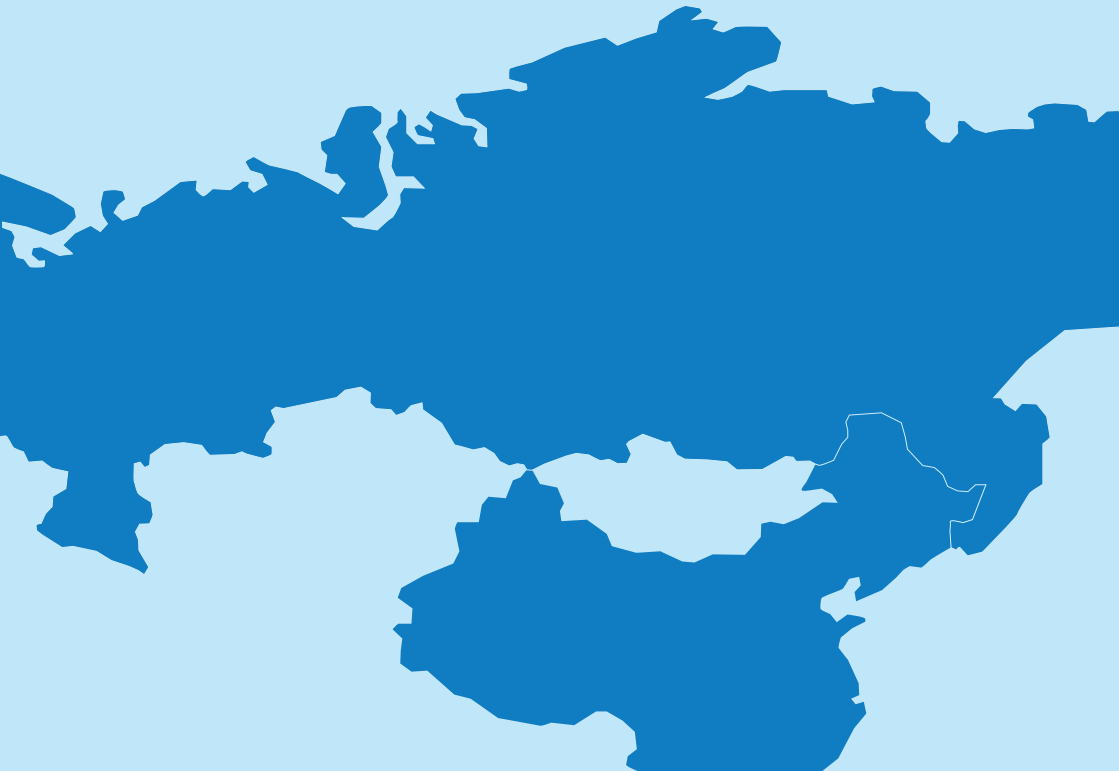
Dreigingsbeeld militaire en hybride dreigingen



Inleiding

Statelijke actoren bedreigen in toenemende mate en op verschillende manieren de nationale veiligheidsbelangen van het Koninkrijk. Door geopolitieke ontwikkelingen zien de AIVD en MIVD een significante toename van hybride dreigingen en door de oorlog in Oekraïne is er een verhoogde militaire dreiging ten aanzien van de fysieke integriteit van het NAVO- en EU-grondgebied. Voor het eerst in lange tijd is de mogelijkheid reëel dat Nederland direct betrokken raakt bij een grootschalig gewapend conflict met een partij of machtsblok, waarvan de gevolgen grote impact op Nederland zullen hebben.

Een militair conflict wordt in de regel voorafgegaan door hybride dreigingen, waarmee wordt gedoeld op activiteiten zoals sabotage, heimelijke beïnvloeding en (cyber)spionage. Gezien de ernstige ontwikkelingen in het huidige dreigingsbeeld, moet Nederland er serieus rekening mee houden dat de grens van een gewapend conflict wordt genaderd. Ruslands optreden en agressie tegen Oekraïne vormen daarbij de grootste risico's. Als onderdeel van het dreigingsbeeld is mondiaal in toenemende mate betrokkenheid van andere staten waarneembaar. Zo vindt Rusland in China een bondgenoot in de (geopolitieke) systeemrivaliteit met het Westen. Door wederzijdse (handels)relaties delen Nederland en China economische belangen. Tegelijk gaat van China een bij uitstek (heimelijke) hybride dreiging uit tegen onze nationale veiligheid. Het voorliggende dreigingsbeeld brengt zowel de samenhang als de onderscheidende aspecten naar voren van de militaire en hybride dreiging voor Nederland. In deze context kan Rusland als de grootste dreiging en China als de grootste uitdaging gezien worden.

