Adviesraad
Internationale
Vraagstukken

Hybride dreigingen en maatschappelijke weerbaarheid

AIV-advies 126
4 juni 2024

Adviesraad Internationale Vraagstukken

Dit advies is voorbereid door de
Commissie Vrede en Veiligheid

Voorzitter
Mr. H.J.J. (Henne) Schuwer

Vicevoorzitter
LGen b.d. G.J. (Jan) Broeks

Leden
Prof. dr. B.A. (Beatrice) de Graaf
J. (Jochem) de Groot MA MSc
Gen-maj vlgr b.d. T.H.W. (Theo) ten Haaf
N.J.A. (Nina) van Lanschot MSc
Mr. dr. A.A. (Anna) Marhold
Prof. dr. F.P.B. (Frans) Osinga
Dr. G.R. (Gulnaz) Sibgatullina
J. (Joris) Teer MSc
Drs. D.H. (Dick) Zandee
A. (Anna) van Zoest MPhil

Voormalig leden
Prof. dr. E. (Edwin) Bakker
Drs. A.J. (Arend Jan) Boekestijn
Drs. L.F.F. (Lo) Casteleijn
Prof. dr. J. (Jolle) Demmers
Jhr. P.C. (Pieter) Feith MA
LGen b.d. dr. D. (Dirk) Starink

Raadsadviseur
Dr. J.W. (Hans) van der Jagt

Projectmedewerkers
Ir. S.K. (Shila) de Vries
T. (Tessa) Postmus MSc
Q. (Quinten) Offenberg BA
A. (Annet) Potting

Inhoudsopgave

Samenvatting

Op 2 juli 2022 diende de Nederlandse regering bij de Adviesraad Internationale Vraagstukken (AIV) een adviesaanvraag inzake hybride dreigingen in. De adviesaanvraag stelt dat hybride activiteiten een steeds grotere bedreiging vormen voor de nationale en internationale veiligheid. Hoe kan de regering – en de Nederlandse samenleving – zich beter voorbereiden op dergelijke dreigingen?

Van hybride conflictvoering wordt gesproken als bepaalde, vaak niet-militaire, machtsinstrumenten georkestreerd en strategisch worden ingezet als een wapen, zonder dat er sprake is van een gewapend conflict. Te denken valt hierbij aan politieke ondermijning, cyberactiviteiten, desinformatie, economische destabilisatie, financiële malversaties of concrete aanvallen op de vitale infrastructuur. Dit zijn activiteiten die onze open samenleving en democratische rechtsstaat ondermijnen en plaatsvinden zonder dat de juridische grens tussen oorlog (in de zin van 'gewapend conflict') en vrede wordt overgegaan (*'below the threshold'*). De dreigingen vinden veelal plaats in domeinen waarin de krijgsmacht van oudsher niet opereert, in het schemergebied tussen oorlog en vrede (*'the grey zone'*). De (internationale) hybride dreigingen richten zich voornamelijk op een ondermijning van samenlevingen als geheel, waardoor de veerkracht en weerbaarheid van deze samenlevingen onder druk komen te staan.

In het advies bespreekt de AIV het veelzijdige fenomeen van 'hybride dreigingen' vanuit een drietal dimensies: de fysieke, virtueel-informatieve en cognitieve dimensie. De fysieke dimensie omvat de wereld zoals we die zintuigelijk waarnemen. De virtueel-informatieve dimensie betreft verwerking, bescherming en verspreiding van informatie. De cognitieve dimensie is het totaal van percepties, waarnemingen en intenties in de samenleving. Hierbij richt de AIV zich, naast de evidente dreigingen in de fysieke dimensie, met name op de uitwerking van hybride activiteiten (of aanvallen) op de virtueel-informatieve en cognitieve dimensie, omdat het voor overheden beleidsmatig erg ingewikkeld blijkt juist op dit type dreiging adequaat te anticiperen. Fysieke aanvallen zijn veelal zichtbaarder en gemakkelijker te attribueren. Daarnaast is veelal direct duidelijk wie verantwoordelijk is voor de fysieke beveiliging en bescherming; deze is over het algemeen ook nog eens redelijk georganiseerd. Daarentegen bestaat over de virtueel-informatieve en cognitieve attributie of bescherming juist veel onduidelijkheid.

Geopolitieke urgentie

Een open democratische samenleving is kwetsbaar. Wie kijkt naar belangrijke en essentiële sectoren waar 'vitale processen' plaatsvinden, komt tot de conclusie dat er maar weinig voor nodig is om deze te ontwrichten; of het hierbij nou gaat om waterbeheer, telecommunicatie, energie, de transportsector, drinkwatervoorziening, productie en opslag van chemische en nucleaire goederen, de openbare orde, de financiële sector of de democratische processen. Dergelijke ontwrichting tast de bestaanszekerheid van de bevolking aan en heeft economische en maatschappelijke gevolgen. Het hoofddoel van deze aanvallen is echter vooral gericht op een psychologisch effect: angst en onzekerheid, een verminderd vertrouwen in de instituties of een algeheel wantrouwen jegens medemensen of overheden.

Hybride conflictvoering wordt ingezet om een betere politiek- en militair-strategische positie te bereiken. Zowel statelijke als niet-statelijke actoren lijken zich in toenemende mate te bedienen van een veelvoud aan hybride instrumenten. Rusland wordt in de wetenschappelijke literatuur vaak als voorbeeld genomen. De Russische militaire doctrine kent geen onderscheid tussen conventioneel en niet-conventioneel optreden, waarbij bewust wordt ingezet op niet-militaire activiteiten zoals de inmenging bij democratische verkiezingen, of het financieren van antidemocratische proxy's.

China maakt evenzeer actief gebruik van hybride instrumenten. De Chinese staat zet buiten de grenzen doelbewust en actief psychologische instrumenten en beïnvloeding van de publieke opinie in als middel van conflictvoering. Ook de Verenigde Staten gebruikt hybride methoden en heeft zich in het verleden meermaals actief betoond op politiek en diplomatiek niveau om regeringen te ondermijnen, dictaturen te laten vallen, of landen politiek en economisch onder druk te zetten.

De NAVO-bondgenoten en de EU-lidstaten zijn eveneens nadrukkelijk bezig met hybride dreigingen, zowel defensief als offensief. Sinds 2015 heeft de NAVO het fenomeen hybride dreigingen belegd in een strategie en sinds 2016 is een vijandelijke hybride activiteit een rechtvaardigingsgrond voor een artikel 5-inzet. Daarnaast zijn tal van nieuwe samenwerkingsinitiatieven en investeringsprogramma's opgezet ter bestrijding van hybride dreigingen.

De EU neemt hybride dreigingen zeer serieus. Hybride dreigingen kunnen artikel 42.7 van het Verdrag betreffende de Europese Unie in werking stellen waarmee EU-lidstaten elkaar bijstaan bij de collectieve verdediging van de Europese Unie. Dit geldt zowel voor conventionele als voor hybride aanvallen.

De EU wil hybride dreigingen bestrijden en de bewustwording ten aanzien van hybride dreigingen onder lidstaten versterken via vele initiatieven, zoals het instellen van een *Hybrid Toolbox* die aan lidstaten een hele keur aan instrumenten biedt om hybride dreigingen tegen te gaan. Daarnaast richt het speciaal ingerichte '*European Democracy Action Plan*' uit 2020 en het '*Defence of Democracy*'-pakket dat in december 2023 is gepresenteerd, zich op het meer weerbaar maken van Europese democratieën, ook voor invloed van buitenaf. Voorts investeert de EU via het Europees Defensieagentschap (EDA) in concrete hardware en software ten behoeve van nieuwe technologieën, mede bedoeld om dreigingen in de virtueel-informatieve en cognitieve dimensie tegen te gaan.

Een belangrijk onderdeel van de hedendaagse hybride dreigingen zijn de assertief wordende non-statelijke actoren. Dreigingen worden steeds vaker uitgevoerd door terroristische groeperingen of civiele personen, al dan niet ingezet als proxy door een statelijke actor. En vanwege het feit dat veel hybride aanvallen worden uitgevoerd met gebruik van nieuwe technologieën (die vaak een *dual use*-karakter hebben) zijn ook de grote multinationale techbedrijven, mondiaal opererende bedrijven of invloedrijke individuen, bewust of onbewust, in toenemende mate betrokken bij hedendaagse conflictvoering. Zij zijn enerzijds doelwit, anderzijds worden zij ook als middel ingezet.

De noodzaak van verdere ontwikkeling van het internationaal recht

Internationaalrechtelijk bezien is het fenomeen hybride dreigingen een ingewikkeld vraagstuk. Wat betekent het non-interventie beginsel in de context van hybride dreigingen? Klassieke oorlogvoering wordt beheerst door het internationaal humanitair recht en internationale afspraken die richtlijnen bieden voor het gebruik van geweld, de behandeling van krijgsgevangen en de bescherming van burgers. Voor hybride dreigingen geldt echter juist dat deze plaatsvinden nog voordat de juridische grens van een gewapend conflict is overschreden. Internationaal humanitair recht is niet ontwikkeld met deze dreigingen en conflicten in gedachten. Dat betekent dat ten aanzien van hybride conflict-voering rechtsontwikkeling noodzakelijk is, waarbij onderliggende rechtsbeginselen en mensenrechten van toepassing zijn. Daarnaast: hoe voorkomen we dat de civiele ruimte van onze open democratie wordt gemilitariseerd? Verplichtingen van de staat voortvloeiend uit de rechten van de mens zijn van cruciaal belang bij het omgaan met hybride dreigingen en het bieden van bescherming daartegen.

Ook als het gaat om het mandaat en wettelijk kader van de Nederlandse krijgsmacht brengen hybride dreigingen nieuwe uitdagingen. De taken van de krijgsmacht zijn belegd in de grondwet. Gebaseerd op de grondwet zijn er door het ministerie van Defensie drie hoofdtaken geformuleerd. Omdat hybride dreigingen, met name in de virtueel-informatieve en cognitieve dimensie, niet adequaat worden geadresseerd, roept de AIV de regering op, samen met juristen, de formulering van deze hoofdtaken onder de loep te nemen en waar nodig te wijzigen, met als doel dat de krijgsmacht zich adequater kan inrichten en voorbereiden op toekomstige dreigingen.

Naar een versterkte maatschappelijke weerbaarheid

Paradoxaal genoeg staan de Nederlandse samenleving en andere democratieën onder druk, juist vanwege het vrije en open karakter ervan. Enerzijds is de openheid een grote kracht – en het verdedigen waard. Tegelijkertijd bevat deze openheid een kwetsbaarheid. Het is cruciaal dat de regering proactief optreedt wanneer Nederlandse belangen geschaad dreigen te worden; en dat kost soms juist openheid of vrijheid.

Hybride dreigingen (of concrete aanvallen) kunnen de samenleving raken op vele fronten. Het is daarom noodzakelijk dat de gehele overheid hierop is ingericht; er is daartoe een '*whole-of-government*'-benadering nodig. Maar er is ook een maatschappij-brede aanpak, een '*whole-of-society*' benadering, nodig. De hele Nederlandse samenleving dient onderdeel te zijn van een bredere veiligheidsaanpak.

De AIV ziet de Finse '*comprehensive security*'-benadering – een breed-maatschappelijke staat van paraatheid ten aanzien van veiligheidsvraagstukken – als voorbeeld van hoe de maatschappelijke weerbaarheid versterkt kan worden. Hoewel Finland in vele opzichten verschilt van Nederland, zijn er zeker lessen te trekken uit de Finse benadering. De Finse overheid zet in op versterking van de onderlinge betrokkenheid van burgers evenals op psychologische weerbaarheid. De interoperabiliteit tussen nationale, internationale en EU-contramaatregelen wordt verbeterd, net als de samenwerking van de overheid, inclusief Defensie, met nationale stakeholders. Verder wordt nadrukkelijk ingezet op de beveiliging van de vitale infrastructuur en de essentiële functionele capaciteiten van samenleving en (hulp)diensten. Dit draag bij aan zowel de maatschappelijke als ook de economische weerbaarheid.

Ook in Nederland zal de gehele samenleving moeten bijdragen aan de maatschappelijke weerbaarheid. Via artikel 99a van de grondwet wordt de mogelijkheid gegeven deze gezamenlijke verantwoordelijkheid te beleggen. De huidige benadering van de Nederlandse overheid sluit onvoldoende aan bij de brede impact van hybride dreigingen. Ondanks goede initiatieven zoals het Rijksbreed Responskader Hybride Dreigingen (RBRK), acteert de Nederlandse overheid bij aanvallen of dreigingen vaak reactief, incident-gedreven en gefragmenteerd. Deze benadering leidt veelal tot een ad-hoc inrichting van crisisteams of een sectoraal georiënteerde respons. Op de korte termijn kan deze handelswijze soms werken, maar om op de langere termijn voorbereid, weerbaar als ook slagvaardig te zijn, is veel meer nodig. En in de samenleving lijkt een bewustzijn te ontbreken voor de grote impact van eventuele hybride aanvallen, of concrete dreigingen. Dit bewustzijn dient te worden versterkt. Dit kan bijvoorbeeld door een nationale veiligheidscursus naar Fins model in te voeren en de Nationale Veiligheidscursus van de Nederlandse Defensieacademie en NCTV Academy uit te bouwen; een vorm van maatschappelijke dienstplicht in te voeren; burgers beter te betrekken bij politieke besluitvorming via burgerberaden en het reservistenbestand uit te bouwen.

Nederland dient daarom nadrukkelijker in te zetten op naleving van de zogenaamde '*7 baseline resilience requirements*' van de NAVO. Deze basisvereisten richten zich op de continuïteit en het functioneren van overheidsdiensten; de energievoorziening; voedsel- en watervoorziening; omgang met grotere verplaatsingen van groepen mensen; capaciteit voor massale groepen slachtoffers; functionerende communicatie- en transportsystemen. Kortom, de essentiële processen om de samenleving in stand te houden ook in crisis en oorlogsomstandigheden. De *requirements* verdienen navolging en stroomlijning met reeds bestaande EU-initiatieven tegen hybride dreigingen. Echter zijn ze volgens de AIV onvoldoende gericht op de dreigingen in de virtueel-informatieve en cognitieve dimensie.

Volgens de AIV is Nederland gebaat bij een proactieve, anticiperende en geïntegreerde benadering van de nationale veiligheid. De AIV constateert dat in Nederland de respons op een acute dreiging te sectoraal georganiseerd is en veelal is gericht op schadebeperking. Tevens constateert de AIV dat er behoefte is aan anticipatie en vroegtijdige informatie-uitwisseling om dreigingen te voorkomen en beleidscoherentie te bevorderen in verband met de noodzakelijke samenhang tussen de verschillende sectoren. De regie hiervoor zou moeten liggen bij de in 2022 opgerichte Nationale Veiligheidsraad (NVR). De raad dient tenminste twee keer per jaar te kijken naar de situatie in Nederland, waarbij hij zich richt op een kwetsbaarheidsanalyse en een weerbaarheidsstrategie, specifiek gericht op hybride dreigingen. Deze NVR dient een effectiever en operationelere invulling te krijgen. Idealiter komt de NVR zoveel mogelijk boven de ministeries te staan, direct vallend onder de minister-president. Alle departementen moeten vertegenwoordigd zijn in de NVR, evenals financiële instellingen, veiligheidsdiensten, bedrijven en kennisinstellingen. De noodzakelijke investeringen moeten zichtbaar worden als gevolg van een vergelijking tussen de dreigingsanalyse en de kwetsbaarheidsanalyse. Daaruit moet een plan van aanpak volgen dat de investeringen rechtvaardigt.

Aanbevelingen

Hybride conflictvoering is een veelkoppig monster. Het advies van de AIV bespreekt veel aspecten van hybride aanvallen en kijkt daarbij in het bijzonder naar de maatschappelijke impact ervan in de fysieke dimensie, virtueel-informatieve en cognitieve dimensie. Gezien de grote geopolitieke urgentie en de noodzaak te investeren in maatschappelijke weerbaarheid komt de AIV met tien pregnante aanbevelingen voor de Nederlandse regering.

► De maatschappij:

1. **Investeer in maatschappelijke weerbaarheid en nationaal bewustzijn ten aanzien van hybride dreigingen.** Het vraagstuk van hybride dreigingen gaat de hele samenleving aan; het gaat hierbij om een collectieve mentaliteitsverandering en versterking van een nationaal narratief: Nederlandse burgers dienen zich bewust te zijn van dreigingen. Laat daarom, conform artikel 99a GW, de hele samenleving meewerken aan maatschappelijke weerbaarheid: burgers, overheden, private bedrijven, kennisinstellingen, het maatschappelijk middenveld; iedereen speelt hierin een belangrijke rol. De AIV stelt tevens een nationale veiligheidscursus voor, geïnspireerd op het Finse model, die ter beschikking wordt gesteld aan Nederlandse burgers. De Nationale Veiligheids-cursus van de Nederlandse Defensie Academie en NCTV Academy verdient verdere uitwerking en bredere navolging specifiek ook voor de top van de overheid, bedrijfsleven, maatschappelijke instellingen zoals media en NGO's en nutsinstellingen functionerend in de vitale infrastructuur; dit om een gezamenlijk dreigingsbeeld te creëren en handelingsperspectieven aan te reiken in het kader van weerbaarheid. De versterking van burgerparticipatie is hierbij essentieel. Voor het creëren van draagvlak voor maatschappelijke weerbaarheid kan, zo denkt de AIV, burgerraadpleging verstandig zijn. Via burgerberaden, waarbij burgers via loting mogen deelnemen aan beleids- en besluitvormingsprocessen, zal het veiligheidsvraagstuk door de samenleving beschouwd kunnen worden als een collectieve verantwoordelijkheid. Mede hierdoor zal ook het pluralisme, als essentiële voorwaarde voor een gezonde democratie, worden versterkt.

► De dimensies:

2. ***Fysiek*:**
Bescherm de vitale infrastructuur, verbindingen en nationale belangen, en bestrijd ongewenste buitenlandse beïnvloeding. Een open democratische samenleving zoals de Nederlandse, is kwetsbaar. De beveiliging van essentiële processen die de samenleving draaiende houden moet dringend worden versterkt. Hiervoor is samenwerking met bedrijven, financiële instellingen en kennisinstellingen noodzakelijk. Omdat hierbij vele publieke en private actoren zijn betrokken, dient dit door de overheid gecoördineerd te worden via een '*whole-of-government*' en een '*whole-of-society*' benadering. Hierbij vraagt de AIV met name aandacht voor de verspreiding van desinformatie en de ondermijning van de openbare orde en de democratische rechtsstaat. Gaat het om waterbeheer, dan dienen de verouderde processen te worden geactualiseerd en de beveiliging van de drinkwatervoorziening te worden aangescherpt. Ook de transportsector en de productie van essentiële goederen dienen beter beveiligd te worden. Ten behoeve van de financiële veiligheid zal de operationele slagkracht voor de beveiliging van de financiële sector versterkt moeten worden. De beveiliging van digitale verbindingen, telecommunicatie en energievoorziening dient te worden aangescherpt. Voorts dienen ook kennisinstellingen nadrukkelijk hun verantwoordelijkheid te nemen ten behoeve van de algehele veiligheid. Waar dat kansrijk is, kan de samenwerking gezocht worden in EU-verband.

3. ***Virtueel-informatief*:**
Bestrijd desinformatie en reguleer sociale media-bedrijven en hun platforms. De invloed van techbedrijven, sociale media-bedrijven en online platforms op Nederlandse burgers is immens. Het kabinet dient, samen met andere EU-landen, kritisch te kijken naar de wijze waarop techbedrijven en sociale media-bedrijven hun platforms inrichten en hen te wijzen op hun zorgplicht. Ten aanzien van desinformatie dient de overheid te werken aan een onderwijscurriculum ter bevordering van mediawijsheid en het herkennen van desinformatie. Tevens dient de regering te werken aan versterking van een pluriform (online) medialandschap, mede ter versterking van democratische processen en instituties.

4. ***Cognitief*:**
Neem het Rijksbreed Responskader Hybride Dreigingen als leidraad, maar kijk nadrukkelijker naar de virtueel-informatieve en vooral de cognitieve dimensie. De nieuwe Veiligheidsstrategie voor het Koninkrijk der Nederlanden bevat aanbevelingen voor een nieuw en strategisch veiligheidsbeleid, inclusief twaalf concrete actielijnen. Belangrijke elementen daarin zijn het werken aan een weerbare democratische rechtsorde en een veerkrachtige samenleving, inzetten op onderwijs, en de bescherming van vitale processen van Nederland. Dreigingen met psychologische effecten op de samenleving dienen nader te worden onderzocht; narratieven die de Nederlandse open samenleving, democratie, rechtsorde en vrije manier van samenleving bekrachtigen, dienen te worden versterkt. Hierbij dient aansluiting te worden gezocht bij het '*European Democracy Action Plan*' en '*Defence of Democracy*' pakket.

► Rechtsontwikkeling:

5. **Werk aan mondiale, volkenrechtelijke regulering omtrent attributie en bestraffing van irreguliere, non-conventionele oorlogvoering en werk aan preventie.** Binnen de Geneefse Conventies dient een stringenter, aanvullend protocol te worden ontworpen om aanvallen, met name binnen de virtueel-informatieve en cognitieve dimensie die thans niet vallen onder internationaal (humanitair) recht, alsnog te kunnen bestraffen. In alle gevallen is bestaand internationaal en Europees recht leidend en ook van toepassing op hybride aanvallen. Toch is, aldus de AIV, actualisering van rechtsregels en verdere rechtsontwikkeling inzake staatsaansprakelijkheid en individuele aansprakelijkheid bij hybride dreigingen noodzakelijk. Nederland zal hierin een leidende rol moeten pakken.

► Een overheidsbrede benadering:

6. **Versterk de Nationale Veiligheidsraad en zorg voor goede governance.** Het voorkomen van, en verdedigen tegen, hybride aanvallen vereist een geïntegreerde aanpak van overheden (nationaal en lokaal), de private sector en de maatschappij als geheel. Een '*whole-of-government*' benadering is noodzakelijk wil er een samenwerking plaatsvinden tussen de verschillende bestuurslagen, net zoals er interdepartementaal betere afstemming dient te komen. Daarvoor dient de Nationale Veiligheidsraad, als centraal veiligheidsorgaan, een steviger mandaat te krijgen. De regering dient te onderzoeken op welke manier de NVR het beste kan worden ingebed, ervan uitgaande dat de NVR een nationaal operatiecentrum is met bevoegdheden om departementaal overstijgend te handelen. De regering moet daarbij kijken op welke manier de NVR in uitvoerende zin effectiever en operationeler kan worden ingericht, waarbij dit orgaan idealiter zoveel mogelijk boven de ministeries komt te staan, direct vallend onder de minister-president. In de NVR zouden alle departementen vertegenwoordigd moeten zijn, evenals financiële instellingen, veiligheids-diensten, kennisinstellingen en bedrijven. De noodzakelijke investeringen moeten zichtbaar worden als gevolg van een vergelijking tussen de dreigingsanalyse en de kwetsbaarheidsanalyse. Daaruit moet een plan van aanpak volgen dat de investeringen rechtvaardigt.

7. **Beleg, mandateer en bestrijd dreigingen binnen de virtueel-informatieve en cognitieve dimensie, stel een Rapporteur voor Digitale Zaken in en investeer in nationale scholing ten behoeve van (digitale) weerbaarheid.** De MIVD, AIVD en NCTV moeten ten aanzien van het optreden in het hybride domein meer bevoegdheden krijgen om nieuw type dreigingen, met name die in de virtueel-informatieve en cognitieve dimensie, preventief te herkennen, binnen het kader van de nieuwe Wiv – waarin het toezicht scherp wordt geformuleerd. Daarnaast acht de AIV het instellen van een Rapporteur voor Digitale Zaken noodzakelijk. Het recht van burgers om beschermd te zijn, heeft ook tot gevolg dat burgers zelf in de positie moeten worden gesteld om zich adequaat te kunnen beschermen tegen digitale dreigingen; daarvoor dient de overheid zorg te dragen. Digibetisme dient actief te worden bestreden: het aanbieden van nationale digi-scholing of digitaliseringscursussen kan daartoe helpen. Tevens dient de Nederlandse overheid nader onderzoek te doen naar de gevaren van het open internet, inclusief monitoring van ondermijnende netwerken. Daarbij zal tegelijkertijd de vrijheid van meningsuiting te allen tijde beschermd moeten zijn. Tevens dient de opleiding van ethische hackers voor de rijksoverheid versneld te worden uitgerold; deze hackers maken het werk van cybercriminelen moeilijker, verdedigen burgers digitaal en dragen bij aan digitale weerbaarheid van Nederland.

► Randvoorwaarden:

8. **Herzie de formulering van de hoofdtaken van de Nederlandse krijgsmacht.** De huidige formulering van de hoofdtaken stamt uit 2000 en sluit onvoldoende aan bij de tegenwoordige veelheid aan hybride dreigingen, met name die binnen de virtueel-informatieve of cognitieve dimensie. Hierdoor heeft de Nederlandse krijgsmacht onvoldoende operationele slagkracht zich afdoende te wapenen tegen eventuele toekomstige aanvallen. De regering dient te zoeken naar formuleringen die beter passen bij de huidige tijd, en waarbij rekenschap wordt gegeven van het gebruik van nieuwe technologieën en dreigingen binnen alle dimensies. Voorts zou Defensie zich ook nadrukkelijker moeten bezighouden met de wisselwerking tussen overheid en burgers en zich nadrukkelijker moeten verhouden tot de '*whole-of-society*'-benadering.

9. **Implementeer en benut de maatregelen en richtlijnen van de Hybrid Toolbox van de EU op nationaal niveau.** Binnen de EU dient Nederland in te zetten op internationale samenwerking om hybride dreigingen tegen te gaan. De *Hybrid Toolbox* van de EU verdient een verdere uitrol waarbij Nederland nadrukkelijker dient te werken aan instrumentaria ter bestrijding van aanvallen of dreigingen in de virtueel-informatieve en cognitieve dimensie. Zoek tevens aansluiting bij het '*European Democracy Action Plan*' en '*Defence of Democracy*'-pakket en de maatregelen en richtlijnen die deze bieden voor Nederland om door te ontwikkelen en implementeren op nationaal en subnationaal niveau.

