenland te beïnvloeden door middel van desinformatiecampagnes die het gevoel van slachtofferschap moeten versterken (Scott, 2022). Bij beïnvloeding van de eigen diaspora gaat de focus waarschijnlijk uit naar het nabije buitenland en in mindere mate uit naar het zogenaamde verre buitenland, waar Nederland deel uit van maakt (Houtkamp & Drost, 2023). Daarnaast voert Rusland nog steeds grootschalige informatiecampagnes uit in Oekraïne zelf en hebben we de afgelopen twee jaar gezien dat het land haar beïnvloedingsoperaties ook direct richt op samenlevingen in Europa. De oorlog in Gaza was bijvoorbeeld de aanleiding voor een beïnvloedingscampagne in Frankrijk, gericht op het vergroten van de maatschappelijke verdeeldheid rondom dit thema (Albertini, 2023). Buitenlandse beïnvloeding kan ook in spillovereffecten resulteren. Een recent voorbeeld is de ontstane rellen tussen Eritrese groepen in Den Haag in februari 2024 (NOS, 2024).

Dreigingscategorie Spionage

Belangrijkste bevindingen en conclusies

Het dreigingsbeeld bij deze categorie is enigszins verslechterd, wat samenhangt met de gegroeide spanningen tussen de grootmachten. Spionage wordt in toenemende mate ingezet als middel ten behoeve van informatievergaring, heimelijke beïnvloeding en sabotage(voorbereiding). We zien tegelijkertijd dat er ook steeds meer aandacht voor en bewustzijn van de dreiging van spionage is binnen belangrijke sectoren.

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

Het onderkennen van in Nederland opererende inlichtingenofficieren blijft een focus van de Nederlandse veiligheidsdiensten. Hierbij concentreert het huidige onderzoek zich vooral op in Nederland opererende Russische en Chinese inlichtingenofficieren (MIVD, 2023). De Nederlandse inlichtingendiensten hebben daarnaast steeds meer aandacht voor de statelijke dreiging van cyberspionage en zien in toenemende mate digitale spionagepogingen van statelijke actoren bij Nederlandse overheidsinstellingen zoals de krijgsmacht, ministeries en ambassades (MIVD, 2023). Verschillende buitenlandse inlichtingendiensten richtten zich in 2023 daarnaast niet alleen op de rijksoverheid en op topsectoren, maar ook op specifieke instituties en lokale overheden (AIVD, 2024a). De huidige stroomversnelling van technologische ontwikkelingen en de mogelijkheden die dit biedt voor cyberaanvallen betekent dat het risico op complexe sabotage- en spionageoperaties is toegenomen.

Er hebben zich de afgelopen jaren mondiaal meerdere aanvallen op onderzeese infrastructuur plaatsgevonden (Kingston, 2024). Dit heeft erin geresulteerd dat "*seabed warfare*" inmiddels een belangrijke bron van zorg is voor onder andere de inlichtingendiensten. Hierbij ging het tot 2023 met name om acties door Russische groeperingen, maar hebben de berichten over aanvallen van de Houthis op onderzeese kabels in de Rode Zee laten zien dat ook niet-statelijke actoren van dit middel gebruik kunnen maken (Martin, 2024).

Met de toename van cyberspionage vormt ook de afhankelijkheid van buitenlandse leveranciers van technologie, een toenemende bron van zorg. Door middel van zogenaamde achterdeurtjes kan technologie immers gebruikt worden voor datavergaring of spionage. Als reactie op deze dreiging worden strategische beleidskeuzes gemaakt met het oog op veiligheid, maar volledige ontkoppeling isniet mogelijk. De zorgen met betrekking tot afhankelijkheid van buitenlandse technologiebedrijven en -platforms hebben geresulteerd in een advies van de Nationale Cybersecurityraad om meer te investeren in nationale technologiebedrijven, waarmee de afhankelijkheid van buitenlandse leveranciers af moet nemen (Okano-Heijmans, 2023).

Spionage en ongewenste buitenlandse beïnvloeding kunnen ook gefaciliteerd worden door middel van deelnames of overnames van vijandige actoren in vitale sectoren van de Nederlandse economie. Dit risico wordt verkleind door middel van de Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo) die in 2023 is ingegaan en die een veiligheidstoets introduceert voor investeringen, fusies en overnames die een risico kunnen vormen voor de nationale veiligheid (Ministerie van Economische Zaken en Klimaat, 2023). Ook het wetsvoorstel strafbaarstelling spionage is een belangrijke maatregel om spionage in de breedte beter te kunnen bestrijden (AIVD, 2024b).

A.6 Georganiseerde criminaliteit

Belangrijkste bevindingen & conclusies

Het merendeel van de reeds in de RbRa omschreven stand van zaken en dynamieken rond georganiseerde criminaliteit blijft onverminderd actueel, zoals de onverminderd hoge druk die georganiseerde criminaliteit uit kan oefenen op instituten verbonden aan het functioneren van de democratische rechtsstaat en het gebruik van facilitators in verschillende sectoren. Een aantal trends hebben de komende periode wel het potentieel om te worden bijgesteld, onder meer op het gebied van cybercrime. De meest in het oog springende ontwikkeling binnen dit dreigingsthema is echter een zeer sterke toename van het gebruik van explosieven als (onder andere) intimidatiemiddel. Gevolg van deze ontwikkeling is een verandering in het dreigingsbeeld rond georganiseerde criminaliteit, in de vorm van een grotere druk op de fysieke veiligheid, economische veiligheid en de sociaal-politieke stabiliteit.

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

In zijn algemeen is het door de per definitie verhulde aard van georganiseerde criminaliteit bijzonder complex om een betrouwbare uitspraak te doen over de precieze omvang hiervan, bijvoorbeeld in de vorm van de hoeveelheid en het type verhandelde, geproduceerde en doorgevoerde verdovende middelen. Desalniettemin blijft de druk vanuit de georganiseerde criminaliteit in de vorm van (gewelds) dreiging op onder meer journalisten, bestuurders, politici en officieren van justitie onverminderd hoog. Zoals reeds in de RbRa gesignaleerd, kan het gevolg hiervan zijn dat mensen steeds minder bereid zijn om deze functies uit te oefenen, worden belemmerd in hun functioneren of mogelijk toegeven aan criminele belangen.

Er is nog steeds veel politieke en bestuurlijke aandacht voor het tegengaan van georganiseerde criminaliteit. Dit uit zich in de vorm van structurele financiering en lopende trajecten op het gebied van wetgeving en (internationale) samenwerking (Ministerie van Justitie en Veiligheid, 2023). Het precieze effect hiervan en de mogelijke uitwerking op het dreigingsbeeld voor georganiseerde criminaliteit is echter nog moeilijk te duiden. Enerzijds doordat de effectiviteit van investeringen en beleid zich mogelijk pas over een periode van jaren doen gelden en anderzijds door de inherent verhulde aard van georganiseerde criminaliteit. Indien het beleid succesvol blijkt en de druk op criminelen toeneemt, bestaat echter wel het gevaar dat dit kan leiden tot een (tijdelijke) toename van bedreigingen en andere vormen van (fysiek) geweld onder meer gericht op personen werkzaam voor de instituten die zijn belegd met de uitvoering van het beleid. Tegelijkertijd

is georganiseerde criminaliteit een onderwerp dat moet concurreren met andere prangende vraagstukken zoals die rond klimaatverandering en een toegenomen druk op de internationale stabiliteit en samenwerking. Het risico blijft bestaan dat als gevolg van toenemende druk op andere onderwerpen, de (financiële) slagkracht rond het onderwerp georganiseerde criminaliteit onder druk kan komen te staan. Voor nu is dit gezien de extra toegewezen middelen nog niet aan de orde.

Criminelen zijn voor het uitvoeren van hun activiteiten voor een deel afhankelijk van mensen die al dan niet (nood) gedwongen optreden als facilitator, waaronder bijvoorbeeld ook corrupte contacten op logistieke knooppunten zoals havens. Naarmate meer mensen zich in een kwetsbare positie bevinden dan wel makkelijk beïnvloedbaar zijn, hoe gemakkelijker het zal zijn voor criminelen om facilitators dan wel slachtoffers van criminele uitbuiting te vinden. De afgelopen periode wordt in dit kader vaak de zorg geuit over de inzet van steeds jongere jongeren die worden ingezet voor het uithalen van drugs uit zeecontainers of het plaatsen van geïmproviseerde explosieven. Tegelijkertijd is het aannemelijk dat onder andere als gevolg van klimaatverandering dan wel afgenomen internationale stabiliteit, er de komende jaren sprake zal zijn van relatie veel (irreguliere) migratie. Met een vreemdelingenketen die reeds onder druk staat, is het goed mogelijk dat steeds meer mensen van de radar verdwijnen of in een kwetsbare positie terecht komen. Vanzelfsprekend zal lang niet iedereen die zich in een instabiele of kwetsbare situatie bevindt op enige wijze betrokken raken bij de georganiseerde criminaliteit, maar hoe meer druk en instabiliteit, hoe groter de groep mensen die hier kwetsbaar voor is.

Wat betreft geweld vanuit de georganiseerde criminaliteit, blijft het aantal liquidaties in Europees Nederland ondanks een kleine stijging vooralsnog relatief laag. Tegelijkertijd zijn er wel signalen dat er sprake is van een verharding van het criminele circuit (WODC, 2021; 2023). Deze verharding uit zich bijvoorbeeld in een toename van excessief geweld in de vorm van niet alleen het steeds vaker plaatsen van explosieven, maar ook in het plaatsvinden van ontvoeringen van (familieleden van) criminelen. De zeer sterke toename van het gebruik van explosieven de afgelopen twee jaar is een in het oog springende ontwikkeling binnen het thema georganiseerde criminaliteit. Het gaat om meer dan een verviervoudiging van ongeveer 200 in 2022 naar 900 aanslagen en pogingen hiertoe in 2023 (Politie, 2023). Het grootste deel hiervan kan (voor zover überhaupt mogelijk) worden toegewezen aan plegers die geassocieerd worden met georganiseerde (drugs)criminaliteit. In kleinere mate is er tevens sprake van *copycat* gedrag door anderen. Explosieven, onder meer in de vorm van zwaar vuurwerk, zijn zeer makkelijk te verkrijgen en een effectief middel om mensen te intimideren,[7] onder druk te zetten of ervoor te zorgen dat (panden van) concurrenten uit het criminele milieu onder de aandacht komen bij politie en justitie. De inzet ervan als intimidatiemiddel is voor de opdrachtgever veel minder riskant en goedkoper dan bijvoorbeeld een liquidatie. Alhoewel er tot nu toe nog geen grote aantallen doden of gewonden zijn gevallen, ligt dit wel in de lijn der verwachting. Er worden niet alleen vaker, maar ook steeds zwaardere explosieven gebruikt die niet alleen leiden tot grote economische schade aan bijvoorbeeld gebouwen, maar ook zeer gevaarlijk kunnen zijn voor mensen die zich in de buurt begeven.

Een laatste ontwikkeling rondom het geweldpotentieel vanuit de georganiseerde criminaliteit is dat als gevolg van de oorlog in Oekraïne het de komende jaren waarschijnlijk is dat er meer én zwaardere wapens op de Europese zwarte markt terecht komen. Hierdoor komen deze wapens mogelijk ook gemakkelijker in de handen van criminelen. Het gaat hier nadrukkelijk niet alleen om klein kaliber vuurwapens, maar mogelijk ook om wapentuig met meer capaciteiten zoals antitankwapens, landmijnen, granaten, etc (Van Nierop, 2023).

Op het gebied van cybercrime blijft het aantal geregistreerde uitingen hiervan in Nederland hoog maar stabiel (NCTV, 2023). Hierbij is er wel een sterk vermoeden van onderrapportage en zijn er aanwijzingen dat veel partijen afzien van het doen van aangifte, bijvoorbeeld uit vrees voor imagoschade, maar ook omdat het soms goedkoper is om bijvoorbeeld in het geval van *ransomware* tegemoet te komen aan de eisen dan de mogelijke (indirecte) kosten van een politieonderzoek. In het algemeen wordt gesignaleerd dat cybercriminaliteit de afgelopen jaren qua slachtoffers, schade en opbrengsten een industriële omvang heeft aangenomen. Ondanks de (tijdelijke) afvlakking van het geregistreerde aantal voorvallen van cybercriminaliteit, bestaat er het risico dat deze aantallen de komende jaren weer sterk toe kunnen nemen. Dit dankzij de gemakkelijke schaalbaarheid en ook de winstgevendheid van cybercriminaliteit (NCVT, 2023), onder meer in de vorm van *ransomware* aanvallen.[8] Binnen Europa is reeds een toename gesignaleerd van cyberaanvallen door criminelen op specifiek vitale sectoren (NCTV, 2023; UK NCSC, 2023). Als deze trend zich specifiek ook binnen Nederland gaat manifesteren, zullen we vaker te maken krijgen met

[7] Het kan hier niet alleen gaan om andere personen binnen het criminele milieu, maar uiteraard ook om buurtbewoners en mensen werkzaam bij aan het functioneren van de democratische rechtstaat verbonden instituten.

[8] Niet alleen criminele actoren, maar ook sommige statelijke actoren met een anti-Westerse agenda gebruiken onder meer *ransomware* aanvallen om aan financiële middelen te komen.

verstoringen rond bijvoorbeeld de elektriciteitsvoorziening als gevolg hiervan. Te meer wanneer tegelijkertijd een toename van het gebruik van '*wiperware*' wordt gezien, waarmee hele systemen kunnen worden gewist (NCTV, 2023; UK NCSC, 2023).

De bredere beschikbaarheid en toegankelijkheid van generatieve AI kan het uitvoeren van cybercrime in de toekomst verder faciliteren en automatiseren. Enkele mogelijk toepassingen zijn steeds geavanceerdere vormen van Whatsappfraude (spraak en beeld), afpersing dan wel chantage door het (dreigen met) verspreiden van door AI gegenereerde beelden en het bewust doorspelen van desinformatie (zoals gemanipuleerde camerabeelden) doorspelen naar politie en opsporingsdiensten. Zie hiervoor ook de hoofdstukken A.9 en B.1.

De oorlog in Oekraïne laat een vermenging zien van statelijke actoren en binnen zowel Rusland als Oekraïne aanwezige niet statelijke criminele groeperingen in het uitvoeren van cyberaanvallen over en weer *(crime as a service)*. Alhoewel Rusland zich in dit opzicht momenteel voor een groot deel richt op Oekraïne, kan dit veranderen. Vooral gezien de verslechterde relaties tussen Rusland en het Westen als gevolg van sancties richting Rusland en steun aan Oekraïne (NCTV, 2023).

Toelichting dreigingsbeeld

Samenvattend is de dynamiek rond georganiseerde criminaliteit niet fundamenteel anders dan zoals geduid in de RbRa, wel leiden een aantal van de bovenstaande ontwikkelingen tot potentieel ernstigere gevolgen voor de nationale veiligheid en daarmee een verslechterd dreigingsbeeld.

Ten eerste is het aannemelijk dat er als gevolg van het wijdverspreid gebruik van explosieven meer (onschuldige) slachtoffers zullen vallen als gevolg van georganiseerde criminaliteit dan eerder voorzien. Door het gebruik van explosieven is de georganiseerde criminaliteit en de dreiging die dit met zich mee brengt voor een grotere groep mensen zichtbaarder geworden dan voorzien. Dit heeft mogelijk zijn weerslag op onder meer het vertrouwen in een aantal van de instituten verbonden aan de democratische rechtsstaat om de situatie het hoofd te bieden. Tevens is het mogelijk dat personen werkzaam voor deze instituten ook via deze weg onder druk kunnen worden gezet dan wel geïntimideerd. Dit kan hun functioneren ondermijnen. Verder valt niet uit te sluiten dat, gezien de verharding binnen het criminele circuit, ook het aantal liquidaties weer toe kan nemen de komende jaren.

Tot slot en onder meer in het licht van de recente brede toegankelijkheid van AI technieken, is er het potentieel dat verschillende vormen van cybercrime (al dan niet als onderdeel van een hybride campagne) tot grotere economische schade kunnen leiden. Te meer wanneer men zich (ook) richt op vitale sectoren. Vooral wanneer er weinig back-up capaciteit is, zoals bijvoorbeeld het geval is in het Caribisch deel van het Koninkrijk, kan dit leiden tot een ernstige verstoring van het vitale proces in kwestie. Mogelijk met tevens druk op de beschikbaarheid van primaire levensbehoeften (fysieke veiligheid) als gevolg.

A.7 Internationale en militaire dreigingen

Het dreigingsthema internationale en militaire dreigingen bevat vier verschillende dreigingscategorieën die hier afzonderlijk worden behandel. Te weten: Fragiliteit rondom het Koninkrijk; multilaterale (veiligheids)organisaties onder druk; conflict tussen de machtsblokken en proliferatie van massavernietigingswapens.

Dreigingscategorie fragiliteit rondom het Koninkrijk

De afgelopen twee jaar is in grote delen van de wereld rondom het Koninkrijk de politieke en economische instabiliteit toegenomen. De spillovereffecten van deze instabiliteit hebben impact op onze nationale veiligheidsbelangen.

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

De oorlog in Oekraïne heeft grote invloed op onze nationale veiligheid. Niet alleen heeft de oorlog gevolgen voor de Nederlandse economische veiligheid en de sociale en politieke stabiliteit, ook de territoriale dreiging en het risico op een militaire confrontatie met Rusland is gegroeid.

Naast de totale oorlog in Oekraïne zijn er in andere regio's rondom het Koninkrijk ook (kleinschaliger) conflicten en militaire spanningen De afgelopen twee jaar is de sluimerende onrust tussen Servië en Kosovo op de Balkan meerdere malen geëscaleerd tot actieve conflictsituaties. Rusland probeert bovendien deze spanningen aan te wakkeren, en daarmee de stabiliteit in de regio te ondermijnen. Daarnaast heeft ook de oorlog tussen Azerbeidzjan en haar etnisch Armeense enclave Nagorno-Karabach de afgelopen twee jaar de fragiliteit ten oosten van Europa vergroot. Het voorheen latente conflict escaleerde mede door veranderende regionale en mondiale machtsdynamieken tot een actief conflict en heeft geleid tot duizenden vluchtelingen en een humanitaire crisis. Het conflict kan gevolgen hebben voor (omringende) regio's die worstelen met vergelijkbare vragen over territoriale integriteit en zelfbeschikking (Landgraf et al., 2024).

De afgelopen jaren is er sprake geweest van toenemende geopolitieke competitie over het Noordpoolgebied, wat sinds inval van Rusland in Oekraïne nog verder is versterkt. Als gevolg van de oorlog is de regionale samenwerking met Rusland in het Poolgebied verbroken. Tegelijkertijd zijn de banden tussen Rusland en China sterker geworden, en brengt dit het risico met zich mee dat ook China, in samenwerking met Rusland, activiteiten kan gaan ontplooien in het Poolgebied (Wall & Wegge, 2023).

Spillovereffecten zien we ook als gevolg van de oorlog in Gaza, zowel in de regio als in Europa. Naast het

destabiliserende effect van de oorlog zelf kan ook de Westerse reactie op de oorlog een negatief effect hebben. De perceptie van Westerse partijdigheid of gebrek aan actie van internationale veiligheidsorganisaties kan dienen als voedingsbodem voor extremisme en jihadisme in de regio. Economische uitzichtloosheid en politieke onderdrukking en instabiliteit blijven een belangrijke factor in het voortbestaan van die voedingsbodem, maar verontwaardiging en boosheid over de oorlog in Gaza kan hierbij een radicaliserend effect hebben op (kwetsbare) groepen en individuen in de regio en daarbuiten (Marcetic, 2023; Al Hussein, 2024).

De afgelopen twee jaar is de instabiliteit in Centraal- en Noord-Afrika verder toegenomen door een serie coups en couppogingen in onder andere Burkina Faso, Soedan, Gabon, Niger en Guinee (Reuters, 2023a). Ook groeiende voedselonzekerheid draagt bij aan de algehele fragiliteit in de regio, en draagt bijvoorbeeld in het geval van het conflict in Soedan verder bij aan de grote regionale vluchtelingenbewegingen. De instabiliteit heeft door deze regionale vluchtelingenstromen ook een verder destabiliserend effect op landen in Noord-Afrika, waar de afgelopen twee jaar al sprake was van een groeiend autoritarisme en politieke instabiliteit (Diwan et al., 2024). Een deel van deze vluchtelingenstromen kan zich vervolgens ook richting Europa bewegen, wat nog meer druk kan zetten op beperkte middelen en capaciteiten voor opvang, en kan leiden tot verdere polarisatie rondom het migratiethema in Europese samenlevingen.

Ook de stabiliteit in de regio rondom het Caribisch deel van het Koninkrijk staat onder druk. Het risico op spillover effecten van geopolitieke competitie in Latijns-Amerika blijft onveranderd aanwezig, met name door competitie tussen Rusland en het Westen. Tegelijkertijd breidt ook China haar belangen in Latijns-Amerika uit, met name in Venezuela. President Maduro slaagt er vooralsnog in een balans te bewaren tussen Moskou en Washington, maar vaart een onvoorspelbare en grillige koers, waarvan president Poetin gebruik maakt door Venezuela verder aan zich te binden. Maduro's onvoorspelbare beleid werd in 2023 ook zichtbaar tijdens de crisis rondom het tussen Venezuela en Guyana betwiste gebied Essequibo. Ook in het grensgebied tussen Venezuela en Colombia is er sprake van instabiliteit. De groeiende competitie tussen verschillende gewapende groepen en criminele organisaties in Colombia heeft betrekking op de controle over illegale handelsroutes, en deze competitie leidt tot een explosie van geweld. De Colombiaanse overheid heeft geen controle over delen van het rurale grensgebied met Venezuela. De instabiliteit in met name Venezuela heeft een directe impact op de veiligheidsbelangen van het Caribisch deel van het Koninkrijk.

Dreigingscategorie Multilaterale (veiligheids) organisaties onder druk

Belangrijkste bevindingen en conclusies
De multilaterale orde staat onder druk, en deze druk vertaalt zich onder andere in een groeiende blokvorming en verlamming binnen multilaterale organisaties (Instituut Clingendael, 2024).

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa
Onder andere als gevolg van de veranderende wereldorde is er een steeds duidelijker trend zichtbaar van toenemende blokvorming in bepaalde multilaterale (veiligheids)organisaties. Tegelijkertijd zien we dat andere samenwerkingsverbanden zoals de NAVO en de EU door de urgentie van de oorlog in Oekraïne juist een boost hebben gekregen. De afgelopen twee jaar zijn er stappen gezet in het verbeteren van de defensiecapaciteiten van de EU. In 2023 stemde het Europees Parlement voor de ASAP Act, die 500 miljoen vrijmaakt voor het opschalen van de Europese wapenindustrie ten behoeve van de productie van munitie en raketten. Ook de EDIRPA overeenkomst uit 2023, die voorziet in een gezamenlijk inkoopbeleid van wapensystemen en munitie, is erop gericht om de industriële en technologische capaciteit van EU-lidstaten te versterken ten behoeve van haar defensiecapaciteiten (Europees Parlement, 2023).

De Amerikaanse houding ten opzichte van het multilateralisme en multilaterale veiligheidsinstituties in van groot belang voor de slagkracht van deze organisaties. De VS heeft onder president Biden gedeeltelijk de multilaterale waarden weer omarmd, wat onder andere blijkt uit zijn terugkeer in de *World Health Organization* en het Klimaatakkoord van Parijs.

Dreigingscategorie Conflict tussen de machtsblokken

Belangrijkste bevindingen en conclusies
Toegenomen grootmachtcompetitie, afgeleide proxy-conflicten in diverse delen van de wereld, en een groeiend escalatiepotentieel hebben een negatief effect op de nationale veiligheidsbelangen.

