Ministerie van Defensie

> Retouradres Postbus 20701 2500 ES Den Haag

de Voorzitter van de Eerste Kamer
der Staten-Generaal
Kazernestraat 52
2500 EA Den Haag

Ministerie van Defensie
Plein 4
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

Onze referentie

MINDEF20250016367

Bij beantwoording, datum, onze referentie en onderwerp vermelden.

Datum 22 april 2025
Betreft MIVD jaarverslag 2024

Geachte voorzitter,

Hierbij bied ik u het openbaar jaarverslag van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) over het jaar 2024 aan. In dit verslag legt de MIVD verantwoording af over de werkzaamheden van het afgelopen jaar.

Hoogachtend,

DE MINISTER VAN DEFENSIE

Ruben Brekelmans

Ministerie van Defensie

Openbaar jaarverslag 2024

Militaire Inlichtingen- en Veiligheidsdienst

22 april 2025

Openbaar jaarverslag 2024

Militaire Inlichtingen- en Veiligheidsdienst

22 april 2025


F 805

INHOUDSOPGAVE

Voorwoord directeur MIVD

Vice-admiraal Peter Reesink

De onrust in de wereld en het dreigingsbeeld voor Nederland en de rest van Europa zijn zorgelijk. De veiligheid van Nederland, onze welvaart en onze manier van leven staan onder druk. De turbulente ontwikkelingen op geopolitiek en bondgenootschappelijk gebied hebben zekerheden ter discussie gesteld waarop we tot voor kort konden bouwen en vertrouwen. De snelheid waarmee dit gebeurt en het potentiële effect op onze veiligheid is ongekend. Het is daarmee des te urgenter dat Defensie en de MIVD op deze ontwikkelingen een passend antwoord kunnen bieden.

De diensten zien de Russische dreiging tegen Europa, ook na een eventuele afloop van de oorlog met Oekraïne, niet afnemen maar toenemen. Dit onderstreept het belang voor Nederland, de NAVO, in het bijzonder voor de Europese lidstaten, om zo snel als mogelijk militaire slagkracht op te bouwen. Dit is noodzakelijk om Rusland af te schrikken en in het ergste geval om Nederland en Europa te kunnen verdedigen tegen een aanval van Rusland.

De MIVD heeft de opdracht om de Nederlandse krijgsmacht daarin te ondersteunen. Dit doen we door tijdig accurate inlichtingen en contra-inlichtingen te leveren, bijvoorbeeld over de ontwikkeling en manier van opereren van de Russische krijgsmacht en Russische spionage en sabotage. We bewaren de samenhang tussen inlichtingen op alle niveaus. Zo draagt de MIVD bij aan de versterking van onze eigen territoriale verdediging en die van onze bondgenoten.

Het conflict in de *grey zone*, het schemergebied tussen vrede en oorlog, is ondertussen al realiteit. Ons land wordt steeds vaker geconfronteerd met statelijke actoren die met hybride aanvallen onze samenleving proberen te ontwrichten en te verzwakken. Met name voor Rusland geldt dat ze met hun (cyber)acties onder het niveau van een gewapend conflict willen blijven. We zien daarbij de risicobereidheid toenemen.

In 2024 zag de MIVD bijvoorbeeld dat een Russische hackersgroep een cybersabotage-aanval deed tegen het digitale besturingssysteem van een publieksvoorziening in Nederland. Dit is zover bekend de eerste keer dat zo'n sabotage-aanval tegen een dergelijk digitaal besturingssysteem in Nederland is uitgevoerd. De aanval heeft uiteindelijk geen schade aangericht. Ook heeft de MIVD een Russische cyberoperatie waargenomen tegen de Nederlandse kritieke infrastructuur, mogelijk als voorbereiding voor sabotage. Doordat het doelwit snel heeft gehandeld, is het de Russen niet gelukt om toegang tot het netwerk te krijgen.

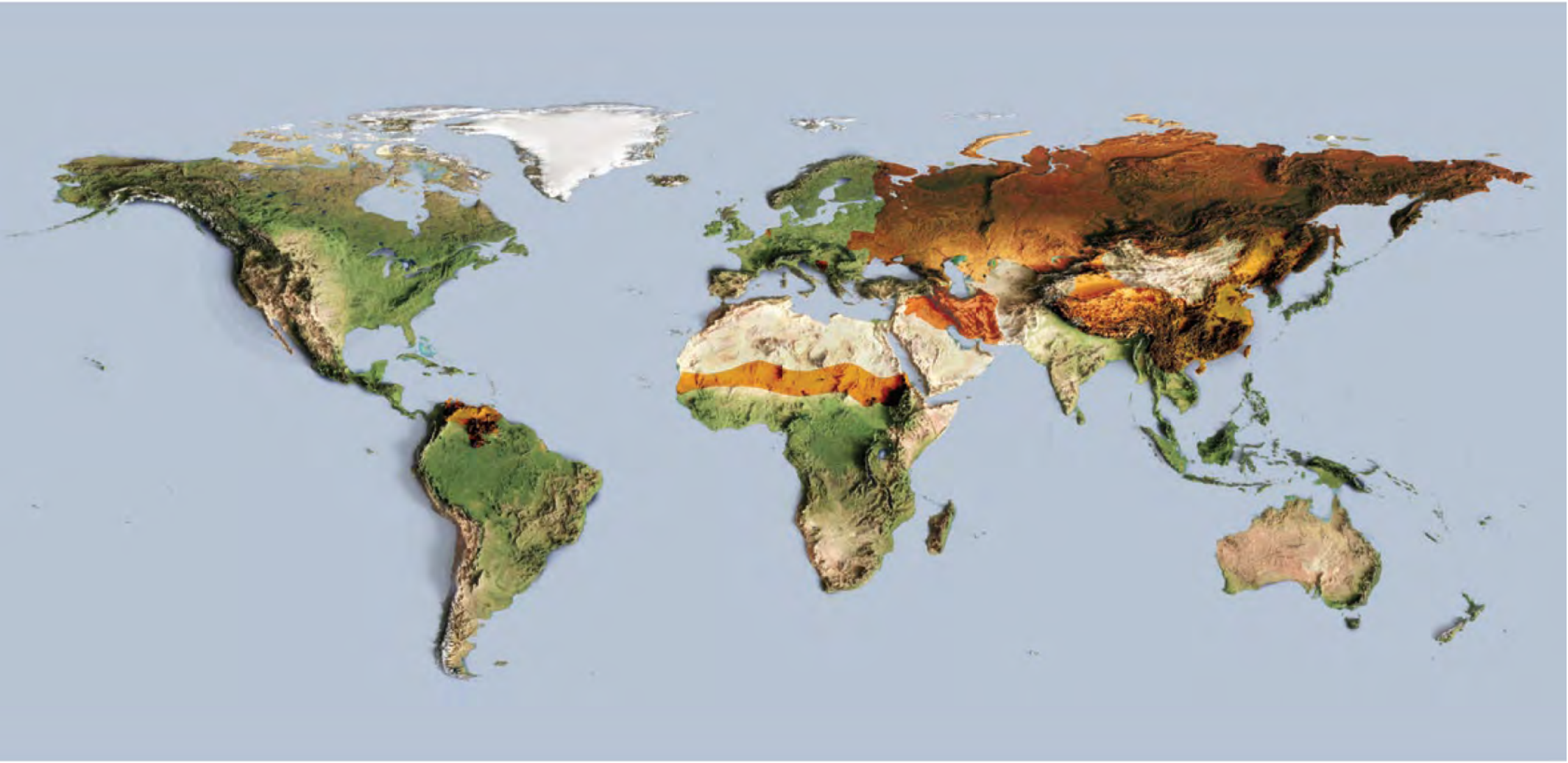
De MIVD waarschuwt al langer voor deze (cyber)dreiging. Zo heeft de MIVD afgelopen jaar de werkwijze van een Russische GRU-eenheid openbaar gemaakt zodat mogelijke slachtoffers zich tegen deze ingrijpende aanvallen en spionage kunnen wapenen. De focus van de hackers van deze cybereenheid van de Russische militaire geheime dienst ligt op het in beeld krijgen en verstoren van de westerse hulp aan Oekraïne.

De MIVD onderkent verder dat verschillende Russische eenheden de infrastructuur van de Noordzee in kaart brengen en (onderwater) activiteiten ondernemen die duiden op spionage en voorbereidingshandelingen voor verstoringen en sabotage. Denk bijvoorbeeld aan internetkabels, drinkwater- en energievoorzieningen. Daadwerkelijke verstoringen kunnen leiden tot grote schade en ontwrichting in Nederland, Europa en de rest van de wereld.

De dreiging komt ook van China en wordt zichtbaar met ondersteuning van Russische oorlogsactiviteiten en de agressieve houding tegen Taiwan en in de Zuid-Chinese Zee. In Nederland hebben we Chinese activiteiten gezien op het gebied van ongewenste kennisoverdracht van hoogwaardige Nederlandse technologie zoals halfgeleiders. Dat kan openlijk door verwerving, investeringen en deelname aan wetenschappelijk onderzoek, maar ook illegaal met ontwijking van exportrestricties en (cyber)spionage. In 2024 publiceerden de Amerikaanse inlichtingen- en veiligheidsdiensten over de Chinese cyberactor *Salt Typhoon*. Deze cyberactor had tenminste een jaar lang toegang tot grote Amerikaanse telecomproviders. Hierbij zou communicatie van politici en ambtenaren zijn ingezien en mogelijk ook toegang zijn verkregen tot geheime informatie van opsporingsdiensten. De berichtgeving past binnen observaties van de MIVD en AIVD. Naar inschatting van de diensten is het waarschijnlijk dat ook Europese telecommunicatieproviders doelwit zijn van geavanceerde hackpogingen.