10. **Stimuleer interoperabiliteit binnen de NAVO-landen in de aanpak van hybride dreigingen.** Met name op het gebied van cyber-weerbaarheid, als aanvulling op de conventionele militaire afschrikking, zullen bondgenoten nadrukkelijk moeten samenwerken. Daarbij moet de digitale infrastructuur van de bondgenoten beter op elkaar aangesloten worden. Ook zal op het vlak van inlichtingen betere samenwerking moeten plaatsvinden. Verder dient de NAVO studie te doen naar de wijze waarop artikel 5 al dan niet ingeroepen dient te worden bij een cyber-aanval. Tevens moet artikel 3 navolging krijgen ten behoeve van de versterking van de collectieve weerbaarheidsdoelen, zowel militair als niet-militair. De AIV ziet de overeengekomen '*7 baseline requirements*' en de weerbaarheidsdoelen van de NAVO als richtinggevend voor Nederland. Daarbij moet Nederland zich nadrukkelijk inzetten om deze weerbaarheidsdoelen vorm te geven voor wat betreft alle dimensies van hybride conflictvoering.

Inleiding

Op 2 juli 2022 diende de Nederlandse regering bij de Adviesraad Internationale Vraagstukken (AIV) een adviesaanvraag in inzake 'hybride dreigingen'.[1] De adviesaanvraag stelt dat hybride activiteiten een steeds grotere bedreiging vormen voor de nationale en internationale veiligheid. De schuivende machtsverhoudingen, de toenemende geopolitieke rivaliteit en de ontwikkelingen ten aanzien van nieuwe technologieën, veranderen de internationale veiligheidssituatie in sterke mate. Deze ontwikkelingen hebben gevolgen voor de Nederlandse veiligheid, op een groot aantal terreinen.

Werkwijze

De AIV heeft de afgelopen twee jaar uitvoerig onderzoek gedaan naar het fenomeen 'hybride dreigingen'. Het advies is gebaseerd op extensief literatuuronderzoek en gesprekken met ruim zeventig deskundigen, waaronder bestuurders en vertegenwoordigers uit het bedrijfsleven, banken, onderwijsinstellingen, verschillende ministeries en de veiligheidsdiensten. De AIV is deze personen zeer erkentelijk voor hun inzicht en tijd.

Opzet

De opzet van dit advies is als volgt. Het eerste hoofdstuk geeft een toelichting op het concept hybride dreigingen en formuleert een definitie. Het tweede hoofdstuk richt zich op nationale kwetsbaarheden en de impact van hybride activiteiten in verschillende sectoren van de samenleving. Het derde hoofdstuk beschrijft de geopolitieke urgentie en de internationale ontwikkelingen. Het vierde hoofdstuk bespreekt het juridische raamwerk. Het vijfde hoofdstuk beschrijft de wijze waarop de maatschappelijke weerbaarheid in Nederland kan worden versterkt. De aanbevelingen ten behoeve van het tegengaan van hybride aanvallen en het versterken van de maatschappelijke weerbaarheid, zijn te vinden voorin het advies.


KY
95-93
C10
C12

Hybride dreigingen

1.1 Niet-militaire dreigingen

Een conflict hoeft niet militair te worden uitgevochten om toch desastreus te kunnen uitpakken en grote gevolgen te hebben. Dagelijks wordt de Nederlandse samenleving getroffen door aanvallen op vele fronten, zonder dat Nederland in oorlog is. In hoeverre is de Nederlandse samenleving ingericht op dergelijke aanvallen? In dit advies bespreekt de AIV vele dreigingen, zoals voor de democratische rechtsorde of het waterbeheer.

De Nederlandse democratie

In toenemende mate zijn buitenlandse actoren actief die de democratische processen in Nederland, zoals eerlijke verkiezingen, trachten te ondermijnen. Een van de belangrijkste instrumenten daartoe is de verspreiding van desinformatie via sociale media en genetwerkte digitale groeperingen. Hierbij wordt bewust misleidende informatie verspreid met als doel schade te berokkenen aan een land. Het effect van misleidende informatie wordt versterkt door het inzetten van (generatieve) kunstmatige intelligentie, waarmee alternatieve 'waarheden' gecreëerd kunnen worden.

Met name Rusland is erg actief, zoals ook blijkt uit een analyse van het *Committee on Democracy and Security* van de NAVO.[2] Het land probeert via desinformatieverspreiding, deepfakes en complot-theorieën verdeeldheid te zaaien binnen de Europese Unie.[3] Recent publiceerde de Tsjechische veiligheidsdienst (BIS) dat Europese politici, waaronder Nederlandse, geld zouden hebben ontvangen in ruil voor pro-Russische propaganda.[4] De Russen zouden een beïnvloedingsoperatie in Europa hebben willen uitrollen in aanloop naar de Europese Parlementsverkiezingen van juni 2024. BIS stelde ook dat de operatie betaald werd door Rusland.[5] Ook China is een steeds actievere actor en neemt in toenemende mate Russische tactieken over – de zogeheten 'russificatie' van Chinese beïnvloedingsoperaties.[6]

Deze hybride tactiek ondermijnt de Nederlandse democratische rechtsorde. Het democratische systeem is gebaat bij vrije en open verkiezingen. Ieder bericht over de mogelijkheid van een corrupte Europese of Nederlandse politicus ondermijnt het vertrouwen in de democratische instituties. En dit vertrouwen is al niet hoog. Met name sinds de tijd van het corona-virus, de lockdowns en het drastische overheidsoptreden in de periode 2020-2022 bestaat er bij sommige Nederlanders een diepgaand wantrouwen jegens de overheid, de media, de rechtspraak of de wetenschap. Via sociale media en genetwerkte digitale groepen vinden en voeden deze mensen elkaar. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) waarschuwde in een fenomeenanalyse uit april 2024 voor de groeiende groep van 'soevereinen', Nederlandse staatsburgers die de autoriteit van de staat willen verwerpen.[7]

Deze ontwikkeling laat zien dat hybride dreigingen, zoals het ondermijnen van de Nederlandse democratie, niet uitsluitend afkomstig hoeven te zijn van buitenlandse actoren. Ook binnenlandse actoren doen hieraan mee of worden gecoöpteerd en geïnstrumentaliseerd door buitenlandse actoren. De grens-overstijgende (digitale) interactie tussen kwaadwillende buitenlandse en binnenlandse actoren maakt de bestrijding van hybride dreigingen erg ingewikkeld.

Het Nederlandse water

Ook het Nederlandse watermanagement kan worden getroffen door een hybride aanval. Nederland staat wereldwijd bekend om de strijd tegen het water. Verschillende drooglegginsprojecten, zoals de Beemster, hebben zelfs een plekje verworven op de UNESCO-werelderfgoedlijst.[8] De NAVO heeft de Nederlandse havens aangewezen als belangrijke Europese 'aanlegsteiger' voor de militaire

bevoorradingen vanuit de Verenigde Staten en het Verenigd Koninkrijk, mocht er in Europa een continentaal conflict uitbreken waarbij NAVO-landen betrokken zijn.

Maar juist vanwege de unieke ligging van Nederland vormt dit water ook een grote kwetsbaarheid en een nationale achilleshiel. Met gebruik van nieuwe technologieën kunnen in korte tijd grote delen van Nederland onder water worden gezet. Sabotage van dijken, gemalen of keringen kan ontwrichtende gevolgen hebben. Zo kan Haarlemmermeer, een gemeente die 160.000 inwoners en de volledige infrastructuur van Schiphol inclusief diverse snelwegen en treinverbindingen huisvest, in korte tijd een meter onder water staan. Er zijn polders die bij een dijkdoorbraak in korte tijd tot meer dan twee meter onder water lopen.

De waterschappen zijn slachtoffer van vele, soms kleine, cyberaanvallen per dag. Bij een grote hack zou dergelijke sabotage direct gevolgen hebben voor het waterbeheer. Zo kunnen de digitale signalen, monitoring, metingen en bedieningen van bruggen, sluizen en waterkeringen worden gemanipuleerd. Voorts kan ook de drinkwatervoorziening van Nederland worden getroffen door digitale aanvallen. Hierover luidde de Algemene Rekenkamer in 2019 al de noodklok.[9]

► 1.2 Hybride aanvallen

Een hybride aanval kan plaatsvinden zonder dat er feitelijk een oorlogssituatie is en zonder dat de juridische grens tussen oorlog en vrede wordt overschreden (‘*below the threshold*’). Voorts vinden deze activiteiten veelal plaats in domeinen waarin de krijgsmacht van oudsher niet opereert, in het schemergebied van activiteiten tussen oorlog en vrede (‘*the grey zone*’). De dreigingen richten zich niet per se op de krijgsmacht, maar op de ondermijning van de samenleving als geheel.

Bij hybride conflictvoering is niet altijd duidelijk aan welke dader een aanval kan worden toegeschreven of bij wie de verantwoordelijkheid ligt – de ‘attributie’. Een hybride aanval kan worden uitgevoerd door zowel een statelijke als een niet-statelijke actor, en door zowel militairen (combattanten) als civiele personen (non-combattanten). Het onderscheid hiertussen valt bij hybride aanvallen soms weg, waardoor het voor overheden ingewikkeld is deze aanvallen tegen te gaan. Ook is niet altijd gelijk helder in hoeverre er daadwerkelijk sprake is van een hybride aanval, of dat het gaat om bijvoorbeeld een terroristische aanslag.

De veranderende internationale dynamiek en opkomst van nieuwe technologieën vraagt om een statelijk instrumentarium dat effectief is in het tegengaan van hybride aanvallen.

► 1.3 DIMEFIL als statelijk instrumentarium

Hybride conflictvoering bestaat al erg lang. Al eeuwenlang worden niet-militaire middelen ingezet om een bepaald politiek-strategisch overwicht te behalen over een vijandelijke mogendheid. Manipulatie, psychologische oorlogsvoering, beïnvloedingstechnieken en misleiding zijn oude machtsinstrumenten.[10] Het concept hybride conflictvoering kent dan ook een voorgeschiedenis.[11] Toch is de hedendaagse hybride conflictvoering van een andere aard dan vroegere varianten: tegenwoordig zijn de hybride instrumenten veelomvattender, zijn er meer spelers en is de potentiële impact van hybride activiteiten groter.

In de adviesaanvraag van het kabinet wordt hybride conflictvoering gedefinieerd als een geïntegreerde inzet van middelen die vallen onder het acroniem DIMEFIL (zie kader).[12]

DIMEFIL

Diplomatie. Bij hybride activiteiten in het diplomatieke domein moet worden gedacht aan het opschorten van verdragen, het dwarsbomen van internationale besluitvorming en het creëren van concurrerende allianties op bestaande gedomineerde structuren.

Informatie. Binnen het informatiedomein wordt gepoogd via het verspreiden van desinformatie onzekerheid te creëren in besluitvormingsprocessen van overheden en burgers.

Militair. Binnen het militaire domein wordt gepoogd de inzet van militaire middelen te gebruiken bij demonstratieve inzet van conventionele militaire middelen en militaire interventies of humanitaire hulp.

Economisch. Instrumenten in het economische en financiële domein zijn het beperken van toegang tot markten, handelsroutes, grondstoffen of energievoorzieningen; het doen van buitenlandse overnames of investeringen; het creëren van strategische afhankelijkheid door monopolisering of het instellen van economische sancties of boycots.

Financiën. Financiële instrumenten kunnen worden ingezet om druk te zetten op de financiële markten om de slagkracht van overheden te verminderen en politiek draagvlak te ondermijnen.

Inlichtingen. Inlichtingen kunnen worden gebruikt om een ander politiek narratief te ontwikkelen. Via inlichtingendiensten kan aan beïnvloeding (van politici, media, studenten, de publieke opinie) en inmenging (in buitenlandse diaspora groepen bijvoorbeeld) gedaan worden.

Juridisch. Binnen het juridische domein kan bij een hybride dreigingscampagne gebruik gemaakt worden van het verlagen of verhogen van wettelijke drempels of verplichtingen, het vermijden van aansprakelijkheid of het misbruiken van juridische processen om een nieuw narratief te creëren.

Dit acroniem beschrijft hybride dreigingen vanuit het principe van statelijke macht. Dat betekent dat de instrumentaria die hiermee worden beschreven ook uitsluitend statelijk van aard zijn.[13]

Minder aandacht binnen deze definitie is er voor dreigingen die afkomstig zijn van niet-statelijke actoren. Terwijl cyberaanvallen, desinformatiecampagnes, ondermijning van democratische processen, of het doorknippen van onderzeekabels ook kunnen worden uitgevoerd door groeperingen, individuen, al dan niet opererend als proxy's. Ook bedrijven, universiteiten en andere kennisinstellingen kunnen worden getroffen door hacks, bedrijfsspionage, financiële chantage uitgevoerd door niet-statelijke actoren, zoals ook de AIVD in een recente publicatie liet zien.[14]

Naast de dreiging van niet-statelijke actoren, blijkt bovenstaande DIMEFIL-benadering ook onvoldoende aandacht te hebben voor de rol van nieuwe technologieën die worden geproduceerd voor zowel militaire als civiele doeleinden, de zogeheten *dual use*-technologieën. Terwijl die juist in toenemende mate worden gebruikt bij hybride aanvallen.

► 1.4 De dimensies: fysiek, virtueel-informatief en cognitief

Het brede karakter van hybride aanvallen, de veelheid aan potentiële actoren en de mogelijke gecombineerde inzet met conventionele militaire middelen maakt een precieze afbakening van het begrip 'hybride dreiging' lastig. Om zo concreet mogelijk te kunnen adviseren, en het onderzoek beleidsmatig zoveel mogelijk af te bakenen, kijkt de AIV naar drie dimensies waarin hybride aanvallen plaatsvinden: de fysieke, virtuele en cognitieve dimensie.

Fysiek

In het militaire denken is de fysieke component vooralsnog het belangrijkst en leidend voor strategische besluitvorming.[15] De fysieke dimensie is de dimensie van de 'echte wereld' waarbij gedacht moet worden aan fysieke activiteiten, mensen, culturen en de interactie hiertussen, maar ook aan de hardware-kant van informatiesystemen en cyber operaties.[16] Deze dimensie beslaat personen (individuen, besluitvormers), commando- en controlesystemen, media, communicatietechnologieën zoals computers en infrastructuur. Krijgsmachten zijn zodanig ingericht dat met name aan fysieke dreigingen een weerwoord kan worden gegeven. Overheden gebruiken conventionele militaire middelen om een politiek-strategisch voordeel te behalen.

Virtueel-informatief

De virtuele of informatie dimensie beslaat verwerking, bescherming en verspreiding van informatie. Activiteiten in deze dimensie hebben invloed op hoe en waar informatiestromen ergens terecht komen.[17] De opkomst van disruptieve technologieën, zoals (generatieve) kunstmatige intelligentie en quantumtechnologie zal de virtuele wereld nog meer verweven doen worden met de analoge wereld. De virtuele wereld is een integraal onderdeel geworden voor het leven van veel mensen; men is ervan afhankelijk geworden. En daarmee is deze dimensie tegelijkertijd een grote kwetsbaarheid.

De virtuele wereld geeft potentiële agressors de mogelijkheid om de ervaren realiteit van mensen te veranderen. Zo kunnen *Generative Adversarial Networks* levensechte deepfakes mogelijk maken – dit zijn extreem gelijkende maar valse foto's en videobeelden van bekende en onbekende personen en situaties.

In een belangrijke publicatie vestigt RAND de aandacht op deze snelgroeiende virtueel-informatieve dimensie, waarin wordt gewaarschuwd dat met virtuele activiteiten aanhoudende verstoring en manipulatie kan plaatsvinden. Vooral met de opkomst van het Internet of Things, generatieve AI evenals algoritmische en big data-gestuurde besluitvorming, worden gedigitaliseerde samenlevingen zoals Nederland afhankelijk van netwerken van informatie en gegevensverzameling, uitwisseling, communicatie, analyse en besluitvorming.[18]

De frontlinie van conflicten worden steeds vaker uitgevochten in de heimelijke sfeer van uitwisseling van inlichtingen, informatiedominantie, desinformatie, data-analyse en encryptie. Omdat deze dreigingen zich afspelen buiten het zicht van media en samenleving lijken ze veelal onzichtbaar. Toch hebben ze wel degelijk grote impact. De AIV vraagt nadrukkelijk aandacht voor het risico van onderschatting van deze dimensie.

Cognitief

De cognitieve dimensie kan gezien worden als het totaal van persoonlijke percepties, meningen, waarnemingen en intenties (gevoed door zowel de fysieke dimensie als de virtuele dimensie). Het gaat hierbij om alle aspecten van de intellectuele, onderbewuste en emotionele functies die de menselijke besluitvorming bepalen.[19] Deze dimensie beslaat zowel individuen als groepen, hun overtuigingen, normen, motivaties, ervaringen, emoties enzovoort.

Een aanval in het cognitieve domein draait om het creëren van een sterk psychologisch effect. Hierbij wordt doelbewust ingezet op het veranderen van wereldbeelden en perspectieven.[20] Allerlei middelen kunnen worden ingezet met als doel het transformeren van het bewustzijn of gedragspatronen van het doelwit.[21]

Psychologische oorlogsvoering (‘*psywar*’) en het creëren van botsende perspectieven worden al lange tijd en met wisselend succes ingezet bij conflictvoering. Sinds mensenheugenis worden fysieke militaire middelen samen met psychologische middelen ingezet om uiteindelijk de mentale weerbaarheid van een volk te breken. Tegenwoordig lijken deze middelen niet uitsluitend te worden toegepast in oorlogstijd, maar ook in vredestijd. Wetenschappers verwachten dat de rol van psywar bij de beleidsvorming in vredestijd zal toenemen.[22] En dat deze strijd, met de inzet van virtuele instrumenten, in de cognitieve dimensie zal plaatsvinden.

Een perceptie-oorlog

Fysieke aanvallen zijn veelal zichtbaarder en gemakkelijker te attribueren dan een virtuele of cognitieve aanval. Daarnaast is veelal direct duidelijk wie verantwoordelijk is voor de fysieke beveiliging en bescherming; deze is over het algemeen ook nog eens redelijk georganiseerd. Daarentegen bestaat over de virtuele en cognitieve bescherming juist veel onduidelijkheid.

Volgens de AIV is hybride conflictvoering uiteindelijk gericht op de beïnvloeding van de cognitieve dimensie, via aanvallen op de fysieke dimensie (bijvoorbeeld infrastructuur) en via gebruik van de virtueel-informatieve dimensie.[23] Hybride dreigingen monden steeds vaker uit in een strijd tussen percepties. Met de opkomst van nieuwe technologieën, zoals kunstmatige intelligentie lijken de activiteiten in een genetwerkte samenleving als Nederland dan ook een groter verstorend effect te kunnen genereren. En dat effect is soms ook zichtbaar in de fysieke wereld.

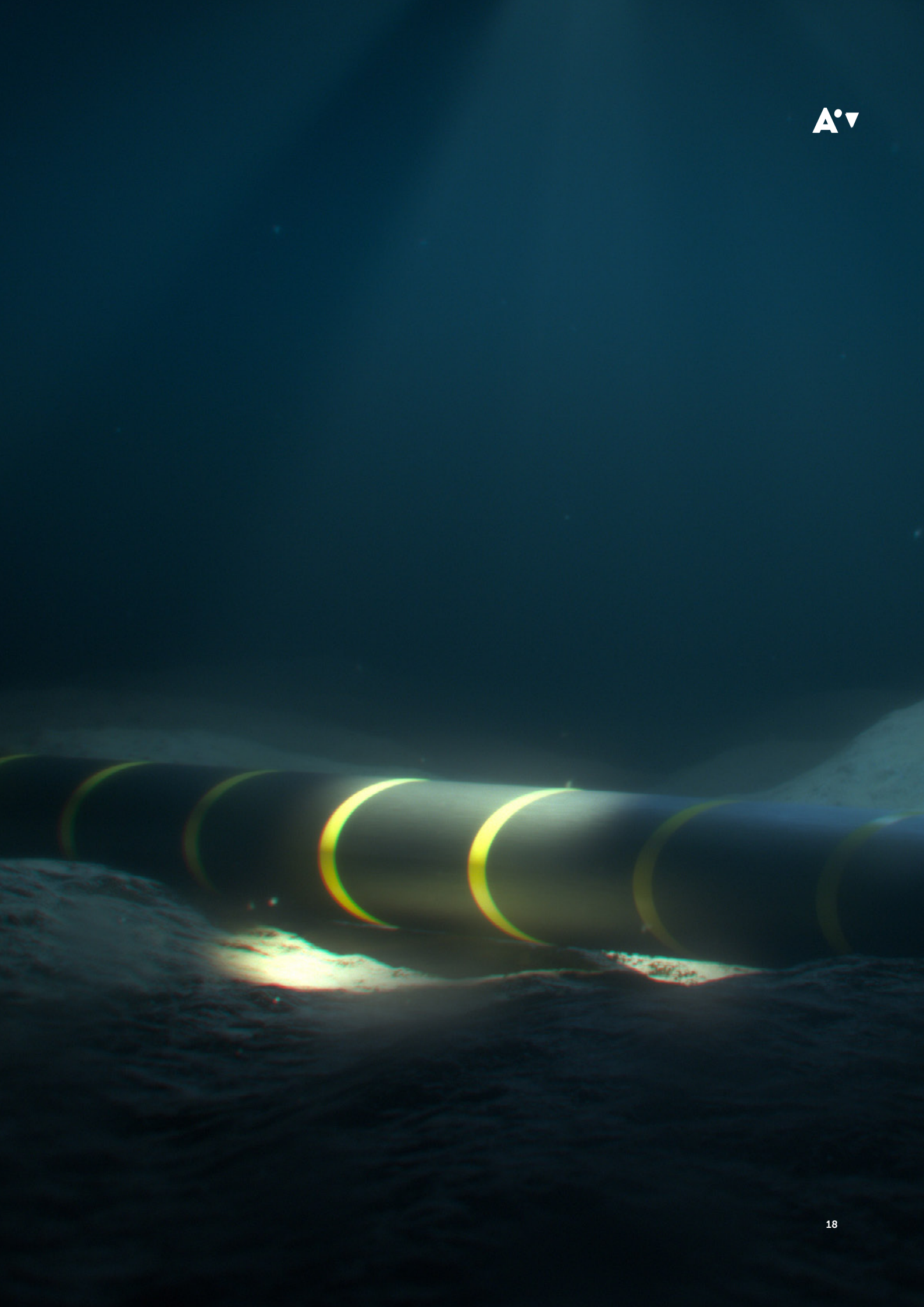
Hybride aanvallen hebben uiteindelijk tot doel de interpretatie van de situatie door een individu en in het massabewustzijn te veranderen. De Nederlandse beleidsmatige respons zou zich dan ook sterker moeten richten op de virtueel-informatieve en de cognitieve dimensie. Volgens de AIV is er binnen de nationale beleidskaders onvoldoende aandacht voor deze uitwerking, waardoor een adequate respons ontbreekt.

► 1.5 Conceptualisering en definitie

De in april 2023 gepubliceerde Veiligheidsstrategie voor het Koninkrijk der Nederlanden omschrijft hybride dreigingen als “dreigingen tegen de nationale veiligheid, die zich grotendeels manifesteren onder het niveau van een openlijk gewapend conflict. Daarbij is sprake van een meervoudig gebruik van middelen door statelijke of niet-statelijke actoren, met als doel bepaalde strategische doelstellingen te bereiken. Voorbeelden hiervan zijn militaire intimidatie, spionage en sabotage, cyberaanvallen, desinformatiecampagnes, ongewenste buitenlandse inmenging in diasporagemeenschappen, kennisdiefstal of de inzet van economische instrumenten”.[24]

De AIV volgt de kern van deze definitie uit de Veiligheidsstrategie, maar voelt evenzeer de vrijheid er nog enkele elementen aan toe te voegen. Om evenwichtig te kunnen adviseren hanteert de AIV een definitie waarin het rekenschap geeft van een zekere balans. Een te brede definitie zal onbruikbaar blijken voor regering en parlement, maar een te nauwe definitie zal de veelomvattendheid inperken. Zeker als het gaat om de impact van nieuwe technologieën of de impact van private bedrijven, maar ook het feit dat veel hybride dreigingen niet per se plaatsvinden in de fysieke wereld, maar steeds vaker in de virtueel-informatieve en cognitieve dimensie, lijkt deze definitie te moeten worden opgerekt. Dit overwegende heeft de AIV ertoe gebracht de volgende definitie te hanteren:

> Hybride conflictvoering is het intentioneel schade toebrengen binnen de fysieke, virtueel-informatieve en cognitieve dimensie, met behulp van een mix van niet-militaire en militaire middelen zoals manipulatie, chantage of sabotage, om bepaalde politieke of ideologische doelen te bereiken, uitgevoerd door zowel statelijke als niet-statelijke actoren op internationaal en nationaal niveau.



Hoofdstuk 2

De nationale veiligheid onder druk

Hybride activiteiten ondermijnen de sociale cohesie, politieke stabiliteit, economische activiteiten en technologische ontwikkeling. In de geglobaliseerde en genetwerkte wereld van vandaag zijn vooral open democratische samenlevingen, zoals de Nederlandse, kwetsbaar. Inmenging in de democratische processen, bedrijfsspionage, cyberaanvallen, het ontwrichten van de vitale infrastructuur en het misbruiken van migratiestromen zijn slechts enkele voorbeelden van de brede hybride instrumenten die kunnen worden ingezet als vijandelijk wapen tegen open samenlevingen. In dit hoofdstuk zal de AIV een aantal sectoren accentueren die kwetsbaar zijn.

► 2.1 Nationale kwetsbaarheden

Door de NCTV is een aantal sectoren aangestipt waarbinnen processen plaatsvinden die vitaal zijn voor het functioneren van de Nederlandse samenleving. Dit zijn de sectoren energie, telecommunicatie, transport, drinkwatervoorziening, waterbeheer, productie en opslag van chemische en nucleaire producten, de financiële processen, het overheidsfunctioneren, de openbare orde en veiligheid en de inzet van Defensie.[25] De AIV kiest ervoor een aantal sectoren uit te lichten en de (mogelijke) dreigingen te beschrijven. Dat wil evenwel niet zeggen dat in niet genoemde sectoren geen dreigingen plaatsvinden, of dat dit geen vitale processen zijn.