Deze publicatie stelt deze twee mondiale hoofdrolspelers centraal, maar ook Noord-Korea en Iran hebben een (toenemende) actieve rol in de dreiging. Zo blijft Noord-Korea raketten ontwikkelen. Enerzijds intercontinentale ballistische raketten en anderzijds korteafstandsraketten die het aan Rusland levert. Ook heeft Noord-Korea de banden met Rusland aangehaald door militairen te leveren voor de strijd tegen Oekraïne. Voorts werkt Iran op diverse gebieden (o.a. op diplomatiek en veiligheidsgebied) samen met Rusland. De toenemende betrokkenheid van deze actoren middels steeds verdergaande samenwerking met Rusland geven een mondiaal karakter aan het conflict. Hiermee intensiveren ze de dreiging die van Rusland uitgaat.

Dit beknopte dreigingsbeeld is opgesteld op basis van de openbare jaarverslagen van de AIVD en MIVD. Deze analyse legt de nadruk op de grootste hybride en militaire dreigingen voor Nederland van dit moment en hoe deze mogelijk in de nabije toekomst kunnen ontwikkelen. Dit dreigingsbeeld kan bijdragen aan de bewustwording van de dreiging en geeft inzicht in de mogelijke impact op de samenleving en waar we ons op moeten voorbereiden.

Rusland

Rusland vormt een acute bedreiging voor de veiligheid van Europa en ook Nederland. Rusland probeert de Europese veiligheidsstructuren ingrijpend te wijzigen door de NAVO en de EU te ondermijnen. Met dat doel voor ogen zet Rusland een verscheidenheid aan hybride middelen in om daarmee het democratische proces in het Westen te beïnvloeden.1 In het jaarverslag 2023 van de MIVD staat nadrukkelijk dat de grootschalige Russische invasie van Oekraïne aantoont dat dreigingen kunnen omslaan in militair geweld met verstrekkende gevolgen, ook op het Europees continent.2 Rusland ziet bovendien deze oorlog als een breder conflict met het Westen. Hiermee heeft deze oorlog voor Rusland een existentieel karakter. Deze significant andere perceptie, gecombineerd met de Russische status van nucleaire grootmacht, zal een politieke oplossing om de Russische agressie tegen Oekraïne te stoppen en op een bestendige manier om met elkaars verschillen om te gaan, uiterst complex maken.. De Russische militaire, politieke en economische dreiging is er één van de lange termijn is. Rusland bereidt zich voor op een post-Oekraïne conflict situatie waarin de NAVO de belangrijkste tegenstander is.

Het is belangrijk om er rekening mee te houden dat Rusland controle zal (willen blijven) behouden over delen van Oekraïne. Dit zorgt in het beste geval voor een aanhoudende financiële en/of materiële inzet van het Westen. De huidige ontwikkelingen maken dat een gewapende confrontatie tussen Rusland en het Westen in de komende jaren en decennia tot de mogelijkheden behoort. Nederland wordt geconfronteerd met een situatie waarin Rusland stappen blijft zetten op de escalatieladder tegen de NAVO, zowel via Russische nucleaire retoriek als militaire intimidatie. De hervorming van de Russische krijgsmacht is bovendien gericht op conflict met de NAVO in de toekomst. In deze dynamiek bestaat ook risico tot ongewilde escalatie. Er zijn geen signalen dat Rusland serieus bereid is te onderhandelen met Oekraïne of stappen wil zetten om de relatie met NAVO-landen te ontspannen.

1 NOS, “VS stelt sancties in tegen Russen om inmenging bij presidentsverkiezingen”, 4 sept. 2024

2 MIVD-jaarverslag 2023

China

Naast de militaire dreiging vanuit Rusland, is er een groeiende hybride dreiging op het gebied van spionage, economische veiligheid en cyber vanuit China waarneembaar. Chinese actoren hanteren een breed palet aan activiteiten om in de Chinese inlichtingenbehoefte te voorzien, die voortvloeit uit de ambitie van de Chinese Communistische Partij om in 2049 een wereldmacht te zijn. 3 Vooral in de halfgeleider- industrie, lucht- en ruimtevaart en de maritieme industrie vormt Nederland voor China een aantrekkelijk spionagedoelwit. Ook beschikt de Nederlandse krijgsmacht over kennis van modern materieel en over militair-operationele expertise die China nodig heeft om zijn eigen krijgsmacht verder op te bouwen.