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa
Tegen de achtergrond van de groeiende grootmacht-competitie, nemen de spanningen tussen China en Taiwan toe, wat de spanning tussen de VS en China op hun beurt potentieel ook kan laten escaleren. Taiwan heeft gewaarschuwd dat er een sterke stijging in spanning is met China, als gevolg van China's toegenomen militaire activiteiten en oefeningen nabij Taiwan. Dit vergroot ook de onrust tussen de VS en China.

Naast de spanningen met Taiwan heeft China ook een beladen relatie met India. Sinds de oorlog in Oekraïne en in de context van de toegenomen spanningen tussen de grootmachten heeft India een nieuwe, belangrijkere rol in het internationale veiligheidslandschap gekregen. India is traditioneel ongebonden (“*non-aligned*”) en wil dit vooralsnog ook graag blijven. Tegelijkertijd zijn er groeiende spanningen met China als gevolg van een grensconflict dat met enige regelmaat opleeft. Naast China heeft ook India sterke (militaire) banden met Rusland, en is het land ook sinds de oorlog in Oekraïne doorgegaan met handel met Rusland. Tegelijkertijd is, gezien de spanningen met China in de regio, India een belangrijke veiligheidspartner voor de VS, en zien we dat de VS probeert India sterker aan zich te binden via economische en militaire samenwerking (Ayres, 2023). Hoewel de grootmachtcompetitie grote invloed kan hebben op het ontstaan van spanningen en de ontwikkeling van proxy-conflicten, kunnen nationale of regionale conflicten op hun beurt ook hun weerslag hebben op de grootmachten en hun onderlinge relaties. De oorlog in Gaza heeft belangrijke spillovereffecten op de spanningen tussen andere (grote) mogendheden, zowel regionaal als in het Westen.

Dreigingscategorie Proliferatie van massavernietigingswapens

Belangrijkste bevindingen en conclusies

Door de toegenomen spanningen tussen de grootmachten zien we bestaande wapenwedlopen in een stroomversnelling komen, en nieuwe wapenwedlopen ontstaan.

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

De druk op multilaterale wapenbeheersingsregimes is de afgelopen jaren toegenomen als gevolg van toegenomen competitie tussen de grootmachten. Rusland heeft bijvoorbeeld het *New Start Treaty* gepauzeerd, waarna de VS in reactie daarop stopte met delen van het onder het Verdrag verplichte data (Williams, 2023). Rusland heeft zich daarnaast ook teruggetrokken uit het *Comprehensive Nuclear Test Ban Treaty (CTBT)* (Bugos, 2023). China bouwt de afgelopen jaren in recordtempo zijn nucleaire capaciteiten verder uit. Het land importeert nu meer uranium uit Rusland dan ooit (Dolzikova, 2023). Tegelijkertijd hebben in november 2023 ook voor het eerst in vijf jaar weer gesprekken over nucleaire wapenbeheersing plaatsgevonden tussen China en de VS. Hoewel deze gesprekken een belangrijke opening zijn geweest hebben de ontmoetingen nog niet geresulteerd in vervolgstappen (Reuters, 2024).

In tegenstelling tot ontwikkelingen in de gesprekken met China is er in de relatie met Iran geen sprake van lichtpuntjes met betrekking tot het nucleaire issue. Sinds onder voormalig president Trump de VS zich in 2018 uit de JCPOA terugtrokken lijkt een functioneel vervolg van de gemaakte afspraken ten behoeve van nucleaire wapenbeheersing met Iran ver weg. De kwartaalrapporten van het IAEA laten duidelijk zien dat Iran doorgaat met zijn nucleaire programma. Wapeninspecteurs van het Internationaal Atoomagentschap hebben inmiddels aangegeven dat Iran uranium heeft verrijkt tot 84%, dichtbij de 90% benodigd voor een nucleair wapen, al gebeurt dat nog niet op grote schaal zoals bij lagere verrijkingspercentages het geval is. Hoewel Iran aangeeft dat haar atoomprogramma slechts voor vreedzame doeleinden is bedoeld blijft het onduidelijk met welk doel de hogere verrijking heeft plaatsgevonden (Reuters, 2023b).

Naast het negatieve effect op nucleaire proliferatie heeft de toegenomen competitie tussen de grootmachten ook het risico op nieuwe wapenwedlopen vergroot. De afgelopen twee jaar zagen we een toename van competitie in nieuwe wapentechnologie, waaronder hypersonische wapens en AI-ondersteunde wapensystemen (Pincus, 2023). Met betrekking tot chemische en biologische wapens hebben de ontwikkelingen met betrekking tot generatieve AI de kennisdrempel verlaagd, waardoor mogelijk een breder spectrum van actoren de capaciteiten kunnen ontwikkelen om chemische en biologische wapens te creëren, zie voor meer informatie A.2 infectieziekten.

A.8 Economische dreigingen

Binnen het thema economische dreigingen wordt ingegaan op vijf dreigingscategorieën: strategische afhankelijkheden & handelskrimp of verstoring van de internationale handel; bedreigingen van de knooppuntfunctie van Nederland; buitenlandse inmenging bij het bedrijfsleven; en destabilisatie van het financiële systeem.

Belangrijkste bevindingen & conclusies Economische dreigingen

De reeds in de RbRa omschreven economische dreigingen blijven grotendeels actueel. De geopolitieke onrust en de daarbij behorende (economische) competitie en conflict dragen het meest bij aan nieuwe onzekerheden. De grootste schok komt van de oorlog in Oekraïne die resulteerde in sancties en hogere energieprijzen en indirect in bredere inflatie en hogere rentes. De initiële schok is grotendeels geabsorbeerd, maar de oorlog leidt nog altijd tot kosten (steun en opvang). Ook is de aandacht voor geopolitieke risico's, zoals rondom strategische afhankelijkheden en kennisveiligheid, toegenomen. Dit uit zich bijvoorbeeld in exportrestricties en nieuwe industriepolitiek. De infrastructuur, en daarmee handel, blijft daarnaast vatbaar voor verstoringen van moedwillige en niet-moedwillige aard. Binnen financiële markten zijn de kredietrisico's toegenomen door onder andere de hogere rentes. Dit kwam concreet tot uiting bij verschillende risicovolle gebeurtenissen, maar bleef zonder grote financiële gevolgen.

Dreigingscategorieën strategische afhankelijkheden & handelskrimp of verstoring van de internationale handel

De grootste (economische) schok sinds het verschijnen van de RbRa in 2022 is de verdere doorwerking van de oorlog in Oekraïne. Dit komt terug op verschillende manieren, zoals bijbehorende publieke kosten (o.a. militaire steun, opvang van vluchtelingen) en de vitaliteit van de economie (hogere gasprijzen en bredere inflatie, toegenomen onzekerheid; Rijksoverheid, n.d.-a; Ministerie van Defensie, n.d.; Ministerie van Financiën, 2023). De risico's rond de strategische afhankelijkheid van Rusland (van o.a. gas) bleken onderschat, maar er zijn vlot alternatieven gevonden (bijv. energiebesparing, LNG; Rijksoverheid, 2023a). Door het geleidelijk invoeren van strengere sancties tegen Rusland is de westerse economie relatief bespaard gebleven, maar boeten de maatregelen ook in op effectiviteit.

De oorlog tussen Israël en Hamas leidde met name aan het begin ook binnen financiële markten tot onzekerheid en kan bij verdere escalatie van invloed zijn op de vitaliteit van de Nederlandse economie (Koenis, 2023). Een aantal maanden na het uitbreken van oorlog lijkt dit echter beperkt en is de wereldhandel met name getroffen door aanvallen van Houthi-rebellen bij vaarroutes over de Rode Zee. In april 2024 dreigde de directie confrontatie tussen Israël en Iran tot escalatie in de regio en daarmee mogelijke impact op bijvoorbeeld olieprijzen.

Na jaren van verdere liberalisering van de wereldhandel kende de afgelopen jaren een omslag als gevolg van de COVID-crisis, de oorlog in Oekraïne en de daaropvolgende energiecrisis. Ook de opkomst van en het economisch conflict met China leiden tot een toegenomen aantal handelsbeperkingen en vormen van staatssteun. Zo voerde Nederland sinds 2019 onder druk van de Verenigde Staten steeds uitgebreidere exportbeperkingen in voor geavanceerde chipmachines van ASML (ASML, 2023; 2024). Ook heeft de Europese Commissie verschillende onderzoeken ingesteld naar handel verstorende maatregelen van de Chinese overheid (o.a. elektrische auto's; Europese Commissie, 2024). Binnen Europa leidt de ongelijke ondersteuning van de binnenlandse industrie voor de hogere energieprijzen voorlopig tot verstoring

van de interne markt (Europese Commissie, 2023). In de Verenigde Staten wordt de Amerikaanse industrie ondersteund middels de *Inflation Reduction Act*. De aandacht voor industriepolitiek is daarmee sterk toegenomen. Klimaatverandering (zie ook onderdeel A.1) leidt in de (zeer) nabije toekomst – onder andere door extreem weer – al tot materiële schade en andere stijgende kosten (investeringen in mitigatie en adaptatie). Daarnaast zijn er mogelijk bredere economische gevolgen door verstoorde handel, zowel direct (ontoegankelijke handelsroutes) als indirect (bijvoorbeeld mislukte oogsten). Zo is de capaciteit van het Panamakanaal sterk verlaagd door historische droogte (Jumelet, 2023).

Dreigingscategorie bedreigingen van de knooppuntfunctie van Nederland

De Nederlandse infrastructuur is door meerdere redenen een risicofactor voor de economische vitaliteit in Nederland. Zo is er, in het verlengde van Nord Stream II, de dreiging van (fysieke) sabotage van onderzeese infrastructuur, zoals voor de energielevering en internetconnecties (Ministerie van Defensie, 2024; NOS, 2023a). In dit kader is in Nederland het Programma Bescherming Noordzee Infrastructuur opgezet (AIVD, 2024). Andere risico's komen voort uit de grote vereiste investeringen voor het onderhouden van de algehele infrastructuur, wat steeds vaker leidt tot oponthoud en vertragingen, mede door de personeelstekorten (Prorail, 2023; Kompeer, 2023). Ook extreem weer, zoals langdurige droogte, komt steeds vaker voor en verstoort daarmee vaker handelsroutes in binnen- en buitenland, zoals vaarwegen (zie ook het hoofdstuk over klimaat- en natuurrampen; Van der Maas, 2023; ING, 2023).

Ook is de maatschappelijke en politieke aandacht voor de omgeving(seffecten) de afgelopen jaren toegenomen – zoals rond de luchtvaart en vervuilende industrie (NOS, 2023b; Evofenedex, 2023). Dit kan effect hebben op economische beslissingen, zowel vanuit de Nederlandse politiek als het (internationaal) bedrijfsleven. Daarnaast gelden de juridische beperkingen rondom stikstof nog altijd en is de netcongestie als gevolg van de energietransitie verder toegenomen (Rooijers, 2024; Rijksoverheid, 2024). Bovendien dreigen strengere (of juridisch gehandhaafde) milieunormen rondom mest of de waterkwaliteit tot additionele belemmeringen te leiden voor zowel het bedrijfsleven als burgers (Van der Boon & Gras 2024; Van der Boon & Kakebeeke, 2024; Vestergaard, 2023).

Dreigingscategorie buitenlandse inmenging bij het bedrijfsleven

Cyberdreigingen (zie ook het desbetreffende dreigingsthema) blijven zeer actueel voor zowel financiële instellingen als het bredere bedrijfsleven. Binnen ondernemingen groeit de strategische aandacht hiervoor, maar bijvoorbeeld door minder goed voorbereide organisaties in de toeleverings- en uitbestedingsketens blijven bedrijven mogelijk kwetsbaar.

Ook waarschuwen de AIVD en MIVD opnieuw voor (cyber) spionage bij het Nederlandse bedrijfsleven, waarbij nog altijd China als voornaamste dreiging wordt genoemd (AIVD, 2024; Ministerie van Defensie, 2024). Mede door de weklekrisico's rondom hoogwaardige kennis en technologie zijn de exportrestricties voor ASML ingesteld.

De opkomst van nieuwe digitale technologieën – zoals AI en (verder in de toekomst) quantumtechnologie – brengt risico's met zich mee, zowel direct (technologie als wapen of machtsinstrument) als indirect (het achteropraken van bedrijven en onderzoeksinstellingen en daarmee de vitaliteit van de Nederlandse economie). Echter kan te stevige inperking van risico's juist ook groeimogelijkheden van de binnenlandse kenniseconomie beperken. Nieuwe Europese wet- en regelgeving om grondrechten te borgen zorgt bijvoorbeeld mogelijk ook voor nieuwe hordes voor het Europese bedrijfsleven.

Tot slot is in Nederland beleid ontwikkeld en geïntroduceerd om gevoelige overnames en investeringen en inmenging vanuit het buitenland te beperken, zoals de Wet Vifo (Rijksoverheid, 2023b; Ministerie van Economische Zaken en Klimaat, 2023). Ook Europese verordeningen gericht op vitale aanbieders (zie ook het desbetreffende dreigingsthema) borgen de economische veiligheid (Rijksoverheid, 2022; AFM, 2024).

Dreigingscategorie destabilisatie van het financiële systeem

Door de gestegen inflatie in de Westerse wereld zijn de rentepercentages sterk toegenomen. Een combinatie van toenemende rente- en kredietrisico's, de verlaagde liquiditeit op financiële markten en de aanhoudend relatief hoge inflatie zorgen voor een blijvend hoog risico voor de financiële stabiliteit (DNB, 2023a; b). Dit kwam concreet tot uiting bij verschillende bankfalen begin 2023 in de VS (o.a. Silicon Valley Bank) en Zwitserland (Credit Suisse).

De Nederlandse bancaire sector keert naar binnen. Na de Brexit zijn banken niet meer teruggekomen naar Nederland. De Nederlandse bancaire sector is niet meer zo gezichtsbepalend als zij rond bijvoorbeeld 2000 was. Voor het financieel bestel zitten er daarnaast risico's aan de cryptomarkt. Het omvallen van een grote speler in de financiële sector kan grote gevolgen hebben op het beleggersvertrouwen en daarmee leiden tot een recessie of (financiële) crisis. Het omvallen van cryptoplatform FTX in 2022 bleef desondanks zonder grote financiële gevolgen.

A.9 Cyberdreigingen

Belangrijkste bevindingen & conclusies

Cyberaanvallen zijn aan de orde van de dag. Uit de dreigingsbeelden van de afgelopen jaren blijkt dat de digitale dreiging onverminderd hoog en aan constante verandering onderhevig is. Tegelijkertijd zijn tot nog toe cyberaanvallen met zeer ontwrichtende impact op de nationale veiligheid in het Koninkrijk uitgebleven. Door schaalvergroting en automatisering van aanvallen, nieuwe technologieën die in aanvallen worden gebruikt en toegenomen afhankelijkheden blijft het van belang om de digitale veiligheid goed op orde te hebben om zorg te dragen voor het beschermen van de nationale veiligheidsbelangen (NCTV, 2023; ENISA, 2023; AIVD, 2024).

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

Artificial Intelligence toepassingen: dreigingen en kansen

De afgelopen jaren heeft het *Artificial Intelligence* (AI) technologiegebied zich snel ontwikkeld. Dit technologiegebied kent vele toepassingen, zo ook binnen cybersecurity. De inzet van AI binnen cybersecurity is niet nieuw, maar heeft een nieuwe impuls gekregen door de opkomst van generatieve AI (Zie ook de technologieverkenning later in deze Verdieping op de Trendanalyse). Deze technologie kan door kwaadwillenden worden ingezet voor het ontwikkelen van malware, desinformatiecampagnes, of het automatiseren en grootschaliger uitvoeren van cyberaanvallen. Het gebruik van *Generative Adverserial Networks* (GAN) in aanvallen kan ervoor zorgen dat cyberaanvallen minder goed gedetecteerd kunnen worden. Met name de schaalbaarheid en de mogelijkheid tot het personaliseren van AI-ondersteunde cyberaanvallen vormen een risico. Ook kan op basis van AI worden bepaald wat de beste timing zou kunnen zijn van een cyberaanval, wanneer de impact in potentie het grootst is. Naast schaalvergroting en verminderde mogelijkheid tot detectie zorgt de beschikbaarheid van *Large Language Models* (LLM's) die malware kunnen creëren ervoor dat het makkelijker wordt voor kwaadwillenden om aanvallen uit te voeren (NCTV, 2023; UK NCSC, 2024).

Tegelijkertijd kan AI ook in de verdediging tegen cyberaanvallen worden ingezet, waarbij algoritmes eveneens kunnen worden toegepast om verdedigingsmechanismen te automatiseren of aanvallen beter te detecteren. Hierdoor ontstaat een wedloop tussen aanvallers en verdedigers (Janjeva et al., 2023). Desalniettemin hebben dergelijke automatische verdedigingsmechanismen op basis van AI over het algemeen een goede dataset nodig op basis waarvan het mechanisme kan worden getraind, wat bij veel organisaties ontbreekt (Lohn, Knack et al, 2023).

Naast in de cybersecurity sector wordt AI op allerlei manieren toegepast in verschillende sectoren, zoals de gezondheidszorg, de financiële sector, de mobiliteitssector en Defensie. De toename van het gebruik van AI zorgt daarmee voor een toename van het belang van AI-security. AI kan worden gemanipuleerd door de input data of het algoritme zelf te manipuleren. Dit kan ertoe leiden dat systemen waarin AI functioneert worden verstoord of misleid.[9] In 2017 werden bijvoorbeeld algoritmes van Google zodanig gemanipuleerd dat een schildpad voor een wapen werd aangezien (Vincent, 2017). En in 2019 toonde een groep Chinese hackers aan dat een Tesla zodanig gemanipuleerd kon worden dat de auto plotseling van baan wisselde en op tegemoetkomend verkeer afreed. Gezien het verwachte wijdverspreide gebruik van AI is de potentiële impact van dit soort aanvallen groot. Een voor de hand liggend voorbeeld uit de militaire context: raketafweersystemen kunnen worden gemanipuleerd om een dreiging te negeren, of wapensystemen kunnen zichzelf vernietigen of een verkeerd doelwit aanvallen (Galle, 2022).

Om grip te krijgen op de snelle ontwikkelingen in dit technologiegebied wordt binnen de Europese Unie gewerkt aan de *Artificial Intelligence Act*, wetgeving waarin toepassingen van AI worden gecategoriseerd en toepassingen met een hoog risico worden verboden. Voorbeelden van toepassingen met een hoog risico zijn het ongericht scrapen van het internet en CCTV beelden om databases voor gezichtsherkenning te creëren, het biometrisch categoriseren van groepen op basis van gevoelige kenmerken zoals politieke voorkeur of religie en systemen die emoties kunnen herkennen in werk- of opleiding gerelateerde organisaties (Europees Parlement, 2023). Tegelijkertijd moet de effectiviteit van dergelijke pogingen tot regulatie van AI nog blijken, zo zijn er zorgen over in hoeverre de verordening daadwerkelijk mondiaal effect gaat hebben op de manier waarop AI wordt doorontwikkeld (Krasodomski, Buchser, 2024).

Cyberaanvallen als geopolitiek instrument

De oorlog in Oekraïne en geopolitieke spanningen hebben geleid tot een opleving in hacktivisme en door staten gesponsorde cybercrime groepen. Zo werd de website van het Europees Parlement platgelegd nadat deze Rusland als sponsor van terreur had bestempeld (Van Sant, 2022) en werden aanvallen uitgevoerd na aankondiging van wapenleveringen aan Oekraïne en tijdens het bezoek van Oekraïense president Zelensky aan Nederland (NCSC, 2023). Ook DDoS aanvallen worden veelvuldig uitgevoerd door zowel pro-Russische als pro-Oekraïense groeperingen (NCTV, 2023).[10] Hacktivistische aanvallen zijn aanvallen die met ideologische of politieke overwegingen worden uitgevoerd. Deze aanvallen zijn meestal niet geavanceerd en de (operationele) impact blijft over het algemeen beperkt. Tegelijkertijd hebben dergelijke aanvallen ook een ander oogmerk, namelijk het zaaien van angst en beïnvloeding van de bevolking. Opvallend in dit kader was ook de hack van kindertelevisiezender BabyTV waarbij tot twee keer toe Russische propagandabeelden werden uitgezonden (NOS, 2024). Er zijn nog geen cyberincidenten met grote impact in Nederland geweest met een duidelijke link met de oorlog in Oekraïne (NCTV, 2023). Een andere trend in dit kader is het toegenomen gebruik van *wiperware*, een vorm van malware waarbij data van systemen wordt gewist. *Wiperware* is niet nieuw, maar sinds 2022 is een toename van de inzet van *wiperware* zichtbaar in de context van de Oekraïne oorlog. Deze aanvallen worden vooralsnog door statelijke actoren ingezet, maar kunnen in de toekomst ook door cybercriminelen worden ingezet om dergelijke aanvallen op grote schaal uit te voeren voor financieel gewin (NCTV, 2023; Manky, 2023).

Ook de dreiging vanuit statelijke actoren op cybervlak blijft relevant. Begin 2024 werd door de MIVD melding gemaakt van de aanwezigheid van malware op een Defensienetwerk (NCSC & AIVD, 2024). Deze malware genaamd COATHANGER is zeer waarschijnlijk ingezet door China en had spionage als doel. Hoewel de schade beperkt bleef, aangezien de malware toegang had gekregen tot een geïsoleerd researchnetwerk, laat dit incident zien dat Nederland een doelwit blijft voor spionage van statelijke actoren. Afhankelijk van de geopolitieke ontwikkelingen is het mogelijk dat deze actoren in de toekomst ook proberen om systemen te saboteren middels digitale aanvallen, met mogelijk aanzienlijke maatschappelijke impact.

Waar China zich voorheen voornamelijk richtte op het stelen van intellectueel eigendom, wordt de aard van de digitale dreiging vanuit China nu meer geopolitiek van aard. Op steeds grotere schaal worden kwetsbaarheden geïdentificeerd en systematisch ingezet tegen diverse doelwitten (Cary, 2023). Zo waarschuwen Amerikaanse inlichtingendiensten voor voorbereidende activiteiten ten behoeve van sabotage door cybergroepen gelieerd aan China (zoals *Volt Typhoon*). Dergelijke activiteiten richten zich op IT-systemen van Amerikaanse vitale infrastructuur (CISA, 2024). Naast dergelijke voorbereidingen, zijn digitale aanvallen op vitale infrastructuur aan de orde van de dag in de oorlog in Oekraïne (zowel aan Russische als aan Oekraïense kant). Dit maakt dat, gezien de volatiele

[9] De technologieverkenning in de Verdieping (onderdeel C) wordt onder AI het *predictability problem* verder toegelicht.

[10] *Distributed Denial-of-Service*; een aanval waarbij een server te maken krijgt met een zeer groot aantal verzoeken tegelijkertijd, waardoor het verkeer van en naar de website geblokkeerd kan raken en de server van de dienst kan crashen (plat gaan)

geopolitieke situatie, ook binnen het Koninkrijk de (digitale) weerbaarheid van vitale sectoren hoger op de agenda komt te staan (Ministerie van Defensie, 2024).