Openbare orde, democratie en desinformatie

Een niet te onderschatten desastreus effect van hybride dreigingen is de ondermijning van de democratie en rechtsorde. Deze dreiging vindt bij uitstek plaats binnen de virtuele en cognitieve dimensie.

Gevoed door jarenlang en grootschalig falen van de overheid in de kindertoeslagaffaire, de aardbevingen in Groningen en de stikstofcrisis komen burgers op grote afstand te staan van de overheid. Mede door desinformatie kan deze overheidskritiek omslaan in anti-gouvernementeel denken. Mede door dergelijke ontwikkelingen – en dit is niet alleen in Nederland gaande, maar in veel Europese landen, evenals in de VS – wordt het publieke domein steeds vaker het strijdtoneel van concurrerende wereldbeelden, complottheorieën en alternatieve waarheden.

De AIVD, MIVD en NCTV doen de laatste jaren in hun jaarlijkse 'Dreigingsbeeld statelijke actoren' steeds vaker melding van bewuste pogingen om in de samenleving bepaalde anti-gouvernementele sentimenten aan te wakkeren of uit te buiten.[26] Zoals blijkt uit dit statelijke dreigingsbeeld zijn tactieken die hiervoor worden gebruikt: desinformatieverspreiding; het voeren van mediacampagnes; '*hack-and-leak*'-acties; het mobiliseren van bepaalde personen en groepen; het financieel, facilitair of ideologisch ondersteunen daarvan alsmede het heimelijk beïnvloeden van personen, de politiek en politieke besluitvorming.[27] Aangewakkerd door sociale media lijkt de grens tussen '*Dichtung und Wahrheit*' – zoals Goethe ooit beschreef – soms flinterdun te zijn.

In Nederland is er een groeiende groep burgers die bezig is met het creëren van een parallelle samenleving en ook een groep mensen die zichzelf buiten de samenleving willen plaatsen ('de soevereinen').[28] Dit zijn zorgwekkende ontwikkelingen, zo stelt de AIV. De bewustwording van deze dreiging in de samenleving lijkt vooralsnog te weinig aanwezig. De normalisering van dit denken ondermijnt de rechtsstaat.

Het bestrijden van desinformatie blijkt erg ingewikkeld. De AIV wijst uitdrukkelijk op het gevaar dat onder het mom van het bestrijden van desinformatie er een neiging bestaat dat feitelijke waarheden,

subjectieve meningen of anderszins persoonlijke uitingen die ergens tegenin gaan, zullen worden bestreden. Terwijl het recht op meningsvrijheid te allen tijde moet worden beschermd.

Artikel 10 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 11 van het Handvest van de grondrechten van de Europese Unie beschermen het recht op de vrijheid van meningsuiting en informatie. In Nederland is dit recht geborgd in artikel 7 van de Grondwet. De Nederlandse regering dient nauwkeurig te kijken naar de wijze waarop de bestrijding van desinformatie hand in hand gaat met de bescherming van de grondwettelijke vrijheid van meningsuiting.[29]

Bedrijven en burgers hebben een gezamenlijke verantwoordelijkheid ten aanzien van de online activiteiten. Enerzijds zijn burgers verantwoordelijk voor hun eigen online gedrag en veel van de online content. Anderzijds zijn de platforms verantwoordelijk voor de wijze waarop algoritmen zijn opgebouwd en het digitaal sturen van het surfgedrag van internetgebruikers. Bedrijven zouden hun zorgplicht ten aanzien van het gebruik van de online platforms beter moeten nakomen, zoals de AIV eerder al schreef in 2020 in het advies 'Regulering van online content.[30] Voor de burgers stelt de AIV voor de digitale weerbaarheid van internetgebruikers sterk te vergroten, daarom is media-wijsheid en gedegen digi-onderwijs hard nodig.[31]

Democratische processen en de openbare orde kunnen ook onder druk worden gezet door migratie. Migratie kan daarbij worden ingezet als een middel om de sociale cohesie of de rechtsstaat onder druk te zetten, of bij het frustreren van maatschappelijke processen of het creëren van polarisatie in de samenleving.[32] Dat migratie bewust kan worden ingezet als politiek wapen om andere samenlevingen te destabiliseren, werd zichtbaar in Belarus in 2021 toen president Loekasjenko doelbewust in korte tijd tienduizenden migranten, vooral uit Irak, naar de EU liet doorstromen.

Waterbeheer en drinkwatervoorziening

De huidige waterwerken in Nederland zijn een internationaal paradepaardje, maar tegelijkertijd deels ook sterk verouderd. De waterwerken functioneren op gedateerde automatiseringssystemen en zijn gekoppeld aan digitale netwerken om deze op afstand te kunnen bedienen, waarvan de beveiliging sterk te wensen overlaat. Waterbeheer – meer specifiek het keren en beheren van waterkwantiteit – is dan ook aangestipt als 'vitaal'.

Het ministerie van Infrastructuur en Waterstaat heeft aangegeven dat ook rioolwaterzuiveringen als vitaal gekenmerkt moeten worden omdat ontwrichting hiervan tot veel vervolgschade kan leiden zoals ziekte en vervuiling. Tevens hebben waterschappen, die kritieke infrastructuur zoals rioolwaterzuiveringen en dijken beheren, een plaats in de veiligheidsregio's en werken zij nauw samen met het Nationaal Cyber Security Centrum (NCSC). Samen met Rijkswaterstaat worden zij gemonitord door een gespecialiseerd CERT-team die waterschappen en Rijkswaterstaat op de hoogte stelt van cybersecurityontwikkelingen.[33]

De AIV stelt vast dat de verouderde processen van het waterbeheer zo snel mogelijk geactualiseerd moeten worden. Ook zijn investeringen in de verdere beveiliging van de operationele technologie noodzakelijk voor het veilig functioneren van de systemen. Hierbij dient ook de beveiliging van de drinkwatervoorziening onder de loep te worden genomen. Uit de beleidsnota Drinkwater 2021-2026 blijkt hoezeer de continuïteit van de drinkwatervoorziening bedreigd kan worden door onder meer cybercrime. De AIV onderschrijft het in deze beleidsnota onderkende belang van een beveiligde en weerbare drinkwatersector. Om dit te realiseren moeten evenwel het Rijk, provincies, gemeenten, waterschappen en drinkwaterbedrijven nog beter en efficiënter samenwerken bij het identificeren van dreigingen, het beheersen van risico's en het aanpakken van kwetsbaarheden.[34]

Transportsector

De transportsector is het kloppende hart van de Nederlandse economie. Het internationale karakter van deze sector is een grote kracht, maar ook een kwetsbaarheid. Met name nu blijkt dat China toenemend actief is binnen deze sector in Europa en ook in Nederland. Dit bleek al in 2019 uit de deal

tussen China en Servië waarbij vanuit het Chinese Jinan de trein 'Qilu' in Belgrado arriveerde, het eerste Europese spoorstation op de Chinese Nieuwe Zijderoute – het '*Belt and Road Initiative*' (BRI).[35]

Natuurlijk hoeft zakendoen met China of met Chinese bedrijven geen bedreiging te zijn. Integendeel zelfs, het is van groot belang voor de Nederlandse economie en valt grotendeels onder activiteiten die horen bij een gezonde economische concurrentie of normale handelspolitiek. Toch is waakzaamheid geboden. Een toenemende Chinese assertiviteit kan op de langere termijn uitmonden in een te grote afhankelijkheid. Dat blijkt bijvoorbeeld ten aanzien van de havensector. Nadrukkelijker dan via de spoorwegen is China actief binnen het transport via water. Dit betreft in Europa bijvoorbeeld de havens van Piraeus, Thessaloniki, Genua, Antwerpen, Zeebrugge, Hamburg, en Valencia. Ook de haven van Rotterdam is reeds (deels) in Chinese handen.

Vanwege deze houding van China bestaat er voor Europa (en Nederland) een reëel risico dat de handelsstromen, essentiële economische bouwblokken zoals chips en grondstoffen, en specifieke producten binnen de transportsector worden ingezet als politiek drukmiddel. Deze economische strijd lijkt in vredestijd te vallen onder een 'handelsoorlog', maar worden acuut zodra ergens daadwerkelijk een gewapend conflict dreigt, zoals de afhankelijkheid van Russisch gas voor Europa ineens een nog groter probleem werd na de Russische invasie in Oekraïne.[36]

Het risico op sabotage en ondermijning neemt toe op het moment dat afhankelijkheden van rivaliserende staten, zoals China, groot zijn. Het drukke spoorwegennet evenals de drukbezochte luchthavens in Nederland vormen naast een belangrijke infrastructurele hub ook risicovolle verbindingen. Ze zijn essentieel in het vervoer van mensen, diensten en goederen waardoor sabotage of cyberaanvallen destructieve uitwerkingen kunnen hebben. In 2020 concludeerde de Algemene Rekenkamer bijvoorbeeld dat Schiphol erg kwetsbaar is voor cyberaanvallen.[37]

Essentiële goederen: medicijnen, chemie, microchips

Er bestaan goederen die essentieel zijn voor het draaiende houden van de samenleving en waarvan burgers afhankelijk zijn. De AIV bespreekt enkele voorbeelden.

De COVID-19 pandemie heeft laten zien hoe belangrijk het is om bepaalde medische middelen zelfstandig te kunnen produceren. De mondiale crisis bracht internationaal een groot tekort aan specifieke medicijnen aan het licht, waardoor in korte tijd, voor zover mogelijk, alsnog lokaal moest worden geproduceerd. Dit was niet zozeer een Nederlands probleem, maar gold voor bijna alle landen in Europa. Binnen de Europese Commissie klinkt daarom sindsdien de aanhoudende roep om een nieuwe aanpak op het gebied van de productie van geneesmiddelen.[38]

Het uitblijven van productie en levering van medicijnen kan, in tijden van crises, een geopolitiek pressiemiddel worden. Hoog tijd dat de Nederlandse regering haast maakt met nieuwe initiatieven binnen Europa en Nederland om de noodcapaciteit en noodproductie op orde te krijgen, zo stelt de AIV.[39] Dit geldt eigenlijk evenzeer voor grote delen van de chemische industrie. Er vinden in Nederland belangrijke processen plaats in de productie van chemische goederen, vaak ook met een sterk internationaal belang, waarbij de beveiliging van deze processen van groot belang is. Nauwe samenspraak met de producenten en leveranciers zou deze veiligheid kunnen garanderen.

Voorts is ook de microchipindustrie (oftewel de halfgeleiderindustrie) van groot belang voor de Nederlandse economie, maar tegelijkertijd ook een sector die wordt gekenmerkt door kwetsbaarheden. Er is wereldwijd grote interesse in de technologie van ASML en NXP. Chips zijn de olie van een moderne en gedigitaliseerde maatschappij; geen enkel digitaal product functioneert zonder halfgeleiders. Belangrijke sectoren zoals de telecommunicatie, energie, defensie of de medische sector leunen allemaal sterk op componenten waarin halfgeleiders verwerkt zijn.

Voor geopolitieke grootmachten is controle over de chipindustrie van belang om twee redenen: 's werelds meest geavanceerde chips worden gebruikt om het militaire vermogen van krijgsmachten te versterken en daarnaast zijn chips essentiële bouwblokjes waarop de vitale sectoren van hoog-technologische economieën in sterke mate leunen.[40]

Het gebrek aan een duidelijke Europese industrie- en innovatiepolitiek, stroperige procedures in Nederland en vele andere barrières verzwakken de industrie. De grootschalige halfgeleidersubsidies en het krachtige industriebeleid van de Amerikaanse, Chinese, Taiwanese, en Koreaanse overheden maken dat Nederland op het vlak van de halfgeleiderindustrie op achterstand dreigt te raken. Daarmee wordt niet alleen een voor Nederland zeer belangwekkende industrietak langzaam afgesneden, maar wordt op de lange termijn ook de economische weerbaarheid (en daarmee de samenleving) verzwakt.

De AIV acht het van belang dat er een betere harmonisatie plaatsvindt in de Nederlandse en Europese regelgeving over veiligheidsvraagstukken ten aanzien van de industrie. Europese samenwerking is noodzakelijk. Niet alleen tussen overheden onderling, maar ook tussen overheden en het bedrijfsleven. Daarbij is het van belang de snelheid van informatiedeling ten behoeve van de beveiliging van bedrijfsprocessen te versterken. Tevens is het belangrijk, zo vindt de AIV, dat ook bedrijven hun bedrijfshuishouding ten aanzien van veiligheidsprocessen op orde krijgen.

De financiële sector

De financiële sector is een reëel doelwit en banksystemen zijn kwetsbaar. Deze kwetsbaarheid wordt versterkt doordat de financiële infrastructuur in Europa sterk genetwerkt is en bestaat uit vele digitale verbindingen, elektriciteitsleveringen en de vitale infrastructuur. Het bankwezen als geheel, en specifiek het betalingsverkeer, kan alleen bestaan bij de gratie van veilige, goed functionerende verbindingen. Als bij een grootschalige aanval zowel de elektriciteit als digitale verbindingen worden uitgeschakeld, moeten banken dit kunnen opvangen.

Het Nederlands Instituut voor Publieke Veiligheid (NIPV) bracht een paar jaar geleden de veiligheidsrisico's voor de financiële sector in kaart. Zo houdt de Europese Centrale Bank (ECB) toezicht op de financiële soliditeit van de belangrijkste banken in de Europese Unie die te allen tijde moeten kunnen voldoen aan hun bancaire verplichtingen.[41] Verantwoordelijk voor het toezicht op financiële instellingen, zoals banken, pensioen- en beleggingsfondsen, is de Nederlandsche Bank (DNB). De ECB kan DNB richtinggevende instructies geven over de uitoefening van het toezicht. Daarnaast houdt de Autoriteit Financiële Markten (AFM) toezicht op het gedrag van ondernemingen.[42] Als er urgente risico's zijn, zoals een dreigende bankenrun, dan heeft in Nederland de minister van Financiën de bevoegdheid om, in overleg met de banken en de veiligheidsdiensten, een bankenmoratorium in te stellen.

Desalniettemin is financiële stabiliteit en veiligheid meer dan alleen een toezichtsvraagstuk. Het gaat ook om de wijze waarop deze instellingen hun eigen veiligheid hebben ingericht. Er vinden bij banken, pensioenfondsen en verzekeraars dagelijks cyberaanvallen plaats. Vanwege de permanente dreigingen is een Europees veiligheidssysteem ontwikkeld, DORA, wat een wettelijke basis legt voor toezicht op veiligheid. De AIV onderschrijft het belang van DORA en stelt dat financiële instellingen versnelt stappen moeten ondernemen, conform de vereisten die nodig zijn om DORA-'proof' te zijn.

Een nauwere samenwerking tussen banken en overheden is van groot belang. Momenteel zijn banken bij cyberdreigingen verplicht om ernstige incidenten binnen hun vitale processen direct te melden aan het Nationaal Cyber Security Centrum (NCSC). Afhankelijk van de dreiging of het incident nemen vitale aanbieders uit de financiële sector deel in de ICT Response Board (IRB) dat door het NCSC wordt gefaciliteerd. De IRB is een publiek-privaat samenwerkingsverband dat bij elkaar komt wanneer – al dan niet sector overstijgend – een ICT-crisis dreigt.[43]

Voor het veiligheidsoverleg tussen overheden en banken is verder een belangrijke rol weggelegd voor het Tripartiete Crisismanagement Operationeel (TCO). TCO is bedoeld als crisisrespons voor operationele verstoring van systemen. Dit orgaan bestaat uit DNB, AFM en het ministerie van Financiën. Verder zijn ook andere financiële instellingen vertegenwoordigd via adviesgroepen en de consultatiegroep van het TCO.[44] Ook Euronext en Euroclear zijn aangesloten.

Inmiddels bestaat er in enige mate publiek-private samenwerking tussen banken, politie en de veiligheidsdiensten. De AIV stelt vast dat deze samenwerking momenteel vooral nog incident gedreven is. De eenheden die zich met concrete veiligheidsvraagstukken bezighouden zijn vaak beperkt in hun handelingsopties. Banken lijken vooral bezig met interne processen, en het afdekken van bedrijfsrisico's (compliance), en te weinig met denken vanuit de concrete veiligheidsrisico's voor de Nederlandse burgers. Omdat banken ook een publieke taak hebben, moet dit beter geregeld worden, zo stelt de AIV.

De AIV benadrukt dat de operationele slagkracht voor de financiële sector versterkt moet worden ten behoeve van de financiële veiligheid. Het TCO zou een grotere en meer coördinerende rol moeten vervullen. Deze zou onderdeel moeten vormen van de Nationale Veiligheidsraad (zie hoofdstuk 5). Tevens zou dit overlegplatform ook een operationeel mandaat moeten krijgen waarmee het crisis-management voor de financiële sector kan worden ingericht. Deze betere coördinatie zal bijdragen aan nationale veiligheid, informatie-uitwisseling en digitale weerbaarheid.

Digitale verbindingen, telecommunicatie en energie

Nederland geldt als een data-knooppunt. Vanwege de gunstige ligging van Nederland worden er grote datacentra gebouwd en is de telecommunicatie van geavanceerd niveau. De Nederlandse digitale en data-infrastructuur is erg complex. Denk bijvoorbeeld aan de Amsterdam Internet Exchange (AMS-IX), het internetknooppunt waarlangs het grootste deel van de data van Nederlandse internetgebruikers loopt, maar met name ook de data tussen de trans-Atlantische partners. Deze AMS-IX heeft in de afgelopen kwart eeuw een erg groot en complex netwerk opgebouwd.

De grote concentratie van datastromen via netwerken in Nederland maakt tegelijkertijd de Nederlandse telecommunicatie kwetsbaar. Iedere dag hebben telecom- en data-bedrijven te maken met digitale aanvallen. Dat kunnen bijvoorbeeld DDOS-aanvallen zijn of aanvallen via ransomware. Ook klassiekere aanvallen zoals het afsluiten van stroomtoevoer, telefonie of elektriciteit op lokaal niveau vormen bedreigingen voor de telecomsector. In een sterk geglobaliseerde en genetwerkte wereld waarbij de handel grotendeels digitaal plaatsvindt, is een te grote of eenzijdige connectiviteit ook een risico. Hoewel bedrijven als KPN de nieuwe technologie juist ook inzetten voor een betere herkenning van ongebruikelijk dataverkeer. Het toezicht hiervoor ligt in handen van de Rijksinspectie Digitale Infrastructuur.

Het toenemend dataverkeer heeft fysieke gevolgen: in opdracht van Nederlandse telecombedrijven en netbeheerders als KPN, TenneT, Energienet of andere aanbieders worden er steeds meer kabels aangelegd op de zeebodem (*subsea-level*), zowel bedoeld voor dataverkeer als bijvoorbeeld windenergie op zee. De onderzeekabels zijn in de huidige geopolitieke constellatie van wereldbelang. Tegelijkertijd is Nederland wat dat betreft kwetsbaar. Het is een publiek geheim dat in Nederland veel van de onderzeekabels bij IJmuiden en Zandvoort binnenkomen, in de regio Amsterdam. Als gevolg van het sterk toegenomen dataverkeer en het gebruik van windenergie neemt ook de productie en aanleg van onderzeekabels, bijvoorbeeld door bedrijven als Boskalis, Van Oord, Alcatel Submarine Networks, WIND Subsea Cable Services en andere bedrijven, explosief toe. Recent is het initiatief genomen door vijftien (inter)nationale telecommunicatiebedrijven, samen met de gemeente Rotterdam, voor de aanleg van een nieuwe onderzeekabel tussen Nederland en het Verenigd Koninkrijk, de zogeheten 'Erasmus'-kabel. Deze kabel is bedoeld ter versterking van Nederland als 'digitale toegangspoort tot Europa' en om de regio Rotterdam beter te bedienen, maar ook om hiermee de kwetsbaarheid en afhankelijkheid van de bestaande datanetwerken te verminderen.[45] [46]

Deze toegenomen kabelaanleg levert ingewikkelde veiligheidsvraagstukken op. Wie is er bijvoorbeeld verantwoordelijk voor de bescherming van de meer dan 1 miljoen kilometer aan wereldwijde glasvezelkabels en de ander type onderzeekabels? Over het algemeen zijn dat de bedrijven zelf; zij zijn verantwoordelijk voor de fysieke veiligheid. Maar kunnen zij ook de veilige doorloop van de data of de windenergie via deze kabels garanderen? Wordt data interceptie of het aftappen van energie tijdig tegengegaan? De recent aangelegde trans-Atlantische kabelverbinding tussen de VS en Europa, als gevolg van het sterk toenemende online dataverkeer, laat zien dat de aanleg niet alleen een steeds nauwere afstemming tussen multinationals met nationale overheden betekent, maar ook direct nadrukkelijk beslag legt op de publieke ruimte en op de nationale veiligheidsbelangen.[47]

Dit geldt overigens evenzeer voor de booreilanden en de windparken op zee; deze zijn steeds belangrijker voor de Nederlandse energievoorziening.[48] Deze zijn belangrijk voor Nederland en voor het Europese achterland waaraan energie geleverd wordt. Gezien de hoeveelheid elektriciteitskabels en gaspijpleidingen die door de Nederlandse territoriale wateren lopen is het van belang dat sabotage, zoals recent van de Nord Stream pijpleidingen, wordt tegengegaan.

De Nederlandse overheid is verantwoordelijk voor de publieke ruimte en de zee tot 12 zeemijl uit de kust. Daarbinnen dient er een nauwe samenwerking plaats te vinden met bedrijven. Daarom heeft de regering in december 2023 besloten te investeren in een versterkte veiligheid van de vitale infrastructuur op de Noordzee.[49] Er zal meer camera-, radar- en satelliet-toezicht komen ten behoeve van onderzeekabels (evenals van windmolens en booreilanden). Tevens wordt gewerkt aan de aanschaf van twee nieuwe schepen voor Defensie, bedoeld voor *intelligence*, *surveillance* en *reconnaissance* (ISR).

De AIV erkent het belang van deze investeringen, maar acht dit onvoldoende voor een gedegen toezicht. De regering zal substantieel moeten investeren in het beschermen van de gehele kustlijn. Maatwerk zal nodig zijn voor specifieke vitale verbindingen. Vanuit het idee van risicospreiding zal er concreet gewerkt moeten worden aan de aanleg van meerdere toegangspoorten waar kabels de kust bereiken, een grotere spreiding van kabels en een groter aantal '*transformerblocks*' op zee – de punten waar kabels uit één windpark samenkomen – alsmede een grotere hoeveelheid kabels.

Nationale initiatieven, zoals de Zeekabel Coalitie – een samenwerkingsplatform van de rijksoverheid, onderzeekabelbedrijven, telecombedrijven en investeringsfondsen, ziet de AIV als zeer relevant en belangrijk.[50] Bij dergelijke samenwerkingsplatforms zou nadrukkelijk aandacht moeten bestaan voor de bescherming en beveiliging van de infrastructuur. De AIV moedigt de regering aan ook de veiligheidsdiensten en de veiligheidsregio's aansluiting te laten vinden bij initiatieven zoals deze.

Cyber en data

Cyberdreiging bevat onder meer de ongeautoriseerde inzage in informatie, spionage, het ondermijnen van digitale processen als gevolg van sabotage en de inzet van ransomware en schending van de digitale ruimte, bijvoorbeeld door misbruik van mondiale ICT-leveranciersketens. De recente explosieve toename en brede beschikbaarheid van generatieve-AI applicaties, die door zowel statelijke als niet-statelijke actoren worden ingezet om cyberdreigingen als phishing en ransomware sneller, preciezer, efficiënter, autonomer en complexer uit te voeren, maken de kwetsbaarheid van digitale systemen alleen maar groter.

Het Cybersecuritybeeld Nederland 2022 stelde dat digitale veiligheid niet expliciet of separaat benoemd dient te worden als nationaal veiligheidsbelang, omdat dit als een rode draad door de zes nationale veiligheidsbelangen heenloopt. De zes veiligheidsbelangen, zoals benoemd in de Veiligheidsstrategie voor het Koninkrijk der Nederlanden, zijn territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, sociale en politieke stabiliteit en internationale rechtsorde.[51]

De AIV onderschrijft dat cybersecurity dwars door de andere nationale veiligheidsbelangen heenloopt. Het is evenwel de vraag of dit thans voldoende is om voldoende weerbaar te zijn tegen de grote verscheidenheid van aanvallen en het attribueren van achterliggende actoren. De AIV is van mening dat cybersecurity en digitale weerbaarheid de gehele samenleving aangaan; deze dienen derhalve op nationaal en centraal niveau te worden gecoördineerd.

De samenwerking tussen zowel verschillende overheidsorganisaties als tussen de publieke en private sector ten aanzien van cyberveiligheid verloopt soms moeizaam. Wat dat betreft onderschrijft de AIV de inzet van de regering om de drie reeds bestaande overheidsorganisaties op het gebied van cybersecurity onder te brengen in één nationale cyberorganisatie eind 2025.[52] Samenwerking tussen de private en publieke sector is hierin essentieel. Het gezamenlijk uitvoeren van oefeningen op grote schaal is hier een goed voorbeeld van, evenals de opleiding tot cyberreservist bij het Defensie Cyber Commando (DCC).

Regelmatig wordt cybersecurity door bedrijven nog beschouwd als een lastige kostenpost, naast vele andere kostenposten; een die door veel commerciële bedrijven, met name het midden- en kleinbedrijf, niet nadrukkelijk wordt ingevuld vanwege het feit dat dit te duur is: de kosten worden ingeschat als *te hoog* in relatie tot het ervaren risico. Cyberaanvallen en datalekken worden door bedrijven vaak niet eens gemeld, zo constateerde de Autoriteit Persoonsgegevens in de recente jaarrapportage van datalekken over het jaar 2023.[53] Terwijl als gevolg van de dataleks miljoenen mensen slachtoffer zijn.