De in 2024 in werking getreden Tijdelijke wet moet ons in staat stellen om Nederland effectiever te verdedigen door bestaande bevoegdheden zoals kabelinterceptie en hacken in te zetten. De Tijdelijke wet wordt in overleg met de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) gedeeltelijk toegepast. Uitgangspunt is en blijft volledige toepassing van de Tijdelijke wet onder het noodzakelijke toezicht, op de kortst mogelijke en voor alle partijen uitvoerbare termijn.

Tot slot wil ik benadrukken dat we onze taken alleen kunnen uitvoeren door de inzet van onze medewerkers. Zij hebben het afgelopen jaar weer een knappe prestatie geleverd en zullen zich ook dit uitdagende jaar blijvend inzetten voor de krijgsmacht en de veiligheid van Nederland.



1 INLICHTINGEN EN VEILIGHEID VOOR NEDERLAND

Ook in 2024 stond de krijgsmacht en daarmee de MIVD voor de taak het hoofd te bieden aan complexe dreigingen die onze veiligheid, stabiliteit en welvaart bedreigen. Deze dreigingen zijn onder andere het gevolg van de huidige geopolitieke verhoudingen en assertief optredende statelijke en niet-statelijke actoren die gebruik maken van nieuwe technieken met een grote impact. Middelen en technieken die vaak onzichtbaar zijn, moeilijk tijdig te onderkennen en moeilijk toe te schrijven zijn aan daders. Naast het klassieke optreden spelen conflicten zich voor een steeds groter deel af in de *grey zone*, het grijze gebied tussen oorlog en vrede. De huidige ontwikkelingen kenmerken zich door een toenemende onvoorspelbaarheid, waarin traditionele grenzen tussen oorlog en vrede, vriend en vijand, en internationale samenwerking en conflict, steeds vager worden.

De oorlog in Oekraïne duurt nog altijd voort. Daarbij is de spanning tussen Rusland en het Westen historisch hoog, met implicaties die mogelijk verder rijken dan de Europese veiligheidsstructuur alleen. De wereld ziet zich geconfronteerd met de mogelijkheid van een nieuw conflict, waarin de strategische rivaliteit tussen het Westen en grootmachten zoals Rusland en China, opnieuw centraal staat. Ook bij een eventuele beëindiging van de oorlog zal de spanning tussen Rusland en het Westen, alsmede de wederopbouw van Oekraïne veel inspanning van de krijgsmacht en daarmee de MIVD blijven vragen. Naast de oorlog in Oekraïne is de spanning in het Midden-Oosten als gevolg van het conflict tussen Israël en Hamas nog altijd hoog. Ook in andere delen van de wereld zoals in Soedan, de Democratische Republiek Congo en Kosovo waren er conflicten of oplopende spanningen. Al deze gebeurtenissen onderstrepen het beeld van een onzekere, veranderlijke veiligheidscontext.

De MIVD moet in deze onzekere veiligheidscontext in staat zijn om snel te reageren op crises en tegelijkertijd duurzaam strategisch inlichtingen-onderzoek te kunnen verrichten naar bijvoorbeeld de dreiging vanuit China en Rusland. De onzekere en veranderlijke veiligheidscontext vraagt veel van de wendbaarheid van de krijgsmacht en de diensten, omdat crises snel opkomen en dreigingen divers en omvangrijk zijn. De MIVD ondersteunt wereldwijd de inzet van de Nederlandse krijgsmacht met inlichtingen die betrouwbaar en actueel zijn. De MIVD maakt diverse inlichtingenproducten, zoals dreigingsappreciaties en inlichtingenberichten, ten behoeve van de militaire inzet en de politieke besluitvorming die hieraan gerelateerd is.

Naast de strategische dossiers, aandachtsgebieden en de ondersteuning aan de krijgsmacht, heeft de MIVD ook veiligheidsbevorderende taken. De MIVD beschermt bijvoorbeeld de militaire geheimen en operaties van Defensie, spoort cyberaanvallen op, ontmaskert buitenlandse inlichtingen-officieren die op heimelijke en soms illegale wijze inlichtingen vergaren. De Nederlandse Defensie-industrie, bedrijven, kennisinstellingen en wetenschappers zijn een potentieel doelwit van diverse statelijke actoren die (heimelijk) hoogwaardige, al dan niet militair relevante, technologie proberen te verwerven. De MIVD draagt bij aan de weerbaarheid en veiligheid van Defensie en de Defensie gerelateerde industrie door bijvoorbeeld onderzoek te doen naar de beveiliging van bedrijven die moeten voldoen aan de veiligheidseisen van Defensie[1].

De grote verscheidenheid aan dreigingen vereist dat de MIVD ook op een veelheid aan onderwerpen een relevante en betrouwbare inlichtingen-positie moet hebben, en informatie snel moet kunnen vergaren, verwerken, analyseren en verspreiden. De MIVD werkt hiertoe nauw samen met onder andere de krijgsmacht, de AIVD, de NCTV en met buitenlandse collega diensten.

1 *Algemene Beveiligingseisen voor Defensieopdrachten 2019 (ABDO 2019)*

MIVD en AIVD: 'Buitenland achter hack politie' *(oktober 2024)*
Het is zeer waarschijnlijk dat een ander land verantwoordelijk is voor het cyberincident bij de politie. Dat blijkt uit onderzoek van de MIVD en AIVD, zo heeft minister van Justitie David van Weel in oktober 2024 in een brief naar de Tweede Kamer geschreven. De diensten hebben niet openbaar gemaakt om welk land het gaat. De MIVD en AIVD waarschuwen onder meer in hun jaarverslagen al langer voor de toename van offensieve cyberactiviteiten van een aantal landen.

Leeswijzer

Dit jaarverslag behandelt in hoofdstuk 1 de inlichtingenonderzoeken, missieondersteuning en aandachtsgebieden op basis van een geografische en thematische verdeling en als laatste de veiligheidsbevorderende taken. Hoofdstuk 2 beschrijft de verantwoording naar de samenleving. Hoofdstuk 3 beschrijft vervolgens de MIVD als organisatie en tenslotte geeft hoofdstuk 4 een overzicht van de kengetallen over 2024 weer.

1.1 De Russische Federatie

De relatie tussen Rusland en het Westen heeft in 2024 een nieuw dieptepunt bereikt. Moskou percipieert de oorlog in Oekraïne als onderdeel van een breder en existentieel conflict met het Westen. In Russische ogen heeft deze confrontatie een 'totaal' karakter. Dit betekent dat, ongeacht de afloop van de oorlog in Oekraïne, het conflict tussen Rusland en het Westen er een van de lange duur is. In het Russische narratief is de westerse steun aan Oekraïne erop gericht om Rusland een strategische nederlaag toe te brengen en de binnenlandse politiek te destabiliseren.

Het Kremlin presenteert Rusland, zowel aan de eigen bevolking als aan de buitenwereld, als unieke beschaving met een eigen normen- en waardenstelsel, dat als alternatief zou moeten dienen voor de door de VS-gedomineerde wereldorde. Vooralsnog weet Rusland de uitdagingen die de oorlog met zich meebrengt het hoofd te bieden. Putin's regime is stabiel, al wordt deze stabiliteit afgedwongen met steeds repressievere middelen en is zij niet verankerd in werkende democratische instituties. Er is nog altijd veel draagvlak bij de Russische bevolking voor de oorlog, die een onderdeel is van een breder conflict met het Westen en wordt gezien als een oorlog ter verdediging tegen westerse agressie.

Rusland heeft in 2024 een aantal zorgwekkende escalatiestappen gezet. De publicatie van de herziene Nucleaire Doctrine waarin de nucleaire drempel nog verder is verlaagd, de eerst inzet ooit van een *Intermediate Range Ballistic Missile* (primair een wapen met een nucleaire taak) en verklaringen dat Rusland gereed is om nucleaire testen te hervatten, zijn bedoeld om onzekerheid te creëren bij de Verenigde Staten (VS) en de Navo. Zorgwekkend zijn niet alleen het nucleaire karakter van de dreigementen, maar ook dat het aantal niet-nucleaire escalatiemogelijkheden afneemt. Daarnaast moeten de westerse landen er rekening mee houden dat onder het regime van Putin de Russische opstelling tegenover het Westen eerder zal verharden dan verzachten.

Russische federatie: oorlog in Oekraïne

Tenslotte werd in 2024 duidelijk dat Rusland steun is blijven ontvangen vanuit China, Noord-Korea en Iran voor de oorlogsinspanningen. China en Rusland hebben hun bilaterale banden in 2024 verder aangehaald. China verleent Rusland politieke en diplomatieke rugdekking in multilaterale fora zoals de Verenigde Naties (VN). Chinese bedrijven blijven belangrijke leveranciers van componenten die voor de Russische oorlogsindustrie van cruciaal belang zijn. Noord-Korea was in 2024 de grootste leverancier van artilleriegranaten en de eerste staat die officieel troepen naar Rusland zond voor actieve deelname aan de oorlog. Rusland en Iran hebben het afgelopen jaar de bilaterale samenwerking verder voortgezet op onder andere politiek, economisch, militair en nucleair vlak. Iraanse wapenleveranties aan Rusland (waaronder verschillende types *OWA-UAS*[2], munitie en *Close Range Ballistic Missiles* (CRBM's) en de onderlinge

[2] *OWA-UAS: One way attack- unmannend Aerial Systems. (o.a. drone's voorzien van een camera, sensoren, navigatieapparatuur en een explosieve lading, welke na lancering 'in' het doel vliegt en explodeert.*

militair-technologische samenwerking hebben bijgedragen aan het Russisch voortzettingsvermogen in Oekraïne. Door deze samenwerking ziet de Navo zich in toenemende mate geconfronteerd met de inzet van Iraanse wapensystemen (en Russische verbeterde kopieën daarvan) aan haar oostflank.