Een andere potentiële dreiging tegen de krijgsmacht en Nederland vormt de in 2023 bekend geworden Chinese cybersabotagecampagne VOLT TYPHOON. Deze is gericht op prepositionering in Amerikaanse militaire en civiele vitale infrastructuur om daarmee inzetopties te creëren voor tijdens een gewapend conflict. Hoewel er vooralsnog geen activiteiten uit dit programma tegen Europa bekend zijn, is het waarschijnlijk dat ook andere landen , waaronder Nederland, in de nabije toekomst met dit soort Chinese activiteiten te maken zullen krijgen.4 China beschikt over een significante cybercapaciteit met een grote hoeveelheid en verscheidenheid aan betrokken actoren. Uit inlichtingen van de diensten blijkt bijvoorbeeld dat tientallen Chinese bedrijven offensieve cyberoperaties ondersteunen met softwarekwetsbaarheden, malware, (semi-)anonieme aanvalsinfrastructuur en specialistische soft- en hardware voor digitale aanvallen.

In het jaarverslag 2023 van de MIVD staat dat China steeds meer zijn eigen strategische belangen laat prevaleren boven het behouden van een goede relatie met het Westen en zich lijkt voor te bereiden op een strategische confrontatie met het Westen en de VS specifiek.

3 MIVD jaarverslag 2023

4 MIVD jaarverslag 2023

Geopolitieke machtsverschuivingen

Rusland en China hebben hun economische, politieke en militaire samenwerking in 2023 voortgezet en verder geïntensiveerd. Beide landen ambiëren een meer multipolaire wereld, waarbij de rol van de VS (en NAVO) teruggebracht wordt en waarbij China en Rusland een prominentere stem hebben in de regionale en wereld-politiek. China's versterkte relatie met Rusland droeg in 2023 direct en indirect bij aan het in stand houden van de Russische oorlogs-inspanningen in Oekraïne. Daarmee verzwakt China de effectiviteit van Nederlandse en bondgenootschappelijke maatregelen tegen Rusland. De toenemende samenwerking biedt Rusland en China een mogelijkheid de kracht van hun strategische partnerschap verder uit te dragen.

Resumerend ondergaan we een paradigmaverschuiving waarbij de huidige ontwikkelingen in Europa, maar ook in de rest van de wereld (zoals de Indo-Pacific), leiden tot een nu nog ongewisse nieuwe mondiale machtsbalans.

Dreigingen tegen vitale infrastructuur en potentiële effecten daarvan

Specifiek zien we dat de verschillende ontwikkelingen op het gebied van geopolitieke spanningen, de energietransitie en strategische afhankelijk- heden impact kunnen hebben op de continuïteit en beschikbaarheid van vitale processen. De afgelopen jaren is gebleken dat vitale infra- structuur een steeds aantrekkelijker doelwit is voor statelijke actoren.

Waar eerder vooral digitale aanvallen werden uitgevoerd met spionage en verkenning als doel, tonen recente gevallen van brandstichting en dergelijke in onder andere het Verenigd Koninkrijk, Polen en de Baltische staten dat actoren bereid zijn om daadwerkelijk tot fysieke sabotage over te gaan.5 Nederland kan ook de gevolgen ondervinden van sabotage van vitale infrastructuur elders in Europa. Een ander voorbeeld van sabotage van vitale infrastructuur is de verstoring van (civiele) satellietcommunicatie- systemen in Europa. Deze werden verstoord door een malafide software-update die waarschijnlijk gericht was op het platleggen van Oekraïense satellietcommunicatie.6

Van alle cyberdreigingen heeft digitale sabotage potentieel de grootste impact op de Nederlandse samenleving, omdat die bij uitstek kan leiden tot ernstige verstoringen van (de voorbereidingen voor) militaire operaties, grote economische schade en maatschappelijke ontwrichting. De AIVD en de MIVD zagen in 2023 verschillende buiten- landse cyberoperaties, waaronder Russische en Chinese, die gericht waren tegen Europese en NAVO-bondgenootschappelijke doelwitten. Sommige van deze cyberoperaties zijn waarschijnlijk uitgevoerd met als doel een digitale positie binnen vitale infrastructuur te creëren, om deze op een later moment te kunnen saboteren. Bijvoorbeeld tijdens, of kort voorafgaand aan een conflict.7