Voor bedrijven zou de digitale veiligheid topprioriteit moeten zijn en aan het begin moeten staan van een gezonde en goede bedrijfsvoering. Dit is niet alleen nodig om de veiligheid van het eigen bedrijf te waarborgen, maar ook om impact op de verdere *supply chain*, maar ook de samenleving te minimaliseren. De overheid kan veiligheidseisen stellen aan nieuwe bedrijven. Bijvoorbeeld door bij de oprichting van bedrijven en de inschrijving bij de Kamer van Koophandel een effectief veiligheidsplan voor de inrichting van cybersecurity verplicht te stellen; dit alvorens bedrijven hun activiteiten mogen opstarten.[54]

Daarnaast moet de overheid ook naar zichzelf kijken. De wijze waarop bijvoorbeeld de gemeentelijke basisadministratie wordt opgeslagen is extreem kwetsbaar: een aanval zoals in de gemeente Hof van Twente in 2020 is zeker ook mogelijk in veel andere gemeenten en heeft grote gevolgen voor het gemeentebestuur en de inwoners. Maar ook moet er aandacht bestaan voor de zorgwekkende situatie dat een groot deel van de huidige capaciteit op het gebied van cyberveiligheid van de Nederlandse overheid in handen ligt van een Brits bedrijf.[55]

Het tegengaan van cyberdreigingen vereist niet alleen een nationale, maar vooral ook een gezamenlijke Europese aanpak. Er dient meer aandacht te komen voor maatschappelijke digitale weerbaarheid. De wetgevingsinitiatieven op Europees niveau zoals de *Cyber Resilience Act* voor cyberveiligheid in ontwikkelde hardware en software, NIS II aangaande wetgeving voor bedrijven en organisaties in de kritieke infrastructuur, en DORA voor veiligheidsnormen in de financiële sector zijn belangrijke en positieve ontwikkelingen op dit gebied.

Vanuit Brussel moet er meer toezicht komen op Europese techbedrijven, en op hun concurrenten uit de VS en China die in Europa actief zijn. Hiervoor is een actieve industriepolitiek ten aanzien van de tech-industrie noodzakelijk. Juist door de controle te vergroten zal de Europese weerbaarheid worden versterkt.

Veel Europese overheden – waaronder de Nederlandse – hebben hun digitale systemen belegd bij Amerikaanse bedrijven als Microsoft of Google, zoals blijkt uit een recent rapport van Clingendael.[56] Instrumenten als '*ethics by design*' (of '*safe by design*'), waarbij opvattingen over ethiek en veiligheid reeds in de ontwerpfase van productontwikkeling worden meegenomen, kunnen zowel op nationaal

als Europees niveau bijdragen.[57] Hierbij moet er een realistische verhouding blijven bestaan tussen de normstelling enerzijds, en de mogelijke rem op innovatie anderzijds.[58]

Kennisveiligheid

Hoewel kennisinstellingen door de NCTV formeel niet worden aangestipt als 'vitaal', ziet de AIV de kennissector wel als essentieel voor Nederland. Het is een sector waar beïnvloeding en andersoortige hybride dreigingen veelvuldig kunnen plaatsvinden, zeker als de kennisveiligheid niet op orde is. Hybride dreigingen treden namelijk ook op als er ongewenste overdracht van sensitieve kennis en technologie plaatsvindt of als in Nederland opgedane kennis direct wegvloeit naar vijandelijke mogendheden. In de kamerbrief kennisveiligheid uit december 2022 zegt de minister van Onderwijs, Cultuur en Wetenschap (OCW) hierover: "Kennis en technologie worden door statelijke actoren ingezet om de eigen militaire, technologische, politieke en economische macht te vergroten. Ze zijn daarmee in toenemende mate een strategisch machtsmiddel geworden."[59]

Met het vergroten van de dreigingen en de groeiende complexiteit van technologie- en kennisontwikkeling in het algemeen (multidisciplinariteit), is het belang van kennisveiligheid gegroeid en heeft de Nederlandse overheid de afgelopen jaren ingezet op het bevorderen van bewustzijn en zelfregulering op dit gebied.

Om dit te bereiken hebben de ministeries van OCW, J&V en EZK, in samenwerking met o.a. de veiligheidsdiensten en NCTV, nauw samengewerkt met hogescholen, universiteiten, TO2-instellingen, enzovoorts. Een belangrijk aandachtspunt hierbij is en blijft, dat de juiste balans tussen veiligheid en openheid wordt nagestreefd. Kennisdeling, samenwerking en internationale werving zijn intrinsieke en essentiële onderdelen van kennisontwikkeling en onmisbaar om de doelen te bereiken die Nederland heeft om een voorloper te zijn op het gebied van kennis en innovatie.

Binnen het domein van kennisveiligheid en het beleid van de Nederlandse overheid worden bestaande maatregelen als exportcontrole en sanctiewetgeving onder de aandacht gebracht en wordt er in gezamenlijkheid gezocht naar de juiste inbedding en regulering bij de kennisinstellingen. Het gaat hierbij zowel om de overweging of bepaalde kennis naar buiten gebracht kan worden (middels publicaties en/of samenwerkingsverbanden), als om het mogelijk screenen van nieuwe medewerkers of studenten die met bepaalde sensitieve technologie komen te werken.

De geplande overheidsmaatregelen zijn deels nog in ontwikkeling. Ingezette beleidsinstrumenten zoals het Wettelijk kader Screening Kennisveiligheid, de Nationale Leidraad Kennisveiligheid en het Loket Kennisveiligheid nemen het probleem van kennisveiligheid zeer serieus. Het beleid op internationaal niveau (binnen Europa maar ook breder) behoeft nog de nodige aandacht om een gelijk speelveld te krijgen. Ondertussen breiden de universiteiten hun kennisveiligheidsteams uit en organiseren ze interne campagnes om het onderwerp onder de aandacht te brengen.

Het spanningsveld tussen nationale veiligheid en (academische) vrijheid zal binnen dit domein blijven bestaan. Tevens dient niet elke vorm van onderlinge academische verbondenheid of afhankelijkheid van buitenlandse technologie, kennis en werknemers als dreiging gezien te worden. Het is belangrijk om de kennisinstellingen voldoende eigen ruimte te geven om invulling te geven aan de maatregelen, uiteraard met inachtneming van het veiligheidsbelang.

Kennisveiligheid kan op gespannen voet staan met principes als kennisdeling en transparantie; openheid die juist zo belangrijk is voor kennisontwikkeling. Beperkende maatregelen zouden in eerste instantie gericht moeten zijn ten aanzien van promovendi en studenten uit de landen Rusland, China, Noord-Korea en Iran. Omdat de verantwoordelijkheid voor het toezicht hierop vooralsnog bij de kennisinstellingen zelf ligt – en zij commerciële of particuliere overwegingen veelal laten prevaleren boven publieke belangen – zou het verstandig zijn als de Nederlandse overheid in dit toezicht een grotere rol speelt.

Tegelijkertijd druist een blokkade van kenniswerkers, of het invoeren van al te nadrukkelijk toezicht, in tegen het principe van onafhankelijk academisch onderzoek of tegen gezonde internationale concurrentie; er dient derhalve goed gekeken te worden naar de juridische ruimte en geldende internationale afspraken. Hierbij moet ook rekening gehouden worden met inclusie en diversiteit en het non-discriminatiebeginsel.[60]

► 2.2 Rijksbrede risico's: de Caraïbische delen van het Koninkrijk

Hybride dreigingen vinden plaats in een Rijksbrede context. De regering dient daarom ook oog te hebben voor de zorgwekkende situatie in de Caraïben, met name de ABC-eilanden waar de politieke en economische instabiliteit van buurland Venezuela een grote impact heeft.

De ABC-eilanden zijn qua economie erg afhankelijk van Venezuela.[61] De plotselinge oproep van de Venezolaanse president Maduro om tweederde deel van buurland Guyana te annexeren, maakt de situatie voor de eilanden zorgwekkend.[62] De Venezolaanse president kan diverse middelen inzetten om de eilanden verder onder druk te zetten. Als gevolg van de economische en politieke malaise zijn de afgelopen jaren grote aantallen migranten de druk op de Arubaanse, Curaçaose en Bonairiaanse samenlevingen vergroot. Zo verbleven in 2019 op Curaçao tussen de 8.000 en 10.000 (met name illegale) vluchtelingen, op een bevolking van 160.000.[63]

Als migratie wordt ingezet als machtspolitiek en strategisch pressiemiddel om daarmee een ander land onder druk te zetten dan spreken we van een hybride dreiging. Ondanks dat er momenteel geen signalen zijn dat de Venezolaanse president migratie bewust inzet als politiek middel (zoals de president van Belarus dat wel deed), valt niet uit te sluiten dat, gezien de grote Venezolaanse migratiecrisis in 2018, dit niet alsnog gebeurt. Hiervoor waarschuwden althans het Amerikaanse ministerie van Binnenlandse Veiligheid evenals de *European Union Agency for Asylum* (EUAA) recent nog maar eens.[64]

Naast potentiële dreigingen vanuit het buurland Venezuela speelt ook de beperkte digitale weerbaarheid van de Caraïbische rijksdelen een rol. Nederland heeft een verantwoordelijkheid deze digitale weerbaarheid te versterken. De situatie in de Caraïbische delen van het Koninkrijk gaat ook Nederland aan. Ditzelfde geldt voor het bestrijden van desinformatie en het tegengaan van de ondermijning van de democratie. In de relatief kleine gemeenschappen op de eilanden raken boven- en onderwereld steeds meer vervlochten. Deze ontwikkeling baart de AIV grote zorgen.[65]

Net als in Nederland blijken ook in de Caraïbische rijksdelen de onderzeekabels een toenemende publieke kwestie te worden. Deze samenwerking tussen overheid en onderzeekabel-bedrijven roept soms vragen op, getuige het recente WOO-verzoek over machtigingen aan de Saba Statia Cable System B.V. voor de aanleg, het gebruik en onderhoud van een onderzeese glasvezelkabelverbinding in Saba en Sint-Eustatius.[66] De wijze waarop publieke-samenwerking plaatsvindt in de Caraïbische rijksdelen verdient de aandacht.

Om veiligheid voor de Caraïbische rijksdelen beter in te bedden in een rijksbrede strategie, moet er nauwer worden samengewerkt met de eilanden. Ook dient er meer duidelijkheid te komen over de verhoudingen tussen de ministeries Justitie en Veiligheid, Defensie en Buitenlandse Zaken inzake de Caraïben. Hierbij moet met name gekeken worden naar de wijze waarop de operationele slagkracht bij internationale crises is georganiseerd. Voorts dient nadrukkelijk gekeken te worden naar de reeds bestaande mogelijkheden op het gebied van veiligheid binnen het Statuut voor het Koninkrijk der Nederlanden, zoals de AIV reeds adviseerde in 2020 in het advies 'Veiligheid en rechtsorde in het Caribisch gebied'.[67]

De geopolitieke urgentie

Hybride instrumenten worden ingezet om een betere militair-strategische positie te bewerkstelligen. Hierbij kunnen allerlei middelen worden ingezet.[68] Door globalisering, digitalisering en nieuwe technologieën, is de impact groter dan voorheen. Staten en niet-statelijke actoren lijken zich nadrukkelijker te bedienen van het hybride metier. De grijze zone van het hybride conflict omspant een breed spectrum van middelen. Er bestaat daarom een grote politieke en maatschappelijke urgentie om dit fenomeen te herkennen en te duiden.

► 3.1 Rusland

Bij de beschrijving van hybride conflictvoering wordt Rusland vaak als uitgangspunt genomen. Dit komt met name doordat de inzet van hybride instrumenten al meer dan honderd jaar onderdeel vormt van de Russische militaire doctrine. De Russische oorlogsstrategie bevat geen scheiding tussen conventionele en niet-conventionele activiteiten. Misleiding, politieke oorlogvoering en heimelijke operaties worden ingezet om zo veel mogelijk informatie over de tegenstander in te winnen en deze te verzwakken. Dit gebeurt door een combinatie van traditionele militaire operaties en niet-militaire middelen.[69]

Ondanks dat deze strategie sinds lange tijd gebruikelijk is voor de Russen, werd deze in 2013 nieuw leven in geblazen onder leiding van generaal Gerasimov, sindsdien dan ook de '*Gerasimov-doctrine*' genoemd. Rusland kon daarmee strategische voordelen behalen op vele fronten, bijvoorbeeld door verkiezingscampagnes te dwarsbomen of door het financieren van extremistische en antidemocratische politieke groeperingen.[70] Dit zagen we expliciet naar voren treden ten tijde van de annexatie van de Krim in 2014 en in de acht jaren erna, tot aan de daadwerkelijke militaire invasie in 2022.[71]

De Russische oorlogsdoctrine benadrukt het belang van '*maskirovka*', oftewel militaire maskering, misleiding en verrassing. Dit gebeurt meestal geïntegreerd en als een onderdeel van een bredere aanval, ook al vindt er internationaalrechtelijk nog helemaal geen oorlog plaats.[72] Rusland kan bijvoorbeeld een cyberaanval uitvoeren als onderdeel van een grotere informatieoorlog waarbij een actieve infiltratie van buitenlandse computersystemen plaatsvindt gelijktijdig met elektronische oorlogsvoering en psychologische operaties.[73] Daarnaast gebruikt Rusland methoden zoals het bewust niet vervolgen of uitleveren van ransomware-groepen, om economische schade (en daarmee instabiliteit) te creëren in andere landen.[74] Ook de heimelijke financiering van specifieke politieke partijen valt onder hybride conflictvoering.

De afgelopen tien jaar werd zichtbaar hoezeer Rusland opereerde binnen het cognitieve domein. Rusland zette openlijk in op een krachtig nationaal narratief en historisch wereldbeeld: het verhaal van een eeuwenoud, machtig Russisch rijk; een diepgewortelde verenigde Russische cultuur, een helder en eendimensionaal verhaal. Met Dmitry Adamsky kunnen we stellen dat dit narratief de Russische strategische cultuur in Rusland zelf versterkt, en tegelijk de zogenaamde '*strategic coercion*' naar buiten toe extra kracht geeft.[75] Van de strijd aan dit tweede front – het front waarop wereldbeelden botsen – is het Westen te weinig doordrongen. Autocratische leiders zoals Poetin proberen vrije democratieën te verzwakken, mede door beïnvloeding van politieke partijen en stromingen die vatbaar zijn voor de eendimensionale Russische benadering. Dat was ook zichtbaar in aanloop naar de Oekraïne-oorlog, zoals de AIV reeds beschreef in het advies 'De Oekraïne-oorlog als geopolitieke tijdschok'.[76]

► 3.2 China

China is een voorbeeld van een mogendheid die een veelvoud aan hybride middelen inzet, zonder dat het juridisch gezien in oorlog geraakt. In 2003 werd in China de zogenoemde '*three-warfares*'-doctrine aangenomen die inhield dat zonder geweld een strijd gevoerd kan worden in het eigen belang met behulp van de wet, psychologische oorlogvoering en de publieke opinie.[77] De wet wordt nochtans gebruikt als middel – '*legal warfare*' – om politieke en economische doeleinden te behalen. China gebruikt dit om bijvoorbeeld claims te leggen op territoria.[78]

De Chinese psychologische oorlogvoering tracht internationale besluitvorming te ontwrichten, de bevolking te misleiden en anti-leiderschapssentimenten aan te wakkeren. Hierbij wordt ook '*media warfare*' gebruikt. De claim van Chinese staatsmedia dat de uitbraak van Covid-19 in 2019 was ontstaan nadat het Amerikaanse leger dit virus bewust naar Wuhan zou hebben overgebracht, is hiervan een voorbeeld.[79]

Ondanks dat China zich steeds meer lijkt te richten op een coöptatie van de Russische hybride strategie, is er wel degelijk een verschil. China beschouwt hybride conflictvoering als een middel om zijn politieke en economische invloed buiten zijn grenzen uit te breiden. De Chinese aanpak omvat het gebruik van economische macht, propaganda, cyberspionage en andere niet-traditionele middelen, maar benadrukt, anders dan Rusland, het belang van het vermijden van militaire confrontaties.[80]

President Xi ziet deze bewuste politieke strategie als een noodzaak voor China: "We moeten de afhankelijkheid van de internationale productieketens van China aanscherpen en een krachtige tegenmaatregel en afschrikmiddel vormen tegen buitenlanders die de toevoer (naar China) kunstmatig willen afsluiten."[81] Om dit politieke doel te bereiken worden ook de media, universiteiten, NGO's en bedrijven ingezet.[82]

► 3.3 Verenigde Staten

Ondanks dat de adviesaanvraag van het kabinet met name kijkt naar hybride dreigingen vanuit Rusland en China, en deze landen inderdaad de veiligheid van Nederland (en de EU) onder grote druk zetten, dient niet te worden vergeten dat de inzet van hybride middelen ook Westerse landen niet vreemd is.

De VS heeft zich meermaals actief betoond op politiek en diplomatiek niveau om regeringen te ondermijnen, regeringen te laten vallen, of landen politiek en economisch onder druk te zetten. Amerikanen spreken in dat geval veelal van '*counter hybrid insurgency*'.[83] In zijn benadering richt de VS zich op het gebruik van niet-militaire middelen om politieke doelstellingen veilig te stellen. De VS maakt gebruik van moderne technologie om een militair-strategisch doel te behalen. Daarbij wordt deze technologie ten dienste gesteld aan verschillende middelen, zoals politieke invloed en economische destabilisatie.

Het Amerikaanse Ministerie van Defensie onderneemt steeds vaker activiteiten in de grijze zone "to reinforce deterrence and frustrate adversaries", met name in het cyber-domein.[84] Het ontbreken van landsgrenzen maakt dat het voor staten lastig is te opereren in het cyberdomein. Daarom zet de VS in op een wereldwijd netwerk van bondgenoten en partners om zo het cyberdomein te beschermen en om tegelijkertijd mogelijk te maken dat staten in dit domein bijtijds kunnen optreden tegen dreigingen.[85]

3.4 NAVO

Ook de NAVO is actief in het hybride domein, zowel defensief als offensief. Steeds meer NAVO-landen zien er de noodzaak van in zich bezig te houden met hybride dreigingen. Dit is ook de reden dat de NAVO zelf inzet op contra-hybride maatregelen. Binnen de NAVO speelt de strijd tegen hybride activiteiten een steeds belangrijkere rol.[86] Sinds 2015 bestaat er een NAVO-strategie om hybride dreigingen tegen te gaan. *The Joint Intelligence and Security Division* onderzoekt en analyseert de dreigingen waar NAVO-lidstaten mee te maken hebben of die mogelijk een risico kunnen vormen. Daarnaast wordt er geïnvesteerd in civiele en militaire instrumenten om lidstaten weerbaarder te maken tegen hybride dreigingen. Vanaf 2016 ziet het bondgenootschap hybride dreigingen tegen lidstaten als een bedreiging die zou kunnen leiden tot het in werking stellen van artikel 5 (zie ook hoofdstuk 4).[87]

Verder heeft de NAVO het CCDCOE opgericht voor onderzoek en analyse ten behoeve van cyber-dreigingen en het programma DIANA voor specifiek de verdere ontwikkeling van '*emerging disruptive technologies*' (EDT's), zoals kunstmatige intelligentie en quantumtechnologie, in samenwerking met bedrijven en de wetenschap.[88]

Sinds april 2022 intensiveert de NAVO de politieke dialoog met vier *Asia-Pacific* partnerlanden teneinde samenwerking te intensiveren op het gebied van cyberspace, nieuwe technologieën en het tegengaan van desinformatie. Er zijn '*Individual Partnership Cooperation Programmes*' ontwikkeld om bovengenoemde dreigingen tegen te gaan, maar ook om samen te werken op het gebied van klimaatverandering en maritieme veiligheid.[89]

De NAVO werkt samen met de EU op het gebied van het tegengaan van cyberaanvallen. Verder is er een *NATO-Ukraine Platform on Countering Hybrid Warfare* opgericht en werkt het bondgenootschap samen met verschillende expertise-hubs in Finland, Letland, Estland en Litouwen. Er valt qua samenwerking tussen de NAVO en EU nog veel te winnen op het gebied van informatie-uitwisseling en gedeelde communicatie.[90]

De NAVO benadrukt, zoals omschreven in het Strategisch Concept van 2022, dat het zal investeren in tegengaan van hybride dreigingen. Dit laat zien dat de NAVO het gebruik van hybride tactieken zeer serieus neemt. Daarom heeft de NAVO ook zelf nadrukkelijk ingezet op actieve strategische communicatie ('*StratCom*') waarvoor het een specifiek kenniscentrum voor heeft ingericht, het NATO Strategic Communications Centre of Excellence.[91] De AIV vraagt zich bij dergelijke instanties af waar de grens ligt tussen strategische communicatie en waar het regelrechte beïnvloeding of propaganda wordt. Juist in een tijd van opkomende desinformatie is dit een belangrijk vraagstuk voor de NAVO-bondgenoten.

3.5 Europese Unie

Ook de EU roert zich steeds meer in het hybride domein. Russische desinformatiecampagnes, als onderdeel van bredere Russische hybride conflictvoering, worden gezien als grote dreiging voor de EU.[92] De annexatie van de Krim in 2014 en daaropvolgende schendingen van internationale verdragen deden de aandacht voor de Russische desinformatiecampagnes in Europa groeien.[93] In 2016 en 2017 werd de focus op hybride dreigingen in het kader van het Rusland-Oekraïne conflict versterkt met de oprichting van de *Hybrid Fusion Cell* binnen de *European External Action Service* (EEAS).

In 2016 publiceerde de Europese Commissie een *Joint framework on countering hybrid threats*, dat tot doel had hybride dreigingen tegen te gaan, de bewustwording van hybride dreigingen te versterken, en te streven naar effectieve communicatie en samenwerking om deze dreigingen het hoofd te bieden.[94] De EU heeft bepaald dat hybride dreigingen artikel 42.7 van het Verdrag betreffende de Europese Unie (VEU) in werking kunnen stellen waardoor EU-lidstaten elkaar bijstaan bij de collectieve verdediging van de Europese Unie.[95] Deze 'bijstandsclausule' is enkel nog ingeroepen door

Frankrijk na de terroristische aanslagen in Parijs in 2015. Desalniettemin heeft de EU bepaald dat dit artikel ook bij een cyberaanval – of een andersoortige hybride aanval – kan worden ingeroepen. Hoewel deskundigen de kans hierop klein achten, is het zeker niet onmogelijk.[96]

In 2017 richtten de EU, de NAVO en negen lidstaten *The European Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE) op. Deze organisatie is gezeteld in Helsinki en draagt bij aan het versterken van de weerbaarheid van lidstaten door middel van onderzoek, training en expertise in het tegenaan van hybride dreigingen.[97] Dit CoE is formeel geen EU of NAVO-organisatie en staat open voor alle Europese- en Europese NAVO-lidstaten.

Binnen de EU wordt momenteel gewerkt aan een Europese versie van een responskader voor hybride dreigingen, de *EU Hybrid Toolbox*, zoals vastgesteld door de Europese Raad in juni 2022.[98] Met deze toolbox hebben EU-lidstaten verschillende concrete instrumenten in handen om hybride dreigingen tegen te gaan. Voorts bestaat er de *Foreign Information Manipulation and Interference* (FIMI), waarmee het tegengaan van desinformatie gestructureerd wordt aangepakt. Maar hybride dreigingen, zo stelt ook de Europese Raad, gaan om zoveel meer dan alleen desinformatie.[99]Anders dan de veelzijdige *EU Hybrid Toolbox* heeft FIMI een wat beperktere reikwijdte, omdat het voornamelijk wordt ingezet tegen desinformatie en alleen tegen hybride dreigingen in den brede als er geen andere EU-instrumenten voor handen zijn.

Daarnaast richt het speciaal ingerichte '*European Democracy Action Plan*' uit 2020 en het '*Defence of Democracy*'-pakket dat in december 2023 is gepresenteerd, zich op het meer weerbaar maken van Europese democratieën, ook voor invloed van buitenaf. Voorts investeert de EU via het Europees Defensieagentschap (EDA) in concrete hardware en software ten behoeve van nieuwe technologieën, mede bedoeld om dreigingen in de virtueel-informatieve en cognitieve dimensie tegen te gaan.

Er zijn momenteel verregaande Europese initiatieven ten aanzien van hybride dreigingen zoals de EU cyberbeveiliging-strategie en de strategie voor energiezekerheid.[100] In het Strategisch Kompas uit 2022 heeft de EU aangegeven dat ze willen investeren in cyberdefensiebeleid en cyberdiplomatie, en dat ze instrumenten willen ontwikkelen om buitenlandse inmenging en manipulatie tegen te gaan.[101]

Om meer te doen aan maatschappelijke en economische weerbaarheid in Europa, en tegelijk de groeiende afhankelijkheid van China in te perken, presenteerde de Europese Commissie in 2021 het investeringsproject *The Global Gateway*. De EU wil hiermee investeringen doen in infrastructuurprojecten en economische partnerschappen buiten Europa, oplopend tot 300 miljard euro in 2027. Dit project – bedoeld als ontwikkelingssamenwerking, maar zeker niet zonder Europese industriepolitieke belangen – breekt officieel met de lange traditie waarbij het Westen, en met name Europa, niet aan industriepolitiek wilde deelnemen. Tevens probeert de EU hiermee de Europese strategische autonomie en geopolitieke relevantie te vergroten.[102]

► 3.6 Frankrijk en Duitsland als voorbeeld

In een grootschalige en inzichtelijke RAND-studie is onderzoek gedaan naar de wijze waarop veel landen hun afschrikking en weerbaarheid hebben georganiseerd rond het optreden in het schemergebied van hybride conflictvoering.[103] Enkele voorbeelden van EU-landen, relevant voor Nederland, zijn Frankrijk en Duitsland.