Grondgebonden operaties

Nog altijd wordt de oorlog in Oekraïne gekarakteriseerd als een slijtage-oorlog, waarbij beide partijen hoge personele en materiële verliezen leiden. Hoewel de Oekraïense inval in het Russische Koersk plaatselijk en tijdelijk het initiatief heeft geboden, heeft Rusland over het algemeen nog steeds de overhand en voert het langs het gehele front offensieve acties uit. Het numerieke overwicht in personeel, materieel en vuursteun is nog steeds sterk in het voordeel van Rusland, mede doordat de Oekraïense strijdkrachten te maken hebben met structurele tekorten aan personeel en materieel.

Eind oktober zijn de Russische strijdkrachten begonnen met een offensief in de Donbas waarbij relatief veel terrein in korte tijd is veroverd, met name in het zuidelijk deel van de Donetsk Oblast. Het scenario is reëel dat Rusland erin slaagt om, ten koste van hoge personele en materiële verliezen, het komende half jaar steden in de Donbas te veroveren die als belangrijke logistieke knooppunten dienen voor de Oekraïense strijdkrachten. Dit zal het Oekraïense vermogen om in de toekomst de Donbas te verdedigen beperken.

Luchtdomein

In het afgelopen jaar zijn de Oekraïense luchtverdediging en luchtstrijd-krachten verder versterkt met westerse grondgebonden systemen en gevechtsvliegtuigen. Hierdoor was Oekraïne in staat om een belangrijk deel van de voortdurende Russische aanvallen met kruisvluchtwapens, drones en andere langeafstandswapens te onderscheppen. Oekraïne heeft echter nog steeds onvoldoende middelen om alle kwetsbare infrastructuur, de bevolking en de strijdkrachten adequaat te beschermen. Met name de sterk toegenomen massale Russische inzet van glijbommen resulteert vrijwel dagelijks in aanzienlijke burgerslachtoffers in kwetsbare Oekraïense steden als Kharkiv.

Op zijn beurt werd ook Rusland geconfronteerd met een toenemende luchtdreiging achter de eigen linies. Met steeds geavanceerdere, zelfgeproduceerde langeafstandsdrones voert Oekraïne inmiddels aanvallen uit tot meer dan duizend kilometer in het Russische achterland. Deze aanvallen brengen de oorlog niet alleen publicitair naar het hart van de Russische macht, maar hebben ook zichtbare verstorende effecten op onder meer de Russische petrochemische sector, de defensie-industrie, de munitieaanvoer en de luchtverdediging. Daarnaast kreeg Oekraïne eind 2024 met de versoepeling van de restricties op de inzet van westerse langeafstandswapens een belangrijke extra capaciteit om doelen in Rusland zelf aan te grijpen.

Maritiem domein

De intensiteit van de oorlog in het Zwarte Zeegebied is in 2024 sterk afgenomen, omdat de Russische vloot ervoor heeft gekozen zich meer oostwaarts te positioneren als gevolg van de voortdurende dreiging van Oekraïense aanvallen op zee. Oekraïne heeft echter ook dit jaar meerdere succesvolle aanvallen uitgevoerd met steeds geavanceerdere *Unmanned Surface Vessels* (USV's) tegen militaire doelen in het Zwarte Zeegebied. Hierdoor werd Rusland beperkt in het maritieme optreden.

Herstel en uitbreiding Russisch militair vermogen

Het gecombineerde vermogen van de Russische industrie om militair materieel te produceren, reviseren en moderniseren, is tezamen ruim voldoende voor Rusland om de in Oekraïne geleden verliezen kwantitatief te compenseren. Naast de sterk opgeschroefde binnenlandse productie krijgt Rusland daarbij ook significante hulp vanuit China, Iran, Belarus en Noord-Korea. Hierdoor kan Rusland de oorlog in Oekraïne voortzetten evenals in beperkte mate invulling geven aan de ambitieuze uitbreidingsplannen van de eigen krijgsmacht. Rusland is, terwijl de oorlog

in Oekraïne voortduurt, begonnen met een omvangrijke hervorming en uitbreiding van de krijgsmacht met het oog op een post-conflict situatie. Hierin is voorbereiding op een mogelijk militair conflict met de Navo voor Rusland de belangrijkste drijfveer.

Russische dreiging richting Europa

Als gevolg van het Russische dreigingsbeeld en verhoogde spanningen tussen Rusland en het Westen, mede als gevolg van de oorlog in Oekraïne, manifesteert de Russische dreiging zich steeds nadrukkelijker op een hybride wijze in Europa. Dit uit zich bijvoorbeeld in de vorm van zowel fysieke als digitale (klassieke)[3] spionage, (heimelijke) beïnvloeding van het publiek debat, het politiek-bestuurlijk bestel en diplomatie, offensieve cyberaanvallen en campagnes, sabotage en de inzet van energiebeleid als pressiemiddel.

Dit gebeurt via een diffuus, opportunistisch, en onvoorspelbaar samenspel van Russische overheidsentiteiten (waaronder de Russische inlichtingen- en veiligheidsdiensten), een diverse groep Russische of pro-Russische individuen, organisaties en netwerken in Rusland en in het Westen, die worden ingezet of zich actief aanbieden voor het verrichten van vaak lucratieve activiteiten. Daarbij toont Rusland inmiddels een grotere risicobereidheid, die zich manifesteert via meer brutale, agressieve of provocatieve activiteiten in zowel het fysieke als het cyberdomein met soms ook een geweldscomponent. Deze acties richten zich onder meer op organisaties die op verschillende wijzen betrokken zijn bij (het ondersteunen van) de oorlog in Oekraïne, maar steeds nadrukkelijker ook op militaire en logistieke locaties in Europa.

Het doel van deze sabotageactiviteiten is meerledig. Enerzijds richten de activiteiten zich op het vertragen van de westerse leveranties aan Oekraïne, anderzijds op het zaaien van verdeeldheid in het Westen en het ondermijnen van steun aan Oekraïne. Daarnaast kan Rusland met sabotageactiviteiten testen waar het Westen rode lijnen trekt als het gaat om Russische agressie op het eigen territorium. Tenslotte hebben deze activiteiten tot doel de westerse reactie(s) op dergelijke activiteiten in kaart te brengen, waarbij Rusland op zoek lijkt naar een model waarbij het westerse steun aan Oekraïne maximaal kan verstoren zonder een volwaardige militaire reactie van het Westen uit te lokken.

> **MIVD-directeur in FD: 'Rusland kan binnen enkele jaren een groot conflict met de Navo aan'** *(december 2024)*
> Ondanks de zware verliezen in Oekraïne vult Rusland zijn wapen- en munitievoorraden 'vele malen sneller aan' dan de Navo-landen. Moskou kan volgens de directeur van de MIVD, vice-admiraal Peter Reesink, voor 2030 klaar zijn voor een gewapend conflict met de Navo. De directeur houdt rekening met een scenario waarin de Russen ook daadwerkelijk aanvallen. Reesink: 'We denken dat het mogelijk is dat Rusland een regionaal conflict begint als het klaar is met Oekraïne.' Doel daarvan is volgens hem om te 'kijken of de alliantie uit elkaar te spelen is.'

Russische dreiging richting Nederland

Nederland is, en blijft, een interessant doelwitland voor Rusland, vanwege zijn voortrekkende rol van westerse steun aan Oekraïne, als thuisbasis van internationale organisaties, zoals het OPCW en het internationaal strafhof, de aanwezigheid van bedrijven uit de high tech sector (zoals *Brainport* Eindhoven), een mainport (belangrijke transportroutes waaronder haven van Rotterdam, luchthaven Schiphol) en een informatieknooppunt in Europa. De Russische inlichtingen- en veiligheidsdiensten (GRU, SVR en de FSB) voeren verschillende activiteiten uit waar een spionage en/of sabotage- en beïnvloedingsdreiging van uitgaat richting West-Europese landen en Navo-bondgenoten. Voor een deel van de onderkende activiteiten en plannen bestaat onduidelijkheid over de mate van betrokkenheid van Rusland. Naast de (klassieke) inlichtingendreiging middels activiteiten in zowel het fysieke- als het cyberdomein, ontplooit Rusland activiteiten in Nederland om op heimelijke wijze technologie te verwerven.

[3] *Het ontsluiten van informatie uit zogenaamde menselijke bronnen.*

Russische Federatie: Militaire techniek

Het Russisch Militair-Industrieel Complex (MIC) is omvangrijk en kenmerkt zich door focus op productie, techniek gerichte Research & Development en ontwikkeling van hoogwaardige nieuwe wapensystemen. Rusland blijft ondanks steeds zwaardere sancties wapens en militaire technologie ontwikkelen, produceren en exporteren. Om de aanhoudende behoefte aan wapens en munitie als gevolg van de oorlog in Oekraïne in te vullen, vergrootte Rusland de productiecapaciteit hiervan. Hierbij lijkt Rusland steeds beter in staat alternatieven te vinden voor gesanctioneerde artikelen, bijvoorbeeld door succesvolle importsubstitutie en heimelijke verwerving. Bovendien gebruikt Rusland geïmporteerde onderdelen, maar ook complete wapensystemen zoals Iraanse en Chinese drones. Desondanks streeft Rusland een zo groot mogelijke strategische onafhankelijkheid na waarbij het ook geïmporteerde wapensystemen het liefst vervangt door nationaal ontwikkelde en geproduceerde systemen.

Het Russische MIC richt zich op (door-)ontwikkeling van wapentechniek voor afschrikkings-, defensieve en offensieve doeleinden. Te denken valt aan robuuste ballistische en hypersonische raketten, hoogwaardige luchtverdedigingssystemen maar ook relatief goedkope OWA-UAV's. Door het conflict in de Oekraïne weet Rusland beproefde technieken te verfijnen en nieuwe, tegen westerse wapensystemen gerichte concepten te ontwikkelen. Hierbij laat het MIC zien te beschikken over een groot adaptief vermogen om snel in te spelen op concrete behoeften vanuit de Russische krijgsmacht. Het MIC produceert en ontwikkelt primair voor de Russische krijgsmacht, maar exporteert traditioneel ook op grote schaal wapens en wapentechniek.

