Dreigingsbeeld Statelijke Actoren 2025

Aanhoudende dreigingen in tijden van groeiende onzekerheid

Foto omslag: *Ruim twee maanden voor de aanvang van de NAVO-top, is de straat waar de bijeenkomst eind juni wordt gehouden, niet meer toegankelijk voor verkeer.*

Aanhoudende dreigingen in tijden van groeiende onzekerheid

Het Dreigingsbeeld Statelijke Actoren (DBSA) 2025 verschijnt in een turbulente tijd waarin internationale betrekkingen onvoorspelbaarder worden. In de afgelopen twee jaar zijn de statelijke dreigingen richting Nederland en onze belangen op veel vlakken onverminderd sterk aanwezig gebleven en is de dreiging van sabotage toegenomen. Geen van de in het DBSA beschreven dreigingen is afgenomen. De weerbaarheid tegen statelijke dreigingen gaat echter steeds meer gepaard met onzekerheid over de nabije toekomst.

Veranderingen in de mondiale verhoudingen

De machtsbalans in de wereld is aan het veranderen en het is de vraag hoe de wereldorde eruit komt te zien. De tijd waarin liberaal-westerse waarden de boventoon voeren lijkt voorbij te zijn. Landen uit het 'Mondiale Zuiden' laten zich minder aan het Westen gelegen liggen en zetten nieuwe instituties en samenwerkingsverbanden op om tegenwicht te bieden aan bestaande politieke invloedsferen. Veranderingen in de wereldorde lijken steeds meer effect te hebben, bijvoorbeeld doordat landen steeds meer bereid zijn om hun macht actief in te zetten om hun belangen te verdedigen bij internationale instituties en samenwerkingsverbanden. Deze veranderingen kunnen grote gevolgen hebben voor Nederland en onze nationale veiligheid; de openheid van de Nederlandse samenleving, democratie en economie maken ons land kwetsbaar.

Dreiging van statelijke actoren onverminderd aanwezig

Binnen deze veranderingen in de mondiale verhoudingen, bedreigen statelijke actoren de Nederlandse nationale veiligheid op verschillende manieren.[i] Een directe militaire aanval van Rusland op NAVO-grondgebied is onwaarschijnlijk, maar doordat de tegenstellingen tussen Rusland en het Westen verdiepen is het risico op (onbedoelde) verdere escalatie toegenomen. Rusland voert steeds meer sabotageacties uit om angst en onrust aan te wakkeren in Europa, vanwege de verwachting dat vervolgens de politieke en maatschappelijke bereidheid afneemt om met het land in conflict te komen. De verwachting is dat zulke acties blijven toenemen, omdat sabotageacties onder de drempel blijven van een militair conflict en daarmee van artikel 5 van het NAVO-verdrag. Rusland kan met sabotageacties haar doelen blijven nastreven, zonder in een daadwerkelijke oorlog met de NAVO te belanden. Fysieke en digitale sabotage kan leiden tot maatschappelijke ontwrichting, ontregeling van vitale infrastructuur, verstoringen van militaire operaties of voorbereidingen daarop en economische schade. Van alle cyberdreigingen heeft digitale sabotage in potentie de grootste impact op de Nederlandse samenleving.

i De zes nationale veiligheidsbelangen zijn: territoriale, fysieke, economische en ecologische veiligheid, sociale en politieke stabiliteit en internationale rechtsorde en stabiliteit.

Veel andere dreigingen zijn onverminderd sterk aanwezig. De dreiging van spionage door landen als China, Rusland en Iran is onverminderd hoog. Daarnaast lijken steeds meer landen te proberen om de Nederlandse samenleving en politieke besluitvorming te beïnvloeden via laagdrempelige, digitale spionage, intimidatie of de verspreiding van desinformatie. Het is mogelijk dat meer landen zulke middelen inzetten als gevolg van de veranderende wereldorde. Ook kan de versterkte Nederlandse inzet op het onderkennen van statelijke dreigingen hebben bijgedragen aan het beter signaleren van zulke dreigingen. Spionage, laagdrempelige verstoringsaanvallen, transnationale repressie en ondermijnende beïnvloeding kunnen gevoelens van onrust en onveiligheid aanwakkeren binnen diasporagemeenschappen of breder in de samenleving. Zulke acties zijn ondermijnend voor de sociale en politieke stabiliteit.

De economie is sterk verbonden met geopolitiek. Strategische afhankelijkheden worden ingezet als politiek of economisch drukmiddel. Steeds meer landen voeren een protectionistisch economisch beleid met handelsbarrières en beperking van handel in technologische kennis en goederen. De inzet van economische instrumenten door statelijke actoren kunnen grote gevolgen hebben voor Nederland. Op korte termijn kan het leven duurder worden door handelsconflicten, exportrestricties of verhoogde energieprijzen.

Daarnaast blijft de dreiging van ongewenste overdracht van kennis en technologie onverminderd hoog. Door ingestelde sancties zoeken statelijke actoren alternatieve manieren om aan technologische kennis te komen, waarvoor ze eerder gebruik maken van heimelijke verwerving. Wanneer andere landen via (heimelijke) verwerving over dezelfde technologische kennis als Nederland beschikken, dan kan op de langere termijn onze koploperspositie in bepaalde technologische domeinen teruglopen of kan het concurrerend vermogen van Nederlandse bedrijven structureel afnemen. Bovendien kan het andere landen militair sterker maken waardoor de effectiviteit van onze krijgsmacht zal afnemen.

Toenemende onzekerheid over weerbaarheid

De dreiging vanuit statelijke actoren is onverminderd sterk aanwezig gebleven, maar de weerbaarheid hiertegen is onzekerder geworden. Nederland en andere Europese landen zijn nog steeds in grote mate afhankelijk van de Verenigde Staten, onder andere op het gebied van veiligheid, defensie, economie, grondstoffen en technologie. De afhankelijkheden op het gebied van veiligheid zijn kwetsbaarder geworden doordat de dreigingsperceptie en waardering van de huidige internationale rechtsorde van Europese landen steeds meer zijn gaan verschillen met die van niet-Europese landen. Keuzes van statelijke actoren hebben impact op Nederland, ook wanneer deze keuzes niet direct tegen Nederland gericht zijn. Dit brengt grote onzekerheden en risico's voor de nationale veiligheid met zich mee. De veranderingen in de wereldorde en onze weerbaarheid kunnen eraan bijdragen dat statelijke actoren minder weerstand krijgen en zich brutaler opstellen. Europa is meer op zichzelf aangewezen en zal vooral zelf zorg moeten dragen voor de veiligheid van het eigen deel van de wereld.

Inhoudsopgave

Finse piloot zit in F18. Vliegbasis Leeuwarden is gastheer van de internationale oefening Ramstein Flag. Deze NAVO-oefening vervangt dit jaar de jaarlijkse oefening van de Koninklijke Luchtmacht, die normaal gesproken Frisian Flag heet.

Inleiding

Voor u ligt het Dreigingsbeeld Statelijke Actoren (DBSA) 2025, opgesteld door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Het DBSA 2025 geeft de belangrijkste ontwikkelingen in de statelijke dreigingen tegen de nationale veiligheid weer sinds het verschijnen van het vorige DBSA, in november 2022. Het doel is het vergroten van bewustzijn over de aard en ernst van deze dreigingen. Het dreigingsbeeld legt hiermee de analytische basis voor beleidsmatige opvolging.

Statelijke actoren proberen hun belangen zo goed mogelijk te behartigen. Sommige staten brengen daarbij ongewild of onbewust schade toe aan anderen, anderen schaden andermans belangen moedwillig. Bewust of onbewust, gewild of ongewild: in alle gevallen kan onze nationale veiligheid worden geraakt. Het DBSA richt zich specifiek op deze dreiging door statelijke actoren. Voor het DBSA wordt uitgegaan van de volgende definitie van statelijke dreigingen:

> *Dwingende, ondermijnende, misleidende of heimelijke activiteiten van of namens statelijke actoren, onder de drempel van gewapend conflict, die de nationale veiligheidsbelangen van Nederland kunnen schaden door een combinatie van nagestreefde doelen, gebruikte middelen en ressorterende effecten.*[1]

Dit DBSA verschijnt in een turbulente tijd waarin internationale betrekkingen onvoorspelbaarder worden. Het meest in het oog springend zijn de oorlogen in Oekraïne en in Gaza, spanningen rondom Taiwan en de Rode Zee, en de onder druk staande trans-Atlantische relatie.[2] Al deze gebeurtenissen raken ook Nederland en onze nationale veiligheidsbelangen. In sommige gevallen raken ze Nederland direct en in andere gevallen is er sprake van een indirecte of sluimerende dreiging waarvoor ons land moet waken.

Ten opzichte van het vorige DBSA uit 2022 is de dreiging op veel vlakken onverminderd sterk aanwezig gebleven en is de sabotagedreiging toegenomen. Geen enkele dreiging is afgenomen. Daarbij gaat de weerbaarheid tegen statelijke dreigingen steeds meer gepaard met onzekerheid over de nabije toekomst, mede door geopolitieke ontwikkelingen. Het blijft daarom van groot belang om statelijke dreigingen te herkennen om vervolgens zo goed mogelijk maatregelen te kunnen treffen.

Methodes en doelwitten van statelijke actoren

De nationale veiligheid wordt op verschillende manieren bedreigd door statelijke actoren, zoals benoemd in de voorgaande DBSA's uit 2021 en 2022. Actoren bedreigen de nationale veiligheid met uiteenlopende methodes, die niet altijd strikt gescheiden zijn en met elkaar kunnen samenhangen. Het gaat om de volgende methodes:

- Militair: onder andere de ontwikkeling en opzichtige manifestaties van conventionele en nucleaire wapens, de inzet van militaire eenheden of operaties – al dan niet door *proxy's*.[ii]
- Spionage: het verzamelen van inlichtingen op fysieke of digitale wijze voor economische, politiek-bestuurlijke en militaire doeleinden, of om zicht te behouden op de diaspora en dissidenten.
- Sabotage: het moedwillig beschadigen van militaire en civiele doelwitten om bijvoorbeeld oorlogsleveranties te vertragen, angst en verdeeldheid te zaaien of te testen wanneer tegenstanders reageren.
- Statelijke inmenging: dit gaat naast vormen van spionage ook om geweldsdreigingen of beïnvloeding van diaspora en ondermijnende beïnvloeding, bijvoorbeeld door het verspreiden van desinformatie of *hack-and-leak*-operaties.[iii]
- Economie: instrumenten binnen het economisch domein, zoals bedrijfsovernames en investeringen, kunnen op legitieme en heimelijke wijze worden ingezet om geopolitieke en militaire doelen via civiele bedrijven te behalen. Ook kan ongewenste overdracht van kennis en technologie (verwerving) plaatsvinden.
- Diplomatiek en politiek: hierbij gaat het om het beïnvloeden of tegenwerken van bestaande instituties, het oprichten van parallelle instituties en het aangaan van bondgenootschappen om zo de eigen invloed te vergroten.

Deze methodes kunnen worden ingezet tegen doelwitten uit de hele breedte van de Nederlandse maatschappij. Bijvoorbeeld tegen democratische processen, beleidsmakers, mensen of organisaties die betrokken zijn bij politieke besluitvorming en (inter)nationale gremia als de NAVO, maar ook tegen onderwijs- en kennisinstellingen of internationale instituties op Nederlands grondgebied. Het bedrijfsleven en topsectoren kunnen slachtoffer worden van bijvoorbeeld spionage, en specifieke diaspora en geloofsgemeenschappen kunnen door statelijke actoren worden gebruikt om tweespalt te zaaien. Kortgezegd: zowel de methodes die statelijke actoren kunnen inzetten als hun doelwitten zijn divers.

ii Proxy's zijn derde partijen, zoals bedrijven, hackergroeperingen of lokale criminele groepen die door buitenlandse overheden worden ingezet vanwege hun capaciteiten en de mogelijkheid om de eigen betrokkenheid te verbergen.

iii Hack-and-leak-operaties zijn het verkrijgen van toegang tot persoons- of organisatiegevoelige informatie via een hackaanval, om deze informatie vervolgens, al dan niet gemanipuleerd, te delen via (sociale) media of bepaalde personen en instanties.

De nationale veiligheidsbelangen

Als statelijke actoren één of meerdere van de nationale veiligheidsbelangen dusdanig bedreigen dat er sprake is van mogelijke maatschappelijke ontwrichting, dan is de nationale veiligheid in het geding. Dreigingen tegen de nationale veiligheid zijn ongeacht de impact ongewenst. De bescherming van de nationale veiligheid moet ervoor zorgen dat personen, organisaties en gemeenschappen ongestoord kunnen functioneren. DBSA 2025 beschrijft de belangrijkste geopolitieke ontwikkelingen, de statelijke dreigingen tegen Nederland en de impact van deze ontwikkelingen en dreigingen op onze nationale veiligheid. De impact wordt bezien in de context van de zes nationale veiligheidsbelangen.[3]

Deze zijn:

- Territoriale veiligheid (inclusief digitale veiligheid);
- Fysieke veiligheid;
- Economische veiligheid;
- Ecologische veiligheid;
- Sociale en politieke stabiliteit, en
- Internationale rechtsorde en stabiliteit.

Leeswijzer

Dit DBSA begint met een contextueel hoofdstuk over de veranderende wereldorde, waarin specifiek wordt ingegaan op verschuivingen in de geopolitieke machtsbalans en de opkomst van nieuwe strijdtonelen. Vervolgens zijn er zes hoofdstukken, ingedeeld naar de methodes die statelijke actoren inzetten, namelijk: militair, spionage, sabotage, statelijke inmenging, economie, en diplomatiek en politiek.

Het Hera-ruimtevaartuig in een cleanroom van het European Space Research and Technology Centre (ESTEC). Het ruimtevaartuig van ESA zal onderzoek doen naar de deflectie van asteroïden als onderdeel van een planetaire defensiemissie genaamd Hera.

Nederland in een veranderende wereldorde

De tijd lijkt voorbij te zijn waarin liberaal-westerse waarden de boventoon voeren, veelal gedreven door Amerikaanse dominantie. De machtsbalans in de wereld is aan het veranderen en het is de vraag hoe de wereldorde eruit komt te zien. Duidelijk is wel dat deze veranderingen grote gevolgen kunnen hebben voor Nederland en onze nationale veiligheid. De openheid van de Nederlandse samenleving, democratie en economie maken ons land kwetsbaar. De veiligheid van ons land is dan ook sterk verbonden met de veiligheid in de rest van de wereld.

Verschuivingen in de machtsbalans

De veranderende wereldorde gaat gepaard met fragmentatie; dit loopt als een rode draad door het Dreigingsbeeld Statelijke Actoren 2025. Het WRR-rapport *Nederland in een fragmenterende wereldorde* beschrijft de fragmentatie langs drie sporen: machtspolen, tonelen en wereldbeelden.[4]

In de eerste plaats verandert de unipolaire wereldorde naar een multipolaire. In zo'n andere wereldorde zal de dominantie van de Verenigde Staten en het gehele Westen afnemen in het voordeel van landen als China, Rusland, India, Iran, Saoedi-Arabië, Turkije en Indonesië. Het mondiale zwaartepunt – demografisch, economisch en anderszins – beweegt richting het oosten en zuiden. Landen laten zich minder aan het Westen gelegen liggen en zetten nieuwe instituties en samenwerkingsverbanden op om tegenwicht te bieden aan bestaande politieke invloedsferen. Iedere macht komt op voor zijn eigen belangen, die vaak haaks staan op de belangen van anderen. Zo is het partnerschap tussen China en Rusland verder verdiept, zonder dat zij dezelfde doelstellingen hebben. Voor nu lijkt de totstandkoming van zo'n multipolaire wereldorde onvermijdelijk.