Frankrijk blijkt regelmatig het doelwit te zijn van cyber- en informatieoperaties van Rusland. Een piek van deze activiteiten was gedurende de verkiezingen van 2017 waarbij Emanuel Macron het doelwit was van een desinformatiecampagne en een cyberaanval. De desinformatiecampagne bestond uit zogenaamde onthullingen over zijn seksuele geaardheid en verborgen offshore bankrekeningen. Deze aantijgingen kwamen van groepen verbonden aan de Russische overheid.[104]

Duitsland wordt ook geregeld geraakt door cyberaanvallen.[105] In 2015 werden overheidswebsites aangevallen door de CyberBerkut hackergroep toen de toenmalige premier van Oekraïne, Arseni Jatsenjoek, naar Berlijn kwam voor een vergadering met Angela Merkel. Daarnaast werden van 14 parlementsleden 16GB aan data van hun computers gestolen door de Fancy Bear groep, zo ontdekte de Duitse inlichtingendienst. Deze zelfde groep bleek later zo'n 200 journalisten digitaal te hebben aangevallen.[106]

Voorts werd in november 2016 een Duits telecombedrijf digitaal aangevallen en zijn ook Duitse politici en politieke partijen geregeld slachtoffer van vijandelijke cyber-activiteiten. Ook de Duitse krijgsmacht wordt geconfronteerd met cyberaanvallen, spionage en desinformatie. Begin 2024 publiceerde Rusland vertrouwelijke gesprekken van een groep Duitse luchtmachtofficieren die een briefing voor de Duitse minister van Defensie voorbereidden; deze gesprekken waren gevoerd via het online vergaderplatform Cisco Webex.[107]

3.7 Terroristische groeperingen

Steeds vaker worden hybride dreigingen uitgevoerd door terroristische groeperingen, waarbij alle middelen worden ingezet om samenlevingen te ontwrichten. Door de inzet van verschillende aanvalsmiddelen tegen staten wordt wel gesproken van irreguliere of asymmetrische conflict-voering.[108] Door een complexe mix van militaire, niet-militaire en technologische middelen en de vele onduidelijke actoren (subgroepen van strijders) lijkt, vanuit internationaalrechtelijk perspectief, het onderscheid tussen combattant en niet-combattant soms moeilijk aan te geven. Terwijl dit onderscheid juist essentieel is voor een goede toepassing van het internationaal recht.

In de bloedige terreurstrijd van Islamitische Staat, en bij veel Afrikaanse terreurgroeperingen valt eenzelfde handelswijze op. Lokale groeperingen bedienen zich van *dual use*-technologie waarmee ze eigenhandig nieuw type wapens produceren.[109] Deze groeperingen treden meedogenloos op, ze vermoorden en onthoofden mensen, ze verkrachten vrouwen en zaaien veel angst – de uitwerking van een aanval in de cognitieve dimensie. Via sociale media lukt het ze veelal om hun perceptie van de strijd tegen het Westen tamelijk succesvol voor het voetlicht te brengen. Het veelvoudige gebruik van hybride middelen maakt het voor staten lastig om een duidelijk onderscheid te maken tussen combattant en non-combattant.

3.8 Multinationals en techbedrijven

Ook multinationals, techbedrijven en hun bestuurders spelen een grote rol bij hybride dreigingen. De infrastructuur die nodig is voor conflictvoering ligt veelal in private handen. Daardoor wordt de invloed van private partijen – techbedrijven als Microsoft, Google, SpaceX – in het geopolitieke krachtenveld steeds groter.

De toegenomen geopolitieke rol van sommige multinationals evenals de *dual use*-toepassing van bepaalde nieuwe technologieën zal de hybride dreigingen doen toenemen, zo verwacht de AIV. Er dreigt een situatie waarbij machtige individuen, bedrijven en staten zich begeven op het internationaal politieke speelveld terwijl zij zich aan andere regels houden dan staten.[110]

De AIV roept daarom de Nederlandse regering op haast te maken met de regulering van grote techbedrijven, evenals het versterken van het toezicht op deze bedrijven. Tegelijkertijd zijn deze bedrijven voor de overheid juist van belang bij het versterken van een maatschappelijke weerbare samenleving, en dient er dus ook nadrukkelijk samengewerkt te worden tussen bedrijfsleven, overheid en samenleving.

Big Tech en de Digital Service Act

In de huidige tijd, waarin informatie cruciaal is, brengt de dominante rol van technologiebedrijven in de digitale infrastructuur veel kwetsbaarheden met zich mee. Zo zijn Apple, Google en Telegram gezwicht onder druk van het Kremlin om de app 'Slim Stemmen' van oppositieleider Navalny niet aan te bieden aan gebruikers. Bij een eerder verzoek van de Russische autoriteiten weigerden de platforms, maar na forse boetes en dreigingen om het lokale personeel te vervolgen, werd er een brief gepubliceerd waarin viel te lezen dat de app 'illegale informatie' zou bevatten en daarom niet meer in de app stores beschikbaar zou zijn. Ook Instagram wordt beticht van shadow-banning naar aanleiding van de oorlog tussen Hamas en Israël, met als gevolg een eenzijdige informatievoorziening voor gebruikers.

Naast de cruciale rol in informatie- en digitale infrastructuur hebben technologiebedrijven veel marktmacht. De 'Big Five' – dit zijn de vijf grootste techbedrijven Amazon, Meta, Google, Apple en Microsoft – hebben een gezamenlijke beurswaarde van meer dan 6 biljoen euro. Met deze marktmacht kunnen de poortwachters van onze informatievoorziening veel invloed uitoefenen op het maatschappelijke debat. Bijkomend probleem voor de EU is dat veel bedrijven in Amerikaanse handen zijn of afhankelijk zijn van Chinese technologie.

In 2022 heeft de EU de 'Digital Service Act' aangenomen, wat technologiebedrijven dwingt tot juridische verantwoordelijkheid aangaande desinformatie, nepnieuws, propaganda, manipulatie en criminele activiteiten. De wet beperkt hiermee een verdienmodel van algoritmes gebaseerd op illegale of gevaarlijke content. Juridisch afdwingbare maatregelen blijken een belangrijk middel, mits dit in EU verband gebeurt. Ondanks een sterke lobby om de wet af te zwakken lijken de techgiganten, uitgezonderd bedrijven als X, zich grotendeels te schikken naar de nieuwe regelgeving vanwege de grote economische belangen van de Europese markt.

Bronnen:
1. Apple, Google en Telegram zwichten onder druk van het Kremlin - Raam op Rusland
2. Instagram beticht van censureren pro-Palestijnse posts, 'moeilijk hard te maken' - nos.nl
3. De macht van bedrijven als Google en Apple is gigantisch. Zo trekken Europa en de VS de teugels aan - De Correspondent
4. Negen vragen (en antwoorden) over de Digital Services Act - Zembla - BNNVARA

Een juridische puzzel

Bij hybride dreigingen is geen sprake van een 'gewapend conflict' in de traditionele zin. Dat roept een aantal juridische vragen op. De regels van een 'klassiek' gewapend conflict zijn neergelegd in het oorlogsrecht. Hierbij worden staten en niet-statelijke actoren gehouden aan bepalingen om tijdens het gebruik van militair geweld individuen bescherming te bieden en de gewapende strijd zo humaan mogelijk te maken. En er zijn regels voor vredestijd. Maar bij hybride dreigingen die bijvoorbeeld plaatsvinden in de virtueel-informatieve of cognitieve dimensie bestaan er grote juridische uitdagingen.[111] Welke juridische en ethische overwegingen zijn belangrijk bij het nadenken over hybride activiteiten?

► 4.1 Het juridisch kader

Hybride dreigingen vinden plaats in het grijze gebied tussen oorlog en vrede. Echter, omdat hybride dreigingen zo veel verschillende vormen kunnen aannemen, zal per geval apart moeten worden beoordeeld hoe het recht van toepassing is en met welke consequenties.

Zowel internationaal als nationaal recht kunnen van toepassing zijn op hybride dreigen. Ook kan er interactie zijn tussen verschillende rechtsgebieden. Als het gaat om een gewapende aanval is op internationaalrechtelijk niveau het internationaal humanitair recht van toepassing; dit geldt ook voor aanvallen op infrastructuur, water of energie, of andere civiele doelen. Bij beschadiging van vitale goederen buiten een gewapend conflict om moet er gekeken worden welke regelgeving dan van toepassing is; dat kan het nationaal strafrecht als ook de mensenrechten zijn. Zo kunnen tegen aanvallen die niet onder het internationaal humanitair recht (IHR) vallen, ook maatregelen uit het nationaal (straf-)recht genomen worden. Dit mag natuurlijk slechts gebeuren met de inachtneming van de internationale regels met betrekking tot de jurisdictie.

Bij hybride dreigingen gaat het om dreigingen die volgens de in het humanitair recht gegeven definitie geen gewapende aanval zijn. Dit lijkt eenvoudiger dan het is. Een belangrijk onderdeel van hybride conflictvoering is dat het activiteiten bevat die juist niet per se vallen onder het oorlogsrecht, dat van toepassing is bij gebruik van geweld ('*use of force*') bij zowel symmetrische als asymmetrische oorlogsvoering. Klassieke oorlogsvoering wordt beheerst door oorlogswetten, die richtlijnen bieden voor het gebruik van geweld, de behandeling van krijgsgevangenen en de bescherming van burgers. Er zijn echter technologische ontwikkelingen op het gebied van robotica, kunstmatige intelligentie en het gebruik van big data, met name binnen de private sector, waarover ten aanzien van de veiligheidsaspecten (nog) geen wetgeving of consensus bestaat.

In geval van een concrete hybride dreiging en de rol van het internationaal recht daarin moeten er daarom allereerst drie cruciale vragen worden beantwoord: (1) Is er een schending van het geweldsverbod? (2) Welk rechtsgebied is van toepassing op een concrete hybride dreiging en wat zijn de juridische implicaties? (3) Kan de hybride dreiging worden toegerekend aan een staat in verband met staatsaansprakelijkheid en wat zijn de implicaties als dit niet het geval is? Deze vragen zullen hieronder kort worden toegelicht.

Het geweldsverbod

Staten dienen zich op basis van artikel 2 lid 4 van het VN-Handvest te onthouden van het gebruik van geweld tegen een andere staat. De vraag of een hybride aanval als geweldsgebruik moet worden gezien hangt af van de effecten van de betreffende handeling. Een cyberoperatie zal bijvoorbeeld onder het geweldsverbod vallen als de gevolgen vergelijkbaar zijn met een conventionele gevechtshandeling.[112]

Als een hybride aanval inderdaad een schending van het geweldsverbod met zich meebrengt, heeft de staat die slachtoffer (gelaedeerde) is van die gewapende aanval op grond van artikel 51 VN-Handvest recht op zelfverdediging, mits aan de voorwaarden in dit artikel wordt voldaan (onverwijlde kennisgeving aan de VN-Veiligheidsraad, proportionaliteit en noodzakelijkheid).

Ook als de hybride activiteit geen schending is van het geweldsverbod, kan deze alsnog strijdig zijn met het non-interventiebeginsel. Het Internationaal Gerechtshof (IGH) heeft namelijk in de *Nicaragua*-zaak geoordeeld dat staten zich niet door middel van '*methods of coercion*' in aangelegenheden van andere staten mogen mengen.[113]

Welk rechtsgebied is van toepassing op een concrete hybride dreiging?

Op het niveau van internationaal recht wordt onderscheid gemaakt tussen hybride activiteiten in tijden van vrede en in tijden van oorlog. Maar wat houdt dit in bij situaties waar de grens tussen oorlog en vrede vervaagt? In geval van een gewapende aanval is het internationaal humanitair recht (IHR) van toepassing, maar hybride dreigingen kunnen activiteiten omvatten die buiten deze wetgeving vallen.[114]

Toepasselijkheid van mensenrechten

De relatie tussen IHR en internationale mensenrechten is onderhevig aan stevig debat. In tijden van oorlog staat het IHR toe dat een combattant een andere combattant doodt. Dit staat echter haaks op het recht op leven dat onder het internationaal mensenrecht wordt gewaarborgd. Aanvankelijk was de opvatting dat de internationale mensenrechten enkel in situaties van vredestijd van toepassing zouden zijn en niet in tijden van oorlog.[115] Dit geldt ook in het geval er schermutselingen plaatsvinden die niet intensief genoeg zijn om te kwalificeren als 'gewapend conflict'.

Echter, tegenwoordig wordt over het algemeen aangenomen dat, in tijden van oorlog, zowel het IHR als de internationale mensenrechten van toepassing kunnen zijn: op sommige situaties is alleen IHR van toepassing, op andere enkel internationale mensenrechten, en soms zijn beide rechtsgebieden tegelijkertijd van toepassing.[116]

De Raad van Europa heeft in het rapport '*Legal Challenges related to Hybrid War and Human Rights Obligations*' (2018) met betrekking tot hybride dreigingen en oorlog (de Raad gebruikt zowel de term '*hybrid threat*' als '*hybrid war*') expliciet vastgesteld dat mensenrechten te allen tijde moeten worden gerespecteerd.[117]

Hybride activiteiten in tijden van vrede

Omdat hybride dreigingen buiten een oorlogssituatie plaatsvinden is het de vraag welke internationale regels dan gelden. Voor wat betreft het gebruik van geweld, inclusief het gebruik ervan buiten een situatie van gevechtshandelingen – bijvoorbeeld in het kader van rechtshandhaving door de politie, bij het handhaven van de openbare orde of bijvoorbeeld door een drone-aanval buiten een gewapend conflict – geldt dat dit vrijwel altijd in strijd is met het regime van de rechten van de mens.[118] Onder dit mensenrechten-regime is het toepassen van dodelijk geweld alleen toegestaan in nauw omschreven situaties en aan vergaande beperkingen onderworpen.

Hybride dreigingen buiten IHR

Hybride activiteiten kunnen ook buiten het kader van geweldshandelingen en/of directe schending van mensenrechten vallen. Te denken valt bijvoorbeeld aan economische dwang ('*coercion*'), wat niet valt onder deze twee categorieën, maar mogelijkerwijs wel een schending oplevert van het EU-recht (*Anti-Coercion Regulation*) of internationaal recht (de wetten van de Wereldhandelsorganisatie).[119] Daarnaast valt bijvoorbeeld te denken aan het beginsel dat staten moeten verzekeren dat activiteiten op hun grondgebied geen ernstige schade veroorzaken aan het milieu van andere staten ('*prevention of transboundary harm arising from hazardous activities*').[120]

In alle gevallen is bestaand internationaal en Europees recht leidend en ook van toepassing op hybride dreigingen. Toch blijkt hier, aldus de AIV, nadere rechtsontwikkeling en actualisering van rechtsregels noodzakelijk. Nederland kan hierin internationaal optrekken met andere landen en een leidende rol vervullen.

Aansprakelijkheid

Internationaalrechtelijke aansprakelijkheid kan van belang zijn met betrekking tot hybride aanvallen als deze toe te rekenen zijn aan een staat. De regels inzake staatsaansprakelijkheid zijn neergelegd in de door de VN-Commissie voor Internationaal Recht opgestelde *Articles on the Responsibility of States for Internationally Wrongful Acts* (ARSIWA), die grotendeels het internationaal gewoonterecht weerspiegelen.[121] Staten kunnen zo verantwoordelijk worden gehouden voor internationaal onrechtmatige daden zoals het vernietigingen van infrastructuur. Essentieel is hier dat het dan gaat om een schending van een internationale verplichting (zoals neergelegd in verdrag of gewoonterecht) die rust op een staat, en welke aan die staat kan worden toegerekend. Dit is van toepassing op alle internationale verplichtingen die rusten op staten, of het nu gaat om een schending van het geweldsverbod, IHR of andere internationaalrechtelijke verplichtingen.

Echter, de uitdaging met betrekking tot hybride aanvallen is dat vaak moeilijk te achterhalen is welke entiteit verantwoordelijk is – essentieel in het kader van attributie. Zeker als het ook nog eens gaat om iets ongrijpbaars als het ondermijnen van de democratische rechtsgang. Als duidelijk is wie er verantwoordelijk is voor de aanval of dreiging dan kan dit ook vaak een niet-statelijke actor zijn, zoals een terroristische groepering, een individu, een proxy. In dat geval wordt de toepassing van de ARSIWA m.b.t toerekening bemoeilijkt, omdat de regels zich enkel richten tot statelijke actoren. Toerekening van gedragingen van niet-statelijke actoren aan een staat is niet onmogelijk, maar de drempel daarvoor is hoog. Als een niet-statelijke actor verantwoordelijk wordt bevonden voor de schadelijke effecten van een hybride aanval in een andere staat, zal daarom verhaal moeten worden gehaald via nationale wetgeving.

In geval een hybride dreiging leidt tot een schending van een internationale verplichting die wél aan een staat is toe te rekenen, dan kan dit, onder voorwaarden, de gelaedeerde staat het recht geven op tegenmaatregelen (artikel 22 ARSIWA). In de context van bijvoorbeeld cyberaanvallen is hier ook de *EU Cyberdiplomacy Toolbox* van belang.[122]

Desalniettemin zal bij het ontbreken van staatsaansprakelijkheid sprake kunnen zijn van individuele aansprakelijkheid. Vanwege de ingewikkeldheid dit adequaat te kunnen toepassen is ook wat dit aangaat, aldus de AIV, nadere rechtsontwikkeling en actualisering noodzakelijk. Nederland kan ook hierin een leidende rol pakken.

► 4.2 Artikel 5 NAVO en artikel 42.7 VEU

De NAVO stelt dat een cyberaanval aanleiding kan zijn voor een NAVO-bondgenoot om een beroep te doen op artikel 5, ook al zijn er geen specificaties met betrekking tot de geleden schade. Deze ambiguïteit wordt echter strategisch gehanteerd, als afschrikmiddel opdat de grenzen niet opzettelijk worden opgezocht.

Recentelijk is tussen de Vaste Kamercommissie voor Buitenlandse Zaken in de Tweede Kamer schriftelijk van gedachten gewisseld met de minister van Buitenlandse Zaken over de Internationale Cyberstrategie. Hierin stelt de minister dat “de gevolgen van een reeks van significante cyberoperaties mogelijk samen gekwalificeerd kunnen worden als een gewapende aanval, indien de gevolgen van deze cyberoperaties vergelijkbaar zijn met de gevolgen van een aanval met conventionele wapens.”[123]

Ook in NAVO-communiqués kunnen overwegingen gevonden worden die erop duiden dat een hybride aanval aanleiding kan zijn voor een actie onder artikel 5. Uiteraard dient rekening gehouden te worden met het feit dat acties onder artikel 5 zeer uitzonderlijk zijn, onder andere omdat NAVO-besluiten in consensus worden genomen.[124] Ook het inwerkingstellen van artikel 42.7 (VEU) inzake de collectieve verdediging van de Europese Unie is een mogelijkheid voor EU-landen waarmee gezamenlijk tegen hybride dreigingen opgetreden kan worden; hoewel ook dit in de praktijk niet snel zal gebeuren.

► 4.3 *Lawfare*: het recht als hybride middel

Bij hybride aanvallen is een formele oorlogsverklaring niet per se noodzakelijk; deze zal ook niet snel worden afgegeven door partijen die hybride middelen gebruiken. De grijze gebieden, waar het IHR geen betrekking op heeft, worden soms juist ook gebruikt om in te zetten als hybride middel. Dat wordt ook wel '*lawfare*' genoemd. Lawfare wordt ingezet door zowel partijen die zich gehouden voelen aan het IHR als partijen die juist regelmatig buiten die scheidslijnen opereren.

Via lawfare wordt bestaande wetgeving bewust opzijgeschoven. De grijze gebieden geven ruimte om te handelen en biedt partijen de mogelijkheid tot ontkenning van acties ('*deniability*'). De acties kunnen daardoor vaak moeilijk worden toegekend aan een bepaalde partij ('*non-attribution*'). Hierdoor wordt het de tegenstander moeilijk gemaakt om te reageren en kan een gewapende tegenreactie veelal worden voorkomen.[125]

Het gebruik van lawfare is niet voorbehouden aan partijen die onder de grens van IHR opereren. Veelal is het voor sommige juristen een overduidelijke schending van het internationaal recht, terwijl landen hierop niet worden veroordeeld.[126]

► 4.4 Het grondwettelijk mandaat van de Nederlandse krijgsmacht

Bij hybride activiteiten kan feitelijk alles ingezet worden als wapen (oftewel de '*weaponization of everything*' zoals Mark Galeotti het noemt).[127] Dit heeft – naast de juridische consequenties zoals hierboven beschreven – ook gevolgen voor de wijze waarop in Nederland zelf de wetgeving is ingericht voor wat betreft de inzet van militaire middelen.

Formeel liggen de taken van Defensie vast in artikel 97, 98, 99, 99a en 100 van de Grondwet, waarbij voor wat betreft de taakstelling van de krijgsmacht met name artikel 97 richtinggevend is. Hierin staat geschreven: 'Ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde, is er een krijgsmacht.' En in lid 2 van hetzelfde artikel staat: 'De regering heeft het oppergezag over de krijgsmacht.'[128]

Op basis hiervan heeft het ministerie van Defensie in de Defensienota 2000 drie hoofdtaken geformuleerd. Deze taken worden binnen de Defensieorganisatie nog steeds als leidraad genomen en worden als volgt omschreven. Nederland heeft een krijgsmacht (1) ter bescherming van het eigen en bondgenootschappelijk grondgebied, met inbegrip van de Caribische delen van het Koninkrijk; (2) ter bevordering van de internationale rechtsorde en stabiliteit en (3) ter ondersteuning van civiele autoriteiten bij rechtshandhaving, rampenbestrijding en humanitaire hulp, zowel nationaal als internationaal.[129]

Deze drie hoofdtaken zijn gebaseerd op de grondwetsartikelen en internationale verdragen; ze staan niet als zodanig opgenomen in de grondwet en zijn niet bij wet vastgelegd.[130] Deze taken zijn product van een beleidskeuze op basis waarvan de Defensieorganisatie vandaag de dag – bijna een

kwarteeuw later – nog altijd zwaar leunt. De taakomschrijving van de krijgsmacht, zo valt te lezen in het wetenschappelijk commentaar, geldt ook voor de inzet in het digitale domein (sinds 2012 erkend als vijfde domein van militair optreden naast land, lucht, zee en ruimte).[131]

Niet alleen in oorlog, maar ook bij maatschappelijke crises wordt Defensie vaak gezien als de '*last man standing*'. Maar bij dreigingen in de virtuele of cognitieve dimensie is niet duidelijk wat dit concreet betekent en of Defensie überhaupt wel is ingericht om te fungeren als laatste hoop voor de samenleving. De veelheid aan nieuwe typen dreigingen maakt het voor Defensie namelijk lastig manoeuvreren. Zeker als deze dreigingen plaatsvinden zonder dat er sprake is van een oorlogssituatie. Hoe moet de krijgsmacht reageren op toekomstige dreigingen die wellicht zullen vallen buiten het bestaande grondwettelijke mandaat of buiten de drie geformuleerde hoofdtaken?

Dit vraagstuk werd eerder al geadresseerd door onderzoekscommissie-Brouwer (2022). Deze commissie deed onderzoek naar het handelen van het *Land Information Manoeuvre Centre* (LIMC) van de Koninklijke Landmacht, een eenheid die in 2020 gegevens verwerkte van individuen in Nederland zonder dat daar juridische grondslag voor bestond. De commissie constateerde:

> 'De krijgsmacht zit klem tussen bestaande kaders en nieuwe dreigingen; de huidige ontwikkelingen vragen om aanpassingen van de bestaande kaders. De gestelde nieuwe dreigingen van hybride conflictvoering raken aan de kern van de hoofdtaken van de krijgsmacht en vragen om aanpassing van de bestaande juridische en beleidsmatige kaders.'[132]

Specifiek voor de Nederlandse krijgsmacht attendeerde de AIV het kabinet al eens op de verschuiving die tegenwoordig optreedt ten aanzien van de hoofdtaken, in het briefadvies 'Keuzes voor de krijgsmacht' (maart 2022).[133] De AIV beargumenteerde destijds dat er binnen de internationale conflictvoering, en mede vanwege de 'hybridisering' en toegenomen technologisering van conflictvoering, er een toenemende overlap bestaat van militaire en civiele dreigingen. Deze dreigingen raken direct aan de weerbaarheid van de gehele Nederlandse samenleving, zo stelde de AIV destijds. Tegen de achtergrond hiervan, in combinatie met de sterk veranderende, multidisciplinaire benadering van conflicten, was de AIV van mening dat de drie beleidsmatige hoofdtaken van Defensie onvoldoende ruimte bieden voor een effectieve inzet van de krijgsmacht tegen alle aspecten van hybride dreigingen binnen alle dimensies.

Bij de aanbieding van de Defensienota 2021 aan de Tweede Kamer erkende de minister van Defensie dat de Nederlandse Defensieorganisatie onvoldoende voorbereid is op toekomstige en nieuwe type dreigingen: 'De Nederlandse krijgsmacht is er voor de nationale veiligheid en treedt ook op in internationale crisis- en conflictsituaties en bij rampen. Daartoe heeft de krijgsmacht drie hoofdtaken. Defensie is op dit moment niet adequaat toegerust om het Koninkrijk tegen toekomstige (en sommige huidige) dreigingen.' De minister constateerde dit een half jaar voordat de Russische invasie in Oekraïne de internationale verhoudingen op scherp zette en de vrede op het Europese continent op grove wijze verstoorde.[134]

Kijkend naar de huidige tijd kan de AIV niet anders dan constateren dat, ondanks de vele miljarden extra die momenteel in Defensie worden geïnvesteerd, de situatie niet heel veel verbeterd is. En dat heeft niet alleen met investeringen te maken, maar ook met de taakstelling.

In de huidige formulering van de hoofdtaken van Defensie bestaat onvoldoende aandacht voor de brede scope van hybride aanvalsmiddelen binnen alle dimensies. Omdat in het huidig geopolitieke tijdsgewricht hybride dreigingen, met name in de virtueel-informatieve en cognitieve dimensie, door de krijgsmacht onvoldoende adequaat kunnen worden geadresseerd en tegengegaan, loopt Nederland gevaar.

Derhalve roept de AIV de regering op de huidige formulering van de hoofdtaken, die niet letterlijk in de Grondwet staan vermeld, maar door Defensie zelf zijn ingesteld en in een Memorie van Toelichting staan vermeld, met juristen onder de loep te nemen en waar mogelijk te laten wijzigen en actualiseren.[135] Juist omdat binnen de Defensieorganisatie in sterke mate wordt geleund op de drie hoofdtaken zou het verstandig zijn de taakstelling van de krijgsmacht beter in te richten op dreigingen binnen alle drie de dimensies. Deze wijziging zou mogelijk zijn omdat deze door Defensie ingestelde beleidstaken en de Memorie van Toelichting als zodanig niet in de wet zijn vastgelegd. Hoewel met deze wijziging de formele en juridische rechtsgrond van Defensie niet verandert, zal de invulling van taken hierdoor wel anders belegd kunnen worden.