Digitale strategische autonomie

In het kader van de almaar toenemende digitalisering en automatisering, krijgt digitale 'strategische autonomie' steeds meer aandacht. Onder meer in de Agenda Digitale Open Strategische Autonomie wordt op een aantal beleidsprioriteiten aangegeven welke lopende, dan wel nieuwe, acties worden genomen om risicovolle strategische afhankelijkheden (op verschillende niveaus) in het digitale domein te mitigeren. Zo zijn er afhankelijkheden van grote Amerikaanse bedrijven in verschillende sectoren, zoals op het gebied van cloudinfrastructuur (Rijksoverheid, 2023). Begin 2024 was er bijvoorbeeld onrust over het voornemen van Stichting Internet Domeinregistratie Nederland (SIDN) om de domeinregistratie van het .nl domein naar het Amerikaanse Amazon Web Services (AWS) te verplaatsen (Schellevis, 2024; Hofmans, 2024). Een ander voorbeeld is Portbase, het *Port Community System* van de Rotterdamse haven, dat in 2018 naar AWS verhuisde (Portbase, 2018). Volgens critici zorgt deze trend voor onwenselijke afhankelijkheden van een buitenlandse partij en kan een incident extra lange hersteltijden voor Nederlandse infrastructuur opleveren, aangezien AWS wettelijk verplicht is om bij noodsituaties prioriteit te geven aan het herstellen van Amerikaanse overheidsdiensten. Daarbij zorgt afhankelijkheid van één organisatie voor *single points of failure*, waarbij verstoring van de diensten van een grote cloudprovider potentieel grote impact kan creëren. Een kanttekening hierbij is dat cloudinfrastructuur op een dusdanige manier is ingericht dat het onwaarschijnlijk is dat alle diensten in zowel Amerika als Europa tegelijk geraakt worden of volledig zullen uitvallen door een incident. De afhankelijkheid van deze Amerikaanse bedrijven is echter wel dusdanig groot dat zij als geopolitiek drukmiddel zou kunnen worden ingezet door de Amerikaanse overheid.

In de RbRA werd geschetst dat cryptografie steeds belangrijker wordt voor het functioneren van het internet. Ook werd aangegeven dat er een spanningsveld bestaat tussen de privacy en veiligheid van online gegevens waar cryptografie voor zorgt en de wens van opsporing en handhaving om cryptografie te verzwakken door *master keys* in te bouwen zodat men beter zicht kan krijgen op criminele activiteit. Dit debat is recentelijk opnieuw actueel geworden door een Europees wetvoorstel waarmee Europese overheden de mogelijkheid zouden krijgen om aanbieders van browser te verplichten *master keys* in te bouwen. Na weerstand van cybersecurity onderzoekers, wetenschappers en de industrie zijn op het laatste moment wijzigingen doorgevoerd met de bedoeling om de zorgen over verzwakking van cryptografie weg te nemen (iBestuur, 2023). De discussie rondom dit onderwerp toont aan dat dit spanningsveld actueel blijft.

Op langere termijn blijft *quantum computing* een technologische ontwikkeling die grote invloed heeft op cryptografie, zoals ook is geschetst in de RbRa. Daarbij moet er aandacht blijven voor het versterken van het vermogen om als Nederland zelf betrouwbare cryptografische producten te kunnen ontwikkelen onder de Nationale Cryptostrategie (NCS). Hoewel quantumtechnologie nog niet volwassen genoeg is om de rekenkracht van huidige computers te overtreffen, komt voorbereiding op het post-quantum tijdperk steeds hoger op de agenda te staan (AIVD, 2023). In de technologieverkenning wordt binnen het onderdeel quantumtechnologie uitgebreider stilgestaan bij cryptografie.

Cybercrime

De dreiging ten aanzien van cybercrime is grotendeels onveranderd, met name de inzet van *ransomware* blijft een aanvalstechniek die grote schade kan veroorzaken. Hoewel ook in 2023 veel bedrijven slachtoffer zijn geworden met aanzienlijke financiële schade tot gevolg, zijn incidenten met maatschappelijke impact, zoals de NotPetya, WannaCry of Colonial Pipeline aanvallen, niet voorgekomen (NCTV, 2023). Tegelijkertijd krijgt een grotere groep van criminelen toegang tot (*ransomware*) tools, door onder meer de eerdergenoemde ontwikkelingen binnen AI. In generieke zin klinkt dan ook de roep om een proactieve benadering ten aanzien van cybersecurity om weerbaarder te worden tegen allerlei vormen van cyberaanvallen en cybercrime.

Tegelijkertijd wordt op Europees niveau gepoogd cybersecurity te verbeteren, om zo minder vatbaar en kwetsbaar te zijn voor onder meer cybercrime. Onder de voorgestelde verordening cyberweerbaarheid van de EU dienen bedrijven cybersecurity op orde te brengen, complementair aan de NIS-2 verordening. Elk bedrijf dat "producten met digitale elementen" op de Europese markt brengt, moet kunnen aantonen aan een aantal cybersecurity voorwaarden te hebben voldaan (Cyber Risk, 2024). Dergelijke certificatie gaat uit van het '*secure by design*' principe. Hierbij wordt cybersecurity integraal meegenomen in ontwerp en bouw van IT-producten.

Cybersecurity en ruimtevaart

In 2023 is cybersecurity binnen de ruimtevaart door meerdere organisaties als onderwerp benoemd dat op langere termijn steeds belangrijker zal worden (Kaczmarek, 2024; ESA, 2024; NIST, 2024). Aangezien satellieten worden gebruikt voor een groot scala aan militaire en civiele systemen, denk aan GPS, aardobservatie en telecommunicatie, kunnen incidenten die de beschikbaarheid, integriteit, en/of de vertrouwelijkheid van deze satellietdiensten aantasten mogelijk grote impact hebben (ENISA, 2022). In de technologieverkenning wordt binnen het onderdeel ruimtetechnologie uitgebreider stilgestaan bij cybersecurity in de ruimte.

Implicaties dreigingsbeeld

De digitale dreiging blijft onverminderd hoog, waarbij op verschillende manieren de nationale veiligheidsbelangen kunnen worden geraakt. Zo kan de territoriale veiligheid (en specifiek de digitale veiligheid) worden geraakt door moedwillige inzet van cyberaanvallen door staten, aan staten gelieerde hackers en cybercriminelen. Gezien de volatiele geopolitieke situatie, maar ook de toenemende toegankelijkheid van technieken om cyberaanvallen uit te voeren, zullen cyberaanvallen aan de orde van de dag blijven. De afgelopen jaren was het beeld dat statelijke actoren netwerken vooral binnendrongen met als doel spionage of het uitvoeren van verkenningsactiviteiten (NCTV, 2022b). Afhankelijk van hoe de dreiging zich de komende jaren ontwikkelt is het mogelijk dat meer aanvallen met sabotage als doel zullen worden uitgevoerd door statelijke actoren of daaraan gelieerde cybercriminelen. Dergelijke aanvallen kunnen impact hebben op de fysieke veiligheid, indien bijvoorbeeld chemische installaties worden geraakt, of de impact van de cyberaanval dusdanig groot is dat er een gebrek aan primaire levensbehoeften ontstaat. Bovendien kunnen door keteneffecten op bedrijven, de maatschappij en (vitale) processen ook andere veiligheidsbelangen worden geraakt.

Naast cyberaanvallen kunnen de geschetste ontwikkelingen rondom bijvoorbeeld digitale strategische autonomie op lange(re) termijn impact hebben op economische veiligheid. Bovendien kan de sociale en politieke stabiliteit en de internationale rechtsorde onder druk komen te staan door bijvoorbeeld digitale ontwikkeling en verspreiding van desinformatie.

A.10 Bedreiging vitale infrastructuur

Belangrijkste bevindingen & conclusies

Verschillende ontwikkelingen op het gebied van bijvoorbeeld geopolitieke spanningen, de energietransitie, strategische afhankelijkheden en extreem weer kunnen impact hebben op de continuïteit en beschikbaarheid van vitale processen. Vitale infrastructuur is in toenemende mate een aantrekkelijk doelwit voor kwaadwillenden gezien de potentiële impact van verstoring van vitale processen. Tegelijkertijd kent de vitale infrastructuur ook digitale en fysieke kwetsbaarheden, waardoor processen ook niet-moedwillig verstoord kunnen raken of zelfs kunnen uitvallen.

Algemeen overzicht bevindingen en stand van zaken t.o.v. RbRa

Vitale infrastructuur als doelwit

De afgelopen jaren is gebleken dat vitale infrastructuur een steeds aantrekkelijker doelwit is geworden voor statelijke actoren. Waar eerder vooral digitale aanvallen werden uitgevoerd met spionage en verkenning als doel, laat het opblazen van de Nord Stream-gasleidingen september 2022 en het beschadigen van een gaspijpleiding en een telecomkabel tussen Zweden en Estland zien dat actoren bereid zijn om daadwerkelijk tot sabotage over te gaan (Ministry of Defense of Sweden, 2023). Hierbij is het goed om op te merken dat het van belang is om voor te bereiden op samengestelde dreigingen, waarbij verschillende incidenten tegelijkertijd of kort na elkaar plaatsvinden. Dit geldt bijvoorbeeld voor manifestaties van extreem weer, maar ook voor moedwillige acties: statelijke actoren kunnen sabotage activiteiten zo uitvoeren dat zij samenvallen met een andere gebeurtenis (onderhoud, extreem weer), wat de beschikbaarheid van een proces verder onder druk zet. Dit vergt een verhoogd weerbaarheidsniveau.[11]

Naast statelijke actoren bestaat er ook een dreiging vanuit activistische of politiek gemotiveerde groepen. Begin 2024 werd een elektriciteitsmast in de buurt van een Teslafabriek in Duitsland in brand gestoken door een links-extremistische groepering (NOS, 2024). In 2022 werd in de Verenigde Staten een aanval op het elektriciteitsnet uitgevoerd waardoor 45.000 inwoners zonder stroom kwamen te zitten, deze aanval werd vermoedelijk uitgevoerd door een extreemrechtse groepering (Price, 2023; Huizinga, 2022). Ook in Nederland wordt gewaarschuwd voor de opkomst van links-, rechts- en anti-institutioneel extremisme en de verharding die plaatsvindt binnen deze stromingen (AIVD, 2023; 2024). Daarbij wordt ook geconcludeerd dat steeds meer groeperingen zich met het thema klimaat gaan bezighouden. Afhankelijk van de verdere verharding en bereidheid van deze groeperingen om tot sabotage over te gaan, kan ook vitale infrastructuur in het Koninkrijk doelwit worden.

Digitale kwetsbaarheden vitale infrastructuur

Door de generieke afhankelijkheid van digitale systemen zijn vitale sectoren onderling meer verweven. Een voorbeeld hiervan is de afhankelijkheid van GNSS, een bekende afhankelijkheid die recent opnieuw onder de aandacht is gekomen door publicatie van het IKUS II rapport (Rijksoverheid, 2022). Hierin wordt aangegeven dat bij GNSS-verstoringen ontwrichtende keteneffecten kunnen ontstaan. Het is echter niet duidelijk waar precies de afhankelijkheden zitten en wat de potentiële impact is van een verstoring (zie ook de technologieverkenning ten aanzien van ruimtetechnologie). Ten aanzien van afhankelijkheid van GNSS is in de RbRa reeds opgemerkt dat ruimteweerfenomenen een grote impact kunnen hebben op vitale processen (directe verstoring of door verstoring van GNSS-signalen voor tijd- en plaatsbepaling), waarbij de komende jaren door het zonnemaximum de waarschijnlijkheid van dergelijke verstoringen door ruimteweer toeneemt (ANV, 2022).

[11] Denk hierbij aan alternatieve herstelplannen en (crisis)oefeningen in de keten.

Een ander voorbeeld van afhankelijkheid van digitale systemen is de toenemende verplaatsing naar *cloudinfrastructuur*, dit wordt nader toegelicht in A.9 Cyberdreigingen (RDI, 2023; Vuilleumier, 2023). De digitale soevereiniteit kan ook onder druk komen te staan door tekorten aan componenten, chips of apparatuur. Hierbij kan een te grote afhankelijkheid van buitenlandse marktspelers ontstaan, met als gevolg dat men de regie over de digitale infrastructuur verliest en de kans op spionage en datalekken toeneemt (RDI, 2023; Vuilleumier, 2023). Gezien de toenemende automatisering en afhankelijkheid van digitale systemen binnen de vitale infrastructuur, kunnen cyberincidenten in de ICT toeleveringsketen keteneffecten veroorzaken binnen de Nederlandse vitale processen.

Daarnaast zorgt digitalisering ervoor dat vitale processen kwetsbaarder worden voor cyberaanvallen. Het beeld bestaat dat dergelijke aanvallen over het algemeen gemitigeerd kunnen worden als het gaat om een enkelvoudig incident. Dit beeld verandert echter wanneer een aanval wordt gecombineerd met een andere, niet-moedwillige gebeurtenis. Denk aan een aanval op spoorvervoerders op het moment dat er groot onderhoud aan het spoor plaatsvindt, of een aanval op waterbeheerders tijdens een storm. Dergelijke compounding of cascading threats met een moedwillige component worden waarschijnlijker in een geopolitiek volatiele wereld (Wells, 2022).

Fysieke kwetsbaarheden vitale infrastructuur

In de zomer van 2023 heeft een grote verscheidenheid aan verschillende fenomenen met betrekking tot extreem weer plaatsgevonden (bosbranden, (hagel)stormen, overstromingen), zowel binnen als buiten Europa. In een aantal landen heeft noodweer onder andere geleid tot stroomuitval, werd het openbaar vervoer stilgelegd en moest een vliegveld sluiten (NOS, 2023a; b). Voor het Caribisch deel van het Koninkrijk geldt dat de kans op zware orkanen toeneemt en het orkaanseizoen steeds langer wordt. In 2022 was op Bonaire sprake van zware regenval waardoor delen van het eiland onder water stonden en op sommige plekken de stroom uit viel (NOS, 2022). Extreem weer kan in de toekomst ook in Nederland vaker leiden tot uitval van vitale processen.[12] Het is de vraag of processen bij uitval op tijd hersteld kunnen worden, zeker aangezien extreem weer een *common cause failure* is, waarbij meerdere processen tegelijkertijd geraakt kunnen worden door één incident. Ook in dit kader is het fenomeen van *compounding* of *cascading threats* relevant: wanneer de kans op natuurlijke dreigingen groter wordt, wordt de kans op het samenvallen van verschillende dreigingen namelijk ook groter (Argyroudis, 2020). Daarnaast leggen klimaatverandering en de toename van extreem weer fenomenen ook druk op de levering van nutsvoorzieningen als schoon drinkwater en energie: verzilting zorgt ervoor dat de kwaliteit van het grondwater achteruit gaat. Perioden van extreme hitte of kou kunnen zorgen voor een piekbelasting op het netwerk door grotere vraag naar energie voor airco of juist verwarming.

Weerbaarheid vitale processen

Naast ontwikkelingen in het dreigingslandschap is de implementatie van Europese wetgeving voor fysieke, digitale en economische weerbaarheid van onder andere vitale processen een belangrijke ontwikkeling voor dit domein (NCTV, 2024a). Naast de *Critical Entities Resilience* (CER) en de *Network and Information Security 2* (NIS2) richtlijnen zijn ook de *Cyber Resilience Act* (CRA) en de *Digital Operations Resilience Act* (DORA) Europese verordeningen die relevant zijn voor (delen van) de vitale aanbieders. Voor het domein vitale infrastructuur betekent dit dat meer organisaties aan de wetgeving zullen moeten voldoen, het aantal vitale aanbieders zal dus worden uitgebreid. Daarnaast wordt meer van de betrokken organisaties gevraagd, onder andere door het instellen van een zorgplicht voor het nemen van beveiligingsmaatregelen en een meldplicht van incidenten. De CER en de NIS2 zullen in de loop van 2024 worden geïmplementeerd (NCTV, 2024b).

Energievoorziening: uitdagingen rondom de energietransitie

De energietransitie houdt in dat naar een nieuw energiesysteem wordt toegewerkt waarin de energievraag wordt beperkt, fossiele brandstoffen worden uitgefaseerd en meer gebruik wordt gemaakt van duurzame energiebronnen als zonne- en windenergie en energie uit biomassa (trias-energetica) (Ministerie van Defensie, 2023). Er zijn meerdere aspecten hiervan die gevolgen kunnen hebben voor de nationale veiligheid. Ten eerste stappen steeds meer bedrijven en huishoudens ten gevolge van de energietransitie over op elektriciteit als energiebron. Door deze elektrificatie ontstaat een toename in de vraag naar energie. Men is druk bezig de capaciteit van het elektriciteitsnetwerk uit te breiden, maar de toename in capaciteit kan de toename in vraag niet bijhouden. Er is nu al sprake van dat zowel bedrijven als huishoudens niet meer op het elektriciteitsnetwerk kunnen worden aangesloten en dat bijvoorbeeld laadpalen op gezette tijden moeten worden uitgezet vanwege dit capaciteitstekort. De leveringszekerheid van elektriciteit komt hierdoor onder druk te staan en het aantal stroomstoringen op regionaal niveau (op wijkniveau) kan stijgen door de krapte op het elektriciteitsnet. Daarnaast kan dit knelpunt een vertraging van de energietransitie en dus de verduurzaming van ons energiesysteem opleveren (Rijksoverheid, 2024). De roep om energieopslagmethodes en flexibel gebruik vanuit de regionale netbeheerders wordt daarom steeds groter, zowel

[12] Bijvoorbeeld de energiesector (TenneT, 2023)

voor industrie als voor huishoudens (Rijksoverheid 2023a; Tennet, 2024).

Ten tweede is de energietransitie materiaalintensief, waardoor de vraag naar bepaalde mineralen en metalen in de komende jaren zal toenemen. Europa is sterk afhankelijk van landen als China, Turkije en de Democratische Republiek Congo voor de levering van deze *Critical Raw Materials*. De levering van deze materialen kan dus een knelpunt vormen voor de energietransitie en kan bovendien als geopolitiek drukmiddel worden ingezet door de landen waar Nederland afhankelijk van is. Vertraging van de energietransitie kan weer samenvallen met de krapte op het energienet, wat ervoor zorgt dat de leveringszekerheid verder onder druk kan komen te staan (Europees Parlement, 2023).

Een derde aspect van de energietransitie is het gebruik van waterstof als alternatieve energiebron- en drager. Om waterstof te kunnen gebruiken moet onder andere een landelijk dekkend waterstoftransportnetwerk worden aangelegd. Nederland heeft de ambitie om een wereldwijde *Hydrogen hub* te worden, waarbij waterstof in ons land wordt geïmporteerd, opgeslagen en vervoerd. Het gebruik van waterstof brengt ook risico's met zich mee, aangezien het erg licht ontvlambaar is. Daarnaast is het geurloos, kleurloos en smaakloos, wat bijvoorbeeld het detecteren van lekken door menselijke zintuigen lastig maakt. Dit levert vraagstukken op over hoe waterstofinfrastructuur op een veilige manier kan worden ingericht (Gasunie, 2023).

Een vierde aspect dat relevant is voor de leveringszekerheid is de toenemende afhankelijkheid van zonne- en windenergie. Wanneer er langere periode sprake is van een gebrek aan zonne- en windenergie spreekt men van *Dunkelflaute*, wat de leveringszekerheid onder druk zet. Bij het plannen van het nieuwe energiesysteem kan rekening worden gehouden met *Dunkelflautes* door deze periodes op te vangen met andere energiebronnen zoals waterstof of biomassa.

Het laatste relevante aspect van de energietransitie in het kader van deze Trendanalyse is dat digitalisering en de energietransitie hand in hand gaan: in de nieuwe energie-infrastructuur wordt in toenemende mate gebruik gemaakt van digitale producten als slimme meters en laadpalen. Dit zorgt voor een toename van het digitale aanvalsoppervlakte binnen het energiesysteem, wat wordt versterkt door de hoge snelheid waarmee technologie wordt ontwikkeld en geïmplementeerd: hierbij is vaak beperkt zicht op de kwetsbaarheden in deze digitale producten, wat de kwetsbaarheid van deze infrastructuur vergroot.

Drinkwatervoorziening: kwaliteit grondwater onder druk

Een belangrijke trend is de druk die vervuiling en klimaatverandering op de kwaliteit van het grondwater oplevert. Klimaatverandering leidt tot een stijging van de zeespiegel, wat tot verzilting van het grondwater leidt. Verzilting neemt bovendien toe door bodemdaling en doordat rivieren in perioden van extreme droogte zouter worden als gevolg van verminderde waterafvoer (Geudens, 2022). Grondwater is de belangrijkste bron voor winning van drinkwater, daarnaast wordt ook gewonnen uit oppervlaktewater. Bovendien staat de kwaliteit van grond- en oppervlaktewater onder druk door gewasbeschermingsmiddelen, nitraat uit mest en de reststoffen van medicijnen en cosmetica (Rijksoverheid, 2018). Deze stapeling van factoren heeft als gevolg dat de kwetsbaarheid van de drinkwatervoorziening is toegenomen (Rijksoverheid, 2018). Het RIVM waarschuwde in 2023 dat er regionaal sprake is van tekorten in het aanbod van drinkwater en dat bij het uitblijven van maatregelen er vanaf 2030 een structureel tekort in heel Nederland ontstaat (Van Leerdam, 2023; ILT, 2024). Dat door een periode van langdurige droogte de drinkwatervoorziening vanuit grondwater onder druk komt te staan, werd in 2024 nogmaals benadrukt door het Planbureau voor de Leefomgeving (PBL, 2024).

Implicaties dreigingsbeeld

Diverse ontwikkelingen zoals hierboven beschreven zullen impact hebben op de continuïteit en beschikbaarheid van vitale processen. Daarmee worden diverse nationale veiligheidsbelangen geraakt, zoals de fysieke veiligheid en territoriale veiligheid (aantasting digitale ruimte).

De fysieke en territoriale veiligheid van het Koninkrijk kunnen op verschillende manieren worden geraakt binnen het dreigingsthema vitale infrastructuur. Allereerst kunnen (digitale) aanvallen op vitale infrastructuur door statelijke- of activistische/politieke actoren leiden tot het saboteren van het vitale proces en daarmee de beschikbaarheid onder druk zetten. Ten tweede kunnen situaties van extreem weer (bosbranden, overstroming, stormen) ervoor zorgen dat delen van het Koninkrijk zonder stroom komen te zitten en sluiting van vitale processen zoals het openbaar vervoer. Het is de vraag of deze processen bij uitval op tijd hersteld kunnen worden, zeker wanneer meerdere processen tegelijkertijd geraakt zullen worden (*compounding threats*). Daarnaast is de vitale infrastructuur nu al doelwit gebleken voor digitale aanvallen, wat leidt tot een aantasting van de integriteit van de digitale ruimte. Tot slot, zorgt de toenemende druk op het elektriciteitsnetwerk ervoor dat de leveringszekerheid onder druk komt te staan.

Onderdeel B
Technologieverkenning

Technologische ontwikkelingen hebben in belangrijke mate invloed op de samenleving. De ontwikkeling van technologische toepassingen gaat snel en er wordt gestreefd naar een technologische voorsprong ten opzichte van anderen. Naast een belangrijke rol van technologie in onder meer het Nederlandse verdienvermogen, is technologie van belang om (internationale) maatschappelijke uitdagingen aan te pakken. Tegelijkertijd is er ook een keerzijde van technologische ontwikkelingen, waarbij technologische toepassingen op verschillende manieren een dreiging voor de nationale veiligheid vormen.

De behoefte om grip te krijgen op de snelheid, impact en toekomst van technologische ontwikkelingen is terug te zien in het grote aantal strategieën, beleidsdocumenten en wetenschappelijke analyses. Zo is begin 2024 de Nationale Technologie Strategie uitgebracht, maar ook internationaal worden doorlopend rapporten gepubliceerd over technologische trends.

Hieronder wordt ingegaan op zeven technologiegebieden. Deze technologiegebieden zijn grote families van technologieën en kennen talloze toepassingen, al dan niet in combinatie met technologieën uit andere families. Gezien de beperkte omvang van deze Trendanalyse, is het onmogelijk om hier een volledig beeld te schetsen van relevante technologieën voor de nationale veiligheid. Wel wordt een beknopt overzicht gegeven van een aantal belangrijke technologische ontwikkelingen, relevant in het kader van de nationale veiligheid.