De MIVD doet onderzoek naar Russische militair-technologische ontwikkelingen, mede om de Nederlandse krijgsmacht met haar bondgenoten in staat te stellen goed onderbouwde keuzes te maken als het gaat om aanschaf van nieuwe militaire systemen en ontwikkeling van adequate tactieken voor nu en de toekomst. Uit het in 2024 uitgevoerde onderzoek heeft de MIVD vastgesteld dat de dreiging die uitgaat van de huidige en toekomstige Russische militaire middelen groot is en blijft. Het is mogelijk dat de Nederlandse krijgsmacht als onderdeel van de Navo, direct of indirect in aanraking kan komen met hoogwaardige Russische wapensystemen, mede door de wereldwijde proliferatie (export) van deze systemen door Rusland.

Russische Federatie: (cyber)spionage

De MIVD onderzocht in 2024 spionage door of in opdracht van verschillende buitenlandse inlichtingendiensten. De MIVD onderzocht in 2024 in gezamenlijkheid met de AIVD (mogelijke) activiteiten van de Russische inlichtingen- en veiligheidsdiensten GRU, SVR en FSB gericht tegen Nederland en bondgenoten. Rusland probeert ook in Nederland heimelijk aan technologie en technologische kennis te komen.

Nederland is voor het Russische regime bovendien een targetland vanwege de steun aan Oekraïne, de hier gevestigde internationale organisaties en het logistieke knooppunt dat Nederland is.

Cyberspionage is en blijft voor Rusland van groot belang. De oorlog met Oekraïne heeft de noodzaak voor Rusland om inlichtingen te vergaren over politieke en militaire aangelegenheden doen toenemen. Sinds de Russische oorlog met Oekraïne onderkent de MIVD een toename in het aantal cyberactoren binnen de Russische overheid die door hen worden ondersteund of aangestuurd. Een groot deel van deze cyberactoren voeren cyberoperaties uit die ook Nederland direct of indirect kunnen raken. De MIVD onderneemt waar mogelijk stappen om acties te treffen tegen deze actoren, zowel heimelijk als publiekelijk. Zo heeft de MIVD eerder dit jaar meegeschreven aan de door de Amerikaanse overheid uitgebrachte *Cyber Security Advisory* over een Russische actor die door de MIVD verantwoordelijk wordt gehouden voor het uitvoeren van verschillende cyberoperaties tegen onder meer de vitale infrastructuur[4] in Navo-landen.

[4] *Vitale infrastructuur: Processen en diensten die het fundament vormen waar Nederland op draait, zoals elektriciteit, toegang tot internet en drinkwater. Bron:www.nctv.nl/onderwerpen/vitale-infrastructuur*

Ook Nederland is doelwit geweest van Russische cyberoperaties. Het afgelopen jaar heeft de MIVD verschillende cyberspionagepogingen tegen de Nederlandse overheid waargenomen. Daarnaast kan Nederland indirect slachtoffer worden van cyberoperaties, bijvoorbeeld door operaties tegen bondgenoten. Op deze manier hebben Russische cyberactoren gevoelige data bemachtigd zoals persoonsgegevens van Nederlandse overheidsmedewerkers en Nederlandse bedrijven.

Voor het onderkennen van Russische cyberoperaties werkt de MIVD nauw samen met private beveiligingsbedrijven om cyberoperaties te detecteren en te mitigeren. Deze samenwerking vormt een essentieel onderdeel in de digitale weerbaarheid van Nederland.

Russische Federatie: cyber

Voor het uitvoeren van Russische cyberoperaties hanteert de Russische overheid in toenemende mate een '*whole-of-society*'[5] benadering. Meerdere Russische entiteiten, van private bedrijven tot de hoogste kringen binnen de Russische overheid, vervullen een rol binnen het Russische offensieve cyberprogramma dat wordt ingezet tegen het Westen en Oekraïne, maar zelfs ook tegen Russische bondgenoten.

De diensten nemen waar dat staatsgesteunde groeperingen een toenemende dreiging vormen voor Nederland en zijn bondgenoten. Het afgelopen jaar is gebleken dat verschillende van deze groeperingen cybersabotage-aanvallen hebben uitgevoerd tegen vitale infrastructuur in westerse landen en actief bijdragen aan Russische beïnvloedings-campagnes. Ondanks dat de impact van deze groeperingen beperkt is gebleven, neemt de MIVD een toenemende bereidheid waar van dergelijke groeperingen om daadwerkelijk tot sabotage over te gaan. Tevens ziet de MIVD dat de technische capaciteiten en kennis binnen dergelijke groeperingen toeneemt. Deze ontwikkelingen kunnen volgens de MIVD resulteren in een verhoogd risico op ingrijpende aanvallen met zowel digitale als fysieke effecten.

Oekraïne: cyber

Rusland voert de oorlog met Oekraïne ook op grote schaal via het digitale domein. Een belangrijk deel van de Russische cybercapaciteiten wordt dan ook ingezet in cyberoperaties tegen Oekraïne. Oekraïne heeft daardoor continu te kampen met een groot aantal Russische cyberoperaties tegen Oekraïense overheidsorganisaties en vitale sectoren. Ook kleinere bedrijven zijn doelwit. In de eerste fase van de Russische oorlog met Oekraïne lag de focus van de Russische inzet op cybersabotage, door middel van het gebruik van grote hoeveelheden *wipers*[6] tegen Oekraïense systemen. Inmiddels ligt de Russische focus meer op het verkrijgen van inlichtingen, ofwel cyberspionage.

In 2024 heeft de MIVD een toename vastgesteld van Russische cyberactoren die cyberoperaties uitvoeren om tactische inlichtingen te verkrijgen. Deze inlichtingen bieden direct ondersteuning aan het Russische militair-tactische optreden in Oekraïne. Rusland weet deze inlichtingen snel bij de uitvoerende eenheden binnen de Russische krijgsmacht te krijgen en in te zetten voor kinetische operaties. Zo maakt Rusland onder meer gebruik van kwetsbaarheden in applicaties op mobiele telefoons om locaties te achterhalen van Oekraïense militairen en militair materieel, om die vervolgens kinetisch aan te grijpen.[7] Cyber neemt hiermee in toenemende mate een belangrijke rol in binnen het Russische militaire optreden in Oekraïne. Ook in 2024 heeft de MIVD inlichtingen uit het eigen cyberonderzoek gedeeld met de Oekraïense overheid, om bij te dragen aan de fysieke veiligheid van personen en materieel in Oekraïne.

Cybersabotage

Vorig jaar nam de MIVD een toename waar van cyberoperaties tegen Europese en Navo-bondgenootschappelijke doelwitten. Deze aanvallen hadden waarschijnlijk als doel om een digitale positie te bemachtigen binnen vitale infrastructuur om deze op een later moment te saboteren. Dit jaar is een cyberoperatie waargenomen tegen de Nederlandse vitale

[5] *Whole-of-society benadering: een aanpak waarbij de gehele samenleving betrokken is (overheid, bedrijfsleven, kennisinstituten en burgers).*

[6] *Malware gericht op het wissen van gegevens op geïnfecteerde systemen.*

[7] *Kinetisch aangrijpen: Het gebruik van een diversiteit aan wapensystemen en/of manoeuvre eenheden met als doel het uitschakelen van de eenheid, object of doel.*

infrastructuur, mogelijk ter voorbereiding voor cybersabotage. Doordat het doelwit snel heeft gehandeld is het de actor niet gelukt om toegang te krijgen tot het netwerk.

In 2024 heeft een staatsgesteunde groepering een cybersabotageaanval uitgevoerd tegen het digitale besturingssysteem van een openbare faciliteit in Nederland. Dit is voor zover bij de MIVD bekend de eerste keer dat een groepering als deze een cybersabotageaanval heeft uitgevoerd tegen een dergelijk controlesysteem in Nederland. Ondanks dat de impact van de aanval minimaal is geweest, is de MIVD bezorgd over de dreiging van cybersabotage tegen Nederland en Navo-bondgenoten, zowel vanuit de Russische staat als vanuit staatsgesteunde hackers.

MIVD waarschuwt: Russen hebben het gemunt op westerse hulp Oekraïne *(september 2024)*
De MIVD heeft in september 2024 gewaarschuwd voor Russische cyberoperaties van GRU-eenheid 29155. De focus van de hackers van deze Russische militaire geheime dienst ligt onder meer op het in beeld krijgen en verstoren van de westerse hulp aan Oekraïne. Hun operaties richten zich met name op westerse overheden en vitale infrastructuur.

De MIVD heeft samen met de VS en andere partnerdiensten een waarschuwing en een technisch advies uitgebracht. Hierin staat hoe landen en organisaties deze operaties kunnen onderkennen en zich hiertegen kunnen bewapenen. Volgens de betrokken westerse inlichtingendiensten probeert '29155' zicht te krijgen op militaire verplaatsingen van westerse wapenleveranties aan Oekraïne. De cyberoperaties zijn er mogelijk ook op gericht om fysieke sabotage waar 29155 om bekend staat, te ondersteunen.

De MIVD bracht deze eenheid eerder in verband met cybersabotage-operaties tegen Oekraïne. Die speelden zich af in aanloop naar de grootschalige Russische inval in Oekraïne in februari 2022. Verder verbindt de MIVD de hackers van 29155 aan voorbereidingshandelingen voor destructieve cyberoperaties tegen vitale infrastructuur en overheidsinstellingen in westerse landen. Deze GRU-eenheid wordt ook al langer verantwoordelijk gehouden voor het plegen van fysieke sabotage en pogingen daartoe in Europa. Verschillende landen hebben 29155 onder meer gelinkt aan de vergiftiging van voormalig GRU-officier Sergej Skripal in 2018, een couppoging in Montenegro en de moordaanslag op een Bulgaarse wapenhandelaar.