5 Reuters, "Russia's suspected sabotage campaign steps up in Europe", 21 okt. 2024
6 Dreigingsbeeld Statelijke Actoren, 2022, p. 24.
7 AIVD Jaarverslag 2023; MIVD Jaarverslag 2023

Economische Veiligheid

Vanuit Rusland en China gaat ook een sterke dreiging uit tegen de Nederlandse economische veiligheidsbelangen. Nederland is een open handels- en kenniseconomie met internationaal goed aangeschreven universiteiten en goede transportfaciliteiten. Daarnaast kent de Nederlandse private sector bedrijven die hoogwaardige technologische toepassingen produceren. Nederland is internationaal toonaangevend op strategische thema's als kwantum, AI, lucht- en ruimtevaart, half-geleiders, fotonica en maritieme technologie. Nederlandse bedrijven vergroten bovendien de slagkracht van onze krijgsmacht, en die van bondgenoten, omdat we veel hoogwaardige technologie militaire toepassingen kennen.

Het is van belang voor onze economische en militaire veiligheid om te voorkomen dat unieke en strategische Nederlandse kennis en technologie hun weg vinden naar Rusland of China. Dit verzwakt niet alleen het economisch verdienvermogen, maar ondermijnt ook de slagkracht van onze krijgsmacht. De kans dat de Nederlandse krijgsmacht in aanraking komt met Chinese wapens wordt steeds groter omdat China deze systemen wereldwijd exporteert. Tevens moeten we voorkomen dat Nederland voor de toevoer van strategische grondstoffen en goederen afhankelijk wordt van staten die een bedreiging vormen voor de belangen van Nederland. Zulke risicovolle strategische afhankelijkheden kunnen ertoe leiden dat Nederland kwetsbaar wordt voor politieke of economische dwang. Het gaat hier niet om een potentiële dreiging. De diensten zien op dagelijkse basis dat statelijke actoren gevoelige kennis en technologie bij bedrijven en kennisinstellingen proberen te verwerven. China probeert zowel openlijk als heimelijk Nederlandse kennis en technologie te bemachtigen die bijdragen in het streven om in 2049 een wereldmacht te zijn. Ook zijn er legio voorbeelden van hoe China zijn economische macht aanwendt om invloed over andere landen uit te oefenen. Russische activiteiten zijn vooral gericht op het omzeilen van sancties zodat het goederen kan verkrijgen die de militaire capaciteiten en het militaire voortzettingsvermogen vergroten.

Kortom, de hybride en militaire dreigingen tegen Nederland nemen toe, het is daarom noodzakelijk om onze weerbaarheid in brede zin te vergroten om de dreiging het hoofd te bieden.

Voorbeelden

1. **Quantumtechnologie voor Russische kernwapenprogramma**

   (Uit interview directeur-generaal AIVD in FD: 'AIVD baas Akerboom: Mensen zijn sneller in staat en bereid geweld te plegen', augustus 2024)
   Rusland verbreedt zijn agenda naar technologische en weten-schappelijke innovatie. Een voorbeeld is het Russische Uranium One Holding, dochter van Rostom (Russische staatskernenergie bedrijf). Dit bedrijf verwierf kwantumtechnologie in Nederland voor het Russische kern-wapenprogramma. De Nederlandse tak werd gefinancierd om kwantumtechnologie uit onder meer Nederland te verwerven voor de Russian Quantum Computing Roadmap (QCR), die onder de verantwoordelijkheid van Rosatom valt. Rusland ziet kwantumcomputing als sleuteltechnologie op tal van militaire toepasbare onderzoeksterreinen. Ook voor de modernisering van zijn kernwapens, vooral omdat met krachtige rekenkundige modellen atoomexplosies gemodelleerd zouden kunnen worden. De export van kwantumtechnologie naar Rusland valt onder Europese sancties en ook enkele Rosatom-entiteiten met een militaire link zijn gesanctioneerd. Deze inlichtingen zijn gedeeld met partners zodat de export van deze technologie gestopt kan worden.