Er is gebruik gemaakt van verschillende bronnen om te komen tot de selectie van technologiegebieden, waaronder de reeds genoemde Nationale Technologie Strategie (Rijksoverheid, 2024), de Herijking Sleuteltechnologieën (Van Bree, 2023), de technologie trendrapporten van NATO Science & Technology Organization (Reding, 2023) en diverse publicaties vanuit de private sector.

Tabel 1. Selectie van 7 technologiegebieden ten behoeve van de Trendanalyse Nationale Veiligheid, inclusief definitie

Artificial Intelligence	Artificial Intelligence (AI, Kunstmatige Intelligentie) is een overkoepelende term voor een familie van methodes, modellen, en algoritmes, geïnspireerd op het menselijk denken en handelen, en gericht op het ontwikkelen van het vermogen van systemen om intelligent gedrag te vertonen (ANV, 2020).
Ruimtetechnologie	Ruimtetechnologie is technologie gericht op het gebruik van de ruimte middels satellieten, grond- en verbindingsstations en mogelijk in de toekomst ruimtewapens (Bronkhorst, 2020; US Department of Defence, 2020; NAVO, 2024).
Quantumtechnologie	Quantumtechnologie berust op specifieke verschijnselen uit de kwantumfysica (zoals verstrengeling en superpositie) en benut het bijzondere gedrag van energie en materie op atomaire en subatomaire schaal, oftewel de allerkleinste quantumdeeltjes, om op een radicaal nieuwe manier te kunnen rekenen, communiceren en meten (Van Bree, 2023; Rijksoverheid, 2023).
Robotica en autonome systemen	Robots zijn mechanische apparaten die zelfstandig taken kunnen uitvoeren in de lucht, op de grond, op- of onder water. Om deze taken uit te voeren worden robots uitgerust met regeltechniek en sensoren (zoals camera's, thermometers en lichtmeters). De technologie is gericht op het ontwikkelen van methoden, tools en middelen op het gebied van mechanische structuur, bediening op afstand, en autonomie (Bronkhorst, 2020).
Fotonicatechnologie	Fotonicatechnologie richt zich op het opwekken, transporteren en detecteren van lichtgolven en lichtdeeltjes, ook wel fotonen genoemd (Rijksoverheid, 2023; Bronkhorst, 2020; Photondelta, 2024).
Energietechnologie	Energietechnologie is een breed gebied dat een scala aan technologieën omvat voor de productie, opslag, transport en gebruik van energie, zoals technologieën om energie uit de omgeving te benutten (fossiele brandstoffen, kernenergie en hernieuwbare energiebronnen) (Bronkhorst, 2020).
Biotechnologie	Biotechnologie behelst het bewerken van organismen met de doelstelling om het functioneren van organismen, planten, mensen of dieren te verbeteren (COGEM, 2023).

B.1 Artificial Intelligence

Artificial Intelligence (AI, Kunstmatige Intelligentie) is een overkoepelende term voor een familie van methodes, modellen en algoritmes, geïnspireerd op het menselijk denken en handelen, en gericht op het ontwikkelen van het vermogen van systemen om intelligent gedrag te vertonen (oftewel het nabootsen van menselijke vaardigheden als redeneervermogen, beeld- en spraakherkenning en leervermogen) (ANV, 2020; Van Bree, 2023). AI is een technologiegebied waarin ontwikkelingen en doorbraken zich snel opvolgen en wat fungeert als een belangrijke *enabling* technologie die andere innovaties mogelijk maakt (Rijksoverheid, 2024). De toepassingsmogelijkheden zijn zeer groot, onder meer op het gebied van energietransitie, gezondheidszorg, mobiliteit en Defensie kan AI toegepast worden voor bijvoorbeeld optimalisatie, voorspellingen, monitoring en diagnostiek (Rijksoverheid, 2023a; 2024). Tegelijkertijd leven er ook zorgen over de verantwoorde toepassing van dataverwerking, lerend vermogen en besluitvormingsmodellen.

In het kader van de nationale veiligheid is de opkomst van generatieve AI een belangrijke ontwikkeling. Door generatieve AI kunnen onder meer teksten en (bewegende) beelden automatisch worden gegenereerd op basis van input vanuit de gebruiker. Een toepassing van generatieve AI is een *Generative Adversarial Network* (GAN), waarin één neuraal netwerk het realisme beoordeelt van de output van een ander neuraal netwerk (Gonzalez, 2024). Bekende generatieve AI toepassingen zijn OpenAI's *ChatGPT* (tekstgeneratie) en *Sora* (videogeneratie). Hoewel generatieve AI veel kansen biedt (zoals voor de doorontwikkeling van chatbots), zijn er ook belangrijke keerzijdes van deze ontwikkeling. Zo kan dezelfde technologie ingezet worden om desinformatie te ontwikkelen. Niet alleen kan hierdoor de hoeveelheid desinformatie toenemen, ook de kwaliteit van de producten neemt toe doordat beelden en tekst nauwelijks meer van echt te onderscheiden zijn. Zo kunnen *deepfakes* ook interactie bevatten, in plaats van alleen een video van iemand die bijvoorbeeld een speech geeft. Daarnaast biedt de technologie mogelijkheden om echte beelden met synthetische beelden te combineren. Ook wordt desinformatie steeds meer toegespitst op de ontvanger, om zo beter te resoneren (Janjeva, 2023). Tegelijkertijd bieden AI-toepassingen juist ook verbeterde mogelijkheden tot detectie van desinformatie, waardoor het huidige kat-en-muis-spel tussen aanvallers en verdedigers in stand blijft (Janjeva, 2023).

Ook heeft de toepassing van AI impact op de digitale veiligheid. GANs maken het ook voor de minder technisch-onderlegde cyberaanvallers makkelijker om te experimenteren met technieken om cyberaanvallen uit te voeren (Janjeva, 2023). Bovendien kunnen bepaalde taken in bijvoorbeeld het ontdekken van kwetsbaarheden in software worden overgenomen door AI systemen (Hazell, 2023). Ook hier speelt opnieuw dat dergelijke technologie zowel door aanvallers als ter bescherming ingezet kan worden (zie tevens Onderdeel A.9 Cyberdreigingen).

Eén van de uitdagingen in de doorontwikkeling en toepassing van AI is het zogenoemde *predictability problem*. We kunnen niet altijd goed voorspellen wat een AI-systeem gaat doen, wat niet alleen potentieel voor onwenselijke uitkomsten zorgt, maar ook op de langere termijn kan zorgen dat het vertrouwen in AI-systemen en (overheids) organisaties die dergelijke systemen gebruiken gaat afnemen (Taddeo, 2022). Deze onzekerheid ingebed in het *predictability problem* komt enerzijds doordat AI systemen (met name *machine learning* systemen) kwetsbaar zijn voor datamanipulatie (moedwillig of anderzijds), waardoor het systeem faalt op een onvoorspelbare manier. Een dergelijke moedwillige manipulatie van AI-systemen (*adversarial AI*) kan potentieel grote impact hebben in een militaire context, denk aan raketafweersystemen die een dreiging negeren, of wapensystemen die zichzelf vernietigen of een verkeerd doelwit aanvallen (Galle, 2022).[13] Anderzijds is de uitlegbaarheid van de rationale op basis waarvan een systeem een conclusie heeft getrokken of een beslissing heeft gemaakt vaak beperkt. Daarnaast zijn huidige systemen simpelweg nog niet altijd goed bestand tegen (nieuwe of onverwachte) data buiten de trainings- of simulatieomgeving en daarmee dus niet robuust in operationele situaties (Nurkin, 2022). Met name in het defensie- en veiligheidsdomein zijn hierdoor uitdagingen in de effectieve toepassing van civiele technologie, niet in de laatste plaats omdat data beperkt beschikbaar is (bijvoorbeeld door vertrouwelijkheid van deze data). Onvoldoende technologische doorontwikkeling op deze uitdagingen en verlies van vertrouwen in AI-systemen leiden tot zorgen over achterblijvende ontwikkeling van AI-toepassingen in hoog-risico toepassingen (zoals het defensiedomein) (Reding, 2023).

Eén van de manieren hoe met name Europa probeert het *predictability problem* aan te pakken, is door het ontwikkelen van regelgeving ten behoeve van de verantwoorde inzet van AI.[14] Aanbieders op de Europese markt moeten aan een aantal vereisten voldoen, waarmee de kwaliteit van AI-systemen moet worden geborgd en waarmee

[13] Zie ook Onderdeel A.9 Cyberdreigingen.

[14] Denk hierbij aan onder meer de AVG, Digitale Markten Verordening (DMA), Digitale Diensten Verordening (DSA), DA, DGA, AI Verordening, NIS2-richtlijn, Cyber Weerbaarheidsverordening (CRA), de Cyber Veiligheidsverordening (CSA) en Aanwijzing Algoritmes vastgesteld door de Chief Information Officer (CIO) van Defensie. Zie onder meer Defensie Strategie Data Science en AI 2023-2027 (Rijksoverheid, 2023a)

het vertrouwen in dergelijke systemen kan toenemen (Rijksoverheid, 2024). Daarnaast, om grip te houden op de besluitvorming van AI-modellen, is betekenisvolle menselijke controle (*meaningful human control*) een belangrijk concept ten aanzien van de toepassing van AI in het defensie- en veiligheidsdomein gedurende alle fasen van *governance*, design, ontwikkeling en gebruik (Heijnen, 2024).

Een concretere uitdaging ligt in de capaciteit binnen Nederland, maar ook in de EU, om op te schalen en te kunnen concurreren met buitenlandse partijen. Dit ligt enerzijds aan toegang tot rekenkracht en de bijbehorende infrastructuur (hier bestaat een afhankelijkheid van buitenlandse cloudproviders) en anderzijds aan toegang tot data (om AI-systemen te kunnen trainen) (Rijksoverheid, 2024). Met name de Verenigde Staten en China zijn leidend in de doorontwikkeling van AI (zowel op het gebied van hardware als software) en bepalen daarmee in grote mate op welke manier AI wordt toegepast en data wordt gebruikt (AIVD, 2024; Reding, 2023; Rijksoverheid, 2024).

B.2 Ruimtetechnologie

Ruimtetechnologie is technologie gericht op het gebruik van de ruimte middels satellieten, grond- en verbindingsstations. De technologie omvat ontwikkeling van methoden, tools en middelen op het gebied van satellietobservatie, satellietcommunicatie en ruimtewapens ten behoeve van onder andere PNT (*positioning, navigation and timing*), *early warning* en aardobservatie (Bronkhorst, 2020; US Department of Defence, 2020; NAVO, 2024). De belangrijkste technologische ontwikkelingen op het gebied van ruimtetechnologie zijn miniaturisatie en toenemende betaalbaarheid van satelliet missies (platformen zelf en de lancering) satellieten, het reduceren van kwetsbaarheden en afhankelijkheid van satellieten op aarde, het vergroten van bandbreedte en de ontwikkeling van *counterspace capabilities* (zoals antisatelliet (ASAT) en *directed energy* wapens). Dit leidt tot een toenemende interesse in ruimtelanceringen door zowel staten als private partijen en biedt daarmee de mogelijkheid om ruimtetechnologie sneller, frequenter en efficiënter te testen.

De afgelopen jaren is het aantal gelanceerde satellieten dan ook drastisch toegenomen, waarbij met name constellaties van kleinere satellieten worden gelanceerd. Dergelijke constellaties zijn feitelijk netwerken van honderden tot duizenden verbonden satellietsystemen die onder meer lage latentie breedband data leveren. Door ontwikkelingen rondom miniaturisatie krijgen steeds meer actoren toegang tot de technologie. Ook worden ze stabieler en krijgen ze flexibele configuraties die door meerdere sectoren benut kunnen worden. Denk hierbij aan observatie en surveillance, weersvoorspellingen, breedband communicatie en toegang tot het internet voor afgelegen gebieden (GCHQ, 2022). Ook zijn '*responsive space*' capaciteiten in opkomst: het snel kunnen lanceren van een satelliet met een kleinere raket (in plaats van een gezamenlijke lancering) in reactie op een acute dreiging (DARPA, 2024).

In het kader van Nationale Veiligheid is een drietal ontwikkelingen op het gebied ruimtetechnologie relevant. De eerste belangrijke ontwikkeling slaat op de militarisering van de ruimte als een voortzetting van 'aardse' geopolitieke competitie. Staten als China, de Verenigde Staten en Rusland transformeren van passief militair gebruik van de ruimte naar actieve integratie van de ruimte in conventionele militaire operaties (Reding, 2023; Projectteam Statelijke Dreigingen, 2021). Begin 2024 ontstond er bijvoorbeeld consternatie over een Russisch antisatelliet wapen, waarover de Amerikaanse overheid waarschuwingen naar buiten bracht. Hoewel het onduidelijk is of het gaat om een nucleair-aangedreven satelliet (de meest waarschijnlijke optie), of een daadwerkelijk nucleair wapen (dat in de ruimte weinig schade zou kunnen aanbrengen, los van de elektromagnetische puls), geeft het wel aan dat er geopolitieke spanningen zijn omtrent de ruimte (Lillis, 2024; Wayenburg, 2024; Starling, 2024). Staten claimen hun aanwezigheid in de ruimte en ontwikkelen middelen in- en technologieën met betrekking tot het ruimtedomein, met name op het gebied van counterspace (Projectteam Statelijke Dreigingen, 2021; Reding, 2023). Met *counterspace* technologieën wordt beoogd om dominantie in de ruimte te verkrijgen boven andere actoren, met offensieve acties gericht op satellieten, grondsystemen of de communicatie tussen die twee (Secure World Foundation, 2024). Daarbij is het gedateerde (1960-1980) internationaal recht in de ruimte niet meer bestand tegen het grote aantal actieve (niet-statelijke) actoren en nieuwe activiteiten in de ruimte (Goguichvli, 2021).

Een andere belangrijke ontwikkeling op het gebied van ruimtetechnologie in het kader van nationale veiligheid is het gebrek aan aandacht voor de digitale veiligheid van ruimte infrastructuur, zie ook Onderdeel A.9 Cyberdreigingen en A.10 Bedreiging vitale infrastructuur. Dit zorgt voor een gebrek aan inzicht in mogelijke kwetsbaarheden. Satellieten worden gebruikt voor een breed scala aan militaire en civiele toepassingen, denk aan GPS, aardobservatie en telecommunicatie (ENISA, 2022). Als het gaat om verstoring van GPS (een specifiek GNSS signaal), kunnen ontwrichtende keteneffecten ontstaan, bijvoorbeeld in de vitale infrastructuur (Rijksoverheid, 2022). Naast afhankelijkheden van satellieten ten behoeve van positie- of tijdsbepaling, worden satellieten ook grootschalig gebruikt voor aardobservatie. Fenomenen als luchtvervuiling, ontbossing,

het smelten van de ijskappen, verzakking van dijken en bodem, droogte en stijging van de zeespiegel worden gemonitord vanuit de ruimte (NSO, 2022). Bovendien wordt door de toenemende congestie in de ruimte en de bijbehorende accumulatie van ruimtepuin het risico op botsingen (waardoor satellieten moeten uitwijken), of zelfs een catastrofale kettingreactie volgens het Kessler Syndroom[15] steeds realistischer, wat *space sustainability* urgenter maakt (Wall, 2022). Incidenten die de beschikbaarheid, integriteit en/of vertrouwelijkheid van deze satellietdiensten aantasten kunnen dus mogelijk grote socio-economische impact hebben (ENISA, 2022; Projectteam Statelijke Dreigingen, 2021; OECD, 2022).

Een laatste ontwikkeling binnen ruimtetechnologie relevant voor Nationale Veiligheid is de toenemende hoeveelheid commerciële partijen actief in de ruimte, zoals SpaceX, Blue Origin en Virgin Galactic (Ben-Itzhak, 2022; Reding, 2023; You, 2022). Met name in de V.S. worden met privaat geld grote investeringen gedaan in de ontwikkeling van satellieten, die de toegang tot de ruimte goedkoper en flexibeler maken (NSO, 2022). In de oorlog in Oekraïne zien we hoe de Starlink satellietconstellatie van het Amerikaanse bedrijf SpaceX wordt ingezet voor (het verstoren van) militaire communicatie en internet (Miller, 2022). Tegelijkertijd vormt een dergelijke afhankelijkheid van een commerciële partij ook een kwetsbaarheid, daar er geen garantie is dat SpaceX de dienst zal blijven leveren.

B.3 Quantumtechnologie

Quantumtechnologie berust op specifieke verschijnselen uit de kwantumfysica (zoals verstrengeling en superpositie) en benut het bijzondere gedrag van energie en materie op atomaire en subatomaire schaal, oftewel de allerkleinste quantumdeeltjes, om op een radicaal nieuwe manier te kunnen rekenen, communiceren en meten (Van Bree, 2023). Quantumtechnologie wordt gezien als een *enabling* technologie die nieuwe producten en diensten mogelijk kan maken. Toepassing van quantumtechnologie voor deze nieuwe producten en diensten staat veelal nog in de kinderschoenen. De potentiële impact van quantumtechnologie toepassingen is daarom nog deels onbekend (Bronkhorst, 2020). Dat neemt niet weg dat het in het kader van de nationale veiligheid noodzakelijk is om nu te anticiperen op de komst van allerlei quantumtechnologie toepassingen. Quantumtechnologie wordt veelal uitgesplitst in drie toepassingsgebieden: *quantum computing*, quantum communicatie (inclusief *quantum key distribution*) en *quantum sensing* (Van Bree, 2023).

Een zeer relevante ontwikkeling op het gebied van quantumtechnologie met het oog op nationale veiligheid is de komst van de quantumcomputer.[16] Deze kan naar verwachting worden ingezet als digitaal wapen om de huidige cryptografische standaarden te breken, wat het versleutelen van gevoelige informatie met die standaarden ontoereikend maakt (Neumann, 2021). Verschillende (overheids)diensten maken gebruik van *Public Key Infrastructure* (PKI), zoals de Belastingdienst. De technologie kan daarmee potentieel ingezet worden om verstoring of uitval van vitale processen te veroorzaken. Mogelijk zijn actoren nu al bezig met het opslaan van versleutelde communicatie, om die te decoderen wanneer er een quantumcomputer is met voldoende rekenkracht (TNO, CWI & AIVD, 2023). Het is niet duidelijk wanneer de technologie volwassen genoeg is om dit te bereiken. Aangezien sommige informatie lange tijd gevoelig blijft en ook schade kan toebrengen aan de nationale veiligheid als het over tien, vijftien of twintig jaar wordt gedecodeerd door kwaadwillenden, is het om deze informatie te beschermen voor sommige partijen nu al van belang om te beginnen met het implementeren van post-quantum-cryptografie (AIVD, 2021; TNO, CWI & AIVD, 2023).

Daarnaast zijn er meerdere toepassingen in het militaire domein denkbaar die impact op de operatie kunnen hebben. Verbeterde sensoren kunnen de effectiviteit van radarsystemen sterk verbeteren, waardoor het makkelijker wordt om vijandige voertuigen onder water en in de lucht te detecteren. Stealth technologieën zouden daardoor minder effectief kunnen worden (Lele, 2021). Daarnaast kunnen nauwkeurige klokken ontwikkeld worden, wat navigatie mogelijk maakt voor gebieden waar geen GPS beschikbaar is (Reding, 2023). Quantumtechnologie zal niet alleen nieuwe technologische verbeteringen en mogelijkheden bieden, maar vereist ook de ontwikkeling van nieuwe (militaire) strategieën, tactieken, beleid en beoordeling van dreigingen (Krelina, 2021).

Bovenstaande ontwikkelingen benadrukken ook de relevantie van quantumtechnologie op het gebied van strategische afhankelijkheden. Zo heeft de Europese Commissie in 2023 quantumtechnologie als een van de strategische focusgebieden voor de aanstaande *European Economic Security Strategy* benoemd. Deze strategie (nog in ontwikkeling) ambieert een gemeenschappelijk kader te bieden ten behoeve van strategische autonomie door het bevorderen van het concurrentievermogen, het beschermen tegen risico's ten aanzien van risicovolle strategische afhankelijkheden en het samenwerken met partners (Europese Commissie, 2023a). Daarnaast is quantumtechnologie door de Europese Commissie

[15] Een hypothetisch maar gevreesd scenario waarbij een botsing in de ruimte meer ruimtepuin veroorzaakt, die op haar beurt weer meer botsingen creëert, waarmee een positieve feedbackloop gevormd wordt.

[16] Zie ook het dreigingsthema cyberdreigingen in (A.9).

geselecteerd als een van de vier technologiegebieden (naast geavanceerde halfgeleiders, AI en biotechnologie) waarvan het zeer waarschijnlijk wordt geacht dat het de meest gevoelige en directe risico's met zich mee kan brengen op het gebied van het weglekken van kennis en technologie. Lidstaten worden geadviseerd voor deze technologiegebieden een gezamenlijke risicobeoordeling uit te voeren (Europese Commissie, 2023b). Tegelijkertijd zijn er recentelijk ook unilaterale exportcontroles afgekondigd onder meer op het gebied van quantumtechnologie,[17] ondanks het streven binnen de EU om dergelijke maatregelen gezamenlijk te treffen. Hierdoor ontstaat niet alleen een risico op een "lappendeken" van exportbeperkende maatregelen binnen de EU, maar ook fragmentatie van de gemeenschappelijke markt binnen de EU (Europese Commissie, 2024).

B.4 Robotica en Autonome systemen

Robots zijn onbemande systemen die zelfstandig taken kunnen uitvoeren in de lucht, op de grond, op- of onder water. Robots worden ingezet om zware, saaie of gevaarlijke taken van mensen over te nemen, maar bieden ook een belangrijke offensieve en defensieve capaciteit op het gebied van onder meer inlichtingenverzameling en wapeninzet. Om deze taken uit te voeren worden robots uitgerust met regeltechniek en sensoren (zoals camera's, thermometers en lichtmeters). RAS technologie is gericht op het ontwikkelen van methoden, tools en middelen op het gebied van mechanische structuur, bediening op afstand, en autonome bediening (Bronkhorst, 2020). Autonomie wil zeggen dat een systeem zelfstandig kan handelen in een onverwachte en onzekere situatie, waarbij mensen supervisie houden en bewaken dat de autonome systemen binnen de opgelegde kaders blijven in alle fasen van de ontwikkeling (design, uitvoering, evaluatie en aanpassing) (Reding, 2023; Elands, 2023). De functionaliteit van autonome systemen berust op drie pijlers: een wereldmodel, intelligentie (redeneervermogen) en een opdracht (doelfunctie). Daarbij spelen sensoren een belangrijke rol in het verzamelen van informatie over de omgeving en over het functioneren van het systeem zelf, welke dienen om de informatie te toetsen aan het wereldmodel.

Een belangrijke aanjager in de doorontwikkeling van RAS zijn de vorderingen op het gebied van AI, en daarmee een doorontwikkeling van autonomie in onbemande systemen. Een voorbeeld van de toenemende autonomie is terug te zien in het concept van *'swarming'* (zwermen van onbemande systemen), waarbij systemen in gezamenlijkheid optreden (Bronkhorst, 2020). Dergelijke zwermen van systemen hebben een potentieel disruptieve impact op het gevechtsveld, bijvoorbeeld omdat ze kunnen zorgen voor saturatie van (lucht)verdedigingssystemen. De toename van autonomie in onbemande systemen en daarmee de zorg of men deze systemen nog wel onder controle heeft, baart onder andere het Westen al tijden zorgen, met name de ontwikkeling van *Lethal Autonomous Weapon Systems* (LAWS), autonome wapensystemen (Rathenau Instituut, 2021). Internationale juridische afspraken blijven tot nog toe uit, maar de technologie ontwikkelt door, ook omdat dergelijke autonome wapensystemen gebruik kunnen maken van ontwikkelingen in AI en civiele toepassingen van autonomie (Reding, 2023). Zoals ook besproken bij *Artificial Intelligence*, wordt vanuit het Westen nadruk gelegd op het inbedden van betekenisvolle menselijke controle (*meaningful human control*), maar potentiële tegenstanders zullen andere juridische en ethische kaders hebben betreffende de ontwikkeling, toepassing en inzet van AI-systemen ten behoeve van militaire toepassingen (Rijksoverheid, 2023).