Digitale beïnvloeding

In 2024 heeft de MIVD de Amerikaanse overheid ondersteund bij het verstoren van een Russisch beïnvloedingscampagne. De campagne verspreidde pro-Russische sentimenten door middel van *social media*. De MIVD heeft vastgesteld dat Rusland vergevorderde handelingen treft om kunstmatige intelligentie (AI) bruikbaar te maken in digitale beïnvloedingsoperaties.

Zogenoemde Russische hacktivisten[8] stellen zich tot doel om westerse steun aan Oekraïne te verstoren, de cohesie binnen de Navo te ondermijnen en pro-Russische sentimenten te verspreiden. In 2024 voerden dergelijke groeperingen DDoS-aanvallen uit tegen onder meer websites van politieke partijen en openbaarvervoersbedrijven in Nederland, in een poging het Nederlanders moeilijk te maken hun stem uit te brengen tijdens de Europese verkiezingen.

[8] *Hacktivisme is een samenvoeging van activisme en hacken waarbij het inzetten van hacks, computer kennis en het internet als daad van protest of als subversieve activiteit wordt gebruikt om informaticasystemen aan te vallen om gegevens te stelen of deze buiten werking te stellen.*

1.2 *China*

Het afgelopen jaar vierde de Volksrepubliek China (hierna: China) zijn vijfenzeventigjarig bestaan. Hoewel de Chinese Communistische Partij (CCP) vooral de geopolitieke- en economische wederopstanding die het land gedurende deze periode heeft meegemaakt probeert te benadrukken, wordt het China van Xi Jinping toch ook gekenmerkt door toenemende nationale en internationale spanningen.

In 2024 heeft China zich in toenemende mate bereid getoond om zijn politiek- en militair-strategische belangen op assertieve wijze te bevorderen. In veel gevallen gaat dit ten koste van andere actoren in de Stille Oceaanregio. Zo stelde China zich naar mate het jaar vorderde steeds harder op ten aanzien van Taiwan. Ondanks voortdurende spanningen tussen beide partijen was de militaire druk vanuit China in de eerste maanden van 2024 relatief beperkt. Dit veranderde echter na de inauguratie van de nieuwe Taiwanese president, Lai Ching-te, in mei. De Chinese krijgsmacht voerde in reactie op de inauguratie een grootschalige militaire oefening uit rondom Taiwan, waarmee de spanning tussen beide landen tot een nieuw hoogtepunt werd opgedreven. Vanaf dit moment is de algehele militaire druk vanuit China toegenomen, dit is onder meer te zien aan het feit dat er in de resterende maanden van 2024 tot twee keer toe op grote schaal militaire middelen ontplooide rondom het eiland. Het houden van militaire oefeningen rond het eiland is onderdeel van China's bredere strategie om op den duur het eiland onder het gezag van Beijing te brengen. Militaire intimidatie wordt gecombineerd met economische en politieke druk. Ook past China lawfare[9] toe en wordt er actief desinformatie verspreid.

In de Zuid-Chinese Zee zijn de spanningen tussen China, dat grote delen van het gebied claimt, en omringende landen gedurende 2024 hoog gebleven. Middels de inzet van zijn marine- en kustwachteenheden poogt China vooral rond de *Spratly*-archipel zijn territoriale claims kracht bij te zetten, wat geregeld resulteert in incidenten. Zo hebben confrontaties tussen de Chinese- en Filipijnse eenheden rond de *Second Thomas Shoal*[10] (onderdeel van de Spratly-archipel in de Zuid-Chinese Zee) meermaals geleid tot aanvaringen.

Hoewel Taiwan en de Zuid-Chinese Zee zich bevinden aan de andere kant van de wereld, vormen de toenemende militaire spanningen rond deze gebieden een directe dreiging voor de Nederlandse en bondgenootschappelijke economische- en veiligheidsbelangen. Voor Nederland, als handelsland, zijn de maritieme handelsroutes die tussen Azië en de rest van de wereld door de Zuid-Chinese Zee en de Straat van Taiwan lopen, van groot belang. Ook zijn Taiwanese bedrijven essentieel in de productie van halfgeleiders.

China en de relatie met Rusland

In de relatie met Rusland speelt China een belangrijke rol op het wereldtoneel. China en Rusland hebben hun economische, politieke en militaire samenwerking in 2024 voortgezet en verder geïntensiveerd. Met de toenemende strategische wedijver tussen de VS en China aan de ene kant, en tussen Navo en Rusland aan de andere, vinden Beijing en Moskou elkaar als partner. 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 wereldpolitiek.

China's versterkte relatie met Rusland droeg in 2024 direct en indirect bij aan het in stand houden van de Russische oorlogsinspanningen in Oekraïne. China is een belangrijke afzetmarkt voor Russische energieproducten. Chinese (staats)bedrijven kunnen nagenoeg zonder restricties allerhande goederen aan Rusland leveren, dat deze gebruikt voor zijn oorlogsinspanningen in Oekraïne. Hoewel China in principe geen wapens en munitie levert aan Rusland, leverden Chinese bedrijven wel degelijk *dual-use*-goederen voor de Russische oorlogsindustrie en zelfs aanvalsdrones. Dit gaat in tegen het door China zelf uitgedragen exportcontrolebeleid. Hiermee werd China een directe speler op het

[9] *Lawfare: het gebruik van juridische middelen voor dwang of intimidatie van de tegenstander om strategische doelen te behalen.*

[10] *De Second Thomas Shoal is een onder water gelegen rif dat zich binnen de exclusieve economische zone van de Filipijnen bevindt, maar ook wordt geclaimd door China en Vietnam.*

gebied van Europese veiligheid, en indirect een dreiging voor Nederland en zijn bondgenoten.

Het is twijfelachtig of Beijing een substantiële bijdrage kan (of wil) leveren aan vredesonderhandelingen die recht doen aan de Oekraïense soevereiniteit. Zo nam Beijing, ondanks herhaaldelijke oproepen en uitnodigingen vanuit de internationale gemeenschap, bijvoorbeeld niet deel aan een in de zomer van 2024 georganiseerde internationale vredesconferentie in Zwitserland en kondigde het met Brazilië in de VN een eigen vredesinitiatief aan, zonder Oekraïne bij het ontwerp daarvan te betrekken.

Chinees-Russische militaire samenwerking

De MIVD heeft waargenomen dat China en Rusland in 2024 hun militaire samenwerking verder hebben geïntensiveerd. Dit uit zich onder andere in gezamenlijke (para)militaire oefeningen in verschillende domeinen, zowel in bilateraal als multilateraal verband (met Zuid-Afrika en Iran). Deze oefeningen worden complexer, en bestrijken ook nieuwe geografische gebieden. Zo werden Chinese strategische bommenwerpers tijdens een gezamenlijke patrouille met Rusland voor het eerst boven de poolcirkel gesignaleerd en oefende de Chinese kustwacht voor het eerst met zijn Russische tegenhanger.

Daarnaast is ervaring van de Russische strijdkrachten in Oekraïne en Syrië potentieel zeer belangwekkend voor het Volksbevrijdingsleger (PLA), dat weinig gevechtservaring heeft. Zeker met het oog op de voorbereiding van een mogelijk toekomstig militair conflict waar China zelf bij betrokken is. Dit aspect van de militaire samenwerking met Rusland is sinds de oorlog in Oekraïne voor China steeds belangrijker geworden. Ondanks de groeiende samenwerking en gedeelde belangen is van een natuurlijke alliantie tussen China en Rusland geen sprake. Dit uit zich sterk in, door eigenbelang gedreven, China's beleid ten aanzien van het Oekraïneconflict.

De oorlog in Oekraïne en sancties tegen Rusland hebben gezorgd voor een nieuwe dynamiek in de samenwerking waarin het 'ongelimiteerde partnerschap' op de proef wordt gesteld. Zo resulteert de oorlog in een ingewikkelde dynamiek waarin Rusland in hogere mate afhankelijk is van China en Beijing deze afhankelijkheid succesvol uitbuit. Tegelijkertijd tracht Beijing een balans te vinden tussen zijn ambities als 'verantwoordelijke grootmacht', steun aan partner Rusland en zijn handelsbelangen, met name in Europa.

China: economische veiligheid

China's *whole-of-society*-benadering zorgt ervoor dat het onderscheid tussen normale academische of economische uitwisseling en spionageactiviteiten vervaagt. Daarom kijkt de MIVD, in het kader van economische veiligheid, met name naar ongewenste kennisoverdracht. Dat bestrijkt ook die activiteiten die openlijk en legaal zijn – denk aan investeringen en wetenschappelijk onderzoek – maar die desondanks een bedreiging vormen voor onze economische veiligheidsbelangen.

Daarbij kijkt de MIVD met name naar de overdracht van hoogwaardige Nederlandse kennis en technologie naar China. Die is niet enkel onwenselijk vanwege het risico van ongewenst eindgebruik, zoals militaire toepassingen of aanwending van technologie voor het inperken van mensenrechten. Ook raakt het Nederlandse veiligheidsbelangen omdat het kan resulteren in het verlies van de strategische kennispositie van Nederlandse bedrijven en kennis-instellingen, of omdat het leidt tot een strategische afhankelijkheid van China voor bepaalde grondstoffen, technologieën of diensten.

De Nederlandse halfgeleiderindustrie heeft de aandacht van China. Nederland beschikt over unieke kennis waar China voor een belangrijk deel van zijn productiecapaciteit afhankelijk van is. China probeerde in 2024 op diverse wijzen in Nederland deze cruciale technologie te verwerven. China maakt daarbij gebruik van een combinatie van (cyber)spionage, het werven van experts binnen Nederlandse bedrijven, (strategische) overnames van halfgeleiderbedrijven en het omzeilen van geldende exportrestricties. Naarmate legale

en openlijke verwerving van technologie moeilijker wordt door onder andere screening van investeringen en exportcontroles, neemt het risico op illegale, heimelijke verwerving toe.
Wat betreft strategische afhankelijkheden heeft de MIVD in het bijzonder aandacht voor Chinese aanwezigheid in de vitale infrastructuur. Afzonderlijk lijken de veiligheidsrisico's van aanbestedingen zoals Chinese scanners op Nederlandse lucht- en zeehavens, Chinese aanbieders in onze telecomnetwerken en Chinese camera's in de openbare ruimte te overzien, maar in zijn totaliteit brengt het Nederland in een positie waarbij Nederlandse actoren potentieel kwetsbaar zijn voor economische druk, spionage of zelfs sabotage.