Ten tweede zijn landen op meer tonelen actief en trekken ze deze tonelen in het perspectief van veiligheid. Zo worden economische activiteiten niet alleen vanuit economische motieven ondernomen, maar ook als voorwaarde voor de eigen veiligheid. Een voorbeeld is de mondiale markt voor computerchips, waarbinnen landen maatregelen treffen om te voorkomen dat de meest geavanceerde apparatuur in handen komt van systeemrivalen. Dit geldt ook voor het sociale en digitale toneel, waar statelijke actoren diasporagemeenschappen vanuit het eigen veiligheidsbelang beïnvloeden. Deze tonelen bestaan uiteraard langer, maar hebben in de afgelopen jaren aan belang gewonnen.

In de derde plaats is er de fragmentatie van wereldbeelden. Landen als Rusland en Iran kunnen worden gezien als systeemrivalen van het Westen en ook China, dat nog steeds een belangrijke handelspartner is waarmee Nederland grote economische belangen deelt, moet soms worden beschouwd als een systeemrivaal. China acht een verandering van de internationale rechtsorde noodzakelijk om invloedrijker te kunnen worden op het wereldtoneel of voor binnenlands politiek machtsbehoud. Daarnaast proberen landen bestaande instituties en samenwerkingsverbanden te beïnvloeden in hun voordeel en roepen ze eigen allianties in het leven om de eigen belangen te behartigen. Het is niet waarschijnlijk dat de opstelling van de systeemrivalen tegenover Nederland en onze belangen op korte termijn zal veranderen.

Veranderende houding van de Verenigde Staten heeft gevolgen voor onze nationale veiligheid
Het zwaartepunt van de Amerikaanse veiligheidspolitiek verschuift al jaren weg van Europa en meer richting de machtscompetitie met China. Dit is in een stroomversnelling geraakt met het aantreden van president Trump, die bovendien duidelijk te kennen heeft gegeven dat meer van Europa wordt verwacht ten behoeve van zijn eigen veiligheid. De veranderende, meer transactionele houding van de Verenigde Staten brengt onzekerheid mee voor de Nederlandse nationale veiligheid, mede gelet op de grote afhankelijkheden van de Verenigde Staten onder andere op veiligheidsgebied. De Verenigde Staten zijn een belangrijke bondgenoot, wel is duidelijk dat Europa meer op zichzelf aangewezen is en vooral zelf zorg zal moeten dragen voor de veiligheid van het eigen deel van de wereld.

Van de Noordpool tot de ruimte

Fysieke plaatsen zijn altijd belangrijke strijdtonelen geweest en de afgelopen jaren is dit andermaal gebleken. Zo heeft de Amerikaanse president Trump Groenland en het Panamakanaal expliciet op de kaart gezet en is de belangstelling van verschillende landen voor de Noordpool en de ruimte in de afgelopen jaren sterk toegenomen. De interesse van landen in de Noordpool heeft te maken met de aanwezige voorraden gas en metalen, en met mogelijkheden voor zeevaart.[5] Rusland legt in samenwerking met China volop havens aan bij de noordelijke kust, om de zeevaartroute te kunnen controleren die vanwege klimaatverandering steeds toegankelijker wordt. Ook versterkt Rusland zijn militaire installaties in de regio en werkt het land met China in beperkte maar toenemende mate militair samen rond het Arctisch gebied. De toenemende spanningen rondom het Noordpoolgebied kunnen leiden tot machtsverschuivingen aldaar en mogelijk regionale instabiliteit.

De ruimte als betwist domein

Ook de ruimte is van groter strategisch belang geworden. Wat op de aarde geopolitiek wordt uitgevochten, vindt nu zijn weg in de ruimte. De 'space race' van ongeveer een halve eeuw geleden is wederom in alle hevigheid aan de gang en stimuleert een breed scala aan innovaties. Het aantal spelers in de ruimte neemt snel toe en ruimtegrootmachten vergroten hun capaciteiten en (militaire) ambities. Het ruimtedomein is immers van groot belang voor defensie, veiligheid, economie, wetenschap, onderzoek en innovatie: dagelijks maken mensen over de hele wereld op grote schaal gebruik van satellieten en satellietdiensten voor bijvoorbeeld communicatie, financiële transacties, navigatie, weersvoorspellingen en internet.[6]

Tegelijkertijd wordt de ruimte in toenemende mate een betwist domein: een groeiend aantal landen ontwikkelt capaciteiten om de toegang tot of het gebruik van ruimtemiddelen door andere gebruikers te beperken of hen deze te ontzeggen, variërend van verstoring en degradatie tot aan fysieke vernietiging van satellieten.[7] Met name de dreiging vanuit Rusland en groeiende Chinese ruimtecapaciteiten zorgen in toenemende mate voor uitdagingen om een vrije toegang tot of het gebruik van de ruimte te behouden. Dit kan problematisch worden voor Nederland, omdat zowel militaire als commerciële satellieten een cruciaal onderdeel vormen van de infrastructuur op aarde. Belangrijke functies in onze samenleving zijn afhankelijk van satellieten. Verlies of verstoring van satellietsignalen, al dan niet opzettelijk, heeft direct een ontwrichtend effect op de samenleving.[8] Daarnaast is het ruimtedomein essentieel voor de operaties van Defensie: communicatie met uitgezonden eenheden, het gebruik van satellietgeleide precisiewapens en inlichtingenanalyses gaat op basis van satellietbeelden.

Een patch met het logo voor Bastion Lion, de grootste oefening van de Koninklijke Landmacht dit jaar. Tijdens deze oefening voeren twee Nederlandse gevechtsbataljons van 13 Lichte Brigade en 1 Duits gevechtsbataljon een aanval uit die meerdere dagen duurt op een oefendorp in Duitsland. Zo'n 4.000 militairen, 1.800 voertuigen en 200 drones doen aan de oefening mee.

Militair

Sinds enkele jaren is sprake van een Russische dreiging tegen NAVO-landen, waaronder Nederland. De militaire dreiging tegen de NAVO is in de afgelopen twee jaar min of meer gelijk gebleven. Wel heeft de oorlog in Oekraïne de tegenstellingen tussen Rusland en het Westen verdiept, waarmee het risico op (onbedoelde) verdere escalatie is toegenomen.

Dit toegenomen risico raakt Nederland vanwege artikel 5 van het NAVO-verdrag[iv] en vanwege de mogelijkheid dat er in Nederland sabotageacties worden uitgevoerd (zie hoofdstuk Sabotage). De weerbaarheid tegen een militaire dreiging is bovendien onzekerder geworden sinds de Verenigde Staten duidelijk te kennen hebben gegeven dat meer van Europa wordt verwacht ten behoeve van zijn eigen veiligheid. Sinds de Russische invasie in Oekraïne is de westerse steun aan dat land steeds omvangrijker geworden, maar recent lijkt deze steeds minder vanzelfsprekend. Europa is meer op zichzelf aangewezen en zal vooral zelf zorg moeten dragen voor de veiligheid van het eigen deel van de wereld.

De veranderingen in de wereldorde kunnen eraan bijdragen dat statelijke actoren minder weerstand krijgen en zich brutaler opstellen. Zo is er diverse berichtgeving over de inzet van verboden chemische wapens in Oekraïne door Rusland, zonder dat dat leidde tot sterke internationale veroordelingen. Een gevolg hiervan kan zijn dat de drempel om chemische wapens in te zetten ook in andere strijdgebieden wordt verlaagd. Iran gaat verder met de ontwikkeling van ballistische raketten, waarvoor onder andere wordt geprobeerd om via spionage kennis en apparatuur te bemachtigen in Nederland. Behalve aan bondgenoten in de regio, levert Iran deze raketten aan Rusland voor gebruik in diens oorlog tegen Oekraïne.

iv In artikel 5 van het NAVO-verdrag staat dat een aanval op een lid beschouwd wordt als een aanval op alle leden. Bondgenoten helpen elkaar dus wanneer een van de landen wordt aangevallen.

Grootste militaire dreiging komt uit Rusland

De relatie tussen het Westen en Rusland is sinds de grootschalige Russische oorlog tegen Oekraïne in februari 2022 tot een absoluut dieptepunt gedaald. Het risico is toegenomen op (onbedoelde) militaire escalatie tussen Rusland en de NAVO. Rusland is de grootste militaire tegenstander en de meest waarschijnlijke militaire dreiging voor de territoriale integriteit van het NAVO-bondgenootschap. Hoewel er in Europa stevig wordt geïnvesteerd in NAVO-gevechtskracht, heeft Rusland tijdelijk een militaire voorsprong genomen. Zorgelijk is dat Rusland na het eventueel beëindigen van de oorlog in Oekraïne en onder de – voor Rusland – meest gunstige omstandigheden, indien gewenst slechts een jaar nodig heeft om voldoende capaciteiten op te bouwen voor een beperkte militaire operatie tegen NAVO-lidstaten.

Voor Rusland zijn westerse en Russische veiligheidsbelangen strijdig en onverenigbaar. De confrontatie tussen Rusland en het Westen heeft voor Rusland een 'totaal' en existentieel karakter. In de ogen van Rusland is de oorlog in Oekraïne daarom onderdeel van een breder conflict met het Westen. Een koerswijziging in de Russische houding richting Europa in de afzienbare toekomst is om die reden moeilijk voorstelbaar.

De afgelopen jaren is de westerse steun aan Oekraïne steeds omvangrijker geworden. Dit helpt Oekraïne niet alleen bij de landsverdediging, maar stelt het land ook in staat om, onder voorwaarden, aanvallen uit te voeren in Rusland. Een voortzetting van deze steun is noodzakelijk voor Oekraïne om zich te kunnen verdedigen tegen de Russische militaire agressie. Deze steun is echter niet altijd even vanzelfsprekend.

Russische pogingen om gevolgen oorlog te compenseren

Ondertussen is de oorlog ook voor Rusland een militaire en economische uitputtingsslag. De Russische economie vertoont steeds meer trekken van een oorlogseconomie en hoewel de effecten van de westerse sancties op de Russische economie stevig zijn, is Rusland op korte termijn nog niet genoodzaakt de oorlog te stoppen door economische instabiliteit.[9] Het land probeert de gevolgen van de oorlog te compenseren door het aangaan van nieuwe samenwerkingen en het zoeken naar manieren om internationale sancties te vermijden. Iran, Noord-Korea en Belarus leveren wapens aan Rusland. Hoewel China in principe geen wapens en munitie levert aan Rusland, leveren Chinese bedrijven *dual use* goederen[v] en zelfs aanvalsdrones aan Russische bedrijven die kunnen worden ingezet in de oorlog in Oekraïne. In het najaar van 2024 bleek Noord-Korea naast wapens ook militairen te leveren die daadwerkelijk zijn ingezet tegen Oekraïne.
In ruil daarvoor levert Rusland onder andere olie, waarmee sancties van de Verenigde Naties tegen Noord-Korea worden omzeild. Ten slotte krijgen westerse pogingen om Rusland op mondiaal niveau te isoleren onvoldoende weerklank in de rest van de wereld. Zo gaat de Russische handel met andere delen van de wereld gewoon door.

v Bij dual use goederen is het eindproduct zowel civiel als militair toepasbaar.

Stelselmatige schending van het Verdrag Chemische Wapens

Kort na de Russische invasie in Oekraïne verschenen de eerste berichten dat Rusland op ingenomen Oekraïens grondgebied traangas had ingezet. Het gebruik van chemische wapens als onderdeel van een militaire campagne, inclusief traangas, is onder geen beding toegestaan onder het Verdrag Chemische Wapens, een verdrag dat ook door Rusland is ondertekend. Het Oekraïense ministerie van Defensie heeft sinds februari 2022 meer dan zesduizend incidenten geregistreerd waarbij Rusland chemicaliën heeft ingezet tegen Oekraïense strijdkrachten. De Organisatie voor het Verbod op Chemische Wapens (OPCW) bevestigt met onafhankelijk onderzoek dat traangas is gebruikt.[10]

Sinds maart 2024 berichten media veelvuldig over de inzet van chloorpicrine, een verstikkend chemisch wapen. De Verenigde Staten en het Verenigd Koninkrijk hebben Rusland om deze reden op respectievelijk 1 mei en 8 oktober 2024 sancties opgelegd. Op 4 juli 2025 hebben de AIVD en MIVD, samen met de Duitse buitenlandse inlichtingendienst BND, ook publiekelijk bevestigd dat Rusland stelselmatig chemische wapens inzet, waaronder chloorpicrine. Bovendien bevat deze gezamenlijke publicatie een waarschuwing voor een intensivering van Russische inzet van chemische wapens in Oekraïne. Het gebrek aan een sterke internationale reactie hierop kan eraan bijdragen dat de drempel voor statelijke actoren om chemische wapens in te zetten wordt verlaagd, niet alleen in Oekraïne maar ook in andere strijdgebieden.

Nucleaire retoriek door Rusland en Iran

In november 2024 heeft Rusland zijn nucleaire doctrine herzien, waarmee de drempel om nucleaire wapens te kunnen gebruiken formeel is verlaagd. Deze verlaging staat niet gelijk aan een toegenomen bereidheid om nucleaire wapens in te zetten. Mogelijk gaat het Rusland vooral om de afschrikwekkende werking van dit beleid jegens het Westen.

Nucleaire retoriek beperkt zich niet tot Rusland. Iran had voor de Israëlische en Amerikaanse aanvallen in juni 2025 binnen zeer korte tijd kunnen beschikken over voldoende hoogverrijkt uranium voor de productie van enkele kernwapens.[11] Er waren echter geen aanwijzingen dat Iran bezig was met de andere noodzakelijke activiteiten om een nucleair explosief te ontwikkelen. Wel leidde de toenemende onrust in het Midden-Oosten tot politieke oproepen onder *hardliners* om een *fatwa* uit 2003 tegen kernwapens te herzien. Voorts dreigde Iran uit het Non-Proliferatieverdrag te stappen, in geval van het opnieuw instellen van opgeschorte sancties onder het nucleair akkoord.[12] Het Internationaal Atoomenergieagentschap stelde bovendien dat het door Iran niet in staat werd gesteld om te verifiëren dat Irans nucleaire programma uitsluitend civiele doelen diende.[13] Deze ontwikkelingen vergrootten de zorgen rondom Irans nucleaire programma.