2. **Verstoringsactie van een Russische offensieve cybercampagne**

   (Uit brief min BZK en min DEF d.d. 9 juli 2024 aan de Tweede Kamer)
   In nauwe samenwerking tussen de *Federal Bureau of Investigation* (FBI), *US Cyber National Mission Force* (CNMF), de AIVD, de MIVD en de Nationale Politie is 24 juni jl. een Russische digitale beïnvloedingsoperatie verstoord. Deze operatie was gericht op het beïnvloeden van het publieke debat in de Verenigde Staten van Amerika (VS). Bij deze beïnvloedingsoperatie werd gebruik gemaakt van een server in Nederland. De AIVD en de MIVD achten het zeer waarschijnlijk dat deze software is ingezet binnen Russische operaties gericht op het beïnvloeden van het Amerikaanse publiek debat. Er zijn geen indicaties dat de

offensieve cybercampagne is ingezet om het publieke debat in Nederland of Europa te beïnvloeden. Deze Russische beïnvloedings-campagne past in het normbeeld waarbij Rusland voortdurend probeert westerse landen in een kwaad daglicht te stellen, onderlinge eenheid te ondermijnen en de publieke opinie te beïnvloeden. Hierbij wordt ingespeeld op maatschappelijke onzekerheden en pro-Russische en antiwesterse sentimenten.

3. Chinese hack defensienetwerk: Chinese actor misbruikt kwetsbaarheid in Fortigate

(Uit jaarverslag MIVD 2023)

Defensie werd zelf slachtoffer van Chinese statelijke hackers. In 2023 konden aanvallers binnenkomen bij een defensienetwerk. Een defensieonderdeel gebruikte het netwerk voor samenwerking met derde partijen op het gebied van R&D. De MIVD publiceerde in februari en juni 2024 een openbaar technisch rapport met details op de website van het Nationaal Cyber Security Centrum (NCSC) over de bij het incident aangetroffen malware. De malware wordt ingezet bij systemen (FortiGate) van het bedrijf Fortinet, waarmee computergebruikers beschermd op afstand kunnen werken. De aangetroffen malware installeerde een 'achterdeurtje' door gebruik te maken van een bekende kwetsbaarheid in FortiGate apparaten.

4. Bedrijven, kennisinstellingen en wetenschappers doelwit Chinese spionage

(Uit MIVD Jaarverslag over 2022)

Nederlandse bedrijven, kennisinstellingen en wetenschappers zijn op grote schaal doelwit van Chinese spionage. De MIVD heeft verschillende pogingen ontdekt van China om Nederlandse militaire technologie te bemachtigen. De MIVD heeft verschillende Chinese pogingen onderzocht om buiten de exportrestricties om, militair relevante technologie te verwerven. Daarbij heeft de MIVD onder meer enkele 'coverbedrijven' ontdekt, die daarvoor werden gebruikt. De MIVD heeft maatregelen genomen tegen zulke spionagepogingen, bijvoorbeeld door gesprekken te voeren met mogelijke doelwitten of te zorgen dat bedrijven hun beveiliging verbeteren.

5. Verstorings- en sabotagedreiging Rusland

(Uit Dreigingsbeeld statelijke actoren NCTV/AIVD/MIVD 2022 en Jaarverslag MIVD over 2021)

Russische entiteiten brengen (onderzeese) infrastructuur in kaart en ondernemen activiteiten die duiden op spionage en voorbereidingen voor verstoring. Hierbij moet men denken aan: internetkabels, gasleidingen, drinkwatervoorziening en energie. Daadwerkelijke verstoring en sabotage hiervan kunnen tot grote schade en ontwrichting in Nederland en de rest van de wereld leiden. (Concreet voorbeeld uit najaar 2022) Een Russisch schip heeft geprobeerd om de infrastructuur van windmolenparken voor de Nederlandse kust in de Noordzee in kaart te brengen. Waarschijnlijk onderzochten de Russen de mogelijkheden voor toekomstige sabotage.

6. Russische hackpoging OPCW

(Uit persconferentie Defensie, oktober 2018)

De MIVD en de AIVD hebben een cyberoperatie verstoord in 2018. De operatie was gericht op de Organisatie voor het Verbod op Chemische Wapens (OPCW) in Den Haag. Vier Russische inlichtingenofficieren troffen vlak bij het gebouw van de OPCW met specialistische apparatuur voorbereidingen om de netwerken van deze organisatie te hacken. Nederland is gastland van de OPCW en daarmee verantwoordelijk voor het veilig kunnen functioneren van deze internationale organisatie.

Deze publicatie is een gezamenlijke uitgave van:
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Defensie
Militaire Inlichtingen- en Veiligheidsdienst

December 2024