China: spionage

De MIVD heeft in 2024 Chinese spionageactiviteiten richting Nederlandse en bondgenootschappelijke defensiebelangen vastgesteld. Nederland is duidelijk in beeld en is een interessant spionagedoelwit voor China. Dit komt door de hoogwaardige Nederlandse (defensie)industrie die China nodig heeft om haar gestelde politieke, economische en militaire doelstellingen waar te kunnen maken.

Daarnaast blijft Nederland interessant voor Chinese spionageactiviteiten als onderdeel van de Navo, de EU, als veiligheidspartner van de VS en vanwege de recente militaire Nederlandse aanwezigheid in de Zuid-Chinese Zee. De focus ligt hierbij onder andere op het in kaart brengen van de militaire intenties van de Navo en de VS met betrekking tot China. Medewerkers van de krijgsmachten van Nederland en bondgenoten, ook voormalig medewerkers, waren in 2024 spionagedoelwit voor China vanwege de kennis van hedendaagse westerse militaire operaties, personeel, processen en kennis van hoogwaardig materieel. De informatie die door de Chinese diensten wordt verzameld, betreft niet altijd gerichte en specifieke informatie, maar ook informatie over personen en defensieonderdelen. Alle potentieel interessante informatie is in principe bruikbaar, wanneer niet nu dan wellicht in de toekomst.

China: Cyber

In 2024 voerden Chinese cybereenheden opnieuw cyberoperaties uit tegen Nederland en bondgenoten in de EU en de Navo. Om effectiever te kunnen opereren voerde het Chinese PLA in 2024 een reorganisatie uit. Als onderdeel hiervan vallen de meeste operationele cybereenheden nu onder de *Cyber Space Force* (CSF), welke rechtstreeks wordt aangestuurd door de *Central Military Commission* (CMC) onder leiding van Xi Jinping. De MIVD schat in dat deze reorganisatie de dreiging die uitgaat van PLA-cyberoperaties nog verder zal verhogen.

Inlichtingen van de MIVD wijzen al langer op grote Chinese inspanningen ten behoeve van het bereiken van dergelijke strategische inlichtingenposities, met als doel om inlichtingen te vergaren en handelingsopties te hebben in het geval van een eventueel toekomstig militair conflict. Hoewel China de VS waarschijnlijk ziet als primaire tegenstrever in het cyberdomein, kan het land aanzienlijke cybersabotagecapaciteiten in de toekomst ook in gaan zetten tegen Europese doelen.

De MIVD en AIVD brachten in 2024 rapporten uit over de Chinese malware die de diensten aantroffen op het netwerk van een Nederlands defensieonderdeel[11] en de bredere campagne waar die aanval onderdeel van uitmaakte[12]. De diensten observeerden in 2024 opnieuw dat Chinese cyberactoren met succes misbruik maakten van kwetsbare *edge devices*[13], zoals firewalls en VPN-software[14]. Met een hoog tempo werden softwarekwetsbaarheden uitgebuit vaak binnen enkele uren of dagen nadat deze bekend werden gemaakt. Een campagne kan zo tienduizenden organisaties slachtoffer maken.

[11] *'Ministry of Defence of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT (MIVD & AIVD, 6 februari '24)' en 'Nieuwe malware benadrukt aanhoudende interesse in edge devices (NCSC-NL, 6 februari '24) https://www.ncsc.nl/actueel/nieuws/2024/februari/6/nieuwe-malware-benadrukt-aanhoudende-interesse-in-edge-devices*

[12] *Aanhoudende statelijke cyberspionagecampagne via kwetsbare edge devices (NCSC-NL, 10 juni '24) https://www.ncsc.nl/actueel/nieuws/2024/juni/10/aanhoudende-statelijke-cyberspionagecampagne-via-kwetsbare-edge-devices*

MIVD heeft Chinese cyberspionage blootgelegd *(februari 2024)*
De MIVD heeft Chinese cyberspionage in Nederland blootgelegd. De dienst ontdekte geavanceerde Chinese malware die dit mogelijk maakt. Op basis van eigen inlichtingen stelt de MIVD vast dat een Chinese statelijke actor verantwoordelijk is voor deze malware.

China gebruikt dit type malware voor spionage op computernetwerken. De malware wordt ingezet bij systemen (*FortiGate*) van het bedrijf Fortinet, waarmee computergebruikers beschermd op afstand kunnen werken. Fortinet levert wereldwijd deze cyberbeveiliging.

De MIVD kiest er voor het eerst voor om een technische rapport over de werkwijze van Chinese hackers openbaar te maken. "Het is belangrijk om dergelijke spionageactiviteiten van China te attribueren'': reageerde toenmalig minister van Defensie Kajsa Ollongren. Zo verhogen we de internationale weerbaarheid tegen dit soort cyberspionage.

De MIVD heeft op de website van het Nationaal Cyber Security Centrum (NCSC) informatie over het incident en de kenmerken van de malware gedeeld. Hiermee kunnen gebruikers van het systeem FortiGate vaststellen of zijn slachtoffer zijn geworden. Ook kunnen zij maatregen treffen om zich te verdedigen.

De Chinese cyberactoren kunnen gebruik maken van een faciliterend ecosysteem van naar schatting honderden organisaties. Chinese bedrijven bieden diensten aan om de herkomst van statelijke cyberaanvallen te verhullen, door deze langs kwetsbare netwerkapparatuur van nietsvermoedende particulieren en organisaties in derde landen te routeren. Daarnaast maakt intensieve samenwerking met Chinese bedrijven en kennisinstellingen gespecialiseerde kennis toegankelijk voor Chinese statelijke actoren, zoals onderzoek naar kwetsbaarheden in hard- en software.

Opvallend in 2024 waren publicaties van de Amerikaanse inlichtingen- en veiligheidsdiensten over Chinese cybereenheden die zich op geavanceerde wijze wisten te nestelen in vitale infrastructuur. Dat zij erin slaagden om tenminste een jaar ongezien te werk te gaan, wijst er op dat westerse inlichtingendiensten en cybersecuritybedrijven maar beperkt grip hebben op de Chinese cyberdreiging.

Grootschalige hack op Amerikaanse telecommunicatieproviders
De Chinese cyberactor *Salt Typhoon* had tenminste een jaar lang toegang tot grote Amerikaanse telecomproviders. Hierbij zou communicatie van politici en ambtenaren ingezien zijn en mogelijk ook toegang zijn verkregen tot geheime informatie van opsporingsdiensten.

De berichtgeving past binnen observaties van de MIVD en AIVD. Naar inschatting van de diensten is het waarschijnlijk dat ook Europese telecommunicatieproviders doelwit zijn van geavanceerde hackpogingen.

Hacks op telecommunicatieproviders behoren tot de meest waardevolle inlichtingenposities voor Chinese statelijke actoren. Zo droeg de door *Salt Typhoon* gestolen data waarschijnlijk bij aan de volgende mogelijkheden voor Chinese inlichtingendiensten:

- Inzien van vertrouwelijke communicatie van Amerikaanse politici en hoge functionarissen.
- Identificeren van Amerikaanse ambtenaren, militairen en inlichtingenofficieren.

[13] *Edge devices: een apparaat wat een toegangspunt (gateway) biedt tot (kern)netwerken van ondernemingen of serviceproviders zoals routers, routing switches etc.*
[14] *VPN: Virtual Private Network; beveiligt gebruikers door data te versleutelen en het IP adres te maskeren*

- Ontwaren van de sociale en professionele netwerken en *pattern of life* van deze personen.
- Inzage krijgen in geheime informatie van Amerikaanse opsporingsdiensten via *lawful intercept* tapsystemen.
- Ontdekken van kwetsbaarheden in netwerken van Amerikaanse overheden, defensieonderdelen, I&V-diensten, vitale sectoren en topsectoren.
- Uitvoeren van *supply chain*-operaties via internetaansluitingen van klanten van telecomproviders.

Het nieuws over *Salt Typhoon* komt bovenop eerdere berichtgeving over actor *Volt Typhoon*, die zich zou hebben weten te prepositioneren voor toekomstige sabotage in Amerikaanse militaire en civiele vitale infrastructuur.[15]

China: Militaire techniek en wapensystemen

Met het oog op de ambitie om een krijgsmacht van wereldklasse te worden, zet China alles op alles om militaire troefkaarten in handen te krijgen: nieuwe wapensystemen of bestaande systemen die gebruikmaken van nieuwe technologieën. In zijn plannen ruimt China al geruime tijd veel ruimte in voor het ontwikkelen van technologieën als kwantumtechnologie, kunstmatige intelligentie en biotechnologie, zogenaamde sleuteltechnologieën. Dit doet het land niet alleen om civiel koploper te worden, maar met name ook om zijn krijgsmacht in staat te stellen af te schrikken en te domineren. Deze sleuteltechnologieën kunnen een dergelijk grote ontwrichting van een samenleving veroorzaken, dat ze strategisch[16] van aard zijn.

Eén van die troefkaarten betreft *quantum sensing*. Dit is een technologie waarmee het mogelijk is om met extreem hoge nauwkeurigheid waarnemingen te doen, bijvoorbeeld van versnellingen of magnetische veldsterktes. *Quantum sensing* kan worden toegepast in een breed palet aan wapensystemen. Zo kunnen kwantumradars in staat zijn *stealth*-vliegtuigen te detecteren, waar gangbare systemen daar wellicht moeite mee hebben. Daarnaast zijn kwantummagnetometers waarschijnlijk binnen afzienbare tijd in staat onderzeeboten te detecteren, waardoor hun grootste kracht, te weten “onzichtbaarheid”, teniet wordt gedaan.