Blijvende zorgen over Iraanse wapenontwikkeling

Iran streeft nog steeds naar de verdere ontwikkeling van ballistische raketten. Het Iraanse regime heeft door internationaal opgelegde sancties beperkte toegang tot westerse kennis en technologie. Om die reden probeert Iran deze kennis en apparatuur via spionage te verwerven in landen als Nederland. Dit gebeurt onder meer via heimelijke verwervingsnetwerken, kennisinstellingen, studenten en onderzoekers. Ook zoekt Iran nadrukkelijk de samenwerking op met Rusland om aan meer technologisch hoogwaardige militaire capaciteiten te komen. De sancties ten spijt boekt Iran ook vorderingen bij de ontwikkeling van ballistische raketten. Zo gebruikte het in 2024 voor het eerst zelfontwikkelde ballistische raketten tegen Israël bij de directe escalatie tussen deze twee landen. De dreiging beperkt zich echter niet tot Iran zelf: ook Iraanse bondgenoten als de Libanese Hezbollah en Jemenitische Houthi's gebruikten in hetzelfde jaar raketten die door Iran zijn ontwikkeld. Iraanse wapens kunnen worden gebruikt tegen Nederlandse militairen in Irak en worden gebruikt in de Rode Zee waar de Nederlandse marine actief was in 2024. Daarnaast heeft Iran ballistische korte afstandsraketten en aanvalsdrones geleverd aan Rusland ten behoeve van de oorlog tegen Oekraïne. Daarmee raakt het ballistische raketprogramma van Iran ook direct aan Nederlandse veiligheidsbelangen in Europa.

Aanvallen van door Iran gesteunde groeperingen leiden tot kosten en risico's internationale zeescheepvaart

De instabiliteit in het Midden-Oosten heeft grote risico's voor de internationale zeescheepvaart, met name rondom het Arabisch Schiereiland.[vi] Deze wateren zijn van groot belang voor efficiënt vervoer van grote hoeveelheden goederen, wereldwijd. Nederland is vooral afhankelijk van olie en gas dat vanuit de Perzische Golf via de Straat van Hormuz wordt aangevoerd. Elk onderdeel op deze route is een potentiële bottleneck die het transport kan verstoren voor het gehele verdere traject. Dit geldt bijvoorbeeld ook voor het Panamakanaal, de Bosporus en de zeestraten van Gibraltar, Taiwan of Malakka. Hoe meer van deze zogenoemde Sea Lines of Communication (SLOC) onbruikbaar worden, des te groter de mogelijke onvoorziene effecten.

Sinds november 2023 voeren de Houthi's in de Rode Zee aanvallen uit op (civiele) scheepvaart en richting Israël. Kort na het uitbreken van de oorlog in Gaza lag de focus vooral op het aangrijpen van schepen met een Israëlische link, maar ook andere schepen zijn doelwit van aanvallen geworden. Sindsdien wordt het zuiden van de Rode Zee door steeds meer rederijen gemeden. In 2014 namen de Houthi's de macht over in Sana'a, de hoofdstad van Jemen, en ondertussen zijn ze de de facto autoriteit in het noorden van Jemen. Ze onderhouden warme banden met onder andere Iran, bijvoorbeeld door wapenleveranties, geldstromen en personele ondersteuning van de Iraanse Revolutionaire Garde. Analisten zijn het erover eens dat de Houthi's samenwerken met Iran, maar niet direct door Iran worden aangestuurd.

De impact van de stremming van bestemmingsverkeer is niet direct een kwestie voor Nederland. Dat ligt anders voor het doorgaand scheepsverkeer. Nederlands gevlagde schepen en schepen onder andere vlag die bijvoorbeeld goederen leveren die van economisch belang zijn voor Europa, verleggen nu vaak hun route tussen Europa en Afrika en Azië, om de wateren rondom het Arabisch Schiereiland zoveel mogelijk te mijden. Dit leidt tot langere vaartijden en hogere transportkosten. De Houthi-aanvallen vormen dus niet alleen een fysieke dreiging, maar hebben ook een economische impact, voornamelijk op landen in de regio.

vi Dit betreft het gehele gebied van de Perzische Golf, Straat van Hormuz, Golf van Oman, Arabische Zee, Golf van Aden, Bab el-Mandeb, Rode Zee.

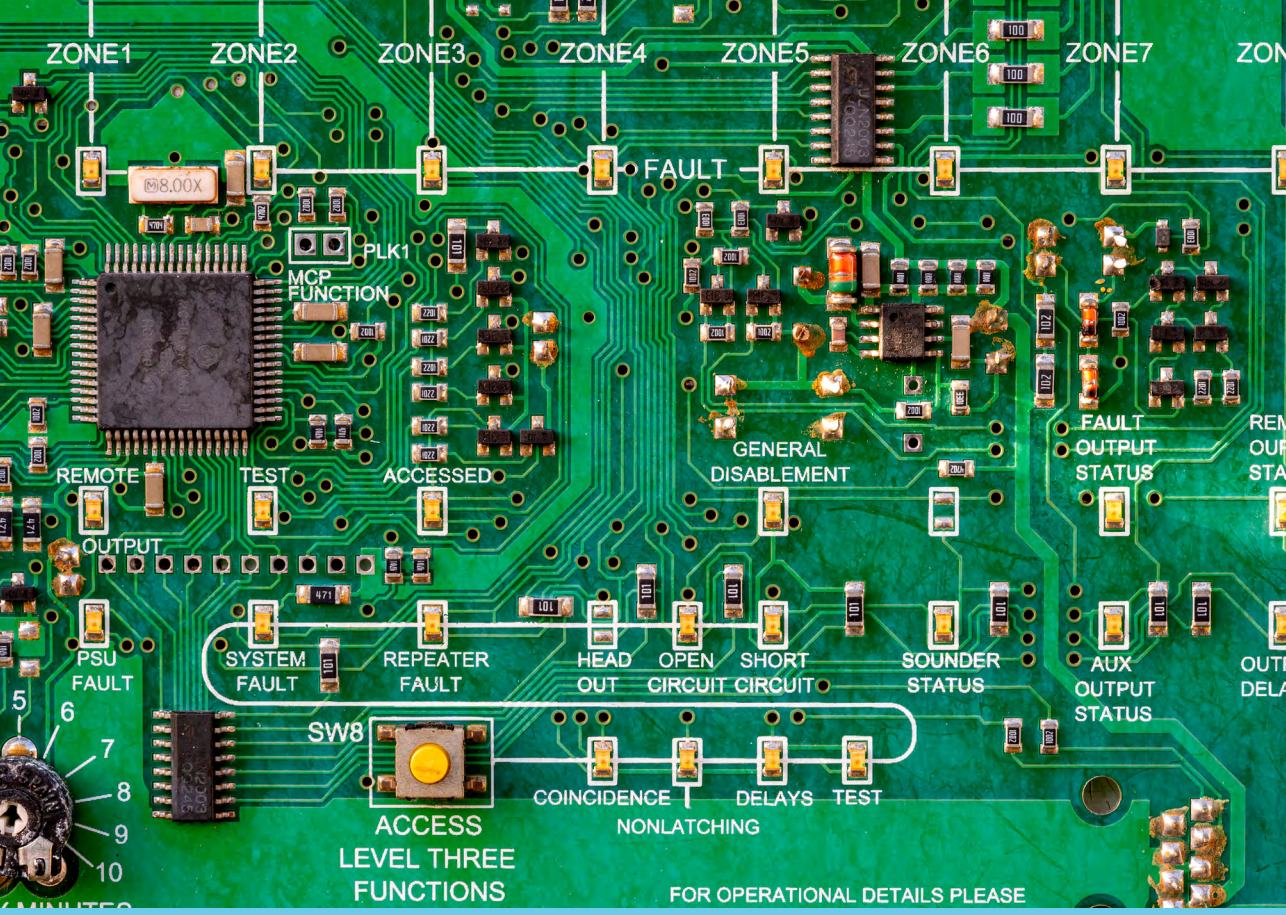
Dreiging tegen het Caribisch gedeelte van het Koninkrijk

Het Caribisch gedeelte van het Koninkrijk der Nederlanden, specifiek de ABC-eilanden Aruba, Curaçao en Bonaire, ondervindt nog steeds direct de gevolgen van de politieke, economische en humanitaire situatie in Venezuela. De relatie tussen Nederland en Venezuela is gespannen, mede doordat het Koninkrijk de door Maduro geclaimde overwinning bij de presidentsverkiezingen in 2024 niet erkent. Het is onwaarschijnlijk dat Venezuela de intentie heeft om een militair conflict met het Koninkrijk aan te gaan, maar de kans op onbedoelde escalatie bestaat als gevolg van de relatief lage militaire professionaliteit in Venezuela.

Daarnaast kan toenemende instabiliteit binnen Venezuela gevolgen hebben voor Aruba, Bonaire en Curaçao, bijvoorbeeld in de vorm van migratie vanuit Venezuela naar de eilanden en grensoverschrijdende criminaliteit. Hoewel de huidige Venezolaanse migratie druk legt op de eilanden, kan een grootschalige migratiestroom de sociale stabiliteit en economie in potentie zwaar onder druk zetten. Dienstverlening van bijvoorbeeld medische voorzieningen en het justitiële apparaat, is op de eilanden kleinschalig en daardoor kwetsbaar.

Betekenis voor Nederland

- *Indien een aanval op NAVO-grondgebied zou plaatsvinden, betekent dat directe betrokkenheid van Nederland vanwege artikel 5 van het NAVO-verdrag. De oorlog in Oekraïne heeft de tegenstellingen tussen Rusland en het Westen verdiept, waarmee het risico op (onbedoelde) verdere escalatie is toegenomen. Dit risico wordt mede bepaald door de aanhoudende investeringen van Rusland in het eigen militaire apparaat, de mate waarin de NAVO in staat is daar militair vermogen tegenover te stellen ter afschrikking, de westerse cohesie en de Russische perceptie daarvan, en de wijze waarop de opbouw van militaire capaciteiten van NAVO-landen invloed heeft op de Russische dreigingsperceptie.*
- *Europa is voor zijn veiligheid steeds meer op zichzelf aangewezen. Een eventuele militaire escalatie vraagt veel van ons land, zowel van de krijgsmacht als de gehele samenleving. Nederland is bijvoorbeeld een doorvoerland voor NAVO-materieel en kan worden betrokken bij de opvang van gewonden en oorlogsvluchtelingen.*
- *Onrust in de wereld raakt Nederland en kan gevolgen hebben voor reizen of internationale handel, maar ook een katalysator zijn voor dreigingen tegen Nederland op bijvoorbeeld het gebied van terrorisme of economie.*



Close up van een groen moederbord met chips en andere componenten. Chips verwerken gegevens volgens bepaalde instructies. Ze worden gebruik in diverse soorten apparaten zoals computers, smartphones, tablets, wasmachines etc. Alle met elkaar verbonden componenten communiceren via het moederbord.

Spionage

Spionage is een methode om informatie en kennis te verkrijgen voor economische, politiek-bestuurlijke en militaire doeleinden, maar kan ook worden ingezet om zicht te behouden op de diaspora en dissidenten. Spionage gebeurt digitaal en via menselijke bronnen, bijvoorbeeld via diaspora, mensen op strategische posities of via inlichtingenofficieren op ambassades.

De dreiging van spionage door landen als China, Rusland en Iran is sinds 2022 onverminderd hoog gebleven. Wel lijken er steeds meer landen te zijn die in Nederland willen spioneren, met name digitaal via offensieve cyberprogramma's. Zulke vormen van spionage zijn laagdrempelig, waardoor ze relatief vaak voorkomen. De toename kan komen door de verschuivingen in de gekende wereldorde, maar heeft mogelijk ook te maken met een verbeterd zicht van inlichtingen- en veiligheidsdiensten op statelijke dreigingen.

Aanhoudende klassieke spionage via menselijke bronnen

Onder meer landen als China, Rusland en Iran ondernemen spionageactiviteiten in Nederland. Buitenlandse overheden en inlichtingendiensten maken gebruik van netwerken van menselijke bronnen. Het kan hierbij ook gaan om leden van diasporagemeenschappen. Ook in Nederland proberen verschillende landen burgers en organisaties te rekruteren om inlichtingen te verzamelen. Het gaat hierbij onder andere om personen die werkzaam zijn op strategische posities, in vitale sectoren of die toegang hebben tot relevante (persoons)data. Ook kunnen landen inlichtingenofficieren stationeren op ambassades.

Sinds de Russische inval in Oekraïne heeft een aantal westerse landen honderden Russische inlichtingenofficieren uitgezet. Dit maakt het voor Russische diensten moeilijker om onder diplomatieke dekmantels menselijke bronnen in westerse landen voor zich te winnen en het contact met bestaande menselijke bronnen te onderhouden. Deze lacune kan mogelijk gedeeltelijk met behulp van digitale middelen overbrugd worden. Daarnaast hebben Russische diensten nog volop mogelijkheden om

niet-diplomatieke dekmantels in te zetten om inlichtingen te vergaren in de Europese Unie, en dus ook in Nederland. Denk hierbij aan het inzetten van zakelijke of academische voorwendselen.

Rusland verzamelt politieke inlichtingen, zoals over de Europese Unie en ministeries van Buitenlandse Zaken, en militaire inlichtingen, bijvoorbeeld over de NAVO en ministeries van Defensie. Ten aanzien van Nederland richt Rusland zich ook op de vele internationale organisaties die hier zijn gevestigd (zie hoofdstuk Diplomatiek en politiek).

Aanhouding op verdenking van schending staatsgeheimen
In oktober 2023 werd een man aangehouden op verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie. De rechter heeft nog geen uitspraak gedaan in deze zaak. De man, een Nederlander met Marokkaanse achtergrond, was volgens het Openbaar Ministerie op weg naar Marokko en had tijdens de aanhouding een groot aantal digitale (staatsgeheime) documenten bij zich, waaronder een analyse van de AIVD over Marokkaanse inlichtingenactiviteiten in Nederland. De man, die vanwege zijn functie bij de NCTV toegang had tot dit soort informatie, wordt verdacht van het schenden van staatsgeheimen, al dan niet in opdracht van een buitenlandse mogendheid.[14]

Digitale spionage omvangrijker

Steeds meer landen, waaronder Rusland, China, Iran en Noord-Korea, beschikken over offensieve cyberprogramma's die ingezet kunnen worden om te spioneren.[15] Daarnaast neemt het aantal landen toe dat grotere offensieve capaciteiten in die richting ontwikkelt. Dergelijke programma's zijn vaak onderdeel van (grootschalige) internationale campagnes en kunnen ook worden ingezet tegen Nederland en onze belangen.

Ieder land spioneert uit eigen motieven. Zo zijn Russische cyberactiviteiten tegen Europa gericht op politieke spionage, heimelijke beïnvloedingsactiviteiten en digitale sabotageactiviteiten (zie volgend hoofdstuk). Sinds de Russische inval in Oekraïne in 2022 onderkennen de AIVD en de MIVD een toename in het aantal actoren binnen de Russische overheid of die door de Russische overheid worden gesteund of aangestuurd, die zich bezighouden met digitale spionage. Hun operaties raken Nederland direct of indirect, zoals via compromittering van systemen van Nederlandse bondgenoten.