In recente conflicten zijn autonome systemen daadwerkelijk veelvuldig ingezet. Autonome systemen spelen een belangrijke rol in recente conflicten, waaronder Nagorno-Karabakh, Syrië, Gaza en Oekraïne (Detsch, 2021; Williams, 2023; Pol, 2022). Zowel Oekraïense als Russische strijdkrachten maken gebruik van onbemande systemen voor (ondersteuning van) militaire operaties in de lucht, op de grond en op zee. Daarbij worden de systemen gebruikt voor het beschadigen van vitale infrastructuur, het verstoren van vijandelijke aanvoerlijnen, het uitvoeren van surveillance en evacuaties in vijandige gebieden en het uitschakelen van voertuigen en personeel (Vos, 2023). Hoewel het gebruik van onbemande systemen (drones) grote impact heeft op het gevechtsveld, zijn de ingezette drones in de oorlog in Oekraïne voornamelijk bestuurd door menselijke operators, klein van omvang en opereren niet of zeer beperkt in een genetwerkte structuur. Tegelijkertijd wordt er wel innovatief gebruik gemaakt van commerciële, goedkope systemen (vaak *single use*) die kunnen worden aangepast ten behoeve van militaire doeleinden (Pettyjohn, 2024). Zo worden drones ingezet voor het aangrijpen van doelen (militairen en materieel), maar spelen ze voornamelijk een belangrijke rol op het gebied van inlichtingenverzameling en surveillance (Pettyjohn, 2024). Door de toegenomen inzet van onbemande systemen, nemen tegelijkertijd *counter-drone capabilities* een vlucht (denk aan netten, elektronische oorlogsvoering, digitale aanvallen op de software en meer) (Reding, 2023; Pettyjohn, 2024).

[17] Zoals in Spanje in mei 2023 (Ministerio de Industria, 20230) en Frankrijk in februari 2024 (Haeck, 2024)

B.5 Fotonicatechnologie

Fotonicatechnologie richt zich op het opwekken, transporteren en detecteren van lichtgolven en lichtdeeltjes, ook wel fotonen genoemd. Fotonica lijkt op elektronica, maar in plaats van elektronen, worden fotonen gebruikt om informatie te transporteren (Photondelta, 2024; Van Bree, 2023; Rijksoverheid, 2023a). Fotonica kent zeer brede toepassingsmogelijkheden binnen onder meer de volgende gebieden: de maakindustrie (bijvoorbeeld productiemachines met lasers en 3D-displaytechnologie), gezondheid (zoals diagnose en monitoring met licht), *agrifood* sector (denk aan optische sensoren voor voedselveiligheid en precisielandbouw), halfgeleiders (onder meer voor het maken van chips met licht), ICT (zoals glasvezel en satellietcommunicatie) en energie en milieu (onder andere het meten van fijnstof met optische sensoren) (Parlementaire Monitor, 2018). De technologie wordt in zeer veel 'hightech' producten toegepast, niet alleen in consumentenproducten zoals beeldschermen, camera's, telefoons, internetverbindingen, zonnepanelen en verlichting (zo ook in bijvoorbeeld kassen), maar ook in specifieke militaire producten zoals nachtkijkers of diverse soorten sensoren voor veiligheidstoepassingen. Fotonica is bovendien een belangrijke *enabler* voor de doorontwikkeling van andere technologiegebieden, zoals quantumtechnologie en AI (PhotonicsNL, 2020; Rijksoverheid, 2023a; 2024).

In het kader van de nationale veiligheid zien we een aantal relevante ontwikkelingen. Een van de belangrijkste ontwikkelingen op het gebied van fotonica zijn de toepassingen voor communicatie. Met name fibercommunicatie (glasvezelnetwerken) en optische (satelliet) communicatie zijn relevant, waarbij informatie via licht over grote afstanden wordt verstuurd. Gezien de relatief veilige en robuuste verbinding middels lichtsignalen is de toepassing zeer relevant voor het defensie- en veiligheidsdomein (Rijksoverheid, 2024). Ook is fotonicatechnologie in het militaire domein belangrijk voor de doorontwikkeling van onder meer (optische) lasers (Reding, 2023). Zo heeft het Verenigd Koninkrijk recentelijk een succesvolle test uitgevoerd met een laser *Directed Energy* wapen. Dergelijke wapens kunnen doelwitten aangrijpen met een intense lichtstraal en daarmee een doelwit uitschakelen of grote schade toebrengen (Optics.org, 2024).

Een opkomend deelgebied van fotonicatechnologie is geïntegreerde fotonica. Bij geïntegreerde fotonica worden optische systemen toegepast in de chipindustrie (*Photonic Integrated Circuits*, PICs), en deze fotonische chips beloven een toekomstig efficiënter en energiezuiniger alternatief voor de huidige elektronische chips (Rijksoverheid, 2023b).

Ook de technologieën die worden gebruikt om zeer kleine halfgeleidercomponenten te produceren (*Extreme Ultraviolet Lithography* (EUV) en optische metrologie) zijn deelgebieden van fotonica (Rijksoverheid, 2024). Machines (zoals die van ASML) brengen patronen aan op een chip die processor of geheugen elementen vormen. De halfgeleiderindustrie is zoals eerder benoemd een belangrijk toepassingsgebied van fotonica, zeker in Nederland. In generieke zin ervaren fotonicabedrijven binnen de EU uitdagingen in de toeleveringsketen, waarbij het niet alleen gaat om tekorten in materialen, maar ook in halffabricaten en machines waarbij een afhankelijkheid geldt van leveranciers buiten de EU (Rijksoverheid, 2023b). Tegelijkertijd geven exportmaatregelen ten aanzien van de halfgeleiderindustrie uitdrukking aan de geopolitieke spanningen tussen onder meer de VS en China, waarbij China juist ook afhankelijk is van Westerse bedrijven als ASML.

B.6 Energietechnologie

Energietechnologie is een breed gebied dat een scala aan technologieën omvat voor de productie, opslag, transport en gebruik van energie, zoals technologieën om natuurlijke energiebronnen te benutten (fossiele brandstoffen, kernenergie en hernieuwbare energiebronnen) (Bronkhorst, 2020). Het gebied is volop in ontwikkeling door de overgang van het gebruik van fossiele energie naar hernieuwbare energie. Omdat de energietransitie veel maatschappelijke sectoren raakt staat het volop in de belangstelling.

Ten aanzien van energie zijn ontwikkelingen op het gebied van nucleaire energie, hernieuwbare energiebronnen en duurzame brandstoffen (zoals biobrandstoffen en waterstof) relevant (Reding, 2023). Tweede generatie briobrandstoffen zoals cellulose, algen en afvaloliën worden gebruikt voor de productie van bijvoorbeeld bio-ethanol, maar ook CO_2 en waterstof (zie ook A.10 bedreiging vitale infrastructuur) als grondstof voor chemische technologie zijn in opkomst (COGEM, 2023). Een belangrijk uitgangspunt is dat dergelijke technologische doorontwikkeling niet om grondstoffen concurreert met de voedselproductie (COGEM, 2023). Door de groeiende afhankelijkheid van hernieuwbare elektriciteit en de toenemende elektrificatie van de samenleving, wordt robuuste en betrouwbare elektriciteitsopslag (zoals batterijen, maar ook vliegwielen) steeds belangrijker (Reding, 2023). Elektriciteitsopslag is essentieel om de piekvraag en -aanbod van stroom op te vangen, evenals decentralisatie om zo netwerken te creëren die onafhankelijk zijn van elkaar. In A.10 bedreiging vitale infrastructuur staat een uitgebreidere toelichting ten aanzien van de uitdagingen rondom de energietransitie in relatie tot vitale sectoren. In het militaire domein zijn

brandstofleveranties op dit moment een van de kritieke punten ten aanzien van voortzettingsvermogen van de operatie. Dit heeft mede te maken met wapensystemen die om meer energie vragen (denk aan lasertoepassingen). Elektriciteitsopslag wordt ook in dit kader daarom steeds belangrijker (Ministerie van Defensie, 2023).

Daarnaast zijn technologische ontwikkelingen belangrijk ten aanzien van energietransmissie (zoals *micro grids* (voor de gebouwde omgeving), warmtenetwerken en andere manieren om flexibiliteit in het energiesysteem te bevorderen, met name als het gaat om een stabiel elektriciteitsnet (rijksoverheid, 2023a; Reding, 2023). Tegelijk is het binnen onder meer de vitale infrastructuur van cruciaal belang om aandacht te besteden aan de 'tussenfase': wanneer nieuwe technologieën ten behoeve van de energietransitie nog niet helemaal zijn doorontwikkeld en al wel geïmplementeerd worden naast bestaande infrastructuur en technologie. In die fase moet zorg gedragen worden dat nieuwe en bestaande technologieën aan elkaar kunnen worden gekoppeld, waarbij de leveringszekerheid van bijvoorbeeld elektriciteit gegarandeerd moet blijven (Tennet, 2023).

Tegelijkertijd is er sprake van beperkte Nederlandse en Europese strategische autonomie als het gaat om de doorontwikkeling van energietechnologieën. Enerzijds wordt levering van energie zelf als strategisch wapen ingezet door bijvoorbeeld Rusland. Anderzijds bestaat er afhankelijkheid op het gebied van de daadwerkelijke ontwikkeling van en onderzoek naar hernieuwbare energiebronnen, met name van China, die zelf tot doel heeft gesteld CO_2-neutraal te zijn in 2060 (Rijksoverheid, 2024). Naast dergelijke investeringen, is China tevens dominant in de waardeketen van zeldzame aardmetalen die cruciaal zijn voor bijvoorbeeld batterijtechnologie (Rijksoverheid, 2023a). Naast investeringen in opkomende technologieën als natrium-ion waar minder kritieke grondstoffen voor nodig zijn, wordt onder meer in de Nationale Technologie Strategie gesteld dat Nederland moet "streven naar een duurzame en veerkrachtige toeleveringsketen voor kritieke grondstoffen om mogelijke risico's te minimaliseren en de energietransitie op een betrouwbare en stabiele manier te bevorderen." (Rijksoverheid, 2024, p.81). Een belangrijk initiatief naar aanleiding van de constatering dat de EU in grote mate afhankelijk is van het buitenland voor wat betreft kritieke grondstoffen, is de kritieke grondstoffen verordening (2023/0079) van de EU (Europese Commissie, 2023). In deze verordening staat een set van acties om te kunnen waarborgen dat de EU toegang heeft en houdt tot een veilig, gediversifieerd, betaalbaar en duurzaam aanbod van kritieke grondstoffen. Ook wordt onderzoek gedaan naar recycling (van windmolenbladen bijvoorbeeld (TNO, 2024)) als mogelijke (deel)oplossing voor het tekort aan materialen (Pommeret, 2022).

B.7 Biotechnologie

Biotechnologie is een technologie die levende organismen, cellen of componenten daarvan gebruikt om nieuwe producten te ontwikkelen. Door ontwikkelingen op het gebied van sequencing (bepalen van de basenvolgorde in erfelijk materiaal), gene editing (het aanbrengen van gerichte veranderingen in het genoom)[18] en genetische modificatie (aanpassing van erfelijk materiaal op een manier die natuurlijk niet mogelijk is), in combinatie met de doorontwikkeling van technologieën als informatietechnologie en automatisering, is biotechnologie bezig aan een opmars. Hierdoor kan biotechnologie op steeds grotere schaal worden toegepast (COGEM, 2023). De technologie wordt bijvoorbeeld gebruikt voor het verbeteren van gewassen (zoals plant- of zaadveredeling), in de gezondheidszorg (zoals het bestrijden van ziektes), en voor industriële toepassingen (zoals het vervangen van milieubelastende stoffen door biologische materialen) (Rijksoverheid, 2024). Vaak wordt een kleur-indeling van toepassingsgebieden van biotechnologie gebruikt: industriële toepassingen (wit), landbouw en voedsel (groen), medisch en gezondheid (rood) en marine en milieu (blauw) (Van Bree, 2023).

Ten aanzien van nationale veiligheid kent ook dit technologiegebied zowel civiele als militaire toepassingen en is dus *dual-use* van aard. Zo kunnen door ontwikkelingen op het gebied van synthetische biologie zeer nauwkeurig modificaties bij bestaande organismen worden aangebracht of zelfs geheel nieuwe organismen worden gecreëerd. Synthetische biologie won aan bekendheid door de snelle ontwikkeling van een COVID-19 vaccin (GCHQ, 2022). Dezelfde technieken om een vaccin te ontwikkelen kunnen ook gebruikt worden om een virus te (re)creëren (Van Weerd, 2021). Ook hebben ontwikkelingen op het gebied van *precision health*, waarbij gebruik wordt gemaakt van kennis over het persoonlijke DNA (ten behoeve van gepersonaliseerde behandeling van ziektes) (COGEM, 2023; Reding, 2023), een potentieel malafide toepassing. Zo zouden biologische wapens kunnen worden ontwikkeld die gericht zijn op mensen met specifieke genetische kenmerken en kan genetische informatie worden misbruikt om etnische groepen op basis van ras te identificeren en te discrimineren. Het is daarom van groot belang om databases waarin DNA codes worden opgeslagen[19]

[18] Gene editing (het aanbrengen van gerichte veranderingen in het genoom) heeft een vlucht genomen sinds de toepassing van het CRISPR-Cas9 systeem *(Clustered regularly interspaced short palindromic repeats (CRISPR) associated protein)* ruim 10 jaar geleden. Hierdoor kan namelijk relatief eenvoudig een breuk worden gecreëerd op een specifieke plaats in het DNA en op die plek een verandering in het genoom worden aangebracht (COGEM, 2023).

[19] Denk ook aan bedrijven die online diensten aanbieden om op basis van genetisch materiaal onderzoek te doen naar genealogie.

(digitaal) te beveiligen (Luca, 2023). Overheidsdatabases, zoals de Britse *"biobank"*[20] zijn cruciaal om bijvoorbeeld algoritmes te kunnen trainen op geanonimiseerde data om daarmee onderzoek te kunnen doen naar onder meer onderliggende oorzaken van bepaalde aandoeningen, maar zijn daarmee ook een doelwit van criminelen en andere kwaadwillenden (Alder, 2023; Kuntz, 2024). Eind 2023 is bijvoorbeeld het bedrijf *23andMe* doelwit geworden van een grootschalig datalek, waarbij van bijna zeven miljoen gebruikers data is buitgemaakt. Cybercriminelen kregen toegang tot bepaalde persoonlijke gegevens, zoals stambomen, geboortejaar en geografische locatie, door gebruik te maken van inloggegevens die openbaar werden gemaakt in eerdere hacks (McCallum, 2023; The Guardian, 2024).

Biotechnologie toepassingen kunnen gebruikt worden ten behoeve van *human enhancement*, maar niet alle human enhancement technieken zijn biotechnologie in de zin dat (componenten van) cellen of levende organismen worden gebruikt. *Human Enhancement* draait om het verbeteren van fysieke, cognitieve, fysiologische, zintuiglijke of sociale functies van de mens (Reding, 2023). Echter, nog los van de ethische en juridische kaders, is onderzoek naar de genetische modificatie van mensen en gentherapie nog in een vroeg stadium omdat het zeer complexe processen zijn. Bovendien is op dit moment het meest te behalen op het gebied van training of andere externe, relatief simpele interventies (Van Weerd, 2021). In dit kader is het relevant om de recente ontwikkelingen rond Neuralink te benoemen, het bedrijf van Elon Musk dat zich richt op neurotechnologie en de ontwikkeling van *brain-computer interfaces* (BCI, hersenimplantaten). Dergelijke BCI's zijn bedoeld om met gedachten een computer aan te sturen en zijn daarmee een vorm van human enhancement. Echter, de eerste toepassingen worden voorzien voor mensen met een verlamming, de koppeling met bijvoorbeeld AI om mensen sneller te laten denken is nog zeer ver in de toekomst. Volgens het bedrijf zou het in februari 2024 voor het eerst zijn gelukt om een BCI in te brengen in een mens, waarbij de verdere informatie over de betreffende patiënt zeer beperkt blijft (Guarino, 2024).

Regelgeving binnen de EU op het gebied van biotechnologie is strenger dan in bijvoorbeeld China, gegeven de politieke en maatschappelijke nadruk op ethische overwegingen ten aanzien van genetische modificatie (Rijksoverheid, 2024). Tegelijkertijd ontwikkelt de technologie door, en bestaat het risico dat Europa op een zeker moment geconfronteerd wordt met technologische toepassingen in het Defensie- en veiligheidsdomein zonder dat daarvoor de juiste tegenmaatregelen voor zijn ontwikkeld.

[20] De *UK Biobank*. Zie *https://www.ukbiobank.ac.uk/* voor meer informatie.

Onderdeel C
Methodiek

Om te komen tot de Trendanalyse Nationale Veiligheid is een aantal methodische stappen doorlopen.

Stap 1: inventariseren van ontwikkelingen uit de RbRa
De Trendanalyse brengt in kaart welke nieuwe ontwikkelingen zich hebben voorgedaan sinds het uitvoeren van de Rijksbrede Risicoanalyse (RbRa) en wat de status is van de reeds in de RbRa opgenomen ontwikkelingen. De eerste stap in de analyse betreft dan ook het inventariseren van alle in de RbRa opgenomen ontwikkelingen voor elk van de dreigingsthema's. Deze dreigingsthema's zijn:

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

Stap 2: literatuurscan langs twee sporen
Vervolgens is een uitgebreide literstuurscan uitgevoerd, vormgegeven langst twee sporen. Enerzijds betreft dit een scan vanuit het perspectief van de dreigingsthema's uit de RbRa.[21] Dat wil zeggen dat er vanuit bijvoorbeeld het perspectief infectieziekten is gezocht naar relevante ontwikkelingen. Hierbij is zowel gezocht naar informatie rond de status van reeds in de RbRa opgenomen ontwikkelingen als naar nieuwe ontwikkelingen. Anderzijds is een scan uitgevoerd vanuit het perspectief van meer autonome ontwikkelingen op de domeinen sociaal-demografisch, technologie, ecologie, economie en internationale politiek (STEEP). Wanneer deze twee sporen worden samengebracht, ontstaat er een complementair beeld van voor de nationale veiligheid relevante ontwikkelingen (zie stap 3). Vanuit de organisaties binnen het ANV zijn meerdere scanteams opgesteld, die een aantal onderwerpen (dreigingsthema's dan wel autonome ontwikkelingen) hebben beschouwd. Hierbij is zoveel mogelijk aangesloten bij de expertise van de organisaties in kwestie.

Binnen de literatuurscan zijn verschillende soorten bronnen geraadpleegd, waaronder academische literatuur, grijze literatuur in de vorm van rapporten van overheden en (inter)nationale organisaties, en nieuwsberichten. Voor de literatuurscan zijn alleen nieuwe ontwikkelingen meegenomen die zich hebben voorgedaan sinds het uitvoeren van de analyse voor de RbRa in het eerste kwartaal van 2022, dan wel waar sindsdien meer informatie beschikbaar over is of zich anders hebben gemanifesteerd dan eerder verwacht. Binnen de Trendanalyse zijn publicaties meegenomen die zijn verschenen tot en met 31 mei 2024. Qua tijdshorizon wordt verder primair gefocust op ontwikkelingen die van belang zullen zijn voor de resterende looptijd van de Veiligheidsstrategie voor het Koninkrijk der Nederlanden, tot en met 2029. Voor een aantal meer langdurige ontwikkelingen zoals die rond klimaatverandering is ervoor gekozen om af te wijken van deze grens, te meer omdat deze en andere bewegingen ook op het gebied van mogelijke maatregelen en beleid een langere doorlooptijd hebben. De bevindingen uit de literatuurscan zijn aangevuld en gevalideerd door middel van verdiepende gesprekken met inhoudsdeskundigen. Voor het duiden en ophalen van ontwikkelingen voor het Caribisch deel van het Koninkrijk is een aparte sessie georganiseerd met vertegenwoordigers van de landen en bijzondere gemeenten.

Stap 3: uitwisselen van ontwikkelingen
Waar de scan op ontwikkelingen is vormgegeven langs de individuele dreigingsthema's en ontwikkelingen op de bredere domeinen, is een nadrukkelijke functie van de Trendanalyse juist ook het helpen inzichtelijk maken van de mogelijke samenhang hiertussen. De volgende

[21] De RbRa bevat negen dreigingsthema's. binnen de trendanalyse worden echter tien thema's beschouwd. Reden hiervoor is dat het onderwerp georganiseerde criminaliteit binnen de RbRa is ondergebracht in een overkoepelend thema, maar in de trendanalyse zelfstandig wordt gepresenteerd. Dit om aan te sluiten bij de wijze waarop georganiseerde criminaliteit ene plek heeft gekregen binnen de Veiligheidsstrategie.

stap is dus het uitwisselen van ontwikkelingen tussen de verschillende onderwerpen waarop is gescand. Voor elk van de geïdentificeerde ontwikkelingen is beoordeeld of deze mogelijk ook van toepassing is op een ander dreigingsthema of autonome ontwikkeling. Om dit te bereiken is een werksessie georganiseerd met alle scanteams, waarbij de volgende twee vragen zijn gesteld:

- Welke ontwikkelingen uit dreigingsthema X hebben mogelijk invloed op dreigingsthema Y en zouden ook binnen dit thema moeten worden opgenomen als ontwikkeling?
- Welke bevindingen vanuit het perspectief van de vijf autonome ontwikkelingen zijn van belang voor de individuele dreigingsthema's en zouden ook hier moeten worden opgenomen als ontwikkeling

Resultaat van deze stap is per dreigingsthema en autonome ontwikkeling een meer compleet en integraal beeld van relevante ontwikkelingen.

Stap 4: samenvattend en integraal overzicht van ontwikkelingen (*what's new?*)

Op basis van de bevindingen uit de voorgaande stappen is vervolgens ook een samenvattend en integraal overzicht opgesteld van ontwikkelingen. Hierbij is vooral gekeken naar ontwikkelingen die mogelijke brede implicaties hebben voor bijvoorbeeld meerdere dreigingen en die mogelijk ook veel interactie hebben met andere ontwikkelingen. Dit overzicht richt zich vooral op de vraag 'what's new?' en is vormgegeven langs de lijnen van de STEEP domeinen, zoals ook gehanteerd binnen de literatuurscan. Doel van het overzicht is om niet alleen enkele van de belangrijkste bevindingen uit de voorgaande stappen onder de aandacht te brengen, maar juist ook om aandacht te hebben voor dwarsverbanden.

Stap 5: Duiden van implicaties – strategische inzichten en gevolgen voor het veiligheidsbeeld

De vijfde stap betreft het duiden van de implicaties van alle beschouwde ontwikkelingen. Deze duiding vindt plaats op drie verschillende abstractieniveaus. Om te beginnen is per dreigingsthema geduid wat de mogelijke gevolgen zijn van hieraan gerelateerde ontwikkelingen voor het dreigingsbeeld van het betreffende thema zoals geschetst in de RbRa. Deze duiding is hoofdzakelijk vormgegeven rond de implicaties van ontwikkelingen voor de zes nationale veiligheidsbelangen ten opzichte van de analyse uit 2022, waarbij indien van toepassing ook aandacht is voor de verwachte frequentie van de dreiging(en) in kwestie. Het is echter belangrijk om te benadrukken dat de Trendanalyse geen risicobeoordeling is. Dat wil zeggen dat er geen expliciete uitspraak wordt gedaan over veranderingen in de impact- en waarschijnlijkheidscores voor de verschillende dreigingsscenario's in de RbRa. Ten tweede wordt op vergelijkbare wijze een duiding gegeven aan de bredere ontwikkelingen gezien vanuit de STEEP domeinen. Hierbij is vooral aandacht voor de implicaties op de nationale veiligheid(sbelangen) in het algemeen en voor welke dreigingen de bredere ontwikkelingen mogelijk relevant zijn. Ten derde vindt er een duiding van gevolgen plaats op een meer strategisch abstractieniveau. Hierbij is primair de vraag wat voor dynamieken we zien als we de ontwikkelingen uit de Trendanalyse naast elkaar leggen? Deze beschouwing hanteert meer een systeemperspectief en bouwt hierbij voort op de onder stap vier opgestelde overzichten. Onderdeel hiervan is ook een doorkijk naar mogelijke vragen en uitdagingen voor verdere strategievorming.