Voorts past hierbij ook dat artikel 3 van het NAVO-verdrag wordt meegenomen in de overwegingen. In dit artikel valt te lezen dat NAVO-bondgenoten 'ieder voor zich en gezamenlijk, hun individueel en collectief vermogen om een gewapende aanval te weerstaan handhaven en ontwikkelen door voortdurend en op doelmatige wijze zichzelf te versterken en elkander hulp te verlenen.'[136] Ook hiervoor geldt dat onvoldoende duidelijk is op welke wijze Nederland (en de NAVO-bondgenoten) deze verantwoordelijkheid heeft ingericht tegen de achtergrond van de modernste soorten van hybride dreigingen.

► 4.5 Een grondwettelijke plicht voor de samenleving

In de grondwet zijn verdedigingstaken van Nederland in belangrijke mate belegd bij Defensie. De krijgsmacht kan namens de overheid optreden in het hoogste geweldsspectrum en geldt derhalve als 'zwaardmacht'. Maar omdat aanvallen en dreigingen niet uitsluitend in het militaire domein plaatsvinden, is het van belang dat de krijgsmacht nauwer samenwerkt met de samenleving. De Nederlandse burgers kunnen zelf bijdragen aan collectieve verdediging, veerkracht en maatschappelijke weerbaarheid.

Verdediging is een breder vraagstuk dan enkel bedoeld voor Defensie of politie. Het gaat de gehele samenleving aan; burgers hebben daarin een rol te vervullen. In het verleden is hiervoor al eens aandacht geweest vanuit de wetgever. In 1997 werd via een Memorie van Toelichting, bij een voorstel tot wetswijziging van artikel 97 GW, al voorgesteld de formulering van de taken van de krijgsmacht te moderniseren. Hierbij viel het volgende te lezen over de rol van de samenleving bij de verdediging van Nederland:

> 'Hoewel de bestaande grondwettelijke bepalingen geen belemmering inhouden voor het opleggen van civiele verdedigingsverplichtingen, roepen zij wel ten onrechte het beeld op dat het in de moderne oorlogvoering alleen om militaire verdediging gaat. Door de civiele verdediging met zoveel woorden te vermelden wordt dit onjuiste beeld weggenomen. Voorts wordt door de voorgestelde bepaling gewaarborgd dat als de burgers civiele verdedigingsverplichtingen worden opgelegd dit niet dan door tussenkomst van de wetgever kan geschieden.'[137]

Mede hierom werd met de Grondwetswijziging van 2000 naast de 'verdedigingsartikelen' voor de krijgsmacht, een additioneel artikel opgenomen ten behoeve van civiele verdediging. Bij het benoemen van de taken voor de krijgsmacht, zoals vastgelegd in grondwetsartikelen 97, 98, 99, 100 heeft de wetgever destijds artikel 99a GW toegevoegd. In dit artikel valt te lezen:

> 'Volgens bij de wet te stellen regels kunnen plichten worden opgelegd ten behoeve van de civiele verdediging.'

Hiermee maakte de wetgever duidelijk dat de verdediging van Nederland niet uitsluitend een taak is voor de krijgsmacht, maar voor de hele samenleving. Het wetenschappelijk commentaar bij dit grondwetsartikel luidt onder meer als volgt:

> 'De wetgever kan aan mensen verplichtingen opleggen in verband met de civiele verdediging. Daarmee worden niet-militaire maatregelen bedoeld ter bescherming van de bevolking en haar bezittingen wanneer zich een natuurramp, oorlogsgeweld of een andere noodtoestand voordoet. Het kan dan bijvoorbeeld gaan om de inzet van artsen en verplegend personeel op plaatsen waar dat dringend nodig is, de inzet van burgers bij het in stand houden van verbindingen over de weg en het water of het herstel en de verzekering van de drinkwater- en energievoorziening'.[138]

Dit grondwetsartikel, wat inmiddels alweer bijna 25 jaar oud is, heeft niet aan urgentie ingeboet. De AIV stelt vast dat de Nederlandse overheid, nadrukkelijker dan het nu doet, beroep zou kunnen doen op artikel 99a GW. Daarmee kan een duidelijk appèl gedaan worden op de vorming van civiele verdediging of burgerlijke weerbaarheid. De AIV is zich ervan bewust dat het grondwetsartikel vooral spreekt over 'plichten' die kunnen worden opgelegd aan samenleving. Hiervoor zal in de huidige maatschappelijke context vermoedelijk weinig steun bestaan. Derhalve lijkt het de AIV verkieslijker om te kijken naar een mildere benadering waardoor de bevolking kan worden gemotiveerd en gestimuleerd. De overheid dient de mogelijkheden te verkennen om samen met Nederlandse burgers, meer dan nu het geval is, de maatschappelijke weerbaarheid te laten vormgeven.

Het is daarbij noodzakelijk, zo stelt de AIV, dat deze weerbaarheid voor alle drie de dimensies geldt, dus zowel in de fysieke, virtueel-informatieve en ook de cognitieve dimensie. En dat is een moeilijke opgave. Immers, het verhogen van de maatschappelijke weerbaarheid ten behoeve van een economische aanval, financiële malversatie of een aanval op de vitale infrastructuur valt soms beter in te denken dan een aanval binnen de virtuele of cognitieve dimensie.

Op welke wijze de samenleving moet worden voorbereid en ingezet ten aanzien van hybride dreigingen in alle drie de dimensies, daarover gaat het volgende hoofdstuk.

Hoofdstuk 5

Werken aan weerbaarheid

Veiligheid gaat ons allen aan en is niet gratis. Niet alle Nederlanders lijken zich hiervan bewust.[139] Desalniettemin is veiligheid een essentieel onderdeel van het nationale en maatschappelijke bewustzijn. Volgens de AIV dient de Nederlandse bevolking meer te worden betrokken en gemobiliseerd bij de inrichting van de nationale veiligheid en maatschappelijke weerbaarheid, conform artikel 99a GW. Daarbij dient er een nauwe samenwerking te komen tussen overheid en burgers, evenals tussen burgers en de krijgsmacht.

► 5.1 De Nederlandse driesporenbenadering

Niet alleen de krijgsmacht heeft een taak in het weerbaarder maken van Nederland; de landsverdediging is een taak van de gehele samenleving. De Nederlandse open samenleving en open (kennis-) economie zijn inherent aan een democratische en rechtstatelijk land als Nederland. De Nederlandse publieke belangen zijn gebaat bij handel, transparantie en wereldwijde netwerken. Als juist op die vlakken dreigingen ontstaan die de leefbaarheid onder druk zetten, dan moet er gewerkt worden aan een veiligheidsscherm.

Sinds een jaar of vijf is er aandacht voor hybride dreigingen in de context van de maatschappelijke weerbaarheid, zoals bleek uit onder andere de 'Defensievisie 2035', 'Dreigingsbeeld Statelijke Actoren' en 'Versterkte Aanpak Dreigingen van andere Landen'.[140] Afgelopen jaar werd de 'Rijksbrede Risicoanalyse Nationale Veiligheid' gepubliceerd (ontwikkeld door o.a. AIVD, TNO, MIVD, RIVM), die tot doel had actuele dreigingen in kaart te brengen om overheden, burgers en bedrijven weerbaar te maken tegen (hybride) dreigingen.[141]

Nederland moet zich wapenen tegen potentiële hybride aanvallen. Daarom stelt de regering ook voor om proactief op te treden wanneer het Nederlandse publieke belang wordt geschaad. Nederland wil, zo heeft de regering laten weten, werken aan kennisopbouw, het bevorderen en beschermen van economische veiligheid, het voorkomen van ongewenste kennis- en technologieoverdracht, ongewenste buitenlandse inmenging tegengaan, en het beschermen van de democratische processen en instituties.

Buitenlandse inmenging is een groot probleem, ook in Nederland. Recent bleek, na berichten van de Tsjechische inlichtingendienst, hoe Rusland een netwerk van Europese politici en beleidsmakers cash geld betaalde ter versterking van het pro-Russische narratief.[142] Demissionair minister-president Mark Rutte bestempelde deze ontwikkelingen als een 'bedreiging voor onze democratie, onze vrije verkiezingen, onze vrijheid van meningsuiting, voor alles'.[143]

Het kabinet heeft richtlijnen opgesteld om buitenlandse inmenging tegen te gaan. Daarbij stelde het drie sporen voor.[144] Het *diplomatieke spoor*: het aangaan van de dialoog met landen die zich schuldig maken aan ongewenste inmenging en hen daar consequent op aanspreken, en indien nodig ook diplomatieke stappen ondernemen tegen de betreffende landen. Het *weerbaarheidsspoor*: het vergroten van de bewustwording en verhogen van de weerbaarheid van de kwetsbare groepen die mogelijkerwijs vatbaar zijn voor ongewenste buitenlandse inmenging. Het *bestuurlijk/strafrechtelijke spoor*: het gecoördineerd optreden en verstoren bij actuele of dreigende incidenten, met inzet van een mix van bestuurlijke en strafrechtelijke maatregelen.[145]

5.2 Naar een rijksbrede respons

De NCTV coördineert het 'Rijksbreed responskader voor hybride dreigingen' en een onderliggend afwegingskader. Dit zijn bestuurlijke en beleidsmatige instrumenten waarmee de overheid hybride dreigingen probeert te bestrijden. Grofweg gaat het hierbij om het delen van informatie, het in kaart brengen van responsopties, het inventariseren van internationaal draagvlak voor een gezamenlijke reactie, de coördinatie van een tegenactie, de impactanalyse ervan, en het nauwkeurig in kaart brengen van de juridische opties evenals het zoeken naar een mandaat. Het RBRK maakt het mogelijk om een gecoördineerde rijksbrede respons in te zetten specifiek tegen een statelijke actor waarvan bekend is dat deze achter een kwaadwillende actie zit. Thans is de NCTV bezig met een breder weerbaarheidsconcept in relatie tot hybride dreigingen.[146]

Hybride dreigingen zijn ook een inlichtingenvraagstuk. Sterker nog: inlichtingendiensten en veiligheidsdiensten zijn dagelijks bezig met het tegengaan van vijandelijke beïnvloeding en heimelijke activiteiten in het schemergebied tussen oorlog en vrede. De MIVD en AIVD proberen binnen de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv) te zoeken naar mogelijkheden om preventief aanvallen binnen het hybride domein te bestrijden. Dit is evenwel niet eenvoudig, juist ook doordat diezelfde wettelijke kaders niet altijd even adequaat ingericht met betrekking tot nieuwe typen aanvallen binnen de virtueel-informatieve en cognitieve dimensie als gevolg van de nieuwste technologische mogelijkheden.

Naast institutionele partijen kunnen ook burgers worden ingezet tegen hybride dreigingen. Een voorwaarde daarvoor is, zo stelt de AIV, dat in Nederland de maatschappelijke weerbaarheid wordt verhoogd en het collectieve bewustzijn inzake veiligheidsvraagstukken wordt versterkt. Er is in de grijze zone tussen oorlog en vrede geen begin-of eindpunt, waardoor een permanent bewustzijn en voortdurende paraatheid van de gehele samenleving nodig is. Wil Nederland de maatschappelijke weerbaarheid verhogen en het collectieve veiligheidsbewustzijn versterken, dan is samenwerking met het bedrijfsleven en met kennisinstellingen essentieel. Daarvoor kijkt de AIV – naast het RBRK – ook naar een model dat in Finland met succes wordt gebruikt.

5.3 Het Finse model geschikt voor Nederland?

Na de annexatie van de Krim en de toegenomen Russische dreiging veranderde Finland rond 2017 de nationale veiligheidsstrategie. Er werd afgestapt van het '*Total Defence Concept*' en gekozen voor de '*Comprehensive Security Approach*'. Hierbij werd gestreefd naar nationale en maatschappelijke weerbaarheid die qua intensiviteit meer impact had op de Finse samenleving dan voorheen de norm was. '*Comprehensive Security*' is een soort samenwerkingsmodel, bedoeld om de maatschappelijke en nationale weerbaarheid te versterken, waarbij vitale onderdelen van de maatschappij en stakeholders worden samengebracht. Alle maatschappelijke organisaties en burgers hebben een rol.

Bij de Finse veiligheidsstrategie gaat het om de bescherming van vitale maatschappelijke belangen die gezamenlijk door autoriteiten, bedrijven, NGO's en burgers wordt bewerkstelligd. De verantwoordelijkheden en taken zijn vastgelegd in de wet. Het toezichthoudend orgaan is de *Security Committee* – de Finse Veiligheidscommissie. Deze commissie is agenderend, adviserend, en levert een jaarlijkse veiligheidsrapportage aan de minister-president en regering. In de jaarlijkse rapportage worden zowel publieke als private perspectieven meegenomen; deze rapportage bevat een jaarlijkse staat van veiligheid in Finland en wordt gezien als van top-strategisch belang. Tevens publiceert deze commissie over de nationale veiligheidsstrategie en nationale cyberveiligheid.

In de Finse Veiligheidscommissie komen de overheid en de samenleving samen. De commissie kent vertegenwoordigers van de departementen, de veiligheidsdiensten, de defensieonderdelen, CEO's van vitale bedrijven, de universiteiten, infrastructurele hoofden, de financiële sector, evenals vertegenwoordigers van enkele NGO's. De commissie wordt voorgezeten door de minister van Defensie.

Naast de Veiligheidscommissie bestaat er een nationaal fonds – via belastingen opgehaald – waaruit de kosten worden betaald om de weerbaarheid op peil te brengen en houden. Het gaat hierbij om miljarden euro's. Dit fonds is in beheer van het zogeheten Nationale Noodvoorziening Agentschap – *National Emergency Supply Agency* (NESA).[147] NESA is aangesloten bij de zojuist genoemde Veiligheidscommissie; het is een instelling die het land voorziet in voorraadbeheer bij crises, zowel ten gevolge van hybride dreigingen als in tijden van een conventionele oorlog. Mede hierom worden Finse bedrijven geacht hun productiecapaciteit deels ten dienste te stellen van de staat. Bijna 1000 bedrijven uit verschillende sectoren zijn betrokken.

NESA is een organisatie voor nationale gereedheid. Zij beheert een staatsfonds voor strategische vitale bestedingen, kritieke materialen, producten, brandstof enzovoorts. Tevens is zij verantwoordelijk voor het compenseren van bedrijven die kosten maken ten behoeve van het versterken van de weerbaarheid en het aanvullen van kritieke voorraden. Ook verzamelt NESA informatie van de potentiële dreigingen. Ook de banken en bedrijven zijn erbij betrokken. NESA kan tamelijk zelfstandig opereren, maar de ministeriële verantwoordelijkheid voor de NESA ligt bij de minister van Handel.

Deze Finse preventie-methode heeft nadrukkelijk ook een cognitief effect. Feitelijk gaat het '*comprehensive security*'-model vooral om het versterken van psychologische weerbaarheid en een nationaal (collectief) bewustzijn. Via een versterkte interactie tussen internationale activiteiten en EU-activiteiten, defensie, het binnenlandse veiligheidsbestel, de economie, de infrastructuur, functionele capaciteiten van de samenleving en dienstverlening, kunnen gevoelens van collectieve veiligheid worden vergroot. En dat kan alleen als burgers zelf actief bijdragen. In Finland zijn circa 50.000 schuilkelders gebouwd waar bijna 5 miljoen burgers kunnen schuilen. Deze worden in gezamenlijkheid onderhouden. Verder is er een goed functionerend publiek alarmsysteem. Ook hebben de meeste Finnen in huis nog schuilplaatsen en levensmiddelen om de eerste 72 uur van een crisis in door te komen.

Naast de Veiligheidscommissie en de NESA is er in Finland een zogeheten Nationale Defensie Cursus als derde belangrijk instrument ter bevordering van de maatschappelijke weerbaarheid. Deze opleiding – een gecertificeerde en hoog aangeschreven cursus – wordt betaald uit het budget van het Ministerie van Defensie. Het betreft een cursus van 3,5 tot 4 weken waarbij burgers worden ingedeeld in verschillende cohorten en groepen. Deze groepen komen eens in de zoveel tijd samen voor cursusmomenten. Hierdoor ontstaan genetwerkte groepen van burgers die worden opgeleid in maatschappelijke weerbaarheid. De Commandant der Strijdkrachten nodigt burgers uit deze cursus te volgen, waarbij wordt gekeken naar de verschillende achtergronden en sectoren die deze personen vertegenwoordigen.

► 5.4 Versterking van maatschappelijke betrokkenheid

Uiteraard is het dreigingsniveau in Finland anders dan in Nederland. Toch bevat de Finse benadering voldoende aanknopingspunten en interessante invalshoeken die relevant zijn voor het Nederlandse veiligheidsbeleid, aldus de AIV. De AIV acht het van nationaal belang dat Nederlandse burgers uitgenodigd worden actief mee te werken aan het versterken van maatschappelijke weerbaarheid. In Nederland zou het relatief eenvoudig moeten zijn de onderlinge veiligheidsnetwerken op orde te krijgen. Het mobiliseren van de samenleving ten behoeve van veiligheid vereist een gezamenlijke inspanning.

Om de open Nederlandse samenleving, de openbare orde en het democratisch rechtssysteem te beschermen is het van belang dat de hele maatschappij onderdeel is van het denken over veiligheidsbeleid. Dit begint bij het vergroten van het veiligheidsbewustzijn onder burgers, overheden, bedrijven en andere private actoren en hen de instrumenten aan te bieden om weerbaarheid op te bouwen.

De Nederlandse Defensieacademie (NLDA) is, in samenwerking met de NCTV Academy, recent gestart met een Leergang Nationale Veiligheid. Het doel van deze leergang is het vergroten van kennis over Defensie en veiligheidsvraagstukken en het bevorderen van een netwerk tussen hen die een rol (kunnen) spelen op het gebied van nationale veiligheid. De deelnemers komen uit de overheid, kennisinstituten en het bedrijfsleven. De AIV ziet dergelijke initiatieven als een bevestiging van de aanname dat dit het juiste moment is om te werken aan een brede maatschappelijke weerbaarheid. De AIV stimuleert een verdere uitrol en institutionalisering van deze leergang tot een volwaardig breed-maatschappelijke cursus, met aandacht voor hybride dreigingen en buitenlandse invloed en inmenging. Deze cursus verdient verdere uitwerking en bredere navolging, specifiek ook voor de top van de overheid, bedrijfsleven, maatschappelijke instellingen zoals media en NGO's en nutsinstellingen functionerend in de vitale infrastructuur; dit om een gezamenlijke dreigingsbeeld te creëren en handelingsperspectieven aan te reiken in het kader van weerbaarheid.

Defensie zal zich nadrukkelijker moeten bezighouden met de wisselwerking tussen overheid en burgers. Het werken aan een groter reservistenbestand en de verdere uitrol van een maatschappelijke dienstplicht (MDT) en het Dienjaar voor Defensie, zoals recent is ingesteld, zouden een nadrukkelijker positie kunnen krijgen bij de vorming van veiligheidsbewuste Nederlandse burgers.

Ter versterking van de maatschappelijke weerbaarheid zal ook de civiele betrokkenheid en burgerparticipatie moeten worden vergroot. Daarbij ziet de AIV goede mogelijkheden in het gebruik van burgerberaden. In verschillende landen zijn reeds burgerberaden opgericht.[148] Bij een burgerberaad wordt een groep burgers gevraagd aanbevelingen te formuleren voor hun respectievelijke gemeente, provincie of land.[149] Een burgerberaad bestaat uit een gelote groep van circa 100 tot 250 personen – idealiter zoveel mogelijk een afspiegeling van de samenleving – waarbij de deelnemers een langere tijd in dialoog gaan met elkaar, en eventueel met politici of beleidsmakers, en zij de vrijheid van informatievoorziening hebben.[150] In verschillende Nederlandse steden en provincies wordt momenteel geëxperimenteerd met burgerberaden, meestal over maatschappelijke onderwerpen als gemeente-afval, vuurwerk, klimaatbeleid. Er bestaat inmiddels ook een Landelijk Netwerk Burgerberaad.[151] Thans zijn de eerste resultaten positief.[152] In andere landen wordt al langer gewerkt met dergelijke burgerberaden.

Mede door burgerberaden kan het pluralisme, als essentiële voorwaarde voor een gezonde democratie, worden versterkt. Dit is ook de reden dat de Raad van Europa recent een Europees burgerberaad heeft ingesteld, waarmee een groep Europeanen meedenkt over de toekomst en de versterking van de democratische weerbaarheid in Oekraïne.[153]

Maatschappelijke weerbaarheid betekent ook beschermd zijn tegen digitale aanvallen. Juist op het vlak van digitale verbindingen is Nederland kwetsbaar, zo schreef de AIV in hoofdstuk 2. Burgers moeten in staat worden gesteld zich adequaat te kunnen beschermen tegen digitale aanvallen. Daar ligt een verantwoordelijkheid bij de burgers zelf – hoe richten zij thuis hun digitale veiligheid in? – maar ook bij de overheid. Het aanbieden van nationale digi-scholing en het versterken van de digitalisering kan daartoe helpen, net zoals de verdere uitbreiding van onderwijsvakken ter bevordering van mediawijsheid en het herkennen van desinformatie. Tevens dient ook het overheidstoezicht op digitale ontwikkelingen te worden versterkt. Thans is er, naar tevredenheid van de AIV, door zowel de Eerste als de Tweede Kamer een Vaste Kamercommissie voor Digitale Zaken ingesteld. Het instellen van een Rapporteur voor Digitale Zaken die namens de overheid opereert, lijkt de AIV een noodzakelijke volgende stap.

5.5 Een Europese 'whole of government'

Het Europese Strategisch Kompas voorziet in de ontwikkeling van de *Hybrid Toolbox*. Nederland was hiervan een van de initiatiefnemers. Deze toolbox stimuleert EU-lidstaten tot meer interoperabiliteit in hun strijd tegen hybride aanvallen en de feitelijke implementatie van contra-hybride instrumenten. In de EU Raadsconclusies van 21 juni 2022 over een raamwerk voor een gecoördineerde EU respons op hybride campagnes is de eerste stap gezet in de implementatie en doorontwikkeling van deze toolbox.[154]

De AIV onderschrijft het belang van een krachtige EU-coördinatie voor hybride dreigingen.[155] De toolbox is belangrijk, maar zegt nog niks over concrete operationalisering of crisismanagement op momenten dat er een ernstige verstoring plaatsvindt. Naast de EU dient ook Nederland zelf kritisch te kijken naar het eigen toezicht en in te zetten op doorontwikkeling of implementatie in Nederland van maatregelen en richtlijnen die voortvloeien uit zowel de *Hybrid Toolbox*, het '*Democracy Action Plan*' en het '*Defence of Democracy*'-pakket.

5.6 Nederland en de NAVO *baseline resilience requirements*

De Nederlandse overheid loopt ver achter bij de Scandinavische landen wat betreft de '*whole-of-government*'- en '*whole-of-society*'-benadering. De huidige benadering van Nederland sluit niet aan bij de brede scope van de dreigingen of aanvallen. De Nederlandse overheid acteert vaak incident-gedreven, gefragmenteerd en reactief. Niettemin zijn, naar het oordeel van de AIV, beide benaderingen nodig om het brede palet aan hybride dreigingen adequaat het hoofd te bieden. Niet zonder reden wordt door kenners een hybride aanval, juist vanwege de brede impact, ook wel omschreven als een 'holistische aanval'.[156] Wil Nederland zich hiertegen wapenen dan is een brede, nationale coördinatie noodzakelijk.

De Nederlandse benadering leidt veelal tot een ad-hoc inrichting van crisisteams of een sectoraal georiënteerde respons. Zo ontbrak er in de gezondheidszorg bijvoorbeeld een flexibele schil om bij crises op te schalen, zoals tijdens de COVID-pandemie duidelijk werd. En qua veiligheid zijn er weliswaar veiligheidsregio's ingedeeld die momenteel redelijk goed functioneren, maar waarbij de focus uitsluitend sectoraal en regionaal gericht is. Hierdoor is er onvoldoende zicht op het internationale karakter van hybride dreigingen.

Deze Nederlandse benadering strookt dan ook niet met wat artikel 3 van het NAVO-verdrag stipuleert. Dit artikel stelt dat NAVO-landen individueel en collectief, in gemeenschap met de andere landen, hun eigen weerbaarheid en verdediging op orde moeten hebben. Naast het grote belang dat bondgenoten minimaal 2% van het BBP besteden aan Defensie moeten hun samenlevingen ook voorbereid zijn op niet-militaire aanvallen.

Sinds de top van Warschau in 2016 – waar nadrukkelijk over hybride dreigingen is gesproken – zijn er de zogenaamde '*7 baseline resilience requirements*' opgesteld. Deze basisvereisten richten zich op het continue functioneren van overheidsdiensten; de energievoorziening; voedsel- en watervoorziening; omgang met grotere verplaatsingen van groepen mensen; capaciteit voor massale groepen slachtoffers en op blijvend functionerende communicatie- en transportsystemen. Kortom, de vitale processen om de samenleving in stand te houden, ook in crisis- en oorlogsomstandigheden.

De '*7 baseline requirements*' maken het mogelijk de weerbaarheid van de verschillende landen op elkaar af te stemmen, belangrijk in het kader van de interoperabiliteit. Hybride dreigingen houden immers niet op bij landsgrenzen. Bij de NAVO-Top in Madrid 2022 is daarom ook het oude *Civil Emergency Planning Committee* (CEPC) omgedoopt en gerevitaliseerd in het NATO *Resilience Committee* (RC). Deze RC is het adviserend orgaan voor weerbaarheid en maatschappelijke gereedheid van bondgenoten.

Er zijn belangrijke richtlijnen opgesteld waaraan landen zich hebben gecommitteerd en waarmee landen hun weerbaarheid op orde moeten hebben.

> 'Each NATO member country needs to be resilient against military and non-military threats and challenges to the Alliance's security, such as natural disasters, disruption of critical infrastructure, or hybrid or armed attacks. Resilience is both a national responsibility and a collective commitment rooted in Article 3 of the North Atlantic Treaty.'[157]

Tijdens de NAVO top in Vilnius in juli 2023 hebben de NAVO-bondgenoten besloten de requirements om te zetten in concrete weerbaarheidsdoelen (*'resilience objectives'*). Nederland is in het najaar 2023 begonnen met de nationale invulling van deze doelen, waarbij de NCTV het proces coördineert.