China richtte zich lange tijd vooral op economische spionage, maar van deze beperkte focus is geen sprake meer. Het land heeft een groot, geavanceerd en professioneel digitaal spionageprogramma opgetuigd. Chinese aanvalsgroepen zijn wereldwijd actief en treffen bedrijven, overheden en organisaties. De Chinese informatiebehoefte is ongekend en omvat vrijwel ieder onderwerp dat mogelijk relevant kan zijn voor het land: diplomatiek, parlementaire aangelegenheden, militair, economie, technologie, wetenschap, krijgsmachten, geografie, financiën, dissidenten, gezondheid, sport, persoonsgegevens, reisinformatie, bulkdata en telecommunicatie. Gezien deze grote en diverse informatiebehoefte kunnen cyberaanvallen gericht zijn tegen alle landen in de wereld, en richten Chinese statelijke actoren zich ook structureel op landen in Europa, waaronder Nederland. Daarnaast kunnen vrijwel alle Chinese statelijke cyberactoren zich op opportunistische wijze op Nederlandse belangen richten, als zij daar kwetsbaarheden aantreffen. Deze digitale activiteiten zijn inmiddels dermate geavanceerd en omvangrijk, dat waarschijnlijk slechts een deel van de Chinese cyberoperaties tegen Nederlandse belangen tijdig wordt gedetecteerd en vervolgens gemitigeerd. Dit vormt ook een grote uitdaging voor de Nederlandse weerbaarheid.

Iran gebruikt zijn digitale spionageprogramma vooral in het Midden-Oosten en tegen de Verenigde Staten. Specifiek zet het land in op politieke spionage in de regio en tegen primaire tegenstanders. Daarnaast vergaart Iran kennis over Iraanse dissidenten, organisaties of tegenstanders van het regime ongeacht waar ze wonen, inclusief in Nederland, en verzamelt het land bulkdata aan persoonsgegevens binnen de luchtvaartsector.[16] Dit soort spionageactiviteiten kan voor zowel de diasporagemeenschappen als breder in de samenleving leiden tot gevoelens van onveiligheid of angst.

Noord-Korea gebruikt digitale aanvallen grotendeels voor financieel gewin. Noord-Koreaanse actoren proberen ook in Nederland cryptovaluta te ontvreemden, om met hun aanvallen en buitgemaakte winst de opgelegde sancties tegen Noord-Korea te omzeilen. Het land gebruikt daarbij ook Noord-Koreaanse freelance IT'ers, die zich in het buitenland onder valse identiteit laten inhuren bij bedrijven om op die manier geld te verdienen voor het regime, onder andere door data of cryptovaluta te ontvreemden. Het is voorstelbaar dat de opbrengsten van deze acties ook worden gebruikt om wapenprogramma's te financieren. Zo heeft de Europese Unie sancties opgelegd tegen het hoofd van de Noord-Koreaanse inlichtingendienst RGB.[17] Daarnaast richt het land zich op spionage, bijvoorbeeld in de vorm van diefstal van informatie bij onderwijsinstellingen en onderzoeksinstituten. Er zijn vooralsnog geen aanwijzingen dat Noord-Korea bij zijn digitale aanvallen hulp krijgt van andere landen of geavanceerde commerciële spyware inkoopt.

Betekenis voor Nederland

- *Klassieke spionage via menselijke bronnen is doorgaans gericht op specifieke personen, organisaties of instellingen. Dit kan gevoelens van onveiligheid en angst aanwakkeren binnen diasporagemeenschappen of breder in de samenleving. Deze dreiging is in de afgelopen jaren gelijk gebleven.*
- *Daarnaast spioneren steeds meer landen digitaal, via offensieve cyberprogramma's. Zulke vormen van spionage zijn laagdrempelig en ongericht. Statelijke actoren verzamelen massaal digitale gegevens van Nederlandse ingezetenen, die ze op een later moment kunnen gebruiken voor de behartiging van hun eigen belangen. Mogelijk wordt er meer digitale spionage waargenomen omdat het zicht van inlichtingen- en veiligheidsdiensten op statelijke dreigingen verbetert.*
- *Landen als Rusland en China gebruiken grootschalige spionageprogramma's, waarmee ze ook in Nederland informatie kunnen verzamelen om op een later moment te gebruiken. Zulke informatie kan bijvoorbeeld worden ingezet bij laagdrempelige digitale sabotage- en verstoringsaanvallen (zie het volgende hoofdstuk).*

De Kustwacht bewaakt en handhaaft de veiligheid op de Noordzee.

Sabotage

In het grijze gebied tussen oorlog en vrede vinden door heel Europa sabotageacties of pogingen daartoe plaats. Rusland en aan Rusland gelieerde of pro-Russische personen voeren meer sabotageacties uit dan voorheen en nemen daarbij meer en grotere risico's.

Rusland heeft de aanhoudende intentie om via sabotage onrust aan te wakkeren in Europa, ongeacht het verloop van de oorlog in Oekraïne. Omdat sabotageacties onder de drempel van artikel 5 van het NAVO-verdrag blijven, is de verwachting dat het aantal acties verder blijft toenemen. Rusland probeert met deze acties zijn doelen te bereiken, zonder in een daadwerkelijke oorlog met de NAVO te belanden.

In Nederland zijn weliswaar geen voorbeelden bekend van fysieke sabotageacties door statelijke actoren, maar de AIVD en MIVD hebben wel vanuit Rusland voorbereidende handelingen daartoe ontdekt. Bovendien kunnen gebeurtenissen elders in Europa wel invloed hebben op Nederland. Nederland is namelijk een interessant doelwit, onder andere vanwege de vitale maritieme infrastructuur in de Noordzee en zijn positie van doorvoerland. Wel vinden er kleinschalige digitale sabotage- en verstoringsacties plaats in Nederland, net als voorbereidingshandelingen daartoe. Van alle digitale dreigingen heeft sabotage in potentie de grootste impact op de Nederlandse samenleving. Sabotage kan leiden tot maatschappelijke ontwrichting, ontregeling van vitale infrastructuur, verstoringen van militaire operaties of voorbereidingen daarop en economische schade.[18]

Fysieke sabotage ook in Nederland voorstelbaar

De intensiteit van fysieke Russische sabotageacties in de Europese Unie is sinds de Russische inval in Oekraïne toegenomen, vooral in landen die aan Rusland grenzen. Rusland en aan Rusland gelieerde of pro-Russische personen tonen een grotere risicobereidheid dan enkele jaren geleden en plegen agressieve, provocerende of zelfs gewelddadige activiteiten. Rusland rekruteert ook (criminele) burgers voor dit soort acties, die mogelijk niet beseffen waarvoor ze worden ingezet. Sabotageacties richten zich onder meer op organisaties die op verschillende wijzen betrokken zijn bij de oorlog in Oekraïne of het ondersteunen daarvan, en steeds nadrukkelijker op militaire en logistieke locaties in Europa.

De sabotageactiviteiten hebben meerdere doelen. Enerzijds zijn de activiteiten gericht op het vertragen van de westerse leveranties aan Oekraïne. Anderzijds moeten ze verdeeldheid zaaien in het Westen en steun aan Oekraïne ondermijnen door middel van het aanjagen van angst. Daarnaast kan Rusland door de inzet van sabotageactiviteiten testen waar het Westen rode lijnen trekt als het gaat om Russische agressie op het eigen grondgebied. Rusland lijkt hierbij op zoek te zijn naar een model waarbij het de westerse steun aan Oekraïne maximaal kan verstoren zonder een militaire escalatie van het Westen uit te lokken.

Nederland als mogelijk doelwit

Nederland is een interessant doelwit voor statelijke actoren vanwege zijn positie als doorvoerland in het geval van een grootschalig militair conflict, en de aanwezige vitale maritieme infrastructuur in de Noordzee. In de Noordzee liggen belangrijke internetkabels, gasleidingen en windmolenparken die van cruciaal belang zijn voor het functioneren van Nederland, en het aangrenzend buitenland. De bescherming en monitoring van dit uitgestrekte en vrij toegankelijke gebied vormt een uitdaging voor Nederland. Sabotage van vitale processen kan onze nationale veiligheid bedreigen, of het nu fysiek of digitaal plaatsvindt. Het is voorstelbaar dat Rusland in staat is om fysieke sabotageacties in Nederland uit te voeren, hoewel dit voor zover bekend nog niet is gebeurd. Zo brengt het land naar alle waarschijnlijkheid de vitale infrastructuur in kaart en onderneemt het activiteiten die duiden op spionage en voorbereidings-handelingen voor fysieke verstoring en sabotage.[19]

Doel van deze sabotageactiviteiten is waarschijnlijk het verkrijgen van aanvullende handelingsopties voor Rusland, met name voorafgaand aan een conflictsituatie. Het past in het Russische militair-strategische denken om bij een beginnend conflict zo snel mogelijk vitale processen, zoals communicatie, energievoorzieningen en logistieke capaciteiten, van een tegenstander te verstoren of te beschadigen.

Indien er op grote schaal sabotage van Nederlandse vitale infrastructuur plaatsvindt, kan dit leiden tot maatschappelijke ontwrichting. Daarnaast kan Nederland ook de gevolgen ondervinden van sabotage van vitale infrastructuur elders in Europa.[20] Vanwege de verwevenheid van het Europese stroomnet kan een verstoring in Duitsland bijvoorbeeld ook tot uitval in Nederland leiden. De mogelijke uitval van vitale infrastructuur is al meerdere malen concreet geworden in de Europese Unie.

Laagdrempelige digitale sabotage- en verstoringsaanvallen in Nederland

In Nederland zijn digitale sabotagepogingen waargenomen, evenals voorbereidingshandelingen daartoe. Landen als Rusland, Iran en China gebruiken offensieve cyberprogramma's om (in de toekomst) vitale fysieke en digitale infrastructuur te kunnen verstoren of saboteren. In Nederland zijn sabotagepogingen waargenomen, waaronder door Rusland, evenals voorbereidingshandelingen daartoe.

In Nederland vinden laagdrempelige digitale verstoringsaanvallen plaats. DDoS-aanvallen zijn daar een voorbeeld van. Ze zijn laagdrempelig en hebben vaak beperkte impact. Een digitale sabotageaanval kan daarentegen langdurig de beschikbaarheid van digitale diensten, processen of systemen aantasten. Sommige digitale verstoringsaanvallen zijn gelinkt aan Rusland.[21] Zo meldden verschillende politieke partijen dat hun websites in juni 2024, op de dag van de Europese verkiezingen in Nederland, slecht bereikbaar waren door DDoS-aanvallen. De DDoS-aanvallen werden opgeëist door pro-Russische hacktivisten. Eerder waren in juni en augustus 2023 websites van Nederlandse havens en luchthavens

tijdelijk minder goed of niet bereikbaar door DDoS-aanvallen. Ook deze aanvallen zijn opgeëist door pro-Russische hacktivistische groeperingen, waarvan vermoedens van vermenging met de Russische overheid bestaan. De AIVD en de MIVD hebben vastgesteld dat in 2024 een staatsgesteunde hackersgroepering verantwoordelijk is voor een cybersabotageaanval tegen het digitale besturingssysteem van een openbare faciliteit in Nederland.

In andere Europese landen die Oekraïne expliciet steunen, vonden in 2024 aanvallen plaats door Russische *advanced persistent threats*.[vii] Dit gebeurde onder meer tegen politieke partijen in Duitsland en overheidsinstellingen in Polen en Tsjechië. Eerder vonden vergelijkbare aanvallen plaats in onder meer Litouwen, Slowakije en Zweden.[22] Verder waarschuwde de MIVD in september 2024 voor cyberoperaties van eenheid '29155' van de Russische militaire geheime dienst. De focus van deze hackers ligt onder meer op het in beeld krijgen en verstoren van de westerse hulp aan Oekraïne. Hun operaties zijn met name gericht op westerse overheden en vitale infrastructuur.

Nederland is niet primair doelwit van Iraanse digitale sabotage. Recente Iraanse sabotageactiviteiten tegen westerse bondgenoten baren wel zorgen. In 2023 werden de systemen van verschillende Amerikaanse drinkwater- en waterzuiveringsbedrijven gecompromitteerd door staatsgesteunde Iraanse hackers onder de groepsnaam CyberAv3ngers. Deze groep is volgens de Verenigde Staten gelieerd aan de Iraanse Revolutionaire Garde, het militaire elitekorps van Iran. Toegang tot drinkwater is onderdeel van de vitale infrastructuur; misbruik van toebehorende systemen kan grote impact hebben op de gezondheid van de lokale bevolking.[23]

vii Een advanced persistent threat houdt in dat een actor geavanceerde middelen inzet om voor langere tijd ongezien te opereren.

Betekenis voor Nederland

- *Fysieke en digitale sabotageacties in Nederland kunnen leiden tot maatschappelijke ontwrichting. Een sabotageactie gericht op een van de vitale sectoren kan ertoe leiden dat elektriciteit, internet, betalingsverkeer of schoon drinkwater tijdelijk niet beschikbaar is. Dit kan verstrekkende gevolgen hebben. Zo heeft het uitvallen van elektriciteit gevolgen voor telecomvoorzieningen, internet, treinverkeer of op het functioneren van ziekenhuizen.*
- *Rusland gebruikt sabotage om angst en onrust aan te wakkeren in Europa, vanwege de verwachting dat daardoor de politieke en maatschappelijke bereidheid afneemt om met het land in conflict te komen. De verwachting is dan ook dat het aantal sabotageacties verder blijft toenemen.*

In juni 2024 werd in Haarlem een liquidatiepoging gedaan op een in Nederland wonende Iraniër. De politie heeft twee verdachten aangehouden. Een van hen wordt ook verdacht van de mislukte liquidatiepoging op een Spaanse politicus en Iran-criticus.

Statelijke inmenging

Statelijke actoren proberen de Nederlandse samenleving en politieke besluitvorming te beïnvloeden. Behalve om de eerder genoemde spionagedoeleinden, proberen ze bijvoorbeeld diaspora te intimideren, of vindt er ondermijnende beïnvloeding plaats via desinformatie of hack-and-leak-operaties.

Zo verzamelen landen als Iran, Pakistan, Marokko en Turkije inlichtingen over of via hun diasporagemeenschap in Nederland. Van andere landen, zoals China, Eritrea en Syrië wordt het ook waarschijnlijk geacht dat ze dit doen, omdat bekend is dat ze in andere Europese landen inlichtingen over of via hun diaspora verzamelen.[24] Deze autoriteiten blijven Nederlandse burgers als onderdanen zien omdat zij of hun (groot)ouders daar zijn geboren. In oktober 2024 publiceerden de AIVD en NCTV hun analyse 'Over de grens', over dergelijke statelijke inmenging in diasporagemeenschappen. Ondermijnende beïnvloeding gaat om inspanningen van statelijke actoren om hun reputatie te verbeteren, om hun invloed in het buitenland te vergroten en om de publieke opinie en politieke besluitvorming naar hun hand te zetten.

Statelijke inmenging door de gekende landen is sinds 2022 aanhoudend sterk aanwezig gebleven, ook lijkt het aantal landen dat dergelijke methodes inzet, toe te nemen. Net als bij spionage kan deze toename komen door een verschuivende wereldorde, waardoor meer landen baat hebben bij zulke vormen van inmenging. Tegelijkertijd kan de versterkte Nederlandse inzet op het onderkennen van statelijke dreigingen, hebben bijgedragen aan het beter signaleren ervan.