Verschil met eerdere horizonscans van het ANV

De aanpak van de Trendanalyse 2024 verschilt in een aantal opzichten van eerdere, vergelijkbare producten van het ANV zoals de horizonscan uit 2018, 2019 en 2020. Zo ligt er in deze editie meer nadruk op zowel de implicaties als de samenhang van de verschillende ontwikkelingen, hetgeen zich onder meer vertaalt in een overzicht met inzichten op strategisch niveau. Ook is er binnen deze Trendanalyse tegelijkertijd meer aandacht voor ontwikkelingen (en de gevolgen hiervan) vanuit het perspectief van de verschillende dreigingsthema's. Dit komt ten dele voort uit een ander verschil, namelijk dat de Trendanalyse in tegenstelling tot haar voorgangers nadrukkelijk gekoppeld aan andere analyse- en strategiedocumenten, in dit geval enerzijds de RbRa en anderzijds de Veiligheidsstrategie. Verder is er bij de totstandkoming van de Trendanalyse sprake van meer gestructureerd en frequent overleg met de afnemers van het product. Hiertoe is een stuurgroep gevormd, waarin ook vertegenwoordigers vanuit het Caribisch deel van het Koninkrijk zitting hebben genomen. Tot slot is ook de wijze waarop de bevindingen worden gepresenteerd anders dan in veel van de andere ANV producten. In plaats van de rapportage vorm te geven in dezelfde volgorde als de genomen analytische stappen hierboven, is er juist voor gekozen om in het hoofdrapport juist de meer strategische en overkoepelende bevindingen uit te lichten.

Onderdeel D
Het Analistennetwerk Nationale Veiligheid

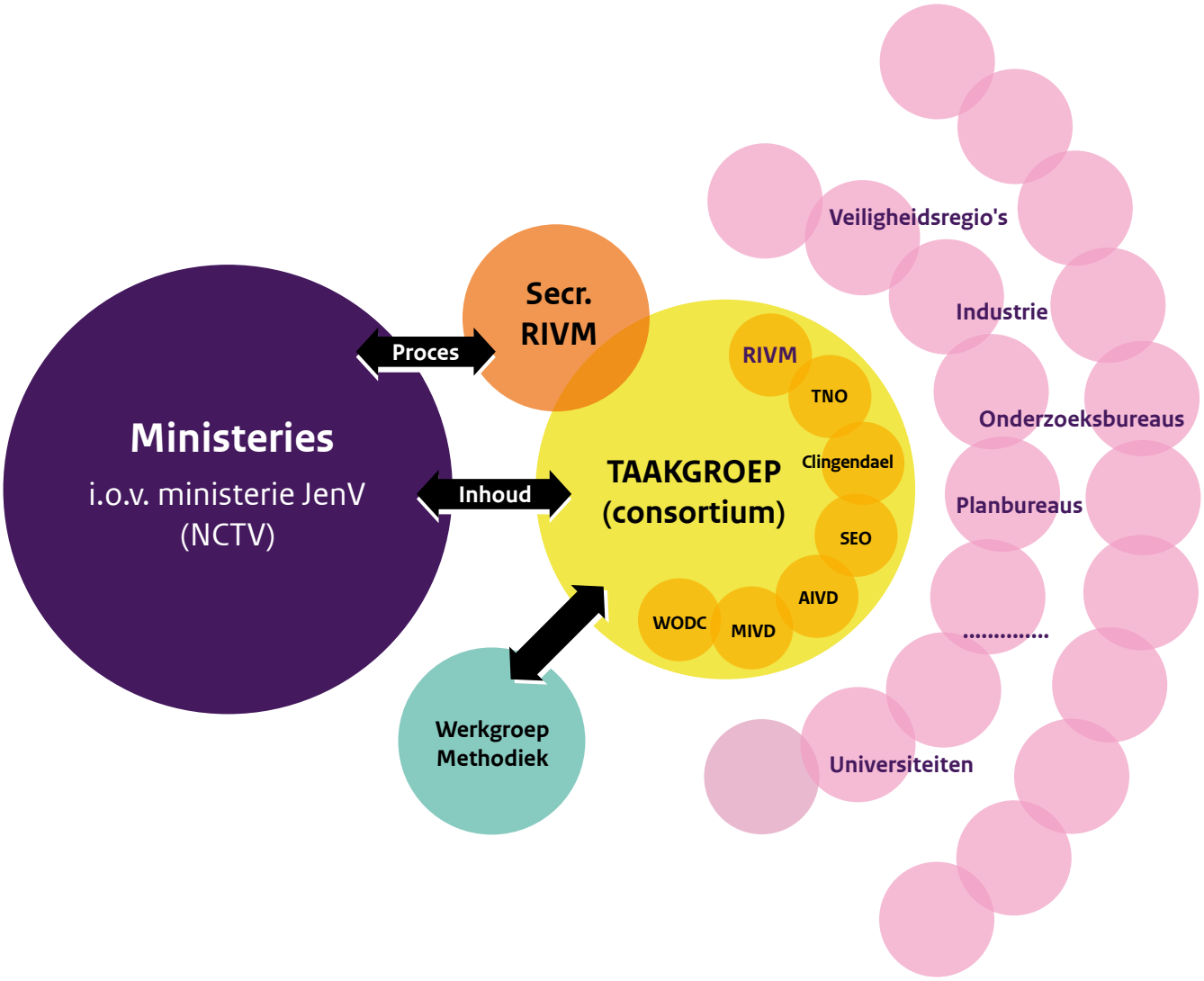
Het Analistennetwerk Nationale Veiligheid (ANV) is een kennisnetwerk dat in 2010 is opgericht. Sindsdien heeft het ANV de periodiek een nationale risicobeoordeling opgesteld en andere verdiepende analysestudies op het gebied van nationale veiligheid verricht. Dit in opdracht van het ministerie van Veiligheid en Justitie namens de toenmalige Stuurgroep Nationale Veiligheid (SNV). In 2016 heeft het ANV het Nationaal Veiligheidsprofiel (NVP), in 2019 de Geïntegreerde Risicoanalyse Nationale Veiligheid (GRA) en in 2022 de Rijksbrede Risicoanalyse Nationale Veiligheid (RbRa)

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

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

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

Figuur 1. Netwerkstructuur ANV



Referenties

Inleiding

Analistennetwerk Nationale Veiligheid (ANV). 2022. *Rijksbrede Risicoanalyse Nationale Veiligheid – Hoofdrapport*. Via: *https://www.rivm.nl/nationale-veiligheid*

A.1 Klimaat- en natuurrampen

Academische Werkplaats Gezonde Leefomgeving (juni 2023). *Wie houdt het hoofd koel?* Beschikbaar via: *https://www.awgl.nl/images/projecten/2023/230710%20Onderzoeksrapport%20Wie%20houdt%20het%20hoofd%20koel.pdf*

Centrale bank Curacao & Sint Maarten (december 2023). *Economic bulletin. Winds of Change: Adapting to Climate Change*. December 2023. Beschikbaar via: *https://cdn.centralbank.cw/media/economic_bulletins_2023/20231213_economic_bulletin_december_2023.pdf*

European Environment Agency (EEA) (2022). *Climate change as a threat to health and well-being in Europe: focus on heat and infectious diseases*. EEA Report No 07/2022. Beschikbaar via: *https://www.eea.europa.eu/publications/climate-change-impacts-on-health*

Koninklijk Nederlands Meteorologisch Instituut (KNMI). (9 oktober 2023). *KNMI'23-klimaatscenario's voor Nederland*. Beschikbaar via: *https://www.knmi.nl/research/publications/knmi-23-klimaatscenario-s-voor-nederland*

Koninklijk Nederlands Meteorologisch Instituut (KNMI) (2 januari 2024). *Jaaroverzicht aardbevingen*. Geraadpleegd op 10-08-2023, beschikbaar via: *https://www.knmi.nl/over-het- knmi/nieuws/jaaroverzicht-aardbevingen-2023*

Nederlands Instituut Publieke Veiligheid (NIPV). (23 januari 2023). *Natuurbrandsignaal '23*. Geraadpleegd op 09-10-2023, beschikbaar via: *https://nipv.nl/natuurbrandsignaal-23-meer-onbeheersbare-natuurbranden-met-grotere-impact-op-samenleving/*

NOS (9 november 2022). Bonaire kampt met hevige regenval, straten overstroomd. *NOS Nieuws.* Geraadpleegd op 06-03-2024, beschikbaar via: *https://nos.nl/artikel/2451698-bonaire-kampt-met-hevige-regenval-straten-overstroomd*

Nu.nl (2023). Nederlands klimaat wordt extremer: nattere winters, drogere en hetere zomers. *Nu.nl*. Geraadpleegd op 06-03-2024, beschikbaar via: *https://www.nu.nl/klimaat/6284004/nederlands-klimaat-wordt-extremer-nattere-winter-maar-veel-drogere-en-hetere-zomer.html*

OECD (2023), *Taming Wildfires in the Context of Climate Change*, OECD Publishing, Paris, Beschikbaar via: *https://doi.org/10.1787/dd00c367-en*

PBL (2024), *Klimaatrisico's in Nederland; De huidige stand van zaken*. Den Haag: Planbureau voor de Leefomgeving. Beschikbaar via: *https://www.pbl.nl/system/files/document/2024-05/pbl-2024-klimaatrisicos-in-nederland-5359.pdf*

Rijksinstituut voor Volksgezondheid en Milieu (RIVM). (31 mei 2021). *Klimaatverandering leidt nu al tot meer sterfte door hitte.* Geraadpleegd op 09-11-2023. Beschikbaar via: *https://www.rivm.nl/nieuws/klimaatverandering-leidt-nu-al-tot-meer-sterfte-door-hitte*

Rijksoverheid (2024). *Afbouw gaswinning Groningen*. Geraadpleegd op 19-04-2024. Via: *https://www.rijksoverheid.nl/onderwerpen/gaswinning-in-groningen/afbouw-gaswinning-groningen*

Stamper, M. (8 juni 2023). 'Eilanders moeten anders gaan denken over klimaatverandering'. *Caribisch Netwerk*. Geraadpleegd op 06-03-2024, beschikbaar via: *https://caribischnetwerk.ntr.nl/2023/06/08/eilanders-moeten-anders-gaan-denken-over-klimaatverandering/*

United Nations. (18 juli 2023). *Health risks on the rise as heatwave initensifies across Europe: WMO*. Geraadpleegd op 09-11-2023, beschikbaar via: *https://news.un.org/en/story/2023/07/1138802*

A.2 Infectieziekten

Carter, S. et al., (30 oktober 2023). *The Convergence of Artificial Intelligence and the Life Sciences.* NTI bio. Beschikbaar via: *https://www.nti.org/wp-content/uploads/2023/10/NTIBIO_AI_Executive-Summary_FINAL.pdf*

Kaiser, J. (17 maart 2023). *Growing number of high-security pathogen labs around world raises concerns*. ScienceInsider. Beschikbaar via: *https://www.science.org/content/article/growing-number-high-security-pathogen-labs-around-world-raises-concerns*

NOS. (15 maart 2024). Vijf vragen over de dalende vaccinatiegraad. *NOS Nieuws*. Beschikbaar via: *https://nos.nl/artikel/2512871-vijf-vragen-over-de-dalende-vaccinatiegraad*

Rijksinstituut voor Volksgezondheid en Milieu (RIVM). *Infectieziekten*. Geraadpleegd op 14 maart 2024, beschikbaar via: *https://www.rivm.nl/klimaat-en-gezondheid/infectieziekten*

Rijksinstituut voor Volksgezondheid en Milieu. (29 juni 2023). *Vaccinatiegraad en jaarverslag Rijksvaccinatieprogramma Nederland 2022*. Beschikbaar via: *https://www.rivm.nl/bibliotheek/rapporten/2023-0031.pdf*

Rijksinstituut voor Volksgezondheid en Milieu. (20 december 2023). *Staat van infectieziekten in Nederland, 2022*. Beschikbaar via: *https://www.rivm.nl/bibliotheek/rapporten/2023-0396.pdf*

A.3 Zware ongevallen

Autoriteit Nucleaire Veiligheid en Stralingsbescherming (Autoriteit NVS). (26 maart 2023). *Veiligheid kerncentrales Oekraïne.* Beschikbaar via: *https://www.autoriteitnvs.nl/actueel/nieuws/2022/02/25/situatie-in-oekraine*

AVIV. (23 maart 2023). *Rapport toetsing realisatiecijfers vervoer gevaarlijke stoffen over het spoor aan de risicoplafonds Basisnet.* Gasunie. Waterstofnetwerk Nederland. Beschikbaar via: *https://www.gasunie.nl/projecten/waterstofnetwerk-nederland*

Gasunie. (30 mei 2024) *Waterstofnetwerk Nederland*. Via: *https://www.gasunie.nl/projecten/waterstofnetwerk-nederland*

Geelen, L.M.J. et al. (22 september 2023). *De bijdrage van Tata Steel Nederland aan de gezondheidsrisico's van omwonenden en de kwaliteit van hun leefomgeving.* doi: 10.21945/RIVM-2023-0171.

Porthos. *CO_2-reductie- door opslag onder de Noordzee.* Beschikbaar via: *https://www.porthosco2.nl/*

Rijksinstituut voor Volksgezondheid en Milieu (RIVM). (30 mei, 2024a). *RIVM houdt nucleaire situatie in Oekraïne in de gaten.* Beschikbaar via: *https://www.rivm.nl/straling-en-radioactiviteit/stralingsincidenten-en-kernongevallen/oekraine*

Rijksinstituut voor volksgezondheid en Milieu (RIVM). (30 mei 2024b). *Verkenning Chemours en Westerschelde*. Via: *https://www.rivm.nl/industrie/onderzoeken/verkenning-chemours-westerschelde*

A.4 Polarisatie, extremisme & terrorisme

Algemeen Dagblad (AD). (4 oktober 2022). *Vertrouwen boeren in overheid is helemaal weg: 'Ze weten niet waar ze over praten'*. Beschikbaar via: *https://www.ad.nl/binnenland/vertrouwen-boeren-in-overheid-is-helemaal-weg-ze-weten-niet-waar-ze-over-praten~a1196e8d/?referrer=https%3A%2F%2Fwww.google.com%2F*

Algemene Inlichtingen en Veiligheidsdienst (AIVD). (17 april 2023). *AIVD Jaarverslag 2022*. Beschikbaar via: *https://www.aivd.nl/documenten/jaarverslagen/2023/04/17/aivd-jaarverslag-2022*

Algemene Inlichtingen en Veiligheidsdienst (AIVD), Nationale politie & NCTV. (9 april 2024). *Met de rug naar de samenleving: Een analyse van de soevereinenbeweging*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2024/04/09/tk-bijlage-24401640-fenomeenanalyse-soevereinen*

Centraal Bureau voor de Statistiek (CBS). (9 mei 2023). *Minste vertrouwen in Tweede Kamer in 10 jaar tijd*. Beschikbaar via: *https://www.cbs.nl/nl-nl/nieuws/2023/19/minste-vertrouwen-in-tweede-kamer-in-10-jaar-tijd*

Commissariaat voor de Media. (14 juni 2023). *Digital News Report Nederland 2023*. Beschikbaar via: *https://www.cvdm.nl/wp-content/uploads/2023/06/CvdM-DigitalNewsReport-2023.pdf*

Macaskill, A., Holden, M., Marsh, S. (24 november 2023). Gaza war increases risk of Islamist attacks in Europe, security officials say. *Reuters*. Beschikbaar via: *https://www.reuters.com/world/europe/gaza-war-increases-risk-islamist-attacks-europe-security-officials-say-2023-11-24/*

Movisie.(November 2023). *Themadossier Israel-Palestina.* Beschikbaar via: *https://www.movisie.nl/artikel/israel-palestina-hoe-blijven-we-nederland-verbinding*

Mulder, J. (14 juni 2023). Jongere haalt nieuws steeds meer van sociale media zoals TikTok, maar vertrouwt die minder. *Trouw.* Beschikbaar via: *https://www.trouw.nl/binnenland/jongere-haalt-nieuws-steeds-meer-van-sociale-media-zoals-tiktok-maar-vertrouwt-die-minder~b3fc37ed/?referrer=https://www.google.com/*

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2023a). *Dreigingsbeeld Terrorisme Nederland December 2023*. Beschikbaar via: *https://www.nctv.nl/onderwerpen/dtn*

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2023b). *Dreigingsbeeld Terrorisme Nederland 58*. Beschikbaar via: *https://www.nctv.nl/documenten/publicaties/2023/05/30/dreigingsbeeld-terrorisme-nederland-58*

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (12 december 2023). *Dreigingsbeeld Terrorisme Nederland.* Beschikbaar via: *https://www.nctv.nl/onderwerpen/dtn*

Rijksinstituut voor Volksgezondheid en Milieu (RIVM). (26 september 2022). *Rijksbrede Risicoanalyse 2022*. Beschikbaar via: *https://www.nctv.nl/documenten/publicaties/2022/09/26/rijksbrede-risicoanalyse-nationale-veiligheid*

Reuters. (24 november 2023a). Gaza war increases risk of Islamist attacks in Europe, security officials Say. *Reuters*. Via: *https://www.reuters.com/world/europe/*

Reuters. (14 december 2023b) *Seven arrested in Germany, Denmark, the Netherlands over suspected terrorism plots.* Beschikbaar via: *https://www.reuters.com/world/europe/copenhagen-police-danish-intelligence-make-arrests-suspicion-preparations-attack-2023-12-14/*

A.5 Ongewenste inmenging en beïnvloeding democratische rechtsstaat

Adviesraad voor Wetenschap, Technologie en Innovatie (AWTI). (28 novemver 2022). *Advies: Kennis in conflict - veiligheid en vrijheid in balans.* Beschikbaar via: *https://www.awti.nl/documenten/adviezen/2022/11/29/index*

Algemene Inlichtingen en Veiligheidsdienst (AIVD). (2023). *AIVD Jaarverslag 2022*. Beschikbaar via: *https://www.aivd.nl/documenten/jaarverslagen/2023/04/17/aivd-jaarverslag-2022*

Algemene Inlichtingen en Veiligheidsdienst (AIVD). (2024a). *AIVD Jaarverslag 2023*. Beschikbaar via: *https://www.aivd.nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023*

Algemene Inlichtingen en Veiligheidsdienst (AIVD). (2024b). *Strafbaarstelling van moderne spionagevormen*. Via: *https://www.aivd.nl/onderwerpen/spionage/strafbaarstelling-van-moderne-spionagevormen*

Albertini, A. (7 november 2023). Etoiles de David taguées à Paris : la piste d'une opération d'ingérence russe privilégiée. *Le Monde*. Beschikbaar via: *https://www.lemonde.fr/societe/article/2023/11/07/pochoirs-d-etoiles-de-david-a-paris-la-piste-d-une-operation-d-ingerence-russe-privilegiee_6198775_3224.html*

Bischoff, K. (30 mei 2023). AI tools in hybrid warfare - A double-edged sword. *Risk Intelligence*. Beschikbaar via: *https://www.riskintelligence.eu/background-and-guides/ai-tools-in-hybrid-warfare-a-double-edged-sword*

Bolle, J. (18 februari 2024). In Den Haag botste de lange arm van het Eritrese regime met de vuist van de oppositie – en niet voor het eerst. *De Volkskrant*. Beschikbaar via: *https://www.volkskrant.nl/binnenland/in-den-haag-botste-de-lange-arm-van-het-eritrese-regime-met-de-vuist-van-de-oppositie-en-niet-voor-het-eerst~b110f345/*

Europese Commissie. (2023). *Critical Raw Materials Act*. Beschikbaar via: *https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/critical-raw-materials-act_en*

Europese Commissie. (2024). *EU Chips Act*. Beschikbaar via: *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en*

Houtkamp, C., Drost, N. (2023). *Oekraïense en Russische gemeenschappen in Nederland*. Instituut Clingendael. Via: *https://www.clingendael.org/sites/default/files/2023-05/Oekra%C3%AFense%20en%20Russische%20gemeenschappen%20in%20Nederland.pdf*

Kingston, T. (4 januari, 2024). European Navies try to Keep up in Cat-and-Mouse Game of Seabed Warfare. *Defense News*. Via: *https://www.defensenews.com/global/europe/2024/01/04/european-navies-try-to-keep-up-in-cat-and-mouse-game-of-seabed-warfare/*

Okano-Heijmans , M. (18 januari 2023). Ontkoppelen is niet de oplossing voor ons probleem met China. *Clingendael*. Beschikbaar via: *https://spectator.clingendael.org/nl/publicatie/ontkoppelen-niet-de-oplossing-voor-ons-probleem-met-china*

Martin, M. (12 maart 2024). Houthi attacks in Red Sea threaten internet infrastructure. *Deutsche Welle*. Beschikbaar via: *https://www.dw.com/en/houthi-attacks-in-red-sea-threaten-internet-infrastructure*

Militaire Inlichtingen en Veiligheidsdienst (MIVD). (19 april 2023). *MIVD Openbaar Jaarverslag 2022*. Beschikbaar via: *https://open.overheid.nl/documenten/ronl-fe92eb9796cac86ecf33c8fdd97167cd1543df8a/pdf*

Ministerie van Economische Zaken en Klimaat. (2023). *Wet veiligheidstoets op investeringen, fusies en overnames*. Via: *https://www.bureautoetsinginvesteringen.nl/het-stelsel-van-toetsen/wet-veiligheidstoets-investeringen-fusies-en-overnames*

NOS. (18 februari 2024). *Waarom voor- en tegenstanders van het Eritrese regime met elkaar botsen.* Via: *https://nos.nl/artikel/2509365-waarom-voor-en-tegenstanders-van-het-eritrese-regime-met-elkaar-botsen*

Ramdharie, S. (12 februari 2024). Europese landen waarschuwen voor grote Russische desinformatie-campagne. *De Volkskrant*. Beschikbaar via: *https://www.volkskrant.nl/nieuws-achtergrond/europese-landen-waarschuwen-voor-grote-russische-desinformatie-campagne~ba31a7f7/*

Rijksoverheid. (28 februari 2022). *Strafbaarstelling spionage gemoderniseerd*. Beschikbaar via: *https://www.rijksoverheid.nl/actueel/nieuws/2022/02/28/strafbaarstelling-spionage-Gemoderniseerd*

Scott, M. (10 maart 2022). As war in Ukraine evolves, so do disinformation tactics. *Politico*. Beschikbaar via: *https://www.politico.eu/article/ukraine-russia-disinformation-propaganda/*

A.6 Georganiseerde criminaliteit

Ministerie van Justitie en Veiligheid. (2023). *Voortgangsrapportage aanpak georganiseerde criminaliteit*.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (3 juli 2023). *Cybersecuritybeeld Nederland 2023*. Beschikbaar via: *https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023*

NOS. (22 maart 2024). Dit jaar al 250 vuurwerkaanslagen ondanks maatregelen. *NOS*. Beschikbaar via: *https://nos.nl/artikel/2513720-dit-jaar-al-250-vuurwerkaanslagen-ondanks-maatregelen*

Politie. (2023). *Mogelijke verdubbeling explosie-incidenten*. Beschikbaar via: *https://www.politie.nl/nieuws/2023/juli/16/mogelijke-verdubbeling-explosie-incidenten.html*

UK National Cyber Security Centre. (maart 2023). *ChatGPT and large language models: what's the risk?* Beschikbaar via: *https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk*

Van Nierop, L. (26 mei 2023). Als de oorlog in Oekraïne voorbij is, gaan de westerse wapens zwerven. *NRC*. Beschikbaar via: *https://www.nrc.nl/nieuws/2023/05/26/als-de-oorlog-in-oekraine-voorbij-is-gaan-de-westerse-wapens-zwerven-a4165707*

Wetenschappelijk Onderzoek- en Datacentrum (WODC). (28 december 2023). *Update liquidaties 2022*. Beschikbaar via: *https://repository.wodc.nl/handle/20.500.12832/3328*

Wetenschappelijk Onderzoek- en Datacentrum (WODC). (30 december 2021). *2e verkennende studie liquidaties*. Beschikbaar via: *https://repository.wodc.nl/handle/20.500.12832/3136*

A.7 Internationale en militaire dreigingen

Ishac Diwan, I., Alaya, H., Meddeb, H. (23 januari 2024). The Buildup to a Crisis: Current Tensions and Future Scenarios for Tunisia. *Malcolm H. Kerr Carnegie Middle East Centre.* Beschikbaar via: *https://carnegie-mec.org/2024/01/23/buildup-to-crisis-current-tensions-and-future-scenarios-for-tunisia-pub-91424*

Al Hussein, M. (16 januari 2024). *The Gaza War May Radicalize the Gulf*. Carnegie Endowment for International Peace. Via: *https://carnegieendowment.org/sada?lang=en*

Al Jazeera. (29 augustus 2023). Taiwan warns of surge in tensions as Chinese fighter jets cross median line. *Al Jazeera.* Beschikbaar via: *https://www.aljazeera.com/news/2023/8/29/taiwan-warns-of-surge-in-tensions-as-chinese-fighter-jets-cross-median-line*

Ayres, A. (21 juni 2023). India Is Not a U.S. Ally – and Has Never Wanted to Be. *Time Magazine*. Beschikbaar via: *https://time.com/6288459/india-ally-us-modi-biden-visit/*

Bugos, S. et al. (november 2023). Russia Withdraws Ratification of Nuclear Test Ban Treaty. *Arms Control Association*.