De AIV ziet de NAVO-requirements als zeer belangrijk en essentieel voor de inrichting van maatschappelijke weerbaarheid. Noodzakelijk bij het aanwijzen van nationale weerbaarheidsdoelen is dat maatschappelijke stakeholders zoals bedrijven, financiële instellingen en kennisinstellingen worden betrokken evenals partnerlanden.

Evenwel stelt de AIV vast dat de voorgestelde weerbaarheidsdoelen van de NAVO met name gericht zijn op fysieke civiele weerbaarheidsdoelen. Minder aandacht is er voor de dreigingen vanuit de virtueel-informatieve en cognitieve dimensie. Derhalve zal de NCTV zich erop moeten richten om dit type dreigingen te integreren in de veiligheidsanalyses. En Nederland zal binnen de NAVO nadrukkelijk aandacht moeten vragen voor dreigingen in de virtueel-informatieve en cognitieve dimensie.

► 5.7 De NVR, een kwetsbaarheidsanalyse en de weerbaarheidsstrategie

Het uitgangspunt voor de collectieve weerbaarheid van de NAVO is de nationale kwetsbaarheids-analyse. Hierbij brengen landen jaarlijks in beeld waar, geredeneerd vanuit de '*7 baseline requirements*', de kwetsbaarheden zitten. Tevens komen landen dan met een gericht plan-van-aanpak om de kwetsbaarheden weg te werken.

Daarbij gaat het niet alleen om het blijven functioneren van de nationale samenleving maar ook om hoe die nationale samenleving de inzet van de nationale krijgsmacht kan blijven ondersteunen alsmede de inzet van de NAVO als geheel. Een treffend voorbeeld voor Nederland hierbij is het '*Host Nation Support*'. Hierbij is Nederland transitland voor verplaatsende troepen uit onder andere de VS, Canada en Groot-Brittannië en speelt met zijn infrastructuur een belangrijke rol bij de ondersteuning en instandhouding van de NAVO-troepen.

Dit vraagt van Nederland om een proactieve, anticiperende en geïntegreerde benadering van de gehele overheid en samenleving. Thans is bij oefeningen in het kader van de troepenverplaatsingen Nederland aangewezen als '*Host Nation Support*'. Dat betekent dat Nederland op het moment van grootschalige verplaatsing van militairen en materieel volop in beweging is met grootschalig gebruik van de spoorwegen, havenwerken, logistieke processen, vliegbases, alles aangestuurd door het Territoriaal Operationeel Centrum (TOC) van de landmacht. Maar deze taakstelling binnen de NAVO is nog te veel aangestuurd vanuit het ministerie van Defensie, samen met andere betrokken civiele stakeholders. Dit geldt ook voor het PESCO-project van de EU waarbij Nederland een belangrijke coördinerende logistieke rol heeft. Dergelijke oefeningen zouden nadrukkelijker ingebed kunnen in het nationale bewustzijn van Nederlanders; burgers zouden hieraan actiever kunnen bijdragen.

Volgens de AIV zou de in 2022 opgerichte Nationale Veiligheidsraad (NVR) hiervoor het aangewezen overkoepelend orgaan moeten zijn. De NVR dient tenminste twee keer per jaar te kijken naar de veiligheidssituatie van Nederland. De eerste keer doet de NVR dit gebaseerd op een dreigingsanalyse van de MIVD, AIVD en NCTV, waarbij de overheid zich richt op het in beeld brengen van de dreigingen door potentiële tegenstanders en actoren en de reactie daarop. De tweede keer dient de NVR te kijken naar de Nederlandse overheid en samenleving en naar de vitale processen: hoe kwetsbaar is de samenleving? Wat kan de overheid doen om, preventief, die kwetsbaarheid te verminderen? En wat kan de samenleving zelf daaraan bijdragen?

Bij het opstellen van deze kwetsbaarheidsanalyses kunnen specifieke maatschappelijke sectoren zelf het voortouw nemen; binnen een sector weet men immers het beste waar de mogelijke dreigingen liggen. Ter voorbereiding op behandeling in de Nationale Veiligheidsraad dienen de verschillende sectorale aanpakken vervolgens te worden samengebracht tot een overkoepelende kwetsbaarheidsanalyse, afgestemd en geanalyseerd op sector-overstijgende impact om fragmentatie tegen te gaan.

De Nationale Veiligheidsraad zal naast een kwetsbaarheidsanalyse vervolgens ook een 'weerbaarheids-strategie' moeten opstellen, specifiek gericht op hybride dreigingen. Hierbij zal vanuit de vitale processen geredeneerd een duidelijke politieke keuze moeten worden gemaakt over welke belangen verdedigd dienen te worden, en met welk doel bepaalde beleidskeuzes worden gemaakt. Hierbij zal ervoor moeten worden gewaakt dat dit geïsoleerd en gefragmenteerd wordt opgesteld en dient de NVR intersectoraal te opereren.

► 5.8 Institutionele versterking van de NVR

De NVR dient op een andere manier te worden ingericht, zo stelt de AIV. Thans is de raad nog 'slechts' een onderraad, waar lang niet alle departementen of stakeholders bij zijn aangesloten. Ook heeft het huidige orgaan geen executieve aanwijzingsmogelijkheden. Vanwege de huidige inrichting lijkt de NVR een te nauwe blik op de nationale veiligheid te hebben. Omdat hybride conflictvoering zoveel sectoren raakt, is binnen de NVR een veel bredere benadering noodzakelijk. Er kan immers een aanval plaatsvinden op een veel breder terrein dan enkel de 'klassieke' veiligheidsdomeinen.[158]

De NVR zal derhalve, zo vindt de AIV, versterkt moeten worden waarbij horizontale en verticale integratie geborgd is en de raad idealiter zoveel mogelijk boven de ministeries komt te staan, direct vallend onder de minister-president. Alle departementen dienen in de NVR zitting te nemen evenals veiligheidsdiensten, bedrijven en kennisinstellingen. Ook de financiële sector moet worden vertegenwoordigd, dat kan bijvoorbeeld via opneming van de TCO binnen de NVR (zie hoofdstuk 2). Daarbij dient er, volgens de AIV, nadrukkelijker aandacht te zijn voor de dreigingen in de virtueel-informatieve en cognitieve dimensies.

Om bovenstaande kwetsbaarheidsanalyses en weerbaarheidsstrategieën centraler te beleggen, aan te sturen en af te stemmen is een voorportaal of een hoog ambtelijk executief comité voor de Nationale veiligheidsraad vereist. Dit voorportaal of ambtelijk comité dient te worden ondersteund door een eigen secretariaat.

► 5.9 Een andere institutionele vorm

Naast een andere en bredere inrichting van de NVR, kan ook worden gedacht aan een ander type orgaan. Omdat hybride dreigingen feitelijk alle ministeries raken, en weerbaarheid een breed-maatschappelijk vraagstuk is, zou het volgens de AIV verstandiger zijn om een overkoepelende governance-structuur in te richten.

HCSS publiceerde recent een uitvoerige studie over de manier waarop de Nederlandse regering een adequate respons ten aanzien van hybride dreigingen kan inrichten. Het rapport spreekt over een "proactieve counter hybride respons", hetgeen inhoudt dat er bij aanvallen niet alleen gereageerd wordt, maar dat de Nederlandse overheid daadwerkelijk op vijandigheden anticipeert.[159] Hierbij moet de overheid op zoek naar maatregelen die de eigen weerbaarheid versterken en tegelijk ook het vermogen van tegenstanders verzwakt, mits, zo maakt HCSS duidelijk, mits dit wenselijk en toelaatbaar is en valt binnen de wettelijke kaders waaraan Nederland zich als liberale democratie conformeert.

Deze 'counter hybride campagne' zou strategische, tactische en operationele actoren effectief met elkaar verbinden. Essentieel hiervoor is dat overheden, bedrijven en kennisinstellingen, maar ook de krijgsmacht en samenleving, beter op elkaar zijn afgestemd. Net als HCSS stelt de AIV dat de Nederlandse overheid hiertoe institutionele of juridisch kaders moet creëren om domein overstijgende samenwerking te stroomlijnen. Tevens is voor een geïntegreerde counter hybride campagne politiek draagvlak nodig.

Deze counter-hybride benadering vraagt om een veerkrachtige samenleving. En deze veerkracht moet ook resoneren in de governance-structuur. Daarom moet weerbaarheid en veerkrachtsvraagstukken ook nadrukkelijk belegd worden. In het Verenigd Koninkrijk kent men daartoe een staatssecretaris van *'Communities and Resillience'*, geplaatst binnen het *Ministry of Housing, Communities & Local Government*. Deze houdt zich intensief bezig met een breed palet aan maatschappelijke weerbaarheids- en veerkrachtsvraagstukken zoals de kustwacht, waterwegen, crisismanagement in noodsituaties, financiële crises, de havenwerken, ondersteuning van lokale overheden, bedrijven enzovoorts. Voor Nederland zou het instellen van een minister of staatssecretaris voor maatschappelijke weerbaarheid ook een mogelijkheid kunnen zijn. Deze zou de brede maatschappelijke impact van hybride dreigingen kunnen adresseren en de maatschappelijke weerbaarheid in de samenleving kunnen vergroten.

Eindnoten

1 'Adviesaanvraag inzake hybride dreigingen', de minister van Defensie en de minister van Buitenlandse Zaken, 12 juli 2022.

2 Rodrigue Demeuse en Joelle Garriaud-Maylam (2023), 'The Russian war on Truth. Defending allied and partner democracies against the Kremlin's disinformation campaigns', General Report, 8 oktober.

3 'Undermining Ukraine. How Russia widened its global information war in 2023', Atlantic Council, Research report, 29 februari 2024.

4 'Tsjechische geheime dienst: "Rusland betaalde cash aan bevriende Nederlandse en Europese politici"', Algemeen Dagblad, 28 maart 2024.

5 Minister van Binnenlandse Zaken en Koninkrijksrelaties. 'Reactie op verzoek van het lid Wilders over het bericht dat de Tsjechische geheime dienst Rusland cash betaalde aan Nederlandse en Europese politici', 1 april 2024.

6 Paul Charon en Jean-Beptiste Jeangène Vilmer (2021), 'Chinese Influence operations. A Machiavellian Moment', IRSEM.

7 'Met de rug naar de samenleving. Een analyse van de soevereinenbeweging in Nederland', AIVD-rapport 9 april 2024. Soevereinenbeweging ondermijnt democratische rechtsorde | Nieuwsbericht | AIVD

8 Unesco | Droogmakerij de Beemster (Beemster Polder)

9 Cybersecurity vitale waterwerken niet waterdicht | Nieuwsbericht | Algemene Rekenkamer

10 Rob de Wijk, Frank Bekkers en Tim Sweijs, 'Hybride dreigingen en hybride oorlog: consequenties voor de Koninklijke Landmacht', HCSS Security rapport, 15 oktober 2020.

11 Hierbij valt te verwijzen naar de *theory of unrestricted warfare* van de Chinese militair-theoretici Qiao Liang en Wang Xiangsui of de *compound warfare* van Thomas Huber. Vgl. Qiao Liang en Wang Xiangsui, *Unrestricted warfare* (Beijing 1999); Thomas M. Huber (red.), *Compound warfare. That fatal knot* (Pacific University Press, Forest Grove, Or. 2004). Hoffman, 2007, p. 8.
De feitelijke grondlegger van de hedendaagse Westerse interpretatie van het concept 'hybrid warfare' is Frank G. Hoffman geweest. Hij paste rond 2007 het concept toe op de asymmetrische conflictvoering tussen de staat Israël en de niet-statelijke actoren (proxy-milities) zoals Hezbollah en Hamas.

12 'Adviesaanvraag inzake hybride dreigingen', de minister van Defensie en de minister van Buitenlandse Zaken, 12 juli 2022.

13 David Kimsey, Jin Woo Kim, John McCoy e.a., 'Utilization of the DIMEFIL Framework in a Case Study Analysis of Security Cooperation Success', *Small Wars Journal*, 11 augustus 2020.

14 'Hybrid and cyber-threats by foreign actors', European Commission, Competence Centre on Foresight, 21 december 2021.
Vgl. M. Normark (2019), 'How states use non-state actors: a modus operandi for covert state subversion and malign networks, Hybrid CoE.'
AIVD-jaarverslag 2021. Jaarverslag AIVD 2021 | Tweede Kamer der Staten-Generaal
Vgl. 'China vormt grootste bedreiging voor kennisveiligheid, zegt de AIVD', 17 april 2023. China vormt grootste dreiging voor kennisveiligheid, zegt de AIVD - ScienceGuide

15 Martin Crilly and Alan Mears, 'Multi Dimensional and Domain Operations (MDDO)', Warvell Room, 26 januari 2022. https://wavellroom.com/2022/01/26/mddo/

16 Zsolt Haig en Veronika Hajdu (2017). 'New ways in the cognitive dimension of information operations', *Land Forces Academy Review*, 22(2).

17 Petra Vejvodová (2019), 'Information and psychological operations as a challenge to security and defence', *Czech Military Review*, no. 3, 83-96. DOI: 10.3849/2336-2995.

18 RAND (2019), 'The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment', Research report.

19 'Cognitive Warfare. Strengthening and Defending the Mind', NATO's Strategic Warfare Development Command, 5 april 2023.

[20] Georgii Pocheptsov (2018), 'Cognitive Attacks in Russian Hybrid Warfare', Information & Security. *An International Journal, vol. 41, pp. 37-43.*

[21] Yuriy Danyk, Chad M. Briggs, 'Modern Cognitive Operations and Hybrid Warfare', *Journal of Strategic Security, Vol. 16, no. 1 (2023) 35-50*. Vgl. 'The Emerging Risk', RAND.

[22] Pocheptsov, 'Cognitive Attacks'.

[23] Sandor Fabian. (2019). 'The Russian hybrid warfare strategy – neither Russian nor strategy', Defense & Security Analysis: Vol 35, No 3 (tandfonline.com); Vgl. Frank G. Hoffman (2007), 'Conflict in the 21st century: the rise of hybrid wars', Potomac Institute for Policy Studies. Arlington, Virginia.

[24] NCTV (2023). 'Veiligheidsstrategie voor het Koninkrijk der Nederlanden', zie voor Europese definities en benaderingen ook: Dick Zandee, Sico van der Meer, Adaja Stoetman (2021). 'Countering hybrid threats. Steps for improving EU-NATO-cooperation', Clingendael rapport.

[25] Overzicht vitale processen, zoals opgesteld door de NCTV: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

[26] AIVD, MIVD, NCTV, 'Dreigingsbeeld Statelijke Actoren 2', november 2022; Rijksbrede Risicoanalyse Nationale Veiligheid | Rapport | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl); Beschermen democratische processen en instituties | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl);

[27] AIVD, MIVD, NCTV (2021). 'Dreigingsbeeld Statelijke Actoren'.

[28] Soevereinenbeweging ondermijnt democratische rechtsorde | Nieuwsbericht | Rijksoverheid.nl

[29] De Wetenschappelijke Raad voor het Regeringsbeleid werkt momenteel aan een advies dat uitvoerig ingaat op het functioneren van de democratie en het gebruik van media. Zie: https://www.wrr.nl/adviesprojecten/media-en-democratie

[30] 'Regulering van online content. Naar een herijking van het Nederlandse internetbeleid', AIV-advies, 113, 24 juni 2020.

[31] 'Migrants say Belarusians Took them to E.U. Border and Supplied Wire Cutters', *The New York Times*, 14 november 2021. Migrants Say Belarusians Took Them to E.U. Border and Supplied Wire Cutters - The New York Times (nytimes.com) Vgl.: Desperate Iraqis the latest pawn in Belarus standoff with EU | CBC News; Baghdad to Lithuania: how Belarus opened new migration route to EU – LRT Investigation - LRT

[32] Monica den Boer en Mark Helgers (2022), 'Schermutselingen aan de Europese buitengrens. Tijd voor een integrale strategie', *Militaire Spectator, jrg. 191, no. 7/8, 410-421.*

[33] Alexander Leeuw (2021), 'Dagelijks duizend cyberaanvallen bij een waterschap', *Binnenlands Bestuur*, 6 september.

[34] Beleidsnota Drinkwater 2021-2026. 'Samen werken aan een toekomstbestendige drinkwatervoorziening', Ministerie van Infrastructuur en Waterstaat. P.11. Vgl. https://www.trouw.nl/binnenland/hoe-kwetsbaar-is-onze-drinkwatervoorziening~bf1b14ee/

[35] First Chinese freight train arrives in Serbia - Xinhua | English.news.cn (xinhuanet.com)

[36] Joris Teer and Mattia Bertolini, 'Reaching Breaking Point: The Semiconductor and Critical Raw Material Ecosystem at a Time of Great Power Rivalry', HCSS, oktober 2022.

[37] Rekenkamer: veel mis met digitale beveiliging van Schiphol (nos.nl)

[38] Zo bepleitten de vicevoorzitter van de Europese Commissie Margaritis Schinas en de Eurocommissaris voor Volksgezondheid Stella Kyriakides: https://netherlands.representation.ec.europa.eu/europa-heeft-een-nieuwe-aanpak-op-het-gebied-van-geneesmiddelen-nodig_nl

[39] Het faillissement in 2022 van de grote medicijnenfabriek InnoGenerics – verantwoordelijk voor o.a. patentvrije medicijnen – zonder dat direct duidelijk is op welke manier Nederland een noodvoorraad medicijnen kan opbouwen, baart de AIV dan ook zorgen.

[40] Chris Miller, (2024), 'Taiwan's security came into question just when they became an irreplaceable supplier of chips', Atlantische Commissie, 18 January. Vgl. Joris Teer, Mattia Bertolini, and Benedetta Girardi (2023), 'Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland: De risico's van Russisch gas, Chinese grondstoffen en Taiwanese Chips', onderzoeksrapport The Hague Center for Strategic Studies (HCSS), maart. https://hcss.nl/news/great-power-competition-and-social-stability-in-the-netherlands/.

41 'Bestuurlijke netwerkkaarten crisisbeheersing', Netwerkkaart 27: Financieel verkeer. Instituut Fysieke Veiligheid, februari 2021.
42 Ibidem.
43 Ibidem.
44 'Begroting Monetaire Zaken 2023', De Nederlandsche Bank,
Vgl. 'Bestuurlijke netwerkkaarten crisisbeheersing'. Netwerkkaart 27: Financieel verkeer. Instituut Fysieke Veiligheid, februari 2021.
45 'Grote interesse bij bedrijven voor ontwikkeling van een nieuwe onderzeese datakabel die Londen en Rotterdam verbindt', Dutch Data Center Association, 14 september 2023. Grote interesse bij bedrijven voor ontwikkeling van een nieuwe onderzeese datakabel die Londen en Rotterdam verbindt - Dutch Data Center Association (dutchdatacenters.nl)
46 Vgl. 'Een onderzeese datakabel tussen Londen en Rotterdam voor een betrouwbaarder internet', Innovation Origins, 16 september 2023.
47 'Undersea 'hybrid warfare' threatens security of 1bn, Nato commander warns', The Guardian, 16 April 2024.
48 Frank Bekkers en Esther Chavannes (2019), 'Geopolitiek en maritieme veiligheid. De visie van HCSS op de toekomstige inrichting van de Koninklijke Marine', *Marineblad, december*.
49 https://www.rijksoverheid.nl/actueel/nieuws/2023/12/19/defensie-koopt-middelen-en-materieel-om-noordzee-te-beschermen
50 Zie voor de Zeekabel Coalitie: https://ecp.nl/project/zeekabel-coalitie/
51 Cybersecuritybeeld Nederland, 4 juli 2022. Cybersecuritybeeld Nederland 2022 | Tweede Kamer der Staten-Generaal
52 Het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Justitie en Veiligheid wordt samengebracht met het Computer Security Incident Response Team voor digitale diensten (CSIRT-DSP) en het Digital Trust Center (DTC) van het Ministerie van Economische Zaken en Klimaat.
53 'Rapportage datalekken 2023', Autoriteit Persoonsgegevens, 10 april 2024.
54 De AIV vindt dat bedrijven hierin een nadrukkelijk nationaal belang dienen hier ook de erkenning voor moeten krijgen. De toekenning van de OKTT-status ('objectief kenbaar tot taak') door minister van Justitie en Veiligheid aan de Stichting NL CISO Circle of Trust (CCoT) is hierin een positieve ontwikkeling. Zie: https://www.ncsc.nl/actueel/nieuws/2023/september/28/stichting-ciso-circle-of-trust-verkrijgt-oktt-status Zo bleek ten tijde van de bankencrisis in 2008, maar ook recenter in 2022 toen de bank Credit Suisse in zeer korte tijd miljarden euro's verloor vanwege berichtgeving over financiële malversaties, speculaties en wanbestuur. Uiteindelijk kon de bank worden gered; evenwel was er sprake van grote paniek in de financiële sector in Europa, ook in Nederland.
55 Te weten de NCC-Group (voorheen: Fox-IT).
56 Alexandre Gomes en Maaike Okano-Heijmans (2024), 'Too late to act. Europe's quest for cloud sovereignty', Clingendael rapport, maart.
57 Vgl. Advies 'Autonome wapens. Het belang van reguleren en investeren', advies AIV en CAVV, 3 december 2021.
Zie ook het interview met prof. dr. Bart Schermer, 12 mei 2021. https://ddma.nl/kennisbank/bart-schermer-consideratie-met-een-ethische-werkwijze-hoef-je-niet-bij-elke-nieuwe-wet-je-businessmodel-aan-te-passen/
58 Bart Schermer (2022) 'De gespannen relatie tussen privacy en cybercrime'. Oratie uitgesproken aan de Universiteit Leiden, 7 november 2022.
59 Kamerbrief 'Voortgang aanpak kennisveiligheid hoger onderwijs en wetenschap', 23 december 2022.
60 Dit geldt met name ook voor instellingen zoals DUO en de houding ten aanzien van studenten met een migratie-achtergrond. Vgl. https://www.rijksoverheid.nl/actueel/nieuws/2024/03/01/kabinet-maakt-excuses-voor-indirecte-discriminatie-bij-controles-op-de-uitwonendenbeurs
Zie ook: https://www.nrc.nl/nieuws/2024/03/01/rapport-indirecte-discriminatie-bij-controles-op-fraude-met-uitwonendenbeurs-a4191795
61 'Curacao ligt aan de ketting van een land in crisis', NRC, 13 januari 2018.
62 'Meeting Guyana-Venezuela negotiations', The Guardian, 14 december 2023.

63 De spanningen tussen Nederland en Venezuela aangaande de ABC-eilanden spelen al langer dan een eeuw. In de periode 1902 - 1908 bracht het beide landen zelfs bijna in oorlog.

64 'Venezuela Country Focus', European Union Agency for Asylum research report', november 2023, Rafael Romo, 'Maduro's immigration card could influence America's election, not just Venezuela's'. CNN, 7 februari 2024.

65 Vgl. 'Veiligheid en rechtsorde in het Caribisch gebied. Noodzakelijke stappen voor een toekomstbestendig Koninkrijksverband', AIV-advies 116, 10 september 2020.

66 https://www.rijksoverheid.nl/documenten/woo-besluiten/2023/05/26/besluit-op-woo-verzoek-over-machtigingen-onderzeekabel-saba-en-sint-eustatius

67 Vgl. Veiligheid en rechtsorde in het Caribisch gebied. Noodzakelijke stappen voor een toekomstbestendig Koninkrijksverband | Publicatie | Adviesraad Internationale Vraagstukken; blz 9.

68 Rob de Wijk, Frank Bekkers en Tim Sweijs, 'Hybride dreigingen en hybride oorlog: consequenties voor de Koninklijke Landmacht', HCSS Security rapport, 15 oktober 2020.

69 Brin Najžer, *The Hybrid Age. International Security in the Era of Hybrid Warfare* (Bloomsbury Publishing Plc, Londen, New York, Dublin, 2020).

70 David Ignatius, 'Is Russia trying to sway the U.S. election?', Belfer Center for Science and International Affairs, 31 juli 2016.
Christian Kaunert, 'EU Eastern Partnership, Hybrid Warfare and Russia's Invasion of Ukraine', 11 augustus 2022.

71 'De Oekraine-oorlog als geopolitieke tijdschok', AIV briefadvies 20 oktober 2022.
Vgl. Frans Osinga, 'Putin's War, A European Tragedy. Why Russia's War Failed and What It Means for NATO' (2024), in: Maarten Rothman, Lonneke Peperkamp en Sebastiaan Rietjens (red), *Reflections on the Russia-Ukraine War*. Leiden University Press, 123-146.

72 Michael Connell en Sarah Vogler, 'Russia's Approach to Cyber Warfare', CNA research paper, maart 2017.

73 S.C. Morrell en M.E. Kosal, 'Military Deception and Strategic Culture. The Soviet Union and Russian Federation', *Journal of Information Warfare, vol. 20, no. 3 (zomer 2021), 127-145*; Michael Kofman, 'Russian Hybrid Warfare and the other Dark Arts', War on the Rocks, 11 maart 2016.