Transnationale repressie tegen diaspora

Statelijke inmenging kan diep ingrijpen in diasporagemeenschappen. Buitenlandse overheden hebben hier verschillende redenen voor, zoals het beschermen van hun interne stabiliteit, vergroten van invloed of tegengaan van kritiek en bedreigingen. Ze kunnen politieke tegenstanders monddood maken, bijvoorbeeld via bedreiging van familie,[25] en leden van diasporagemeenschappen overhalen om inlichtingen te verzamelen, al dan niet onder dwang.[26] In uitzonderlijke gevallen loopt men het risico om slachtoffer te worden van fysiek geweld, ontvoering of zelfs moord. Dergelijke geweldsdreigingen door buitenlandse overheden worden ook wel transnationale repressie genoemd.

Transnationale repressie wordt meestal uitgevoerd door, of op initiatief van, buitenlandse inlichtingendiensten. Landen maken ook gebruik van organisaties en individuen waarmee ze geen directe relatie hebben, oftewel proxy's. Dit zijn bijvoorbeeld organisaties of bedrijven, nationalistische personen of groepen, hackersgroeperingen en lokale criminele groepen. Proxy's beschikken over relevante capaciteiten die overheden kunnen gebruiken voor hun eigen doelen, en hebben bovendien het voordeel van *plausible deniability:* de mogelijkheid om directe betrokkenheid te ontkennen.

Iran in verband gebracht met liquidaties

Met name Iran kent een lange traditie van het plegen van aanslagen op dissidenten in het buitenland.[27] In juni 2024 werd in Haarlem een liquidatiepoging gedaan op een in Nederland wonende Iraniër. De politie heeft twee verdachten aangehouden. Een van hen wordt ook verdacht van de mislukte liquidatiepoging op een Spaanse politicus en Iran-criticus. Op basis van inlichtingen is het waarschijnlijk dat Iran verantwoordelijk is voor de twee liquidatiepogingen. Eerder vermoordden criminelen uit Amsterdam een Iraanse Nederlander in Almere in 2015, en waren criminelen in 2017 mogelijk betrokken bij de liquidatie van een Iraanse Nederlander uit Den Haag.[28] De AIVD beschikt over sterke aanwijzingen dat Iran betrokken is geweest bij beide liquidaties. Vergelijkbare incidenten vonden waarschijnlijk plaats in België, Duitsland, Frankrijk, Groot-Brittannië en Zweden.[29] Daarnaast zet Iran soms extremistische groepen als Hezbollah of individuen in voor het plegen van aanslagen, en gebruikt hierbij geregeld sjiieten met een andere nationaliteit dan de Iraanse of de Libanese.[30]

Iran richt zich in Europa met behulp van criminelen tegen Joodse en Israëlische doelwitten

Behalve diasporagemeenschappen zijn ook Joodse en Israëlische personen, bedrijven, organisaties en diplomatieke vertegenwoordigingen doelwit van Iran.[31] Sinds het uitbreken van de Gaza-oorlog op 7 oktober 2023 is deze dreiging toegenomen. Sinds begin 2024 zijn verschillende aanslagen gepleegd op Israëlische doelwitten in Zweden en Denemarken.[32] In Zweden zou het gaan om aanslagen door jeugdige criminelen, wier bendeleiders door Iran zouden zijn gerekruteerd.[33] Ook zou Iran twee personen undercover naar Zweden hebben gestuurd om Joden te vermoorden.[34] Het land zou vergelijkbare activiteiten uitvoeren in Duitsland en Frankrijk.[35]

Waarschijnlijk probeert Iran Israëlische of Joodse doelwitten te treffen in reactie op de Gaza-oorlog en de Israëlische aanvallen op Libanon, Syrië en Iran. De keuze voor Scandinavië kan samenhangen met de koranverbrandingen in Zweden en Denemarken. Volgens de Zweedse veiligheidsdienst Säpo heeft de Iraanse Revolutionaire Garde een sms-dienst gehackt en opruiende berichten verspreid.[36] Het is vaker voorgekomen dat Iraanse digitale actoren handelen naar aanleiding van bepaalde gebeurtenissen, zoals de koranverbrandingen. Het is daarom voorstelbaar dat ontwikkelingen die politiek gevoelig liggen in Iran, verstoord of beïnvloed worden door Iraanse cyberactoren. Irans activiteiten in Scandinavië zijn mogelijk bepaald door bestaande banden met criminele bendes. Vermoedelijk bevinden de bendeleiders zich in Iran en worden ze door het regime gebruikt om opdrachten te geven aan jeugdige bendeleden in Scandinavië. In ruil voor financieel gewin, eventueel gecombineerd met criminele druk of dwang, zouden jeugdige criminelen aangezet worden tot het plegen van aanslagen.[37]

In Nederland lijken geen jeugdige criminelen op vergelijkbare wijze te worden aangestuurd vanuit Iran. Wel beschikt het land over criminele connecties die in Nederland activiteiten kunnen uitvoeren. Het gaat hierbij om meer ervaren criminele netwerken. In theorie kunnen deze ook richting Israëlische objecten worden ingezet.

Ondermijnende beïnvloeding om beeldvorming te veranderen

Ondermijnende beïnvloeding gaat om inspanningen van buitenlandse overheden om hun reputatie te verbeteren door het tegengaan van kritiek, om hun invloed te vergroten en om de publieke opinie en politieke besluitvorming naar hun hand te zetten. Dit gebeurt op zowel lokaal en nationaal niveau als binnen de Europese Unie. In Europa zijn diverse incidenten van (vermeende) heimelijke politieke inmenging door de media naar buiten gebracht. Zo is in december 2024 een invloedrijke Chinese zakenman Groot-Brittannië uitgezet op verdenking van spionage voor China. Hij bleek banden te hebben met het *United Front Work Department (UFWD)*; een vleugel van de Chinese Communistische Partij die zich bezighoudt met inmenging in andere landen.[38] Eerder dat jaar werd een Chinees-Duitse medewerker van een Europarlementariër van *Alternative für Deutschland* aangehouden op verdenking van het doorspelen van parlementaire stukken van het Europees parlement aan China.[39] De omkoping van Europarlementariërs door Qatar en Marokko in 2022 en de Russische beïnvloedingsoperatie rond digitaal platform 'Voice of Europe'[viii] onderschrijven eveneens dat kopstukken binnen de (inter)nationale politiek worden gebruikt door statelijke actoren.[40]

Dergelijke voorbeelden van ondermijnende beïnvloeding kregen in de afgelopen jaren meer ruchtbaarheid dan daarvoor, maar dit leidt niet tot een afname van zulke acties. Naar verwachting blijven statelijke actoren dan ook heimelijke inmengingsactiviteiten uitvoeren in Europa. Nederland lijkt over het algemeen niet een primair doelwit te zijn, omdat buitenlandse overheden hun activiteiten eerder richten op landen met meer internationale invloed. De gekende pogingen tot heimelijke beïnvloeding gericht op Nederland en de daadwerkelijke effecten hiervan zijn relatief klein gebleken. Statelijke actoren zijn echter opportunistisch; kansen om invloed te verwerven binnen Nederlandse instituties zullen zij aangrijpen.[41] Succesvolle beïnvloedingsacties kunnen in potentie wel significante impact hebben op het functioneren van het Nederlands democratisch bestel. Bovendien verspreiden landen desinformatie om angst en verdeeldheid aan te wakkeren en democratische instituten te ondermijnen. Wanneer dit is gericht tegen andere landen, kan het ook doorwerken in Nederland.

Desinformatie is gericht op het beïnvloeden van diaspora, de Nederlandse samenleving en de politieke besluitvorming. Verspreiding van desinformatie wordt met name gedaan door Rusland, maar ook China speelt een steeds actievere rol. In 2024 werd bijvoorbeeld een pro-Chinees online netwerk van een Chinees PR-bedrijf gesignaleerd, dat desinformatie verspreidde via nepnieuwssites, waaronder enkele Nederlandse websites. Reguliere nieuwsberichten werden afgewisseld met nepartikelen met pro-Chinese narratieven, complottheorieën over het Westen en negatieve berichten over critici van het Chinees bewind. De websites hadden vrijwel geen bereik.[42]

viii Via het digitaal portaal 'Voice of Europe' voerde Rusland een systematische, internationale campagne waarbij de media werden gemanipuleerd en feiten werden verdraaid om Oekraïne, de Europese Unie en haar lidstaten te destabiliseren en om Europese politici aan zich te binden.

Russische pogingen tot ondermijnende beïnvloeding

Rusland richt zijn heimelijke beïnvloeding vooral op landen die het vatbaar acht, of waar het een bepaald strategisch of historisch belang aan hecht. Tevens is Rusland in staat opportunistisch kansen te onderkennen en te benutten in kleinere staten. Met heimelijke beïnvloeding probeert Rusland westerse politieke besluitvorming ten aanzien van Rusland in het eigen voordeel te beïnvloeden en de algehele politieke en militaire steunverlening aan Oekraïne te ondermijnen. Tevens probeert Rusland de westerse politiek-maatschappelijke cohesie te ondermijnen en politieke tegenstanders van Rusland te verzwakken. Tot slot zet Rusland heimelijke beïnvloeding in ten aanzien van het Westen om de Russische binnenlandse stabiliteit te bevorderen.

Rusland ontplooit heimelijke beïnvloeding zowel in het fysieke domein als in het digitale domein, gericht op het beïnvloeden van het publieke debat en het politiek-bestuurlijke besluitvormingsproces. Zo organiseerde Rusland sinds het begin van de oorlog in Oekraïne op heimelijke wijze verschillende zogenaamde 'vredesdemonstraties' in Nederland, die dienden om de Russische binnenlandse bevolking het idee te geven dat Europa zich tegen de steun aan Oekraïne keert. Russische desinformatie vindt in Nederland weerklank in anti-institutionele en de rechts-extremistische bewegingen. Zo gaan er alternatieve verklaringen rond voor het ontstaan van de oorlog in Oekraïne. Deze zou zijn uitgelokt door het land zelf of een gevolg zijn van expansie van het Westen, terwijl het gaat om een illegale invasie van Rusland in een soeverein buurland.

Rusland rekruteert digitaal lokale inwoners in Duitsland om verdeeldheid te zaaien

Rusland rekruteerde in 2024 online meerdere mensen om in Duitsland laagdrempelige sabotageacties met een politieke boodschap uit te voeren. Zo werden meer dan tweehonderdzeventig auto's voorzien van schuim en stickers. In beginsel werden de acties toegeschreven aan milieuactivisten, maar uit onderzoek van Der Spiegel bleek dat het in ieder geval drie mannen betrof uit Duitsland, Servië en Bosnië-Herzegovina, die werden betaald door de Russische geheime dienst. De mannen kregen via berichtenapp Viber instructies voor de acties en het aanleveren van bewijsmateriaal. Volgens het onderzoek van Der Spiegel was het primaire doel haatzaaien over de politieke partij De Groenen (Bündnis 90/Die Grünen).[43] Het is niet de eerste keer dat Rusland 'amateurs' in Europa inhuurt voor de uitvoering van dit soort activiteiten voor relatief lage financiële vergoedingen; ook de Belgische Dienst voor de Veiligheid van de Staat meldde afgelopen jaar een toename te zien van zogenaamde 'freelance-agenten' die voor Rusland werken.[44] In Nederland zijn nog geen activiteiten waargenomen met dergelijke agenten, maar dit is gezien de gebeurtenissen in België, Duitsland en andere Europese landen wel voorstelbaar.

Turks diasporabeleid

Volgens onderzoek van Clingendael voert Turkije een ideologisch gedreven diasporabeleid met gemengde effecten.[45] In Nederland gaat het onder meer om het bevorderen van goed burgerschap, het aanhalen van culturele en religieuze banden met het moederland en het verkrijgen van stemmen voor de grootste Turkse politieke partij, de AKP.[46] Een groot gedeelte van dit beleid bevat geen intimidatie of monitoring van diaspora en is wettelijk toegestaan. Eerder onderzoek van Clingendael stelde dat een kwart van de Nederlanders van Turkse afkomst zich onveilig voelt vanwege de Turkse invloed.[47] Deze onveiligheidsgevoelens leven volgens het rapport vooral bij niet-stemmers en personen die oppositiepartijen aanhangen. Gevoelens van onveiligheid kunnen leiden tot zelfcensuur en daarmee de vrijheid van meningsuiting inperken. Bijna vijftig procent van de Turkse Nederlanders denkt daarentegen dat de Turkse betrokkenheid een positief effect heeft op de veiligheid van de gemeenschap.

Israëlische poging tot beïnvloeding van Nederlandse politiek en samenleving

Ook Israël probeert de politieke en publieke opinie te beïnvloeden in het buitenland, waaronder Nederland. Dit werd geïllustreerd met de verspreiding van een rapport van het Israëlische ministerie van Diaspora en Antisemitismebestrijding, naar aanleiding van ongeregeldheden rondom de voetbalwedstrijd Ajax-Maccabi Tel Aviv in november 2024. Het rapport is niet via de officiële kanalen met de Nederlandse overheid gedeeld, maar is gericht verzonden aan specifieke politici en journalisten.[48] De manier van verspreiding werd door de Nederlandse ministers van Justitie en Veiligheid en van Buitenlandse Zaken ongebruikelijk en, vanwege de mogelijke negatieve gevolgen voor Nederlandse ingezetenen, onwenselijk genoemd.[49] Zo kunnen de genoemde personen worden geïntimideerd of bedreigd, of in het ernstigste geval aangevallen.[50]

Iran gebruikt cyberprogramma voor ondermijnende beïnvloeding

Iran gebruikt een offensief cyberprogramma onder meer voor ondermijnende beïnvloeding. Dit programma wordt vooral ingezet in het Midden-Oosten en tegen de Verenigde Staten, maar ook tegen Nederland. Behalve voor politieke doelen, gebruikt Iran het in mindere mate voor economische of financiële doelen.[51] Iran zet dit programma in voor het verzamelen van kennis over Iraanse dissidenten, organisaties en tegenstanders, politieke spionage en het vergaren van bulkdata aan persoonsgegevens binnen de luchtvaartsector.[52] Ook proberen aan Iran gelieerde online persona's via hack-and-leak-operaties bepaalde boodschappen te versterken of beleidswijzigingen af te dwingen.

Bij een klassieke hack-and-leak-operatie krijgt iemand door middel van een hackaanval toegang tot persoons- of organisatiegevoelige informatie, om deze informatie vervolgens te delen via (sociale) media of met bepaalde personen en instanties. Gevoelige informatie wordt direct gepubliceerd of, afhankelijk van het doel, eerst gemanipuleerd. Op deze manier kunnen intimiderende cyberoperaties worden uitgevoerd door een statelijke actor, een staatsgesteunde hackgroep of door een zelfstandige groep, zoals een hacktivistische groep. Aan Iran gelieerde online persona's richtten zich via zulke operaties op de beeldvorming rondom de Gaza-oorlog. Zo probeerde Iran om Israël in een negatief daglicht te zetten terwijl het eigen handelen positief werd weergegeven. Deze online persona's werden al eerder ingezet door Iran. Tijdens een grootschalige cyberoperatie in Albanië in 2022 maakte zeer waarschijnlijk Iran gebruik van online persona's, om (vermeend) gestolen data te publiceren en de boodschap uit te dragen dat de verzetsbeweging de Iraanse Volksmoedjahedien niet langer welkom zou moeten zijn in het land.