Diwan, I., Alaya, H., Meddeb, H. (23 januari 2024). *The Buildup to a Crisis: Current Tensions and Future Scenarios for Tunisia*. Malcolm H. Kerr Carnegie Middle East Centre. Via: *https://carnegieendowment.org/research/2024/02/the-buildup-to-a-crisis-current-tensions-and-future-scenarios-for-tunisia?lang=en&center=middle-east*

Dolzikova, D. (1 maart 2023). China's imports of Russian uranium spark fear of new arms race. *RUSI*. Beschikbaar via: *https://www.bloomberg.com/news/articles/2023-03-01/china-nuclear-trade-with-russia-risks-tipping-military-balance*

Europees Parlement. (21 november 2023). *European defence industry reinforcement through common procurement act (EDIRPA)*. Beschikbaar via: *https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739294*

Hirsh, M. (11 april 2023). How AI Will Revolutionize Warfare. *Foreign Policy*. Beschikbaar via: *https://foreignpolicy.com/2023/04/11/ai-arms-race-artificial-intelligence-chatgpt-military-technology/*

Instituut Clingendael. (2024). *Strategische Monitor 2023: Barsten en Blokken*. Via: *https://www.clingendael.org/publication/strategische-monitor-2023-barsten-en-blokken*

Kumagai, S. (juli 2023). India-Russia Economic Ties Are Strengthening Rapidly -Especially in Terms of Crude Oil Trade. *Japan Research Institute*.

Landgraf, W. et al. (18 januari 2024). "A frozen conflict boils over, Nagorno-Karabakh in 2023 and future implications", *Foreign Policy Research Institute.* Beschikbaar via: *https://www.fpri.org/article/2024/01/a-frozen-conflict-boils-over-nagorno-karabakh-in-2023-and-future-implications/*

Marcetic, B. (20 december 2023). In Gaza, the next generation of radicalization begins. *Responsible Statecraft*. Via: *https://responsiblestatecraft.org/israel-hamas-war-counterterrorism/*

Pincus, W. (21 maart 2023). The Hypersonic Arms Race is Heating Up. *The Cipher Brief*. Beschikbaar via: *https://www.thecipherbrief.com/column_article/the-hypersonic-arms-race-is-heating-up*

Reuters. (November 2023a). Recent coups in West and Central Africa. *Reuters.* Beschikbaar via: *https://www.reuters.com/world/africa/recent-coups-west-central-africa-2023-08-30/*

Reuters. (December 2023b). Iran undoes slowdown in enrichment of uranium to near weapons-grade -IAEA. *Reuters.* Via: *https://www.reuters.com/world/middle-east/iran-undoes-slowdown-enrichment-uranium-near-weapons-grade-iaea-2023-12-26/*

Reuters. (18 januari 2024). US urges discussions with China on practical nuclear risk reduction steps. *Reuters.* Beschikbaar via: *https://www.reuters.com/world/us-urges-discussions-with-china-practical-nuclear-risk-reduction-steps-2024-01-18/*

Wall, C., Wegge, N. (2023). *The Russian Arctic Threat: Consequences of the Ukraine War*. Centre for Strategic and International Studies. Via: *https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-01/230125_Wall_RussianArcticThreat_0.pdf*

Williams, H. (23 februari 2023). Russia Suspends New START and Increases Nuclear Risks. *Centre for Strategic and International Studies*. Beschikbaar via: *https://www.csis.org/analysis/russia-suspends-new-start-and-increases-nuclear-risks*

A.8 Economische dreigingen

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (23 april 2024). *AIVD-jaarverslag 2023*. Beschikbaar via: *https://www.aivd.nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023*

Autoriteit Financiële Markten (AFM). (2024). *Digital Operational Resilience Act (DORA)*. Beschikbaar via: *https://www.afm.nl/nl-nl/sector/themas/digitalisering/dora*

ASML. (8 maart 2023). *Statement regarding additional export controls*. Beschikbaar via: *https://www.asml.com/en/news/press-releases/2023/statement-regarding-additional-export-controls*

ASML. (1 januari 2024). *Statement regarding partial revocation export license*. Beschikbaar via: *https://www.asml.com/en/news/press-releases/2023/statement-regarding-partial-revocation-export-license*

De Nederlandsche Bank. (21 augustus 2023a). *FSC: "Nederlandse economie en financiële instellingen tonen zich weerbaar, maar risico's voor de financiële stabiliteit blijven hoog"*. Beschikbaar via: *https://www.dnb.nl/algemeen-nieuws/persbericht-2023/fsc-nederlandse-economie-en-financiele-instellingen-tonen-zich-weerbaar-maar-risico-s-voor-de-financiele-stabiliteit-blijven-hoog/*

De Nederlandsche Bank. (9 oktober 2023b). *Risico's voor financiële stabiliteit nemen toe door snel gestegen rentes*. Beschikbaar via: *https://www.dnb.nl/algemeen-nieuws/persbericht-2023/risico-s-voor-financiele-stabiliteit-nemen-toe-door-snel-gestegen-rentes/*

Europese Commissie. (2023). *Temporary Crisis an Transition Framework*. Beschikbaar via: *https://competition-policy.ec.europa.eu/state-aid/temporary-crisis-and-transition-framework_en*

Europese Commissie. (31 mie 2024). *Trade defence investigations*. Beschikbaar via: *https://tron.trade.ec.europa.eu/investigations/ongoing*

Evofenedex. (4 april 2023). *Veel minder nachtvluchten op Schiphol bedreiging voor luchtvracht*. Beschikbaar via: *https://www.evofenedex.nl/actualiteiten/veel-minder-nachtvluchten-op-schiphol-bedreiging-voor-luchtvracht*

ING. (19 oktober 2023). *Extreme weather is making major trade routes less reliable, and it's only going to get worse.* Beschikbaar via: *https://think.ing.com/articles/extreme-weather-makes-major-trade-routes-less-reliable/*

Jumelet, P. (1 november 2023). Capaciteit Panamakanaal wegens recorddroogte nog drastischer omlaag. *Nieuwsblad Transport*. Beschikbaar via: *https://www.nt.nl/scheepvaart/2023/11/01/capaciteit-panamakanaal-wegens-recorddroogte-nog-drastischer-omlaag/?gdpr=deny*

Koenis, C. (2023). Hoe de oorlog tussen Israël en Hamas ook de wereldeconomie raakt. *RTL Nieuws*. Beschikbaar via: *https://www.rtl.nl/economie/artikel/5415250/oorlog-israel-hamas-wereldeconomie-olie-gas-kunstmest?redirect=rtlnieuws*

Kompeer, J., Schellevis, J. (23 augustus 2023). 'Babyboomerbruggen' toe aan groot onderhoud, files en kosten verwacht. *NOS Nieuws*. Beschikbaar via: *https://nos.nl/artikel/2394865-babyboomerbruggen-toe-aan-groot-onderhoud-files-en-kosten-verwacht*

NOS. (19 april 2023a). Nieuwe aanwijzingen voor Russische sabotage op zeebodem. *NOS Nieuws*. Beschikbaar via: https://nos.nl/artikel/2471999-nieuwe-aanwijzingen-voor-russische-sabotage-op-zeebodem.NOS. (1 september 2023b). Ruzie over krimp Schiphol loopt hoog op, VS dreigt met sancties. *NOS Nieuws*. Beschikbaar via: *https://nos.nl/artikel/2488777-ruzie-over-krimp-schiphol-loopt-hoog-op-vs-dreigt-met-sancties*

Ministerie van Defensie. (18 april 2024). *Jaarverslag MIVD 2023*. Beschikbaar via: *https://www.defensie.nl/downloads/jaarverslagen/2024/04/18/jaarverslag-mivd-2023*

Ministerie van Defensie. (n.d.). *Militaire steun aan Oekraïne*. Beschikbaar via: *https://www.defensie.nl/onderwerpen/oostflank-navo-gebied/militaire-steun-aan-oekraine*

Ministerie van Financiën (2023). *Miljoenennota 2024 – 2.2.4 Oekraïne*. Beschikbaar via: *https://www.rijksfinancien.nl/miljoenennota/2024/2153111*

ProRail. (31 augustus 2023). *Meer spoorwerk overdag en doordeweeks*. Beschikbaar via: *https://www.prorail.nl/nieuws/meer-spoorwerk-overdag-en-doordeweeks*

Rooijers, E. (26 februari 2024). Wachtlijsten stroomnet staan vol met 'zombieaanvragen'. *Financieel Dagblad*. Beschikbaar via: *https://fd.nl/bedrijfsleven/1508521/wachtlijsten-stroomnet-staan-vol-met-zombieaanvragen*

Rijksoverheid. (25 juni 2021). *Nationale veiligheidstoets op investeringen, fusies en overnames*. Beschikbaar via: *https://www.rijksoverheid.nl/actueel/nieuws/2021/06/25/nationale-veiligheidstoets-op-investeringen-fusies-en-overnames*

Rijksoverheid. (22 juli 2022). *Nieuwe Europese richtlijn moet veiligheid verhogen*. Beschikbaar via: *https://www.rijksoverheid.nl/actueel/nieuws/2022/07/22/nieuwe-europese-richtlijn-moet-veiligheid-verhogen*

Rijksoverheid. (10 februari 2023a). *Nederland niet meer afhankelijk van energie uit Rusland*. Beschikbaar via: *https://www.rijksoverheid.nl/actueel/nieuws/2023/02/10/nederland-niet-meer-afhankelijk-van-energie-uit-rusland*

Rijksoverheid. (31 mei 2023b). *Kabinet versterkt economische weerbaarheid kennisintensief bedrijfsleven*. Beschikbaar via: *https://www.rijksoverheid.nl/actueel/nieuws/2023/05/31/kabinet-versterkt-economische-weerbaarheid-kennisintensief-bedrijfsleven*

Rijksoverheid (n.d.-a). *Nederlands hulp voor Oekraïne*. Beschikbaar via: *https://www.rijksoverheid.nl/onderwerpen/oorlog-in-oekraine/nederlandse-hulp-voor-oekraine*

Rijksoverheid (2024). *Aanpak stikstofuitstoot verminderen*. Beschikbaar via: *https://www.rijksoverheid.nl/onderwerpen/aanpak-stikstof-natuur-water-en-klimaat/aanpak-stikstofuitstoot-verminderen*

Van der Boon, V., Gras, A. (2 april 2024). Tientallen bedrijven krijgen al geen drinkwater, nieuwbouwwijken volgen. *Financieel Dagblad*. Beschikbaar via: *https://fd.nl/economie/1512002/tientallen-bedrijven-krijgen-al-geen-drinkwater-nieuwbouwwijken-volgen*

Van der Boon, V., Kakebeeke, P., Sie, P. (24 april 2024). Vooral in Zuid- en Oost-Nederland gaan klappen vallen door de mestcrisis. *Financieel Dagblad*. Beschikbaar via: *https://fd.nl/politiek/1514612/vooral-in-zuid-en-oost-nederland-gaan-klappen-vallen-door-de-mestcrisis*

Van der Maas, R. (6 februari 2023). Personeelstekort speelt wegvervoer ook in 2023 parten. *Nieuwsblad Transport*. Beschikbaar via: *https://www.nt.nl/wegvervoer/2023/02/06/personeelstekort-speelt-wegvervoer-ook-in-2023-parten/?gdpr=accept*

Vestergaard, R. (3 december 2023). Nieuwe bedrijfsaansluiting op riool niet langer zeker. *Financieel Dagblad*. Beschikbaar via: *https://fd.nl/bedrijfsleven/1498179/nieuwe-bedrijfsaansluiting-op-riool-niet-langer-zeker*

A.9 Cyberdreigingen

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (4 april 2023). *Het PQC-migratie handboek*. Beschikbaar via: *https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-handboek*

Cary, D., Del Rosso, K. (6 september 2023). Sleight of hand: How China weaponizes software vulnerabilities. *Atlantic Council*. Beschikbaar via: *https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/*

Cyber Risk. (2024). The European Cyber Resilience Act (CRA). Via: *https://european-cyber-resilience-act.com/*

ENISA. (11 november 2022). *Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!*. Beschikbaar via: *https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030*

ENISA. (19 oktober 2023). *ENISA Threat Landscape 2023*. Beschikbaar via: *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023*

European Space Agency. (7 februari, 2024). How ESA ensures cybersecurity in space. Via: *https://www.esa.int/About_Us/Cyber_resilience_at_ESA/How_ESA_ensures_cybersecurity_in_space*

European Parliament. (9 december 2023). *Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI*. Beschikbaar via: *https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai*

Galle, A. (januari 2022). Drinking from the Fetid Well: Data Poisoning and Machine Learning. *U.S. Naval Institute (USNI)*. Beschikbaar via: *https://www.usni.org/magazines/proceedings/2022/january/drinking-fetid-well-data-poisoning-and-machine-learning*

Hofmans, T. (31 januari 2024). SIDN wil domeinregistratiesysteem naar AWS verplaatsen. *Tweakers*. Beschikbaar via: *https://tweakers.net/nieuws/218152/sidn-wil-domeinregistratiesysteem-naar-aws-verplaatsen.html*

iBestuur. (21 november 2023). Privacyzorgen rond eIDAS-wetgeving van de baan. *iBestuur* Beschikbaar via: *https://ibestuur.nl/artikel/privacyzorgen-rond-eidas-wetgeving-van-de-baan/*

Janjeva, A., Harris, A., Mercer, S., Kasprzyk, A., Gausen, A. (december 2023). *The rapid rise of Generative AI. Centre for Emerging Technology and Security (CETAS)*. Beschikbaar via: *https://cetas.turing.ac.uk/publications/rapid-rise-generative-ai*

Kaczmarek, S. (5 februari 2024). *We Need Cybersecurity in Space to Protect Satellites*. Scientific American. Via: *https://www.scientificamerican.com/article/we-need-cybersecurity-in-space-to-protect-satellites/*

Krasodomski, A., Buschser, M. (14 maart 2024). *The EU's new AI Act could have global impact*. Chatham House. Via: *https://www.chathamhouse.org/2024/03/eus-new-ai-act-could-have-global-impact*

Lohn., A., Knack, A., Burke, A., Jackson, K. (2023). *Autonomous Cyber Defense: A Roadmap from Lab to Ops*. CSET & CETAS. Via: *https://cset.georgetown.edu/wp-content/uploads/Autonomous-Cyber-Defense-1.pdf*

Manky, D. (23 maart 2023). The Latest Intel on Wipers. *FortiGuard Labs*. Beschikbaar via: *https://www.fortinet.com/blog/threat-research/intel-on-wiper-malware*

Ministerie van Defensie. (18 april 2024). *Jaarverslag MIVD 2023*. Beschikbaar via: *https://www.defensie.nl/downloads/jaarverslagen/2024/04/18/jaarverslag-mivd-2023*

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (4 juli 2022). *Cybersecuritybeeld Nederland 2022*. Beschikbaar via: *https://www.nctv.nl/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022*

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (3 juli 2022b). *Cybersecuritybeeld Nederland 2022*. Beschikbaar via: *https://www.nctv.nl/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022*

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (3 juli 2023). *Cybersecuritybeeld Nederland 2023*. Beschikbaar via: *https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023*

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (9 februari 2024). *Ministry of Defence of the Netherlands uncovers COATHANGER,a stealthy Chinese FortiGate RAT*. Beschikbaar via: *https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf*

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (9 februari 2024). *Ministry of Defence of the Netherlands uncovers COATHANGER,a stealthy Chinese FortiGate RAT*. Beschikbaar via: *https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf*

Nationaal Cyber Security Centrum (NCSC). (21 februari 2023). *Vier cybersecuritylessen uit één jaar oorlog in Oekraïne*. Beschikbaar via: *https://www.ncsc.nl/documenten/publicaties/2023/februari/21/vier-cybersecuritylessen-uit-een-jaar-oorlog-in-oekraine*

Nationaal Cyber Security Centrum. (2024). DDos – Wat kun je zelf doen?. Via: *https://www.ncsc.nl/wat-kun-je-zelf-doen/dreiging/ddos*

National Cyber Security Center (NCSC). (24 januari 2024). *The near-term impact of AI on the cyber threat*. Beschikbaar via: *https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat*

National Institute of standards and Technology (NIST). (2024). *Cybersecurity for the Space Domain*. Via: *https://www.nccoe.nist.gov/cybersecurity-space-domain*

NOS. (17 april 2024). BabyTV opnieuw gehackt: allerkleinsten kijken kwartier naar Russische propaganda. *NOS*. Via: *https://nos.nl/artikel/2517151-babytv-opnieuw-gehackt-allerkleinsten-kijken-kwartier-naar-russische-propaganda*

Portbase. (1 oktober 2018). *Portbase is met cloudgang klaar voor de toekomst.* Beschikbaar via: *https://www.portbase.com/portbase-is-met-cloudgang-klaar-voor-de-toekomst/*

Rijksoverheid. (17 oktober 2023). *Agenda Digitale Open Strategische Autonomie*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa*

Schellevis, J. (1 februari 2024). Onrust over gedeeltelijke verhuizing .nl-domeinen naar het Amerikaanse Amazon. *NOS Nieuws*. Beschikbaar via: *https://nos.nl/artikel/2507035-onrust-over-gedeeltelijke-verhuizing-nl-domeinen-naar-het-amerikaanse-amazon*

The U.S. Cybersecurity and Infrastructure Security Agency (CISA). (2024). PRC *State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Via: *https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf*

Van Sant, S., Goujard, C. (23 november 2022). *European Parliament website hit by cyberattack after Russian terrorism vote*. *POLITICO*. Beschikbaar via: *https://www.politico.eu/article/cyber-attack-european-parliament-website-after-russian-terrorism/#:~:text=The%20attack%20on%20the%20European,with%20links%20to%20Russia%20indeed*

Vincent, J. (2 november 2017). Google's AI thinks this turtle looks like a gun, which is a problem. *The Verge*. Beschikbaar via: *https://www.theverge.com/2017/11/2/16597276/google-ai-image-attacks-adversarial-turtle-rifle-3d-printed*

A.10 Bedreiging vitale infrastructuur

Algemene Inlichtingen en Veiligheidsdienst (AIVD). (17 april 2023). *AIVD Jaarverslag 2022*. Beschikbaar via: *https://www.aivd.nl/documenten/jaarverslagen/*

Algemene Inlichtingen en Veiligheidsdienst (AIVD). (2024a). *AIVD Jaarverslag 2023*. Beschikbaar via: *https://www.aivd.nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023*

Analistennetwerk Nationale Veiligheid (ANV). (26 september 2022). *Themarapportage Bedreiging Vitale Infrastructuur*. Beschikbaar via: *https://www.nctv.nl/documenten/publicaties/2022/09/26/themarapportage-bedreiging-vitale-infrastructuur-2022*

Argyroudis, S. A., Mitoulis, S. A., Hofer, L., Zanini, M. A., Tubaldi, E., & Frangopol, D. M. (2020). Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. *Science of the Total Environment.* Beschikbaar via: *https://doi.org/10.1016/j.scitotenv.2020.136854*

Europees Parlement. (20 juli 2023). *Future Shocks 2023: Anticipating and weathering the next storms.* Beschikbaar via: *https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2023)751428*

Gasunie. (juli 2023). *Halfjaarbericht 2023*. Beschikbaar via: *https://www.publicatiesgasunie.nl/halfjaarbericht-2023*

Geudens, P., Kramer, O. Drinkwaterstatistieken 2022. *Vewin.* Beschikbaar via: *https://www.vewin.nl/SiteCollectionDocuments/Publicaties/Cijfers/Vewin-Drinkwaterstatistieken-2022-NL-WEB.pdf*

Huizinga, L. (19 december 2022). The Far-Right's Fascination with the U.S. Electric Grid. *UNICORN RIOT.* Beschikbaar via: *https://unicornriot.ninja/2022/the-far-right-fascination-with-the-electric-grid/*

Inspectie Leefomgeving en Transport. (2024). *Drinkwater steeds schaarser: provincie neem verantwoordelijkheid*. Via: *https://www.ilent.nl/documenten/leefomgeving-en-wonen/drinkwater/drinkwater/signaalrapportages/*

Ministerie van Defensie. (2023). *Roadmap energietransitie operationeel materieel*. Via: *https://www.defensie.nl/downloads/publicaties/2023/01/31/roadmap-energietransitie-materieel*

Ministry of Defense – Government Offices of Sweden. (19 oktober 2023). *Damaged telecommunications cable between Sweden and Estonia*. Beschikbaar via: *https://www.government.se/articles/2023/10/damaged-telecommunications-cable-between-sweden-and-estonia/*

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTVa). *Wat zijn de CER- en NIS2-richtlijnen?*. Beschikbaar via: *https://www.nctv.nl/onderwerpen/cer--en-nis2-richtlijnen/wat-zijn-de-cer-en-nis2-richtlijnen*

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTVb). *CER- en NIS2-richtlijnen?*. Beschikbaar via: *https://www.nctv.nl/onderwerpen/cer--en-nis2-richtlijnen 161*

NOS. (9 november 2022). Bonaire kampt met hevige regenval, straten overstroomd. *NSO Nieuws.* Beschikbaar via: *https://nos.nl/artikel/2451698-bonaire-kampt-met-hevige-regenval-straten-overstroomd*