De MIVD constateert dat China in 2024 tevens inzet op zwermtechnologie. Zwermtechnologie omvat de inzet van een groter aantal onbemande eenheden die op autonome wijze kunnen samenwerken om een militair doel te behalen. Autonomie wordt daarbij bewerkstelligd op basis van kunstmatige intelligentie. Voorbeelden van inzet zijn het onschadelijk maken van luchtverdedigingssystemen, het begeleiden van bemande platformen of directe offensieve inzet waarbij de kracht grotendeels voortvloeit uit het opereren in grote aantallen.

China behoort reeds tot de koplopers op het gebied van zwermtechnologie en zet in op ontwikkeling van systemen voor onder meer het lucht- en maritieme domein. Bovendien wordt de ontwikkeling van zwermtechnologie door China gezien als onderdeel van een wapenwedloop voor *high tech*-oorlogsvoering.

China doet er veel aan om koploper te zijn en te blijven, inclusief het weghalen van kennis over de hele wereld. De snelheid en omvang van China’s technologische ontwikkelingen voor militaire doeleinden stellen andere landen, waaronder Nederland, voor uitdagingen op het gebied van defensie en veiligheid. Het is essentieel dat de MIVD deze ontwikkelingen nauwlettend volgt en onze krijgsmacht in staat stelt haar eigen strategieën en capaciteiten aan te passen om effectief te kunnen reageren op de veranderingen in het militaire landschap.

[15] *In dit geval wordt onder strategische sleuteltechnologieën technologieën verstaan die bestemd zijn voor het gebruik als of in wapen(s), waarbij die wapens zelf bedoeld zijn voor totale oorlogsvoering, ook tegen burgerdoelen en bevolkingscentra.*

[16] *In dit geval wordt onder strategische sleuteltechnologieën technologieën verstaan die bestemd zijn voor het gebruik als of in wapen(s), waarbij die wapens zelf bedoeld zijn voor totale oorlogsvoering, ook tegen burgerdoelen en bevolkingscentra.*


LZ115

1.3 *Caribisch gebied*

De MIVD en de AIVD doen gezamenlijk onderzoek naar politieke en militaire ontwikkelingen in Venezuela en mogelijke uitstralingseffecten richting de bijzondere gemeente Bonaire en de landen Aruba en Curaçao binnen het Koninkrijk der Nederlanden

De eerste maanden van 2024 werden in Venezuela gedomineerd door het Essequibo-geschil. Naar aanleiding van een referendum in december 2023 riep Venezuela een substantieel deel van buurland Guyana uit tot Venezolaans grondgebied, waarna de internationale spanningen opliepen. Hoewel Venezuela en Guyana zich beide committeerden aan het vinden van een diplomatieke oplossing, versterkte het Venezolaanse regime desondanks zijn militaire aanwezigheid in het grensgebied om de Venezolaanse intenties kracht bij te zetten. In de aanloop naar de Venezolaanse presidentsverkiezingen die in juli plaatsvonden, nam de Venezolaanse militaire focus op de grens met Guyana echter af. Deze is in de rest van 2024 niet meer volledig teruggekeerd.

De presidentsverkiezingen van 28 juli 2024 zijn in veel opzichten het belangrijkste evenement van het jaar geweest voor Venezuela. Hoewel Nicolás Maduro de overwinning heeft opgeëist, bestaat er overweldigend bewijs dat zijn tegenstander Edmundo González Urrutia met een ruime meerderheid van de stemmen de eigenlijke winnaar van de verkiezingen was. Kort na de verkiezingen is door de Nederlandse diplomatieke vertegenwoordiging in Caracas onderdak verleend aan presidents-kandidaat González tot hij in september uitweek naar Spanje, vanwege de ernstige dreiging die tegen hem uitging.

Een belangrijk deel van de internationale gemeenschap, waaronder de VS, de EU en verschillende Latijns-Amerikaanse landen, erkennen de door het regime geclaimde overwinning van Maduro niet. Het regime heeft daarop de diplomatieke betrekkingen met een aantal Latijns-Amerikaanse landen verbroken en het discours tegen het Westen verder aangescherpt.

Hoewel er geen nieuwe sancties tegen de Venezolaanse oliesector zijn ingesteld, hebben zowel de VS als de EU nieuwe personele sancties tegen regimeleden aangekondigd. Het Venezolaanse regime probeerde ondertussen de samenwerking met zijn bondgenoten Rusland, China en Iran uit te breiden, alsook met andere niet-westerse landen.

De Venezolaanse krijgsmacht heeft met investeringen en ontwikkeling in 2024 de stijgende lijn doorgezet die sinds enkele jaren te zien is. In samenwerking met internationale partners zoals Iran, Rusland en China werkt Venezuela aan het (opnieuw) inzetbaar maken en houden van het bestaande materieel, evenals het verwerven van nieuw materieel en middelen. Ondanks deze stijgende lijn constateert de MIVD dat de Venezolaanse krijgsmacht in 2024 nog steeds te kampen heeft met grote uitdagingen. Zo zijn er grote personeelstekorten, zijn veel eenheden slechts zeer beperkt in staat om te trainen en is er op veel voertuigen en wapensystemen sprake van achterstallig onderhoud. Gemiddeld genomen blijft het gereedstellingsniveau van de Venezolaanse krijgsmacht daarom laag.

1.4 *Contraproliferatie*

De Unit Contraproliferatie (UCP) is een gezamenlijke eenheid van de MIVD en de AIVD. De unit onderzoekt landen die een bedreiging kunnen vormen voor de internationale veiligheid met massavernietigingswapens of de daarvoor benodigde overbrengingsmiddelen (meestal ballistische raketten) ontwikkelen. Ook helpt de UCP te voorkomen dat dergelijke 'landen van zorg'[17] (Russische federatie, Iran, China, Noord-Korea en Syrië) aan technologie en kennis komen om wapenprogramma's te beginnen of uit te breiden.

In 2024 is wederom geconstateerd dat de inzet van massavernieti-gingswapens door landen van zorg, waaronder Rusland, Iran en

[17] *Landen van zorg zijn landen die landen die een bedreiging kunnen zijn voor de internationale veiligheid.*

Noord-Korea, behoort tot de reële mogelijkheden behoort. De inzet van dergelijke wapensystemen vormt niet noodzakelijkerwijs een taboe voor sommige van deze landen. Zoals hieronder uiteen wordt gezet, maakte Rusland in 2024 illegaal gebruik van chemische agentia in de strijd met Oekraïne en heeft Iran ballistische raketten ingezet voor de eerste directe aanvallen op Israël. Daarbij leveren zowel Iran als Noord-Korea wapens (waaronder ballistische raketten) aan Rusland voor de inzet in Oekraïne, en zijn ook de ontwikkelingen op nucleair gebied in Iran en Noord-Korea zorgelijk. Tegen deze achtergrond hebben de diensten ook in 2024 actief opgetreden tegen de ongewenste overdracht van kennis en technologie vanuit Nederland naar dergelijke programma's in (onder meer) de genoemde landen.

Rusland

Rusland schendt stelselmatig het Verdrag Chemische Wapens door chemische agentia te gebruiken in de oorlog in Oekraïne. Al een aantal dagen na de invasie van 2022 verschenen de eerste berichten dat Rusland traangas had ingezet op Oekraïens grondgebied. Sindsdien is de inzet van chemische agentia door Rusland geïntensiveerd en gericht op inzet tegen Oekraïense soldaten. Tevens zijn er incidenten met chloorpicrine gedocumenteerd. Het Oekraïense ministerie van Defensie heeft inmiddels duizenden incidenten gerapporteerd van Russische inzet van chemicaliën tegen de Oekraïense strijdkrachten, iets dat expliciet verboden is onder het Verdrag Chemische Wapens. De inzet heeft in 2024 geresulteerd in aanvullende sancties van de VS en het Verenigd Koninkrijk tegen Rusland.

Iran

In 2024 zijn Iraanse ballistische raketten veelvuldig ingezet in het Midden-Oosten. Zo heeft Iran voor het eerst directe aanvallen uitgevoerd op Israël, waarbij gebruik is gemaakt van door Iran zelf ontwikkelde ballistische raketten. Hierbij claimt Iran dat ook de hypersone ballistische raket 'Fattah' zou zijn ingezet. De dreiging beperkte zich echter niet tot Iran. Ook Iraanse bondgenoten zoals Hezbollah en de in Jemen actieve Houthi's hebben in 2024 gebruik gemaakt van door Iran ontwikkelde raketten. Iraanse raketsystemen hebben daarmee een grote rol gespeeld in de dreiging voor de scheepvaart in de Rode Zee en in de Perzische Golf. Ook heeft Iran in 2024 korteafstandsraketten geleverd aan Rusland. Naar aanleiding van deze levering zijn er door de Europese Unie en een aantal bondgenoten aanvullende sancties ingesteld tegen Iran.

Op het gebied van ruimtevaart heeft Iran in 2024 verdere stappen gezet. Zo heeft het meerdere lanceringen met ruimtevaartuigen uitgevoerd. Technologie uit deze ruimtevaarttuigen kan ook gebruikt worden bij de ontwikkeling van ballistische raketten. Verder zijn verschillende Iraanse satellieten via Russische ruimtevaartuigen succesvol in een baan om de aarde gebracht.