Ook beschuldigde het Amerikaanse Ministerie van Justitie drie leden van de Iraanse Revolutionaire Garde van inmenging, omdat ze via een hack-and-leak-operatie gestolen documenten van campagnepersoneel van een presidentskandidaat wilden delen met de media.[53]

Daarnaast zet Iran waarschijnlijk desinformatie in om zijn doelstellingen na te streven. Voor de verspreiding van desinformatie gebruikte Iran volgens OpenAI nepnieuwssites en kunstmatige intelligentie voor het genereren van content.[54] Tijdens Amerikaanse verkiezingen in 2020, 2022 en 2024 verspreidde Iran desinformatie om het publieke debat te beïnvloeden.

Betekenis voor Nederland

- *De impact van transnationale repressie richting diaspora of individuele belangendragers in Nederland is aanzienlijk. Sommige personen die tot een diasporagemeenschap behoren durven zich niet uit te spreken vanwege gevoelens van onveiligheid, aangewakkerd door bedreigingen of zelfs aanslagen. Transnationale repressie kan ook leiden tot spanningen en gevoelens van onveiligheid tussen verschillende groepen in Nederland. Nederland hecht veel waarde aan de grondwettelijke vrijheden, waaronder de vrijheid van meningsuiting. Dit soort acties tasten de grondwettelijke vrijheden aan van Nederlandse ingezetenen en zijn daarmee ondermijnend voor de sociale en politieke stabiliteit.*
- *Nederland vormt voor de meeste buitenlandse overheden geen belangrijk doelwit voor ondermijnende beïnvloeding en de democratische instituties zijn zodanig weerbaar dat beïnvloedingspogingen lang niet altijd succesvol zijn. Statelijke actoren zijn echter opportunistisch en zullen kansen aangrijpen om aan invloed te winnen in de Nederlandse samenleving en politieke besluitvorming.*
- *De dreiging van statelijke inmenging vanuit gekende landen als Rusland en Iran is sinds 2022 min of meer gelijk gebleven. Het aantal landen dat dergelijke methodes inzet, lijkt wel toe te nemen, behalve door de veranderende wereldorde kan dat ook komen door een verbeterd zicht op statelijke dreigingen.*

De RWG containerterminal op de Rotterdamse Tweede Maasvlakte.

Economie

Statelijke actoren zetten legitieme en heimelijke economische instrumenten in om hun (geopolitieke) doelen te behalen. Wanneer het primaire doel is om de eigen economische positie te bevorderen, kunnen instrumenten als overnames en investeringen ook worden ingezet om andere strategische doelen te behalen. Daarnaast is de economie sterk verbonden met geopolitiek. Zo worden strategische afhankelijkheden ingezet als politiek of economisch drukmiddel. Ook voeren steeds meer landen een protectionistisch economisch beleid met handelsbarrières en de beperking van handel in technologische kennis en goederen. Veel landen zetten economische instrumenten in, met China als bekendste voorbeeld. Sinds het aantreden van de Amerikaanse president Trump neemt de inzet van economische instrumenten door de Verenigde Staten toe.

Ongewenste kennis- en technologieoverdracht, of verwerving, kan eveneens worden ingezet voor economische, maar ook militaire doeleinden. Deze dreiging was al hoog, maar door ingestelde sancties tegen landen zoeken statelijke actoren alternatieve manieren om aan technologische kennis te komen. Door de opgelegde sancties gaan statelijke actoren eerder over tot het gebruik van heimelijke verwerving. Zowel economische instrumenten als technologische kennis, zijn middelen om politieke en militaire macht te vergroten.

Strategische afhankelijkheden ingezet als drukmiddel

Veel landen streven naar een strategisch autonome economie. Het afhankelijk zijn van een product of dienst uit een ander land kan grote risico's met zich mee brengen, vooral als het risicovolle strategische afhankelijkheden betreft. Dat is het geval wanneer het betreffende product, de dienst of de technologie cruciaal is voor het functioneren van publieke belangen, zoals de economie en de maatschappij, of de afhankelijkheid een risico vormt voor de continuïteit van vitale processen of de toegang tot gevoelige informatie voor derden. Het risico op leveringsonderbrekingen hangt onder meer af van de mate van

marktconcentratie en de mogelijkheid tot substitutie, de aard van de betrekkingen met het land en de mate van wederzijdse afhankelijkheid.[55]

Landen zetten afhankelijkheidsrelaties in als strategisch drukmiddel. Een voorbeeld daarvan is Rusland, dat openlijk en in het geheim inventariseert hoe het zijn belangen in de veranderende energiemarkt kan beschermen en de energietransitie kan vertragen. Zo wil het de afhankelijkheid van fossiele energie zo lang mogelijk blijven benutten. Kort voor en na het uitbreken van de Oekraïne-oorlog werden gasleveringen van Rusland aan Europese lidstaten teruggeschroefd of helemaal stopgezet, om politieke, economische en sociale druk uit te oefenen. Dit raakte ook veel Nederlanders financieel via hogere energierekeningen en de daarmee samenhangende inflatie. Inmiddels heeft de Europese Unie haar energieafhankelijkheid van Rusland voor het grootste deel afgebouwd.

Westerse afhankelijkheid van China

Ook China ontwikkelt eigen industriële en toeleveringsketens om minder afhankelijk te zijn van mondiale waardeketens. Tegelijkertijd worden andere landen afhankelijker van China doordat zij in toenemende mate de technologische standaarden bepalen, concurrenten uit de markt prijzen door productie op te schalen en op grote schaal investeren in sleuteltechnologieën. Dit biedt China economische voordelen en de mogelijkheid om invloed uit te oefenen op andere landen. Wanneer er sprake is van een zogenaamd *lock-in effect* op de door China-gestelde standaarden, moeten andere landen voortborduren op de gestelde standaarden, waardoor de statelijke actor een steeds dominantere positie inneemt. Lock-in effecten kunnen leiden tot risicovolle strategische afhankelijkheden, bijvoorbeeld wanneer Nederland afhankelijk wordt van Chinese technologieën en (toe)leveranciers voor de vitale infrastructuur, zoals energievoorzieningen, telecomnetwerken, watervoorzieningen en transportinfrastructuur.

Met name op het gebied van duurzaamheid, zoals groene technologie, en grondstoffen is de westerse afhankelijkheid van China onmiskenbaar. Het land heeft zich ontwikkeld tot een onmisbare speler in de wereldwijde energietransitie en heeft een dominante positie verworven in de toeleveringsketens van groene technologieën. Voorbeeld hiervan is dat de Europese Unie en de Verenigde Staten voor de korte en middellange termijn grotendeels afhankelijk zijn van Chinese zonnepanelen, windturbines en batterijen, evenals van de samenhangende technologieën en grondstoffen die hiervoor nodig zijn. Daarnaast heeft China voor de delving en verwerking van een groot aantal grondstoffen een monopoliepositie. Dit betreft onder andere grondstoffen die een grote rol vervullen in onder meer het digitale domein en het ruimtevaartdomein. China kan deze afhankelijkheid inzetten om druk uit te oefenen op andere mogendheden.

Handelsconflicten forceren Nederland en de Europese Unie te acteren

Steeds meer landen voeren een protectionistisch economisch beleid. Dat doen zij onder andere door hun eigen bedrijven te steunen met financiële voordelen of door handelsbarrières op te werpen richting buitenlandse bedrijven of overheden. Handel in technologische kennis en goederen wordt gehinderd om de eigen veiligheid en economische en technologische ontwikkeling – en daarmee de geopolitieke machtspositie – te beschermen, die van een ander land te verminderen, of om een ander land te straffen voor bepaalde activiteiten. Zo heeft Nederland uit nationale veiligheidsoverwegingen exportrestricties

opgelegd in de halfgeleiderindustrie. Op zijn beurt heeft China exportrestricties afgekondigd voor bepaalde grondstoffen waarvan het Westen afhankelijk is voor de productie van halfgeleiders.

Ook de Verenigde Staten zetten economische instrumenten in. Met het aantreden van president Trump is een handelsconflict tussen de Verenigde Staten en de Europese Unie waarschijnlijker geworden. Daarnaast is de economische spanning tussen de Verenigde Staten en China in de afgelopen periode verder opgelopen, onder meer door de brede inzet van economische instrumenten zoals instelling van importtarieven. Ook daarin lopen landen als Nederland het risico om te worden meegetrokken; de Verenigde Staten zullen in toenemende mate een dwingend beroep doen op partners om mee te bewegen, zeker op technologie-dossiers. Nederland zal in samenwerking met Europese partners zijn eigen nationale veiligheidsoverwegingen blijven maken. In beide gevallen tonen handelsconflicten de kwetsbaarheid van de Europese toeleverancier sketens: veel Europese overheden en bedrijven zijn in de keten afhankelijk van Chinese en Amerikaanse toeleveranciers. Dit kan ertoe leiden dat de Europese Unie in een lastige positie wordt gebracht, indien een van die landen zichzelf wil ontkoppelen van de ander en van de Europese Unie verlangt hetzelfde te doen. Daarnaast kan een handelsconflict worden ingezet om diplomatieke druk uit te oefenen en leiden tot verstoring van de handel, prijsstijgingen en een verlies van afzetmarkten; dit raakt het concurrentie- en verdienvermogen en dus de welvaart van Nederland.

Verwerving van technologie is cruciaal voor machtsstrijd

Technologie en technologische ontwikkelingen staan centraal in de machtsstrijd tussen statelijke actoren. Wie sleuteltechnologieën in handen heeft, zoals biotechnologie, kwantumtechnologie, kunstmatige intelligentie en halfgeleidertechnologie, is ook geopolitiek bepalend en creëert een sterkte uitgangspositie voor haar toekomstig verdienvermogen. Er is dan ook een zogenaamde mondiale *techrace* gaande tussen met name de Verenigde Staten en China. Landen die voorop willen lopen in de ontwikkeling van technologieën investeren op grote schaal. Nederland en de Europese Unie raken in steeds meer technologiegebieden achterop, wat risico's oplevert voor onze veiligheid en economie. Zo ontstaan er economische machtsconcentraties bij landen die succesvol technologieën ontwikkelen, wat schadelijk kan zijn voor het Nederlandse verdienvermogen. Ook ontstaan er risicovolle strategische afhankelijkheden. Daarnaast kan kennis en technologie uit het Westen worden ingezet voor het ontwikkelen van wapensystemen en spionagecapaciteiten, of voor surveillanceapparatuur waarmee mensenrechten onder druk worden gezet.

Wanneer landen zelf niet beschikken over de kennis en technologie die nodig is voor hun geopolitieke ambities, zoeken ze daar actief naar in het buitenland. Verschillende landen proberen Europese en Nederlandse kennis en technologie te verwerven, zowel in de academische als in de private sector. Dat kan openlijk gebeuren, bijvoorbeeld in de vorm van bedrijfsovernames, gezamenlijke publicaties, talentrekrutering, beursverstrekkingen en internationale fora. Het kan echter ook illegaal plaatsvinden, via (digitale) spionage, ondoorzichtige investeringen die staatsbemoeienis verhullen of het omzeilen van exportrestricties.

Een bekende manier van statelijke actoren om kennis en technologie te verwerven is door gebruik te maken van personen die al werkzaam zijn bij een kennisinstelling of bedrijf. Dit worden ook wel insiders genoemd. De zogenaamde *insider threat* is de dreiging die uitgaat van deze insiders om via legale of illegale manieren kennis en technologie weg te lekken aan statelijke actoren. Statelijke actoren kunnen bijvoorbeeld studenten verplichten om – als voorwaarde voor een studiebeurs – na de studie terug te keren naar het thuisland. Dit vergroot de kans dat de in Nederland opgedane kennis overgedragen wordt aan de overheid, of gelieerde organisaties. In sommige gevallen kan het gaan om sensitieve kennis en technologie, zoals dual use technologie voor civiele en militaire toepassingen. Bovendien kunnen buitenlandse inlichtingenofficieren in Nederland ook illegaal een eigen netwerk van menselijke bronnen opbouwen om kennis en technologie te verwerven. Dit netwerk kan zowel bestaan uit Nederlandse als buitenlandse personen.[56]

De heimelijke verwerving van onze kennis en technologie bedreigt de kennisveiligheid van Nederlandse onderwijs- en onderzoeksinstellingen, het vermogen van bedrijven om te innoveren en geld te verdienen, en de slagkracht van de krijgsmacht. Het kan er ook aan bijdragen dat Nederland op strategisch gebied afhankelijker wordt, onder meer op het gebied van vitale infrastructuur. Gezien de toegenomen focus op kennis en technologie als geopolitiek machtsmiddel en de mondiale techrace, zal deze dreiging de komende jaren blijven bestaan en mogelijk zelfs toenemen zolang Nederland koploperspositie blijft houden in bepaalde technologische domeinen. Ook kunnen kennisinstellingen op de middellange termijn hun strategische koploperspositie verliezen.

Er bestaan ook zorgen over de manieren waarop statelijke actoren en daaraan gelieerde bedrijven, (persoons)gegevens van burgers verzamelen. Dit gebeurt bijvoorbeeld via (gratis) apps, (goedkope) producten en diensten of het inkopen van persoonsgegevens. Deze persoonsgegevens kunnen bruikbaar zijn voor technologische ontwikkelingen, maar kunnen ook worden misbruikt wanneer statelijke actoren de persoonsgegevens en aanverwante data op grote schaal gebruiken om analyses uit te voeren over bevolkingsgroepen.

China de grootste dreiging voor de Nederlandse economische veiligheid en kennisveiligheid

China vormt richting Nederlandse bedrijven en kennisinstellingen al jaren de grootste dreiging op het gebied van economische veiligheid en kennisveiligheid. Voor de Chinese president Xi Jinping staan kennis en innovatie nadrukkelijk ten dienste van China's nationale veiligheid. De Chinese overheid streeft ernaar een belangrijke leidende natie in de wereld te worden, waarbij economische en technologische doelen zijn verweven met militaire en andere veiligheidsdoelen. Zo wil president Xi dat het land op termijn zelfvoorzienend en technologisch onafhankelijk is van het buitenland. Hiervoor is de ontwikkeling van hoogwaardige technologieën zoals halfgeleiders, kunstmatige intelligentie en kwantumtechnologie essentieel.

Er is daarbij sterke overlap tussen China's technologiebehoefte en onderwerpen waar ook de Nederlandse kennisinstellingen en het bedrijfsleven onderzoek naar doen. Personen en instellingen met banden met het Chinese militair-industrieel complex blijven toenadering zoeken tot Nederlandse kennisinstellingen om samen onderzoek te doen naar dual use technologieën, zoals kunstmatige intelligentie. In de praktijk blijft het zoeken naar de juiste balans: de uitwisseling van technologische kennis is van (economisch) belang, maar kent dus ook risico's. De Chinese regering blijft enorm veel geld inzetten om mensen met hoogwaardige kennis en kunde naar China te halen of anderszins hun kennis ten dienste te stellen van Chinese belangen middels zogenaamde talentenrekruteringsprogramma's.