74 Rusland is actief in zowel de fysieke als virtuele en cognitieve dimensie. Verschillende groepen die actief zijn in het cyberdomein worden getolereerd – bijvoorbeeld criminele organisaties die hun geld verdienen met ransomware-aanvallen op niet-Russische bedrijven en overheden – dan wel actief strategisch ingezet door de Russische overheid. Dit blijkt onder meer uit een analyse over verschillende cybersabotagegroepen die gelieerd zijn aan de Russische militaire inlichtingendienst GRU, zoals de cybergroep Sandworm. Sandworm wordt in verband gebracht met 'Eenheid 74455', het hoofdcentrum voor Speciale Technologieën van de GRU. Deze eenheid is opgericht om via cyberoperaties de Oekraïense krijgsmacht en samenleving te ondermijnen. Tot de belangrijkste drie taken van deze eenheid behoren cyberspionage, actieve cyberaanvallen en online psychologische beïnvloeding, ook worden door deze taken operaties in de conventionele oorlogsvoering ondersteund. In een uitvoerige analyse van deze eenheid, door Mandiant, internationaal toonaangevend op het gebied van cyberveiligheid en cyberinlichtingen en onderdeel van Google, wordt beschreven hoe de cyberoperaties van deze eenheid door de jaren heen ook buiten Oekraïne plaatsvonden, met grote gevolgen voor vrije samenlevingen, ngo's, journalisten, het maatschappelijk middenveld, kennisinstellingen en bedrijven. Ook multilaterale instellingen zoals de OPCW zijn doelwit. Dit is de reden dat Google deze groep nu kenmerkt als een 'Advanced Persistent Threat' (APT44).
Zie ook de veroordeling van de EU-lidstaten van Russische cyberactiviteiten t.b.v. APT28, oftewel Fancy Bear: 'Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation', 3 mei 2024.
Cyber: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation - Consilium (europa.eu)
Zie: Gabby Roncone, Dan Black, John Wolfram (e.a.), 'APT44: Unearthing Sandworm', Mandiant-Google rapport, 2024.
Vgl. Google's Mandiant elevates Russian threat group Sandworm to APT44 | Cybernews

[75] Vgl. Dmitry Adamsky (2023), *The Russian Way of Deterrence. Strategic Culture, Coercion, and War*. Stanford University Press.

[76] AIV-advies, 'De Oekraïne-oorlog als geopolitieke tijdschok', 20 oktober 2022.

[77] Michael Raska, 'China and the 'Three warfares'', The Diplomat, 18 december 2015.

[78] Het meest urgente voorbeeld is de claim dat Taiwan onderdeel is van China, wat een annexatie door inname zou legitimeren. Winning Without Fighting: Chinese Legal Warfare | The Heritage Foundation

[79] 'China spins tale that the U.S. Army stated the Coronavirus Epidemic', The New York Times, 13 maart 2020.

[80] Andrew Scobell en Larry M. Wortzel, 'The Chinese Way of War', in John Andreas Olsen, and Martin van Creveld (eds), *The Evolution of Operational Art: From Napoleon to the Present* (Oxford, 2010; online edn, Oxford Academic, 1 Jan. 2011)

[81] Xi Jinping (2020) 'Major Issues Concerning China's Strategies for Mid-to-Long-Term Economic and Social Development', CSIS Interpret: China, 31 October, 3.
Vgl.: Timothy R. Heath, Derek Grossman, Asha Clark, 'China's Quest for Global Primacy. An Analysis of Chinese International and Defense Strategies to Outcompete the United States', (2021), RAND onderzoeksrapport.

[82] Aukia, J. (2021). 'China as a hybrid influencer: non-state actors as state proxies', Hybrid CoE. Research report No. 1.

[83] J. Willard, 'The US and hybrid challenges: past, present and future', in: M. Weissmann, N. Nilsson en B. Palmertz (red.), *Hybrid warfare: security and asymmetric conflict in international relations* (Bloomsbury Collections 2022) pp. 157-172; I. Käihkö, 'The evolution of hybrid warfare implications for strategy and the military profession', *The US army war college quarterly: parameters*, 51(3), 2021, pp. 115-127.

[84] https://smallwarsjournal.com/jrnl/art/counter-hybrid-warfare-winning-gray-zone

[85] VS, DoD Cyber Strategy, Fact Sheet (2023).

[86] Jens Stoltenberg, de Secretaris-Generaal van de NAVO, gaf in 2015 woorden aan de veelzijdige betekenis van hybride dreigingen voor de NAVO toen hij sprak: "*Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them.*"
Keynote speech Jens Stoltenberg, Secretaris-Generaal NAVO, 25 maart 2015.

[87] NATO - Topic: NATO's response to hybrid threats

[88] Dit programma investeert via een groot subsidieprogramma in de ondersteuning en ontwikkeling van nieuwe technologie. Hierbij is met name aandacht voor het bijeenbrengen van wetenschappers, ingenieurs, de industrie de eindgebruikers (de overheden)
Zie voor het DIANA programma van de NAVO: https://www.diana.nato.int/about-diana.html

[89] NATO - Topic: Relations with Asia-Pacific partners

[90] Dick Zandee, Sico van der Meer en Adaja Stoetman (2021), 'Countering hybrid threats: steps for improving EU-NATO cooperation', Clingendael rapport.

[91] Zie voor het NATO Strategic Communications Centre of Excellence: StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia (stratcomcoe.org)

[92] action_plan_against_disinformation.pdf (europa.eu)

[93] Non-intervention provisions in the United Nations Charter; Helsinki Final Act of 1975; 1990 Paris Charter; 1997 Treaty of Friendship, Cooperation and Partnership between Russia and Ukraine; 1994 Budapest Memorandum on Security Assurances.
Vgl. The Crimean Factor: How the European Union Reacted to Russia's Annexation of Crimea | Warsaw Institute

[94] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

[95] Voor een toelichting op artikel 42 lid 7 van het Verdrag betreffende de Europese Unie inzake 'Collectieve verdediging'.
Vgl. Verslag Vaste Kamercommissie voor Defensie inzake overleg over de Defensienota 2022, 6 oktober 2022. Defensienota 2022 - Sterker Nederland, Veiliger Europa | Tweede Kamer der Staten-Generaal

[96] P.A.L. Ducheine en B.M.J. Pijpers, 'Cyberoperaties en de EU', *Militaire Spectator*, 1 augustus 2022.

[97] What is Hybrid CoE? - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats

[98] Voor de EU Hybrid Toolbox zie: https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/
Vgl. Kenneth Lasoen (2022), 'Realising the EU Hybrid Toolbox: opportunities and pitfalls', Clingendael Policy Brief, december.

[99] Vgl. https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/

[100] CCDCOE

[101] Volgens het Strategisch Kompas van de EU worden hybride activiteiten ingezet om de kwetsbaarheden van de tegenstander uit-te-buiten en in het eigen voordeel te laten werken. Hierbij worden verschillende instrumenten op een gecoördineerde wijze ingezet, waarbij nooit de grens van formele oorlogvoering wordt gepasseerd. Vgl. Factsheet 'Countering Hybrid Threats', Strategisch Kompas Europese Unie, Maart 2022.

[102] Jakob Albers, 'Is Europa's antwoord op China's Nieuwe Zijderoute meer dan een druppel in de oceaan?', MO Magazine, 17 maart 2023.

[103] Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe (2019), 'Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War', RAND Corporation.

[104] Morris (2019), 45.

[105] Morris (2019), 53-57.

[106] https://www.zeit.de/gesellschaft/zeitgeschehen/2017-12/fancy-bear-russland-hacking-ap-us-geheimdienst

[107] https://duitslandinstituut.nl/artikel/58396/rusland-heeft-top-duitse-luchtmacht-afgeluisterd

[108] Rob de Wijk, Frank Bekkers en Tim Sweijs, 'Hybride dreigingen en Hybride oorlog. Consequenties voor de Koninklijker Landmacht', HCSS rapport 15 oktober 2020.

[109] Vgl. Richtsje Kurpershoek, Alejandra Munoz Valdez en Wim Zwijnenburg (2021), 'Remote Horizon. Expanding use and proliferation of military drones in Africa', Pax for Peace onderzoeksrapport.

[110] 'Elon Musk bezoekt met premier Netanyahu verwoeste kibboets', NOS, 27 november 2023. https://nos.nl/video/2499464-elon-musk-bezoekt-met-premier-netanyahu-verwoeste-kibboets

[111] Alvaro Pastor (2024), 'Cognitive warfare', HAL open science.

[112] A. Nollkaemper, *'Kern van het internationaal publiekrecht'*, negende druk, Boom Juridische Uitgevers, Den Haag, 2022, p 343, onder noot 4; Zie in dit kader ook de Talinn Manual 2.0 – On the International Law Applicable to Cyberoperations 2nd edn, MN Schmitt (ed) (Cambridge University Press 2017), die zich toespitst op hoe het *jus ad bellum* and *jus in bello* (IHR) van toepassing zijn op cyberoperaties.

[113] Nollkaemper, p. 242 en IGH, Military and Paramillitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgement, I.C.J. Reports 1986, par. 205.

[114] Vgl. AIV-advies: 'Autonome wapens. Het belang van reguleren en investeren', december 2021, 32,33. Zie verder: Berenice Boutin, 'Legal Questions Related to the Use of Autonomous Weapon Systems'. Paper prepared for the AIV/CAVV Combined Advisory Committee on updating the Advice on Autonomous Weapons (CAAW). Asser Instituut, juni 2021. Vgl. voor een nadere juridische uitwerking ook: Linell A Letendre, 'Lethal Autonomous Weapon Systems: Translating Geek Speak for Lawyers', International Law Studies, vol. 96 (2020), pp. 278-282.

[115] R. Heinsch, 'International Humanitarian Law', in: C Rose at al (eds), *An Introduction to Public International Law* (Cambridge University Press, 2022) p. 234.

[116] Ibidem.

[117] Vgl. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en

[118] J. Brown (2018), 'An alternative war: The development, impact, and legality of hybrid warfare conducted by the nation state', Journal of Global Faultlines, Vol. 5, No. 1-2 (October-December), pp. 58-82.

[119] https://data.consilium.europa.eu/doc/document/PE-34-2023-REV-1/en/pdf en www.wto.org

[120] Nollkaemper, p 408 en IGH, Legality of the Use by a State of Nuclear Weapons in Armed Conflict, Advisory Opinion, ICJ Reports 1996, par 29.

[121] Vgl. AIV-advies: 'Autonome wapens. Het belang van reguleren en investeren'.

[122] https://www.cyber-diplomacy-toolbox.com

[123] Verslag van een schriftelijk overleg over de Internationale Cyberstrategie. Tweede kamer (2023).

[124] CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence. Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO

[125] J. Brown (2018). 'An alternative war: The development, impact, and legality of hybrid warfare conducted by the nation state', Journal of Global Faultlines.

[126] Brown (2018).

[127] Mark Galeotti, (2022), *The Weaponization of Everything. A Field Guide to the New Way of War.* Yale University Press. New Haven.

[128] Toelichting artikel 97GW: Artikel 97: Krijgsmacht - Nederlandse Grondwet (denederlandse-grondwet.nl)
K.T. Meijer, 'Artikel 97 Grondwet. Wetenschappelijk commentaar', geschreven op basis van het commentaar bij art. 97 GW door J. van Schooten-van der Meer in: A.K. Koekkoek (red.), De Grondwet. Een systematisch en artikelsgewijs commentaar, Deventer: W.E.J. Tjeenk Willink, 3e dr. 2000 (alsook de 2e dr. 1992). Zie: Nederlandsche Rechtsstaat. Over grondwet en rechtsstaat, te raadplegen via: Krijgsmacht - Nederland Rechtsstaat

[129] Meijer, Artikel 97.

[130] Meijer, Artikel 97. Voor de Defensienota 2000 zie: Kamerstukken II 1999/2000, 26900, nrs. 12, Defensienota 2000, p. 41. Minister van Defensie aan de voorzitter van de Tweede Kamer, 21 september 2021. Kamerstuk 34919, nr. 82 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

[131] Meijer, Artikel 97.

[132] Onderzoeksrapport 'Grondslag gezocht', commissie-Brouwer, 1 december 2022.
Vgl. 'De internetninja's van de krijgsmacht lopen stuk op een privacymuur', NRC, 25 januari 2023.

[133] AIV-advies, 'Keuzes voor de krijgsmacht', maart 2022.

[134] Minister van Defensie aan de voorzitter van de Tweede Kamer, 21 september 2021. Kamerstuk 34919, nr. 82 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

[135] Vgl. Memorie van toelichting. Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van bepalingen inzake de verdediging, 2 juni 1997. Kamerstuk 25367, nr. 3 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

[136] NAVO-verdrag, artikel 3. NATO - Official text: The North Atlantic Treaty, 04-Apr.-1949

[137] Vgl. Memorie van toelichting. Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van bepalingen inzake de verdediging, 2 juni 1997. Kamerstuk 25367, nr. 3 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

[138] Artikel 99a- Grondwet. Wetenschappelijk commentaar door J.M. van Schooten, Gert-Jan Leenknegt en Maurice Adams. In: *Nederlandsche Rechtsstaat. Over grondwet en rechtsstaat*, te raadplegen via: https://www.nederlandrechtsstaat.nl/grondwet/inleiding-hoofdstuk-5-wetgeving-en-bestuur/artikel-99a-civiele-verdediging/

[139] Dit bleek recent uit de jaarlijkse barometer van Clingendael, een opinieonderzoek onder de Nederlandse bevolking https://www.clingendael.org/nl/research-program/buitenland-barometer

[140] Defensie in 2035 | Defensie.nl

[141] Rijksbrede Risicoanalyse Nationale Veiligheid | Rapport | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

[142] David Crossland en Bruno Waterfield, 'Exposed: hard-right European politicians 'on Putin's payroll', The Times, 28 maart 2024.
Vgl. 'Poland investigating Russian espionage, security agency says', Reuters, 28 maart 2024.
Zie ook: David Bremmer, 'Tsjechische geheime dienst: Rusland betaalde cash aan bevriende Nederlandse en Europese politici', Het Parool, 28 maart 2024.

143 'Poland investigating Russian espionage, security agency says', Reuters, 28 maart 2024. 'Kamer wil snel debat over Russisch geld naar Nederlandse politici', Trouw, 28 maart 2024.
144 Aanpak statelijke dreigingen en aanbieding dreigingsbeeld statelijke actoren 2 | Tweede Kamer der Staten-Generaal
145 Ibidem.
146 'Kamerbrief statelijke dreigingen', Tweede Kamer, 28 november 2022.
147 https://www.huoltovarmuuskeskus.fi/en/organisation/the-national-emergency-supply-agency
148 Vgl. Eva Rovers (2022), 'Komen politici er niet uit? In deze landen vragen ze het aan burgers', *De Correspondent*.
149 AIVD, MIVD, NCVT, 'Dreigingsbeeld Statelijke Actoren 2', november 2022
150 Tim Wagemakers (2024), 'Amsterdam wil afvalprobleem aanpakken met een burgerberaad: hoe zinvol is dat?', Het Parool, 4 maart.
151 Zie voor het Netwerk Burgerberaad: https://burgerberaad.nu
Vgl. https://www.binnenlandsbestuur.nl/bestuur-en-organisatie/burgerforum-moet-goed-zijn-ingebed-samenleving-en-politiek
152 Burgerberaden: 'Áls het lukt, dan heb je ook wat' | VNG
153 In 2024 heeft de Europese Raad een burgerberaad uitgezet ten behoeve van het project 'Strengthening democratic resilience through civic participation during the war and in the post-war context in Ukraine'. Vgl: Strengthening democratic resilience through civic participation during the war and in the post-war context in Ukraine - Participatory democracy (coe.int)
Zie ook: The Council of Europe project on civic participation announces the selection of coordinators for Citizens' Assemblies in Ukraine - Council of Europe Office in Ukraine (coe.int)
154 Kenneth Lasoen, 'Realising the EU Hybrid Toolbox. Opportunities and pitfalls', Clingendael Policy Brief, december 2022.
155 Zie ook het model van de Hybrid CoE in Helsinki: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf;
Vgl.: 'Fortifying Defence. Strengthening Critical Energy Infrastructure against Hybrid Threats', European Defence Agency research report, 26 mei 2023.
156 Mark Galeotti, 'Why is Russia jamming plane signals across Europe?', The Spectator, 22 april 2024.
157 Verklaring van de NAVO Resilience Committee, 7 oktober 2022:
https://www.nato.int/cps/en/natohq/topics_50093.htm
158 Jos Heijmans, 'Eindelijk hebben ook wij een nationale veiligheidsraad', RTL Nieuws, 5 november 2022.
159 Gerben Bakker en Tim Sweijs (2024), 'Campagnes tegen hybride dreigingen: een handleiding', The Hague Centre for Strategic Studies onderzoeksrapport.

Geraadpleegde personen

- **Martijn Adelaar**
  Plv. Chef de Poste, Nederlandse ambassade Finland
- **Aleksi Aho**
  Analist, European Centre of Excellence for Countering Hybrid Threats, Helsinki, Finland
- **Stefania Benaglia**
  Hoofd Foreign Policy Unit, Centre for European Policy Studies, Brussel
- **Govert-Jan Bijl de Vroe**
  Ambassadeur, Nederlandse ambassade in Finland
- **Sylvia Bijl**
  Directeur Begroting, Hoofddirectie Finance & Control, Ministerie van Defensie
- **LGen. Elanor Boekholt-O'Sullivan**
  Plv. Directeur-Generaal Beleid, Ministerie van Defensie
- **Prof. dr. BGen. Han Bouwmeester**
  Hoogleraar Militair-operationele wetenschappen, Nederlandse Defensieacademie, Breda
- **Martin van Buuren**
  Beleidsadviseur Ministerie Buitenlandse Zaken
- **Canel Özlem**
  Ambassadeur Nederlandse ambassade in Estland
- **Prof. mr. dr. Carel Stolker**
  Voorzitter commissie-Stolker en voorm. Rector magnificus en voorzitter
  College van Bestuur, Universiteit Leiden
- **Allard Castelein**
  Voorm. Chief Executive Officer, Haven van Rotterdam
- **Vladimir Cibic**
  Chief Security Officer, KPN
- **Tanja Cuppen**
  Chief Risk Officer, ABN AMRO
- **Dr. Ingrid d'Hooghe**
  Coördinator China Centre, Clingendael
- **Koen Davidse**
  Directeur-Generaal Beleid, Ministerie van Defensie
- **Guido Dierick**
  Voorm. Chief Executive Officer, NXP
- **Leen van Duijn**
  Voorm. Vice-President Security Services, KLM
- **Liselot Egmond**
  Strategisch beleidsadviseur bij de Nederlandse permanente vertegenwoordiging in Brussel
- **Gen. Onno Eichelsheim**
  Commandant der Strijdkrachten, Ministerie van Defensie
- **Marc Gazenbeek**
  Plv. Secretaris-Generaal, Ministerie van Defensie
- **Nienke Griffioen**
  Directeur Bankentoezicht, De Nederlandsche Bank
- **Mariliis Gross**
  Plv. Directeur, Nationaal Veiligheid en Defensie Coördinatie Bureau Estland
- **Hannust Dea**
  Beleidsadviseur Estse ambassade in Nederland

- **Hanna Haruaki**
  Beleidsadviseur, National Defence Unit, Ministerie van Defensie Finland
- **Kol. Leen van Hijum**
  Beleidsadviseur, Militair Strategisch Element, Defensiestaf, Ministerie van Defensie
- **LGen. Dick van Ingen**
  Nederlands Militair Vertegenwoordiger bij de NAVO en de EU Military Committee
- **Natalie Jaarsma**
  Speciaal Gezant Cyber en Veiligheid, Ministerie van Buitenlandse Zaken
- **Andres Kangur**
  Beleidsadviseur Ministerie van Algemene Zaken, Finland
- **Janne Känkänen**
  Directeur Nationaal Noodvoorziening Agentschap (NESA), Finland
- **Kirsi Karlamaa**
  Directeur-Generaal Transport en Communicatie Agentschap (Traficom), Finland
- **Vesa Kekäle**
  Adviseur Informatieomgeving, afdeling Rusland, Oost-Europa en Centraal-Azië, Ministerie van Buitenlandse Zaken, Finland
- **Käsper Kivisoo**
  Strategisch adviseur Ministerie van Algemene Zaken, Finland
- **Prof. mr. dr. Geert-Jan Knoops**
  Hoogleraar Politiek van het Internationaal Recht en lead counselor van het Internationaal Strafhof in Den Haag
- **Carry Knoops-Hamburger**
  Directeur Knoops Advocaten en legal assistant Internationaal Strafhof Den Haag
- **Maj. Pherdi de Koning**
  Staf adviseur, Ministerie van Defensie
- **Geert Kuiper**
  Directeur Strategie en Kennis, DG-Beleid, Ministerie van Defensie
- **Eero Kytömäki**
  Adviseur Nationale Veiligheid, Ministerie van Binnenlandse Zaken Finland
- **Roger van Laak**
  Nederlands vertegenwoordiger in het Politiek- en Veiligheidscomité van de Europese Unie
- **Karel Lannoo**
  CEO Centre for European Policy Studies – CEPS, Brussel
- **Carolin Laubre**
  Adviseur Internationale Samenwerking, Ministerie van Defensie Estland
- **Hans van Leeuwe**
  Hoofd Counter Hybrid Unit, Ministerie van Defensie
- **Prof. dr. Lokke Moerel**
  Hoogleraar ICT en Recht, Tilburg University en lid Cyber Security Raad
- **Ir. Erwin Medendorp**
  Manager Integrale Veiligheid, Universiteit van Twente
- **Kol. Vahur Murulaid**
  Defensie Attaché ambassade van Estland
- **Dr. Martin Normaa**
  Directeur Cooperative Cyber Defence Centre of Excellence – CCDCOE NAVO
- **Marje Pihlak**
  Deputy Head of Mission/Counsellor Embassy of Estonia Hague
- **Thijs van der Plas**
  Permanent Vertegenwoordiger bij de NAVO
- **Schout-bij-Nacht Peter Reesink**
  Directeur MIVD, voorm. directeur Operaties Defensiestaf
- **Aernout Reijmer**
  Chief Information and Security Officer, ASML

- **Dr. Sebastian Reyn**
  Plv. directeur MIVD
- **Kusti Salm**
  Secretaris-Generaal Ministerie van Defensie, Estland
- **Fanny Sauvignon**
  Onderzoeker Centre for European Policy Studies – CEPS, Brussel
- **Jukka Savolainen**
  COI directeur Hybrid CoE Finland
- **Prof. dr. Bart Schermer**
  Hoogleraar Privacy en Cybercrime, Universiteit Leiden, lid Commissie Mensenrechten AIV
- **Pieter Henk Schroor**
  Hoofd Resources and Armaments, Nederlandse vertegenwoordiging bij de NAVO
- **Maarten Schurink**
  Secretaris-Generaal, Ministerie van Defensie
- **Joost Smits**
  Hoofd Financiële Stabiliteit, Ministerie van financiën
- **Hester Somsen**
  Plv. NCTV en directeur cybersecurity, Weerbaarheid Statelijke dreigingen en economische veiligheid
- **Kalev Stoicescu**
  Onderzoeksfellow, International Centre for Defence and Security
- **Liisa Talonpoika**
  Ambassadeur Hybride Zaken, Ministerie Buitenlandse Zaken Finland
- **Prof. dr. Teija Tiilikainen**
  Directeur European Centre of Excellence for Countering Hybrid Threats, Helsinki, Finland
- **Petri Toivonen**
  Secretaris-Generaal, Comprehensive Security Committee, Finland
- **Ir. SBN bd. Maarten Tossings**
  Lid Raad van Bestuur en Chief Operating Officer TNO
- **Taavi Turu**
  Beleidsmedewerker Nederlandse ambassade in Finland
- **Madis Vaikmaa**
  Beleidsadviseur Strategische Communicatie, Ministerie van Algemene Zaken, Finland
- **LKol. Ben Valk**
  Onderzoeker NATO Cooperative Cyber Defence Centre of Excellence
- **Justus Veldhuizen**
  Adviseur PV EU
- **Jeroen van der Vlugt**
  Chief Information Officer, Ministerie van Defensie
- **Hans de Vries**
  Directeur Nationaal Cyber Security Centrum
- **Bartjan Wegter**
  EU-coördinator voor terrorismebestrijding; voorm. gevolmachtigd minister bij de Permanente Vertegenwoordiging van Nederland bij de NAVO
- **Dr. Peter Weijland**
  Programmadirecteur Veiligheid, Universiteit Leiden
- **Dimitri van Zantvliet**
  Directeur Cybersecurity Nederlandse Spoorwegen
- **Patricia Zorko**
  Wnd. Directeur-Generaal Risicomanagement, Rijkswaterstaat
- **Beate Zwijnenberg**
  Directeur fraudebestrijding ING

Lijst met afkortingen

AFM	Autoriteit Financiële Markten
AI	Kunstmatige intelligentie
AIV	Adviesraad Internationale Vraagstukken
AIVD	Algemene Inlichtingen en Veiligheidsdienst
AMS-IX	Amsterdam Internet Exchange
ARSIWA	Articles on the Responsibility of States for Internationally Wrongful Acts
BRI	Belt-and-Road Initiative
CAVV	Commissie van Advies inzake Volkenrechtelijke Vraagstukken
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CEPC	Civil Emergency Planning Committee
CERT	Computer Emergency Response Team
CISO	Chief Information and Security Officer
DDOS	*Distributed Denial Of Service*
DIANA	Defence Innovation Accelerator for the North Atlantic
DIMEFIL	Acroniem ten behoeve van hybride dreigingen en statelijke responsmiddelen
DNB	De Nederlandsche Bank
DORA	Digital Operational Resilience Act
ECB	Europese Centrale Bank
EEAS	European External Action Service
EU	Europese Unie
EZK	Ministerie van Economische Zaken en Klimaat
FIMI	Foreign Information Manipulation or Interference
GW	Grondwet
HYBRID COE	European Centre of Excellence for Countering Hybrid Threats
ICT	Informatie, communicatie en technologie
IGH	Internationaal Gerechtshof
IHR	Internationaal humanitair recht – humanitair oorlogsrecht
IRB	ICT Response Board
ISR	Intelligence, surveillance en reconnaissance
J&V	Ministerie van Justitie en Veiligheid
LIMC	Land Information Manoeuvre Centre
MIVD	Militaire inlichtingen- en veiligheidsdienst
NAVO	Noord Atlantische Verdragsorganisatie
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NESA	National Emergency Supply Agency – Nationaal Noodvoorziening Agentschap
NGO	Non-gouvernementele organisatie
NIPV	Nederlands Instituut voor Publieke Veiligheid
NVR	Nationale Veiligheidsraad
NXP	Multinationaal halfgeleiderbedrijf
OCW	Ministerie van Onderwijs Cultuur en Wetenschap
RAND	Amerikaanse denktank
RBRK	Rijksbreed Responskader Hybride dreigingen
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
TCO	Tripartiete Crisismanagement Operationeel
TO2	Organisaties voor toegepast onderzoek
UNESCO	Werelderfgoed organisatie
VN	Verenigde Naties

Adviesraad Internationale Vraagstukken

Postbus 20061
2500 EB Den Haag
W: www.adviesraadinternationalevraagstukken.nl
E: aiv@minbuza.nl