NOS. (19 juli 2023a). Vier doden in Kroatië en Slovenië door noodweer. *NOS Nieuws.* Beschikbaar via: *https://nos.nl/artikel/2483455-vier-doden-in-kroatie-en-slovenie-door-noodweer*

NOS. (13 november 2023b). Tienduizenden getroffen door aanhoudende overstromingen Noord-Frankrijk . *NOS Nieuws.* Beschikbaar via: *https://nos.nl/artikel/2497714-tienduizenden-getroffen-door-aanhoudende-overstromingen-noord-frankrijk*

NOS. (12 maart 2024). Tesla-fabriek bij Berlijn weer aangesloten op stroomnet na brandstichting. *NOS Nieuws*. Beschikbaar via: *https://nos.nl/artikel/2512432-tesla-fabriek-bij-berlijn-weer-aangesloten-op-stroomnet-na-brandstichting*

PBL (2024), *Klimaatrisico's in Nederland*; De huidige stand van zaken. Den Haag: Planbureau voor de Leefomgeving. Beschikbaar via: *https://www.pbl.nl/system/files/document/2024-05/pbl-2024-klimaatrisicos-in-nederland-5359.pdf*

Price, J. (1 december 2023). A year after the Moore County power grid attacks, questions and challenges remain. *WUNC*. Beschikbaar via: *https://www.wunc.org/news/2023-12-01/a-year-after-the-moore-county-power-grid-attacks-questions-and-challenges-remain*

Rijksinspectie Digitale Infrastructuur (RDI). (2023). *Toekomstverkenning: de Trendradar*. Beschikbaar via: *https://www.rdi.nl/onderwerpen/onderzoek-en ontwikkelingen/trendradar*

Rijksoverheid. (11 juni 2018). *Structuurvisie Ondergrond*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2018/06/11/structuurvisie-ondergrond*

Rijksoverheid. (21 november 2022). *Eindrapport IKUS-II Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2023/03/07/bijlage-2-rapport-ikus-ii-november-2022-inventarisatie-kwetsbaarheden-uitval-satellietnavigatie.pdf* (overheid.nl)

Rijksoverheid. (2023a). *Kabinet zet in op energieopslag*. Via: *https://www.rijksoverheid.nl/actueel/nieuws/2023/06/07/kabinet-zet-in-op-energieopslag*

Rijksoverheid. (1 december 2023b). *Nationaal Plan Energiesysteem*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2023/12/01/nationaal-plan-energiesysteem*

Rijksoverheid. (2024). *Probleemanalyse Congestie in het laagspanningsnet*. Via: *https://www.rijksoverheid.nl/documenten/rapporten/2024/01/22/bijlage-2-probleemanalyse-congestie-in-het-laagspanningsnet*

TenneT. (14 maart 2023). *Integrated Annual Report 2022*. Beschikbaar via: *https://tennet-drupal.s3.eu-central-1.amazonaws.com/default/2023-11/TenneT_IAR_2022.pdf*

Tennet. (2024). Flexibel elektriciteitsverbruik. Via: *https://www.tennet.eu/nl/flexibel-elektriciteitsverbruik*

TNO. (20 maart 2023). *Transport gevaarlijke stoffen vraagt nu om nieuw veiligheidsbeleid*. Beschikbaar via: *https://www.tno.nl/nl/newsroom/2023/03/transport-gevaarlijke-stoffen/#:~:text=Het%20transport%20van%20gevaarlijke%20stoffen,op%20welke%20plek%20als%20eerste*

Van Leerdam, R., Rook, J., Riemer, L., Van der Aa, N. (3 april 2023). *Waterbeschikbaarheid voor de bereiding van drinkwater tot 2030 - knelpunten en oplossingsrichtingen*. RIVM. Beschikbaar via: *https://www.rivm.nl/publicaties/waterbeschikbaarheid-voor-bereiding-van-drinkwater-tot-2030*

Vuilleumier, P., Kerkdijk, R. (20 maart 2023). Telco security Landscape 2023. *ETIS*. Beschikbaar via: *https://www.etis.org/sites/default/files/content-files/ETIS-Papers/telco_sec_landscape_2023_published.pdf*

Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*. Beschikbaar via: *https://doi.org/10.1016/j.pdisas.2022.100244*

Onderdeel B Technologieverkenning

Analistennetwerk Nationale Veiligheid. (27 januari 2020). AI in de context van Nationale Veiligheid. *TNO*. Beschikbaar via: *https://www.rivm.nl/nationale-veiligheid*

Bronkhorst, A. et al. (2020). *Defensie technologie verkenning 2020*. *TNO*.

Commissie Genetische Modificatie (COGEM), Gezondheidsraad, *Trendanalyse biotechnologie 2023*. *Tijd voor een integrale visie* (Bilthoven: maart 2023), 3.

Reding, D. et al. (maart 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization*. Beschikbaar via: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Rijksoverheid. (2023b). *Besluit toepassingsbereik sensitieve technologie*. Via: *https://wetten.overheid.nl/BWBR0048201/2023-06-01*

Rijksoverheid. (19 januari 2024). *Nationale Technologie Strategie*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie*

Photondelta. (13 februari 2024). *Annual Review 2023*. Beschikbaar via: *https://www.photondelta.com/downloads/*

US Department of Defence. (2020). *Joint Publication 3-14 Space Operations*. Via: *https://irp.fas.org/doddir/dod/jp3_14.pdf*

Van Bree, T. et al. (maart 2023). Herijking Sleutel-technologieën 2023. *TNO/NWO*. Beschikbaar via: *https://www.tno.nl/nl/newsroom/2023/04/nieuwe-lijst-44-sleuteltechnologieen/*

B.1 Artificial Intelligence

Algemene Inlichtingen en Veiligheidsdienst (AIVD). (2024). *AIVD Jaarverslag 2023*. Beschikbaar via: *https://www.aivd.nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023*

Analistennetwerk Nationale Veiligheid. (27 januari 2020). AI in de context van Nationale Veiligheid. *TNO*. Beschikbaar via: *https://www.rivm.nl/nationale-veiligheid*

Galle, A. (januari 2022). Drinking from the Fetid Well: Data Poisoning and Machine Learning. *U.S. Naval Institute (USNI)*. Beschikbaar via: *https://www.usni.org/magazines/proceedings/2022/january/drinking-fetid-well-data-poisoning-and-machine-learning*

Gonzalez, S., Kant, M., Miikkulainen, R. (2024). Evolving GAN formulations for higher-quality image synthesis. *Artificial Intelligence in the Age of Neural Networks and Brain Computing*. Beschikbaar via: *https://www.sciencedirect.com/science/article/abs/pii/B9780323961042000142*

Hazell, J. (2023). Spear Phishing With Large Language Models *[2305.06972] arXiv*. Beschikbaar via: *https://doi.org/10.48550/arXiv.2305.06972*

Heijnen, M., Schoonderwoerd, T., Neerincx, M., van der Waa, J., Kester, L., van Diggelen, J., Elands., P. (2024). "*A Socio-Technical Feedback Loop for Responsible Military AI Life-Cycles from Governance to Operation*," DOI: 10.1201/9781003410379-3

Janjeva, A., Harris, A., Mercer, S., Kasprzyk, A., Gausen, A. (december 2023). The rapid rise of Generative AI. *Centre for Emerging Technology and Security (CETAS)*. Beschikbaar via: *https://cetas.turing.ac.uk/publications/rapid-rise-generative-ai*

Nurkin, T., Konaev, M. (25 mei 2022). Eye-to-Eye-in-AI. *Atlantic Council*. Beschikbaar via: *https://www.atlanticcouncil.org/in-depth-research-reports/report/eye-to-eye-in-ai/*

Reding, D. et al. (maart 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization*. Beschikbaar via: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Rijksoverheid. (21 november 2022). *Eindrapport IKUS-II Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2023/03/07/bijlage-2-rapport-ikus-ii-november-2022-inventarisatie-kwetsbaarheden-uitval-satellietnavigatie.pdf (overheid.nl)*

Rijksoverheid. (2023a). Defensie Strategie Data Science en AI 2023-2027. Via: *https://www.rijksoverheid.nl/documenten/rapporten/2023/05/31/defensie-strategie-data-science-en-artificiele-intelligentie-2023-2027*

Rijksoverheid. (17 oktober 2023b). *Agenda Digitale Open Strategische Autonomie*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa*

Rijksoverheid. (19 januari 2024). *Nationale Technologie Strategie*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie*

Taddeo, M., Ziosi, M., Tsamados, A., Gilli, L., Kurapati, S. (september 2022). AI for National Security: the Predictability Problem. *Centre for Emerging Technology and Security (CETAS)*. Beschikbaar via: *https://cetas.turing.ac.uk/publications/artificial-intelligence-national-security-predictability-problem*

Van Bree, T. et al. (maart 2023). Herijking Sleutel-technologieën 2023. *TNO/NWO*. Beschikbaar via: *https://www.tno.nl/nl/newsroom/2023/04/nieuwe-lijst-44-sleuteltechnologieen/*

B.2 Ruimtetechnologie

Ben-Itzhak, S. (11 januari 2022). Companies are commercializing outer space. Do government programs still matter?. *The Washington Post*. Beschikbaar via: *https://www.washingtonpost.com/politics/2022/01/11/companies-are-commercializing-outer-space-do-government-programs-still-matter/*

Bronkhorst, A. et al. (2020). Defensie technologie verkenning 2020. *TNO*.

Defense Advanced Research Projects Agency. (17 februari 2024). *DARPA Launch Challenge (Archived)*. Beschikbaar via: *https://www.darpa.mil/news-events/darpa-launch-challenge*

ENISA. (11 november 2022). *Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!*. Beschikbaar via: *https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030*

Centre of Excellene. (21 november 2022). *Eindrapport IKUS-II*. Beschikbaar via: *https://open.overheid.nl/documenten/ronl-e7e61227b3dd72448fb767b7d0ed1c779552d421/pdf*

Goguichvli, S., Linenberger, A., & Gillette, A. (1 oktober 2021). The Global Legal Landscape of Space: Who Writes the Rules on the Final Frontier. *Wilson Center*. Beschikbaar via: *https://www.wilsoncenter.org/article/global-legal-landscape-space-who-writes-rules-final-frontier*

Lillis, K. (17 februar1 2024). *Exclusive: Russia attempting to develop nuclear space weapon to destroy satellites with massive energy wave, sources familiar with intel say*. CNN. Via: *https://edition.cnn.com/2024/02/16/politics/russia-nuclear-space-weapon-intelligence/index.html*

Miller, C., Scott, M., Bender, B. (9 juni 2022). UkraineX: How Elon Musk's space satellites changed the war on the ground. *POLITICO*. Beschikbaar via: *https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039*

NAVO. (2024) *NATO's Approach to Space*. Beschikbaar via: *https://www.act.nato.int/our-work/network-community/natos-approach-to-space/*

Netherlands Space Office (NSO). (20 oktober 2022). *NSO Advies voor het ruimtevaartbeleid 2023-2025*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2022/10/20/nso-advies-voor-het-ruimtevaartbeleid-2023-2025*

OECD. (15 september 2022). *Earth's Orbits at Risk: The Economics of Space Sustainability*. Beschikbaar via: *https://www.oecd-ilibrary.org/science-and-technology/earth-s-orbits-at-risk_16543990-en*

Projectteam Statelijke Dreigingen. (9 november 2021). Eindrapport state-of-the-art onderzoek

Statelijke Dreigingen. *Ministerie van Defensie*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2021/11/09/tk-bijlage-wodc-rapport-state-of-the-art-statelijke-dreigingen-fase-1*

Reding, D. et al. (maart 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization.* Beschikbaar via: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Secure World Foundation. (2024). *Global Counterspace Capabilities Report*. Via: *https://swfound.org/counterspace/*

Starling, C. (15 februari 2024). *Russian nuclear anti-satellite weapons would require a firm US response, not hysteria*. Atlantic Council. Via: *https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-nuclear-anti-satellite-weapons-would-require-a-firm-us-response-not-hysteria/*

UK Office of the Chief Scientific Adviser for National Security, Government Communications Headquarters (GCHQ), National Crime Agency. *Joint Emerging Technology Trends: JETT Report 2022.*

US Department of Defence. (2020). Joint Publication 3-14 Space Operations. Via: *https://irp.fas.org/doddir/dod/jp3_14.pdf*

Wall, M. (14 juli 2022). Kessler Syndrome and the space debris problem. *Space.* Beschikbaar via: *https://www.space.com/kessler-syndrome-space-debris*

Wayenburg, B. (15 februari 2024). *Wat zou dat betekenen, een kernwapen in de ruimte?* NRC. Via: *https://www.nrc.nl/nieuws/2024/02/15/een-kernwapen-in-de-ruimte*

You, G. H. (19 mei 2022). Outer Space Security & Governance. *Foreign Policy.* Beschikbaar via: *https://foreignpolicy.com/2022/05/19/outer-space-security-international-governance/*

B.3 Quantumtechnologie

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (23 september 2021). *Bereid je voor op de dreiging van quantum computers.* Beschikbaar via: *https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers*

Bronkhorst, A. et al. (2020). Defensie technologie verkenning 2020. *TNO*.

Europese Commissie. (20 juni 2023a). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL* ON "EUROPEAN ECONOMIC SECURITY STRATEGY. Beschikbaar via: *eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020*

Europese Commissie. (3 oktober 2023b). *Recommendation on critical technology areas*. Beschikbaar via: *https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4735*

Europese Commissie. (2024). *White Paper on Export Controls*. Via: *https://policy.trade.ec.europa.eu/news/commission-publishes-new-guidelines-annual-report-dual-use-export-controls-2024-01-25_en*

Haeck, P. (27 februari 2024). *Europe is ring-fencing the next critical tech: Quantum*. Politico. Via: *https://www.politico.eu/article/how-europe-ring-fencing-quantum-computing-technology-defense/*

Krelina, M. (6 november 2021). Quantum technology for military applications. *EPJ Quantum Technology.* Beschikbaar via: *https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-021-00113-y#citeas*

Lele, A. (2021). Quantum Technologies and Military Strategy. *Springer.* Beschikbaar via: *https://doi.org/10.1007/978-3-030-72721-5*

Ministerio de Industria, Comercio y Turismo. (2023). *Disposición 12785 del BOE núm. 129 de 2023*. Via: *https://www.boe.es/boe/dias/2023/05/31/pdfs/BOE-A-2023-12785.pdf*

Neumann, N., Van Heesch, M., Philipson, F., Smallegange, A. (2021). Quantum Computing for Military y Applications. *2021 International Conference on Military Communication and Information Systems (ICMCIS).* Beschikbaar via: *https://ieeexplore.ieee.org/document/9486419*

Reding, D. et al. (maart 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization.* Beschikbaar via: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

TNO, CWI, Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (december 2023). *Het PQC-migratie handboek, richtlijnen voor het migreren naar post-quantumcryptografie*. Beschikbaar via: *https://www.tno.nl/nl/newsroom/2023/04/pqc-migratie-handboek/*

Van Bree, T. et al. (maart 2023). Herijking Sleuteltechnologieën 2023. *TNO/NWO*. Beschikbaar via: *https://www.tno.nl/nl/newsroom/2023/04/nieuwe-lijst-44-sleuteltechnologieen/*

B.4 Robotica en Autonome systemen

Bronkhorst, A. et al. (2020). Defensie technologie verkenning 2020. *TNO*.

Detsch, J. (30 maart 2021). The U.S. Army Is Using the Nagorno-Karabakh Conflict to Study Drone Warfare. *Foreign Policy.* Beschikbaar via: *https://foreignpolicy.com/2021/03/30/army-pentagon-nagorno-karabakh-drones/*

Elands, P., Heijnen, M. & Werkhoven, P. 2023. Operationalization of meaningful human control for military AI. TNO.

Pettyjohn, S. (8 februari 2024). Evolution Not Revolution: Drone Warfare in Russia's 2022 Invasion of Ukraine. *CNAS.* Beschikbaar via: *https://www.cnas.org/publications/reports/evolution-not-revolution*

Pol, A., Zwijnenburg, W. (oktober 2022). A Laboratory of Drone Warfare. *PAX.* Beschikbaar via: *https://paxforpeace.nl/wp-content/uploads/sites/2/import/2022-11/PAX_Syria_A%20Laboratory%20of%20Drone%20Warfare_2022.pdf*

Rathenau Instituut. (4 januari 2021). *Killer robots. Waarom internationale afspraken nodig zijn*. Beschikbaar via: *https://www.rathenau.nl/nl/digitalisering/killer-robots-waarom-internationale-afspraken-nodig-zijn*

Reding, D. et al. (maart 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization.* Beschikbaar via: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Rijksoverheid. (17 oktober 2023). *Agenda Digitale Open Strategische Autonomie*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa*

Vos, L. (2023). The use of technology and its implications in the Ukraine war. *TNO*.

Williams, D., Al-Mughrabi, N. (23 oktober 2023). Israel carries out limited raids in Gaza, Hamas launches drones. *Reuters.* Beschikbaar via: *https://www.reuters.com/world/middle-east/israel-mounts-limited-gaza-ground-raids-puts-hostage-number-222-2023-10-23/*

B.5 Fotonicatechnologie

Optics.org. (23 januari 2024). *Military laser DragonFire achieves first successful test firing*. Beschikbaar via: *https://optics.org/news/15/1/30#:~:text=During%20a%20trial%20at%20the,a%20weapon%20against%20aerial%20targets*

Ministerie van Defensie. (2023). *Roadmap energietransitie operationeel materieel*. Via: *https://www.defensie.nl/downloads/publicaties/2023/01/31/roadmap-energietransitie-materieel*

Parlementaire Monitor. (17 juli 2018). *Nationale Agenda Fotonica (bijlage bij 33009,nr.64).* Beschikbaar via: *https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkq4lwat43ym* Parlementaire monitor

Photondelta. (13 februari 2024). *Annual Review 2023.* Beschikbaar via: *https://www.photondelta.com/downloads/*

PhotonicsNL. (2022). *Photonics roadmap*. Via: *https://photonicsnl.com/*

Reding, D. et al. (maart 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization.* Beschikbaar via: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Rijksoverheid. (2023a). *Besluit toepassingsbereik sensitieve technologie*. Via: *https://wetten.overheid.nl/BWBR0048201/2023-06-01*

Rijksoverheid. (17 oktober 2023b). *Agenda Digitale Open Strategische Autonomie*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa*

Rijksoverheid. (19 januari 2024). Nationale Technologie Strategie. Beschikbaar via: https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie

Van Bree, T. et al. (maart 2023). Herijking Sleutel-technologieën 2023. *TNO/NWO*. Beschikbaar via: *https://www.tno.nl/nl/newsroom/2023/04/nieuwe-lijst-44-sleuteltechnologieen/*

B.6 Energietechnologie

Bronkhorst, A. et al. (2020). Defensie technologie verkenning 2020. *TNO*.

Commissie Genetische Modificatie (COGEM), Gezondheidsraad. (2023). Trendanalyse biotechnologie 2023, Tijd voor een integrale visie. *COGEM*. Beschikbaar via: *https://open.overheid.nl/documenten/ronl-0cc88c42d7d145c61dfe8a7ed66f9e71db88b021/pdf*

Europese Unie. *Strategic Energy Technology Plan.* Beschikbaar via: *https://energy.ec.europa.eu/topics/research-and-technology/strategic-energy-technology-plan_en#related-links*

Europese Commissie. (16 maart 2023). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) 168/2013, (EU) 2018/858, 2018/1724 and (EU) 2019/1020*. Beschikbaar via: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0160*

Pommeret, A., Ricci, F., Schubert, K. (2022). Critical raw materials for the energy transition. *European Economic Review*, 141. Doi: *https://doi.org/10.1016/j.euroecorev.2021.103991*

Reding, D. et al. (maart 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization.* Beschikbaar via: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Rijksoverheid. (1 december 2023a). *Nationaal Plan Energiesysteem.* Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2023/12/01/nationaal-plan-energiesysteem*

Rijksoverheid. (17 oktober 2023b). *Agenda Digitale Open Strategische Autonomie*. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa*

Rijksoverheid. (19 januari 2024). Nationale Technologie Strategie. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie*

TenneT. (14 maart 2023). *Integrated Annual Report 2022.* Beschikbaar via: *https://tennet-drupal.s3.eu-central-1.amazonaws.com/default/2023-11/TenneT_IAR_2022.pdf*

TNO. (31 mei 2024). *Nieuwe ontwikkeling in recycling windturbinebladen*. Via: *https://www.tno.nl/nl/duurzaam/hernieuwbare-elektriciteit/windparken-zee/duurzaam-ontwerp-windturbines-circulair/recycling-windturbinebladen/*

B.7 Biotechnologie

Alder, S. (2 november 2023). Why Do Criminals Target Medical Records? The HIPAA Journal. Via: *https://www.hipaajournal.com/why-do-criminals-target-medical-records/*

Commissie Genetische Modificatie (COGEM), Gezondheidsraad. (2023). Trendanalyse biotechnologie 2023, Tijd voor een integrale visie. *COGEM*. Beschikbaar via: *https://open.overheid.nl/documenten/ronl-0cc88c42d7d145c61dfe8a7ed66f9e71db88b021/pdf*

Guarino, B. (30 januari 2024). Elon Musk's Neuralink Has Implanted Its First Chip in a Human Brain. What's Next?. *Scientific American.* Beschikbaar via: *https://www.scientificamerican.com/article/elon-musks-neuralink-has-implanted-its-first-chip-in-a-human-brain-whats-next/*

Kuntz, K. (1 mei 2024). Biotech Matters: Problems with Life Science Databases in the United States. CNAS. Via: *https://www.cnas.org/publications/reports/biotech-matters-problems-with-life-science-databases-in-the-united-states*

Luca, J. (15 oktober 2023). DNA Hacking: How Hackers Can Access and Manipulate Your Genetic Data. *Medium.* Beschikbaar via: *https://medium.com/@rmndrathna4/dna-hacking-how-hackers-can-access-and-manipulate-your-genetic-data*

McCallum, S., Tidy, J. (5 december 2023). 23andMe: Profiles of 6.9 million people hacked. BBC. Via: *https://www.bbc.com/news/technology-67624182*

Reding, D. et al. (maart 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization.* Beschikbaar via: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Rijksoverheid. (19 januari 2024). Nationale Technologie Strategie. Beschikbaar via: *https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie*

The Guardian. (15 februari 2024) Hackers got nearly 7 million people's data from 23andMe. The firm blamed users in 'very dumb' move. Via: *https://www.theguardian.com/technology/2024/feb/15/23andme-hack-data-genetic-data-selling-response*

UK Office of the Chief Scientific Adviser for National Security, Government Communications Headquarters (GCHQ), National Crime Agency, *Joint Emerging Technology Trends: JETT Report 2022*

Van Bree, T. et al. (maart 2023). Herijking Sleutel-technologieën 2023. *TNO/NWO.* Beschikbaar via: *https://www.tno.nl/nl/newsroom/2023/04/nieuwe-lijst-44-sleuteltechnologieen/*

Van Weerd, C., Lassche, D. (oktober 2021). National Security Implications of Quantum Technology and Biotechnology. *TNO/HCSS*. Beschikbaar via: *https://hcss.nl/wp-content/uploads/2021/11/Strategic-Alert-Quantum-Technology-HCSS-TNO-2021-2.pdf*

Rijksoverheid

Dit is een uitgave van:

Rijksinstituut voor Volksgezondheid en Milieu (RIVM),
Nederlandse Organisatie voor toegepast-natuur-wetenschappelijk onderzoek (TNO),
Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael' (Clingendael),
SEO Economisch Onderzoek (SEO),
Algemene Inlichtingen- en Veiligheidsdienst (AIVD),
Militaire Inlichtingen- en Veiligheidsdienst (MIVD),
Wetenschappelijk Onderzoek- en Documentatie-centrum (WODC).

Juni 2024

015590