Chinese wetenschappers zoeken toenadering Nederlandse kennisinstellingen
Tussen 2012 en 2022 deden meer dan negentig Chinese (militaire) wetenschappers kennis op bij Nederlandse kennisinstellingen. In 2021 promoveerde een Chinese wetenschapper aan een Nederlandse Technische Universiteit, waar hij onderzoek deed naar hypersone vliegtuigen. De wetenschapper studeerde in China aan de Air Force Engineering University (AFEU), een onderdeel van het Volksbevrijdingsleger dat opleidingen verzorgt in de techniek en trainingen voor luchtgevechten. Na zijn promotie in Nederland kreeg de wetenschapper een vaste aanstelling aan de AFEU. Zijn onderzoek heeft zowel civiele als militaire toepassingen. De kennis kan worden toegepast in onderzoek ten behoeve van de ruimtevaart, maar ook worden gebruikt in de ontwikkeling van hypersone wapens.[57]

Nederland doelwit van technologische verwervingsactiviteiten door Rusland, Iran en Noord-Korea

Ook Rusland, Iran en Noord-Korea proberen in Nederland technologische kennis te verwerven om zo hun machtspositie uit te bouwen. Zo richt Rusland zich op de ontwikkeling van militaire toepassingen van verschillende technologieën - een ambitie die is versterkt door de oorlog in Oekraïne. Internationale sancties bemoeilijken de toegang tot gevoelige technologie en apparatuur. Daarom probeert Rusland deze technologie op heimelijke wijze te vergaren, bijvoorbeeld door de inzet van frontbedrijven om exportrestricties te omzeilen. Zo zijn er in Nederland recente voorbeelden waarbij individuen en bedrijven het sanctieregime tegen Rusland hebben ontdoken en dual-use goederen hebben geleverd aan Russische bedrijven. Dit gebeurt zowel direct als indirect, via 'omleidingslanden' zoals Armenië, Kazachstan, Turkije en Turkmenistan.[58] Het gaat hierbij onder meer om computeronderdelen, drones en chips.

Russische ingenieur verdacht van bedrijfsspionage
Er loopt sinds 2024 een rechtszaak tegen een Russische ingenieur vanwege verdenking van bedrijfsspionage bij ASML. Hij zou onder andere handleidingen van microchips hebben gestolen en deze vervolgens via mails, chats en online bestanden gedeeld hebben. Ook zou hij korte bezoeken aan Rusland hebben gebracht waar hij mogelijk fysiek nog meer informatie overhandigd heeft. De kennisoverdracht zou de Russische chiptechnologie mogelijk verder hebben gebracht.[59]

Ook Iran wil kennis en technologie verwerven in Nederland en andere westerse landen, onder andere via heimelijke verwervingsnetwerken, kennisinstellingen en studenten en onderzoekers. Het betreft hier met name kennis en technologie voor ontwikkeling en onderhoud van ballistische raketten. Noord-Korea vergaart informatie over wetenschappelijke onderzoeken en internationale politieke standpunten. Ook is informatie gestolen bij organisaties die gericht zijn op hoogwaardige (militaire) technologie, inclusief organisaties in Nederland.

Spanningen rondom Taiwan kunnen Nederlandse economie raken

Aan de andere kant van de wereld lopen de spanningen rondom Taiwan op. China heeft onverminderd de intentie om Taiwan met het vasteland te verenigen en controle te krijgen over het overgrote deel van de Zuid-Chinese Zee. Hoewel China de drempel naar een gewapend conflict met Taiwan nog niet heeft overschreden, groeit de laatste jaren het aantal en de schaal van Chinese militaire en paramilitaire oefeningen, patrouilles en verkenningen. Een crisis aldaar zou een directe, grote impact hebben op Nederland. Voor Nederland als handelsland en de wereldeconomie in het algemeen zijn de maritieme handelswegen door de Zuid-Chinese Zee en de Straat van Taiwan van groot belang. Daarnaast zijn Taiwanese bedrijven essentieel in de productie van halfgeleiders. Dit maakt het eiland een kritieke schakel in de productieketens voor civiele en militaire elektronica. De economische impact van een conflict is lastig te voorspellen, maar zou zeer waarschijnlijk groot zijn.

Betekenis voor Nederland

- *De inzet van economische instrumenten door statelijke actoren kan grote gevolgen hebben voor Nederland. Op de korte termijn kan het leven duurder worden door verhoogde energieprijzen en handelsconflicten. Daarnaast dragen handelsbelemmeringen eraan bij dat Nederlandse bedrijven minder productief (kunnen) worden en het concurrerend vermogen structureel (mogelijk) afneemt. Handelsconflicten en exportrestricties op bepaalde grondstoffen of (half) producten kunnen nadelige gevolgen hebben voor zowel de Nederlandse economie als onze koploperspositie in bepaalde technologische domeinen. Dit kan ertoe leiden dat Nederland afhankelijker wordt van andere landen.*

- *De inzet van economische instrumenten door landen als China is onverminderd hoog en ernstig. Het risico op handelsconflicten is toegenomen sinds het aantreden van de Amerikaanse president Trump. Het instellen van sancties tegen de handel in technologische kennis en goederen draagt eraan bij dat statelijke actoren zich eerder gedwongen voelen om over te gaan op heimelijke verwerving. Nederland zal vanwege zijn voorloperpositie in een aantal sectoren een aantrekkelijk doelwit blijven voor statelijke actoren.*

- *Technologie staat steeds centraler in de geopolitieke machtsverhoudingen. Dit leidt tot een mondiale techrace waarin wereldwijd flink wordt geïnvesteerd in sleuteltechnologieën. Nederland en de Europese Unie raken in steeds meer opkomende technologiegebieden achterop. Dit leidt tot strategische afhankelijkheden en kan onze veiligheid en welvaart ondermijnen.*

- *De inzet van economische middelen raakt ook aan de effectiviteit en het voortzettingsvermogen van onze krijgsmacht. De beschikking over cruciale technologieën uit Taiwan kan bijvoorbeeld worden bedreigd door oplopende territoriale- en handelsconflicten. Technologische verwerving kan eveneens verstrekkende gevolgen hebben. Wanneer andere landen de beschikking krijgen over dezelfde technologische kennis, kunnen zij sterker worden en kan de effectiviteit van onze krijgsmacht afnemen.*

Het hoofdkwartier van de Verenigde Naties in New York waar de VN-Veiligheidsraad gehouden wordt.

Diplomatiek en politiek

Landen zijn steeds meer bereid hun macht actief in te zetten om hun belangen te verdedigen bij internationale instituties en samenwerkingsverbanden. Hoewel dit niets nieuws is, lijken de veranderingen in de wereldorde steeds meer effect te hebben. Zo gebruiken landen de mogelijkheden om aan macht te winnen en belangen beter te kunnen behartigen. Dit kan eraan bijdragen dat de Nederlandse invloed op het internationale toneel afneemt.

Statelijke actoren zien internationale instituties en verbanden als een middel om aan invloed te winnen, bijvoorbeeld door hun effectiviteit en geloofwaardigheid te ondermijnen of door de heersende kaders en normen te veranderen. Ook kunnen dergelijke gremia een doelwit vormen van statelijke actoren, wat de continuïteit en onafhankelijkheid van internationale juridische instituten kan ondermijnen en daarmee de internationale rechtsorde direct kan bedreigen. Om hun invloed te vergroten zetten niet-westerse landen tot slot alternatieve instituties en samenwerkingsverbanden op, waarop het Westen beperkte of geen invloed heeft.

Beïnvloeding van bestaande instituties

Verschillende landen zijn ontevreden met de bestaande, op westerse regels gebaseerde wereldorde en willen deze meer in lijn brengen met hun eigen belangen. Zo streven verschillende statelijke actoren naar vermindering of vervanging van de Amerikaanse hegemonie en naar vervanging van het huidige model van de internationale rechtsorde. Ook de Verenigde Staten nemen een andere positie in ten aanzien van de internationale rechtsorde dan in de afgelopen decennia. Nederland is als relatief kleine speler met een open economie en beperkte militaire middelen juist gebaat bij een internationale orde die functioneert op basis van recht in plaats van macht.

Landen proberen aan invloed te winnen door bestaande instituties van binnenuit en van buitenaf te beïnvloeden. Zo gebruiken verschillende staten hun vetorecht in de Veiligheidsraad van de Verenigde Naties voor het blokkeren van resoluties die in lijn zijn met VN-doelstellingen. Daarmee ondermijnen ze de effectiviteit en geloofwaardigheid van de Verenigde Naties. Rusland blokkeerde in 2024 bijvoorbeeld toezichtmaatregelen omtrent internationale sancties tegen Noord-Korea. De Noord-Koreaanse levering van wapens en mankrachten aan Rusland voor de oorlog in Oekraïne is een aannemelijke verklaring voor

het Russische veto.[60] Sinds het uitbreken van de Gaza-oorlog in 2023 blokkeerden de Verenigde Staten per veto meerdere resoluties in de Veiligheidsraad over een staakt-het-vuren in Gaza. Nieuw is dit niet; de vijf permanente leden van de Veiligheidsraad gebruiken hun vetorecht vaker om hun eigen geopolitieke belangen te dienen, drie kwart van alle uitgesproken veto's sinds 1989 komt van Rusland en de Verenigde Staten.[61]

Een consequentie van de veranderende machtsverhoudingen is dat meer landen proberen om de kaders en normen van internationale gremia en instituties van binnenuit te beïnvloeden door posities binnen deze organen in te nemen. Zo probeert China bij belangrijke posten binnen de Verenigde Naties Chinezen geplaatst te krijgen, beginnend vanaf niveau directeur. Op deze wijze hoopt het Chinese belangen en opvattingen steeds meer te integreren binnen de Verenigde Naties, om zo de internationale rechtsorde aan te passen naar een voor China gunstig model.

Instituties als doelwit van statelijke actoren

Internationale instituties en samenwerkingsverbanden kunnen een doelwit vormen voor statelijke actoren, vanwege hun functie, rol en de belangen die landen daarbij hebben. Het kan gaan om het frustreren van die rol of het verwerven van waardevolle informatie. Voorbeelden hiervan zijn de Russische hackpoging bij de OPCW in 2018 en de verstoring door de AIVD in 2022 van een Russische inlichtingenofficier die bij het Internationaal Strafhof in Den Haag stage wilde lopen.[62] Alhoewel Nederland hierbij niet het primaire doelwit was, raken dergelijke activiteiten van statelijke actoren aan de Nederlandse democratische rechtstaat, waarvan deze instituties onderdeel zijn.

Bekende doelwitten van statelijke inmenging zijn in Nederland aanwezige internationale instituties zoals het Internationaal Strafhof en het Internationaal Gerechtshof.[63] De Verenigde Staten en Israël uitten publiekelijk dreigementen richting het hof, en de Verenigde Staten hebben sancties ingesteld.[64] Dit zou de werkzaamheden van het hof kunnen beschadigen of zelfs stilleggen, onder meer omdat het hof mogelijk geen of beperkte toegang heeft tot financiële dienstverlening. Op dit moment zijn er uitsluitend sancties opgelegd tegen een hoofdaanklager vanwege de arrestatiebevelen van het Hof tegen de Israëlische premier en voormalig minister van Defensie. Een verdere invulling van de sanctielijst is op termijn echter reëel. De Amerikaanse sancties kunnen op termijn diepgaande consequenties hebben voor het functioneren van het hof, en daarmee voor de vervolging en berechting van personen die verdacht worden van het plegen van internationale misdrijven, zoals genocide, misdaden tegen de menselijkheid of oorlogsmisdrijven.[65] Ook zijn de hoven voor een groot aantal landen een interessant doelwit van spionage en ondermijnende beïnvloeding, omdat hun onderdanen aldaar berecht kunnen worden.

Dit soort activiteiten kan de continuïteit en onafhankelijkheid van internationale juridische instituten ondermijnen; ze vormen daarmee een directe dreiging tegen de internationale rechtsorde. Bovendien hebben ze impact op Nederland, vanwege de samenwerkingsrelatie en omdat het gastland verantwoordelijk is voor de veiligheid van de hoven. Wanneer Nederland informatie inbrengt bij zulke instituties en deze via heimelijke wegen belandt bij statelijke actoren, raakt dat ook aan de nationale veiligheid.

Parallelle instituties als tegenwicht

Bestaande internationale instituties en multilaterale samenwerkingsverbanden kunnen ook worden beïnvloed of ondermijnd door het opzetten van nieuwe en alternatieve instituties en samenwerkingsverbanden. Door het opzetten van nieuwe samenwerkingsverbanden waarin het Westen beperkte of geen invloed heeft, proberen landen hun geopolitieke invloed uit te breiden. Bovendien kunnen ze tegenwicht bieden tegen bestaande politieke invloedssferen, zoals de Verenigde Staten of de Europese Unie, en zo de wereldorde herstructureren of tenminste diverser maken. China presenteert zich daarbij als leider van het 'Mondiale Zuiden'. Door zijn voortrekkersrol binnen deze instituties en door de lancering van mondiale initiatieven op het gebied van infrastructuur, ontwikkeling en veiligheid, heeft China een 'diplomatieke orde' gecreëerd die parallel loopt aan westerse overlegorganen als de G7. Ieder land heeft het recht om alternatieve samenwerkingsverbanden te initiëren en zodoende invloedrijker te worden, maar dit kan bestaande internationale instituties – waarin Nederland zijn belangen behartigt – op termijn uithollen of ondermijnen. Hierdoor kan de internationale invloed van Nederland afnemen, tenzij Nederland op bepaalde fronten of initiatieven aansluiting vindt.

Bij het oprichten van alternatieve samenwerkingsverbanden spelen middelgrote staten en opkomende spelers een belangrijke rol. Deze landen zijn zich bewust van hun toegenomen strategisch belang en maken gebruik van de rivaliteit en strijd tussen de grootmachten.[66] Dit kwam onder meer tot uiting in 2023, toen meer dan veertig landen hun interesse kenbaar maakten om lid te worden van BRICS, een economisch samenwerkingsverband dat als doel heeft tegenwicht te bieden aan de westerse hegemonie over de wereldeconomie. De inmiddels met vijf landen uitgebreide alliantie heeft de afgelopen jaren verder aan strategisch belang gewonnen. BRICS-landen leggen steeds meer economisch gewicht in de schaal, meer dan vijftig procent van de wereldbevolking woont in deze landen. Bovendien vinden sommige landen elkaar in toenemende mate in een antiwesters sentiment, ondanks hun politieke, geografische en culturele verschillen. Tegelijkertijd zijn de belangenverschillen en de vijandigheid tussen verschillende BRICS-landen nog altijd groot en is er geen eensgezindheid over de houding tegenover het Westen.[67] Sommige landen proberen een groot deel van de internationale rechtsorde op de schop te nemen, terwijl anderen bepaalde aspecten van de bestaande wereldorde proberen te hervormen.

Zoeken naar samenwerking

Ten slotte proberen landen binnen de bestaande en nieuwe samenwerkingsverbanden andere actoren voor zich te winnen voor het nastreven van hun eigen doelen, met de verandering van mondiale of regionale machtsverhoudingen als mogelijk gevolg. Landen ontvangen bij gelegenheid economische, politieke of militaire voordelen in ruil voor steun. Zo werken Rusland, China, Iran en Noord-Korea steeds meer samen op militair en diplomatiek gebied, wat de huidige internationale rechtsorde (verder) ondermijnt. Deze samenwerkingen zijn overigens noch vanzelfsprekend, noch soepel. Verschillende landen, waaronder China en Rusland, halen hun banden aan met Afrikaanse landen. Waar de Chinese aanwezigheid vooral gericht is op economische investeringen, waaronder infrastructurele projecten, zoekt Rusland de samenwerking op binnen het veiligheidsdomein. In ruil ontvangt Rusland met regelmaat steun van verschillende Afrikaanse landen in internationale fora als de Verenigde Naties, bijvoorbeeld in relatie tot de oorlog in Oekraïne.

Rusland steeds actiever in Afrika

Rusland heeft de afgelopen jaren gestaag zijn (para)militaire aanwezigheid in Afrika uitgebreid en heeft de intentie nog actiever te worden op het continent. Wanneer het tot een wapenstilstand komt in Oekraïne, is het waarschijnlijk dat Rusland militair materieel en personeel zal vrijmaken voor inzet in Afrika. De Russische (para)militaire aanwezigheid in Afrika vormt onderdeel van de (hybride) geopolitieke strijd van Rusland als systeemrivaal van het Westen. Afrika vormt de zuidflank van het Europese gedeelte van het NAVO-grondgebied.

De Russische (para)militaire aanwezigheid aldaar kan mogelijk een dreiging vormen voor eenheden van NAVO-landen en de kritieke infrastructuur en aanvoerlijnen waarvan zij afhankelijk zijn. Ook ondermijnt Rusland in Afrika het Westen op militair gebied: Franse en Amerikaanse troepen zijn door pro-Russische regimes gedwongen tot terugtrekking. Daarnaast jaagt Rusland economische belangen na door toegang te verkrijgen tot vitale grondstoffen of probeert het Westen hiervan te onthouden. Tot slot heeft de Russische (para)militaire aanwezigheid in landen invloed op de veiligheidssituatie aldaar, bijvoorbeeld bij de bestrijding van jihadisme.

Betekenis voor Nederland

- *Nederland heeft als gastland van het Internationaal Strafhof en het Internationaal Gerechtshof een bijzondere verantwoordelijkheid. De aanwezigheid van de hoven maakt Nederland ook een nadrukkelijk doelwit van spionage en ondermijnende beïnvloeding. Bovendien kunnen buitenlandse dreigementen en sancties op internationale hoven ook doorwerken richting Nederland. Landen kunnen bijvoorbeeld besluiten om sancties op te leggen die ook Nederlanders kunnen raken, of visumaanvragen van Nederlanders afwijzen.*
- *De beïnvloeding van bestaande instituties en de oprichting van parallelle instituties zijn consequenties van de veranderende machtsverhoudingen. Landen als China gebruiken de mogelijkheden om aan macht te winnen en hun belangen beter te kunnen behartigen. Zulke ontwikkelingen kunnen eraan bijdragen dat de Nederlandse invloed op het internationale toneel afneemt.*

Eindnoten

1 AIVD, MIVD en NCTV, 'Dreigingsbeeld Statelijke Actoren 2', november 2022, p. 7; Analistennetwerk Nationale Veiligheid (ANV), 'Rijksbrede risicoanalyse nationale veiligheid', 2022, p. 36.

2 Wetenschappelijke Raad voor het Regeringsbeleid (WRR), 'Nederland in een fragmenterende wereldorde', 2024.

3 ANV, 'Leidraad risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid', 2022; NCTV, 'Veiligheidsstrategie voor het Koninkrijk der Nederlanden 2023-2029', 2023, p.11-12.

4 WRR, 'Nederland in een fragmenterende wereldorde'.

5 The Arctic Institute-Center for Circumpolar Security Studies, 'China's Polar Silk road: Long Game or Failed Strategy', 14 november 2023.

6 Ministerie van Economische Zaken, 'Kamerbrief met reactie kabinet op lange-termijn ruimtevaartagenda', 21 februari 2025.

7 Ministerie van Buitenlandse Zaken, 'Kamerbrief inzake introductie ruimteveiligheidsbeleid', 5 maart 2021.

8 Ministerie van Defensie, 'Defensie Ruimteagenda', november 2022.

9 Alexandra Prokopenko, 'Russia's Economic Gamble: The Hidden Costs of War-Driven Growth', Carnegie Politika, 20 december 2024.

10 Organisatie voor het Verbod op Chemische Wapens (OPCW), 'Report of the OPCW Technical Assistance Visit on the Activities Carried Out in Support of a Request by Ukraine', 14 februari 2025; OPCW, 'Report of the OPCW Technical Assistance Visit on the Activities Carried Out in Support of a Request by Ukraine', 18 november 2024.

11 Office of the Director of National Intelligence, 'Iran's Nuclear Weapons Capability and Terrorism Monitoring Act of 2022', juli 2024.

12 Jamie Kwong en Nicole Grajewski, 'Will Iran withdraw from the nuclear non-proliferation treaty?', War on the Rocks, 1 november 2024; 'The nuclear fatwa that wasn't: How Iran sold the world a false narrative', The Atlantic Council, 9 mei 2024; Michael Eisenstadt en Mehdi Khalaji, 'Iran's flexible fatwa: How "expediency" shapes nuclear decision making', The Washington Institute for Near East Policy, 4 februari 2021.

13 Internationaal Atoomenergieagentschap (IAEA), 'Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)', 27 mei 2024.

14 'OM: Topmedewerker van Nationaal Coördinator Terrorismebestrijding spioneerde voor Marokko', De Volkskrant, 7 februari 2024; 'Medewerkers NCTV en politie aangehouden', Openbaar Ministerie, 1 november 2023.

15 AIVD, 'Offensief cyberprogramma: een ideaal businessmodel voor staten', juni 2019.

16 AIVD en NCTV, 'Over de grens, statelijke inmenging in diasporagemeenschappen in Nederland', oktober 2024.

17 Council Implementing Regulation (EU) 2025/389, 'Implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine', 24 februari 2025.

18 AIVD en MIVD, 'Dreigingsbeeld: militaire en hybride dreigingen', december 2024.

19 Ministerie van Infrastructuur en Waterstaat, 'Kamerbrief Voortgang Strategie bescherming Noordzee infrastructuur', 10 juni 2024; MIVD, 'Jaarverslag 2023', april 2024; MIVD en AIVD, '24/2 - De Russische aanval op Oekraïne: een keerpunt in de geschiedenis', februari 2023.

20 AIVD en MIVD, 'Dreigingsbeeld: militaire en hybride dreigingen'.

21 NCTV, 'Cybersecurity Beeld Nederland 2024', oktober 2024.

22 Council of the EU, 'Cyber: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation', 3 mei 2024.

23 America's Cyber Defense Agency, 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities', 18 december 2024; 'VS looft 10 miljoen dollar uit voor informatie over aanvallers waterbedrijven', security.nl, 8 augustus 2024; 'VS meldt aanval op industrieel controlesysteem Amerikaans waterschap', security.nl, 29 november 2023.

24 AIVD en NCTV, 'Over de grens'.

25 Dana Moss, Marcus Michaelsen en Gillian Kennedy, 'Going after the family: transnational repression and the proxy punishment of Middle Eastern diasporas', Global Networks (22), 2022, p. 735-751.

26 AIVD en NCTV, 'Over de grens'.

27 Matthew Levitt, Magnus Ranstorp, Norman Roule, 'Mapping Iranian external actions worldwide', The Washington Institute for Near East Policy, 9 augustus 2024; Matthew Levitt, 'Trends in Iranian External Assassination, Surveillance, and Abduction Plots', CTC Sentinel, februari 2022, p.1-11.

28 AIVD en NCTV, 'Over de grens'; '23 jaar en 6 maanden celstraf voor moord op een Iraanse man in Almere in 2015', Gerechtshof Leeuwarden en Arnhem, Rechtspraak.nl, 24 november 2022; 'Liquidatie Iraanse activist Ahmad Mola Nissi (52)', Opsporing Verzocht, 30 juni 2019; 'Rotterdamse criminelen achter moord op Iraanse activist', RTV Rijnmond, 3 juli 2018.

29 Matthew Levitt en Sarah Boches, 'Iranian External Operations in Europe: The Criminal Connection', ICCT, 16 oktober 2024; Levitt, Ranstorp en Roule, 'Mapping Iranian external actions'; 'Iran is using criminal networks in Sweden', Säkerhetspolisen, 30 mei 2024; 'Iran may be behind attacks on Israeli embassies, Sweden says', BBC News, 2 oktober 2024.

30 Levitt en Boches, 'Iranian external operations in Europe'; Ioan Pop en Mitchell D. Silber, 'Iran and Hezbollah's pre-operational modus operandi in the West', Studies in Conflict & Terrorism 44 (2), 2021, p. 156-179; 'PST: Person accused of terrorism in Copenhagen has unclear connection to Norway', NTB, 8 oktober 2024.

31 Levitt, 'Trends in Iranian External Assassination', p.2.

32 'Schietpartij bij defensiebedrijf in Göteborg; laatste in serie anti-Israëlische aanslagen', De Volkskrant, 10 oktober 2024. 'Two Swedish teens arrested in Copenhagen in connection with Israeli embassy blasts', Euronews, 3 oktober 2024; 'Israëlische ambassades in toenemende mate doelwit van geweld', Trouw, 3 oktober 2024; 'Iran may be behind attacks on Israeli embassies, Sweden says', BBC News, 2 oktober 2024; Levitt, Ranstorp en Roule, 'Mapping Iranian external actions'.

33 Levitt en Boches, 'Iranian external operations in Europe'; 'Sweden wants EU to classify Revolutionary Guards as terrorist organization', VOA, 13 oktober 2024; 'Swedish gangs as intermediaries for Iran – this is what has happened', Swedish Herald, update 4 oktober 2024; Levitt en Boches, 'Iranian external operations in Europe'; Levitt, Ranstorp en Roule, 'Mapping Iranian external actions'.

34 'Swedish FM confronts Iran over murder plot against Jews', AFP, 15 februari 2024.

35 'Iran jaagt in Europa op Israëlische doelwitten en tegenstanders: "Ik wist dat ze iemand gingen sturen", zegt de dissident uit Haarlem', NRC Handelsblad, 5 september 2024.

36 'Sweden blames Iran for cyber attacks after Quran-burnings', BBC News, 24 september 2024; Levitt, Ranstorp en Roule, 'Mapping Iranian external actions'.

37 Levitt en Boches, 'Iranian external operations in Europe'.

38 'Chinese vertrouweling prins Andrew als spion VK uit gezet', NOS, 13 december 2024.

39 'Politie doorzoekt kantoor van Europarlementariër Krah in spionagezaak', NOS, 7 mei 2024; 'AfD-lijsttrekker in Brussel blijft aan en zegt aangehouden medewerker te ontslaan', NOS, 24 april 2024.

40 AIVD en NCTV, 'Over de grens'.

41 Idem.

42 'Paperwall: Chinese Websites Posing as Local News Outlets Target Global Audiences with Pro-Beijing Content', Citizen lab, 7 februari 2024.

43 'Niet de "groene activisten", maar de Russen zaten achter Duitse uitlaten vol schuim', NRC Handelsblad, 5 februari 2025; 'Deutschlandweite Sabotageserie offenbar von Russland gesteuert', Der Spiegel, 5 februari 2025.

44 'Rusland schakelt "freelance-agenten" in voor hybride oorlogsvoering, "zoals bij Uber"', Het Nieuwsblad, 17 januari 2025.

45 Christopher Houtkamp, Nienke van Heukelingen, Teun van der Laan, 'Patriottisme ontmoet pragmatisme: het Turkse diasporabeleid in Nederland', Clingendael, 2024, p.11.

46 Idem, p.12.

47 Christopher Houtkamp, Nienke van Heukelingen, Teun van der Laan , Erwin van Veen, 'Het Turkse diasporabeleid in Nederland: Onderzoek naar het perspectief van de Turks-Nederlandse gemeenschappen en het diasporabeleid van Turkije, Clingendael, 2023, p.2.

48 Ministerie van Justitie en Veiligheid, 'Kamerbrief: Rapport Israëlische ministerie van DAb', 29 november 2024

49 Kamerstukken II vergaderjaar 2024, 36651-34; 'Diplomatieke tik op de Israëlische vingers voor rapport vol beschuldigingen', NRC Handelsblad, 29 november 2024

50 'Israël noemt vredesactivist Thomas van Gool spil in aan Hamas gelieerd netwerk, nu wordt hij bedreigd', Het Parool, 24 november 2024.

51 AIVD, 'Offensief cyberprogramma'; NCTV, 'Cybersecuritybeeld Nederland 2024', p.44.

52 AIVD en NCTV, 'Over de grens'.

53 'Three IRGC Cyber Actors Indicted for "Hack-and-Leak" Operation Designed to Influence the 2024 U.S. Presidential Election', US Department of Justice, 27 september 2024.

54 Microsoft, 'Microsoft threat intelligence report: Iran steps into US election 2024 with cyber-enabled influence operations', 9 augustus 2024, p.1-4; Steven Lee Myers, Tiffany Hsu en Farnaz Fassihi, 'Iran Emerges as a Top Disinformation Threat in U.S. Presidential Race', New York Times, 4 september 2024; 'OpenAI blokkeert Iraanse beïnvloedingsoperatie die ChatGPT misbruikte', Dutch IT Channel, 21 augustus 2024.

55 Ministerie van Economische Zaken en Klimaat, 'Kabinetsaanpak Strategische Afhankelijkheden', 12 mei 2023.

56 AIVD en NCTV, 'Over de grens'; AIVD, MIVD en NCTV, Dreigingsbeeld Statelijke Actoren 2, p. 34.

57 'China stuurt gericht tientallen militaire onderzoekers naar Nederland om gevoelige kennis te vergaren', Follow the Money, 20 mei 2022.

58 'Nederlandse bedrijven lijken sancties Rusland te omzeilen, veel handel met "uitwijklanden"', De Volkskrant, 10 december 2024.

59 'AIVD: Opgepakte ASML-medewerker stond in contact met Russische inlichtingendienst', Trouw, 6 februari 2025; 'Russische oud-medewerker ASML verdacht van diefstal bedrijfsgeheimen', Nieuwsuur, 6 december 2024.

60 'Rusland houdt controle op VN-sancties Noord-Korea tegen', NOS, 28 maart 2024.

61 Oxfam Policy and Practice, 'Vetoing Humanity: How a few powerful nations hijacked global peace and why reform is needed at the UN Security Council', 19 september 2024.

62 'MIVD: we hebben Russische hack van OPCW in Den Haag voorkomen', NOS, 4 oktober 2018; 'AIVD: infiltratie Russische spion bij Strafhof voorkomen', NOS, 16 juni 2024.

63 AIVD en NCTV, 'Over de grens'.

64 'Internationaal Strafhof veroordeelt sancties van VS tegen medewerkers', NOS, 7 februari 2025; 'VS dreigt met wraak tegen Strafhof Den Haag', BNR, 30 april 2024.

65 NOS, '79 landen veroordelen Amerikaanse sancties tegen Internationaal Strafhof', 7 februari 2025.

66 ANV, 'Hoofdrapport Trendanalyse Nationale Veiligheid', 2024.

67 Idem.

Juli 2025
Deze publicatie is een gezamenlijke uitgave van:

Algemene Inlichtingen- en Veiligheidsdienst
(AIVD)
www.aivd.nl

Militaire Inlichtingen- en Veiligheidsdienst
(MIVD)
www.defensie.nl

Nationaal Coördinator Terrorismebestrijding
en Veiligheid (NCTV)
www.nctv.nl