De MIVD constateert daarnaast dat Iran, indien gewenst, binnen zeer korte tijd zou kunnen beschikken over voldoende hoogverrijkt uranium voor de productie van enkele kernwapens. De MIVD en AIVD hebben echter geen aanwijzingen dat Iran op dit moment de andere noodzakelijke activiteiten verricht om testen uit te voeren om een nucleair explosief te ontwikkelen. De ontwikkeling van kernwapencapaciteit lijkt in het land echter wel in toenemende mate bespreekbaar te worden. De recente onrust in het Midden-Oosten leidt bijvoorbeeld tot de oproep uit bepaalde kringen binnen de Iraanse politiek om de fatwa uit 2003 tegen kernwapens te herzien. Ook dreigt Iran uit het nucleaire non-proliferatieverdrag (NPV) te stappen wanneer de E3[18] het *snapback*-mechanisme[19] van het *Joint Comprehensive Plan of Action* (JCPOA) zou triggeren. Bovendien stelt het Internationaal Atoomenergieagentschap (IAEA) dat het door Iran niet in staat wordt gesteld om te verifiëren dat Irans nucleaire programma uitsluitend civiele doelen dient. Deze ontwikkelingen bemoeilijken de totstandkoming van een nieuw nucleair akkoord dat de proliferatiezorgen rondom Iran's nucleaire programma moet wegnemen.

[18] *E3: Duitsland, Frankrijk en het Verenigd Koninkrijk.*

[19] *Snapback mechanisme: wanneer Iran het JCPOA niet naleeft kan ieder JPCOA lid (direct, indien lid van de VN veiligheidsraad) of indirect van de VN Veiligheidsraad een procedure starten waarbij er sancties worden ingesteld.*

Noord-Korea

Ook Noord-Korea is in 2024 doorgegaan met de ontwikkeling van zowel korteafstands- als intercontinentale ballistische raketten. Daarbij heeft het land testlanceringen uitgevoerd met tactische ballistische raketten en kruisvluchtwapens met een grotere explosieve lading dan eerder getoond en zijn er testlanceringen uitgevoerd met nieuwe hypersone ballistische raketten en een nieuwe intercontinentale ballistische raket. Daarnaast is door Kim Jong-Un het bevel uitgegeven om de munitieproductie op te schroeven, in een jaar waar de spanningen tussen Noord- en Zuid-Korea blijven toenemen. Net als Iran heeft Noord-Korea in 2024 ook meerdere korteafstandsraketten geleverd aan Rusland. In het geval van Noord-Korea zijn deze raketten ook daadwerkelijk ingezet op het slagveld in Oekraïne.

Noord-Korea heeft in 2024 een uniek inkijkje gegeven in zijn kernwapenprogramma. Het land publiceerde foto's van een uraniumverrijkingsfaciliteit, iets wat niet eerder gebeurd is. Kim Jong-Un geeft hiermee invulling aan zijn voornemen tot uitbreiding van het Noord-Koreaanse kernwapenarsenaal.

Verwerving

Landen van zorg (naast Rusland, Iran en Noord-Korea ook landen als Pakistan en Syrië) waren in 2024 nog steeds afhankelijk van het Westen voor kennis en hoogwaardige technologie. De diensten onderzoeken de verwervingsactiviteiten naar deze kennis en technologie, en heeft ook in 2024 de overheid in staat gesteld om op te treden tegen onder meer Russische en Iraanse verwervingsnetwerken. Dit optreden omvatte diplomatieke, bestuursrechtelijke of strafrechtelijke maatregelen, of operationeel optreden door de diensten zelf.[20]

Uit onderzoek van de diensten blijkt dat Rusland de aangescherpte sancties op de export van '*dual-use*-goederen'[21] omzeilt door die binnen te halen via 'omleidingslanden', waaronder de Verenigde Arabische Emiraten, Turkije, Kazachstan en China. Dat maakt het moeilijker om de export vroegtijdig te onderkennen en tegen te gaan. In enkele gevallen ging het daarbij ook om '*dual-use*-goederen' uit Nederland.
De diensten constateren ook dat bestaande handelskanalen binnen de civiele nucleaire sector door Rusland worden gebruikt voor de verwerving van technologie voor het militair-industrieel complex. Vanwege afhankelijkheidsrelaties waagde het Westen zich tot nu toe niet aan handelsbeperkingen ten aanzien van de civiele nucleaire sector, wat de effectiviteit van de Ruslandsancties in het algemeen niet ten goede komt.

1.5 *Contra-inlichtingen (CI)*

Eén van de taken van de MIVD is het verrichten van onderzoek naar dreigingen van extremisme en terrorisme in het bijzonder in relatie tot de krijgsmacht. In 2024 heeft de MIVD dit onderzoek vooral gericht op rechts-extremisme en anti-institutioneel extremisme. De focus van het onderzoek ligt op dreigingen tegen Defensie en op dreigingen vanuit (aspirant-)defensiemedewerkers richting de democratische en internationale rechtsorde. Met de bevindingen uit dit onderzoek kan de MIVD-belanghebbenden in staat stellen om maatregelen te treffen, zowel tegen specifieke personen als op het gebied van beleidsontwikkeling.

Rechts-extremisme

De MIVD heeft in 2024 meerdere onderzoeken opgestart vanwege mogelijk rechts-extremisme bij (aspirant-)defensiemedewerkers. In sommige van die onderzoeken lijkt geen sprake te zijn van ideologisch gemotiveerde uitingen, maar eerder van andere vormen van ernstige normvervaging. Wanneer de ideologische component wel aanwezig lijkt, is meestal sprake van nazistische sympathieën waarin antisemitische uitingen een prominente rol spelen. De MIVD heeft verder geen indicaties van rechts-extremistische netwerkvorming binnen Defensie, maar ziet wel dat rechts-extremistische (aspirant-)defensiemedewerkers actief zijn in

[20] *In een in 2024 gepubliceerde podcast over het tegengaan van dergelijke verwervingspogingen lichten de diensten een tipje van de sluier waar het gaat om dergelijke operaties.*
[21] *Goederen zijn 'dual-use' als ze zowel voor vreedzame als militaire doelen kunnen worden gebruikt, bijv. zowel voor fundamenteel wetenschappelijk onderzoek als in een massavernietigingswapenprogramma.*


F803

rechts-extremistische netwerken buiten Defensie. De MIVD heeft in 2024 verschillende belangendragers geïnformeerd over rechts-extremistische (aspirant-)defensiemedewerkers om hen in staat te stellen tot het nemen van maatregelen. Bij de MIVD zijn momenteel geen aanwijzingen van een rechts-extremistische geweldsdreiging richting Defensie.

Anti-institutioneel extremisme

Anti-institutioneel extremisten geloven dat er een kwaadaardige elite aan de macht is die het volk ernstig onderdrukt. Deze vermeende kwaadaardige elite zou hiervoor instituties gebruiken zoals de overheid, de media en de wetenschap. Sommige anti-institutioneel extremisten zien Defensie als onderdeel van de kwaadaardige elite of doen een beroep op militairen om in actie te komen en het volk tegen die elite te beschermen. Dit levert een dreiging op voor de defensieorganisatie en de democratische rechtsorde. De MIVD heeft in 2024 onderkend dat enkele defensiemedewerkers het kwaadaardige-elite-narratief aanhangen en daarnaar handelden. In een aantal gevallen was een pro-Russisch sentiment onderdeel van het gedachtegoed van deze defensie-medewerkers. De MIVD heeft belanghebbenden geïnformeerd waar het gedrag van deze defensiemedewerkers ernstige twijfels opriep over hun betrouwbaarheid ten aanzien van de inzetbaarheid van de krijgsmacht en de bescherming van de democratische rechtsorde.
De MIVD heeft momenteel geen aanwijzingen voor gewelddadig anti-institutioneel extremisme richting de krijgsmacht.

Spionage, ongewenste inmenging en economische veiligheid

In 2024 deed de MIVD-onderzoek naar de dreiging van spionage (inlichtingen)activiteiten van andere landen dan de hiervoor specifiek beschreven landen. Deze landen trachten hierbij de positie van de Nederlandse krijgsmacht binnen multilaterale samenwerkingsverbanden te bepalen of proberen specifieke kennis over Defensie of de Defensie-industrie te bemachtigen.

Iran

De MIVD voert onderzoek uit naar de (heimelijke) activiteiten van Iraanse militaire- en civiele inlichtingendiensten gericht op de verwerving van kennis en middelen die een dreiging vormen voor de veiligheid, paraatheid en inzetbaarheid van de krijgsmacht in nationaal of internationaal verband, voor de (Nederlandse) defensie-industrie en voor militaire bondgenootschappelijke organisaties als de Navo. Onderzoek in 2024 heeft opgeleverd dat Iraanse activiteiten tegen Defensie op opportunistische basis, plaats blijven vinden, in binnen- en buitenland.

In 2024 richtten Iraanse cyberactoren zich voornamelijk op belangen die verband hielden met het Israël-Gaza conflict. Door middel van digitale aanvallen met lokale en tijdelijke impact die zich in sommige gevallen ook op kritieke infrastructuur richtten, trachtte Iran zich te laten gelden. Zo proberen aan Iran gelieerde personen door middel van *hack-and-leak* operaties online (door middel van diverse fora zoals o.a. social media) bepaalde boodschappen te versterken en in het uiterste geval beleids-wijzigingen af te dwingen. Hierdoor werden de Iraanse cyberactiviteiten ook zichtbaarder ten opzichte van eerdere jaren.

Naast de meer zichtbare activiteiten, heeft Iran afgelopen jaar zijn heimelijke spionageactiviteiten tegen experts die zich bezighouden met het conflict in het Midden-Oosten geïntensiveerd. Iraanse actoren gebruikten hiervoor soms zeer geavanceerde social engineering technieken om vervolgens door *phishing*[22] en *spearphishing*[23] methodes communicatiemiddelen te compromitteren.

[22] *Phising: een vorm van internetfraude waarbij cybercriminelen proberen persoonlijke gegevens of wachtwoorden te stelen.*

[23] *Spearphishing: een gerichte vorm van phishing waarbij een specifiek individu of een kleine groep personen via e-mail, telefoon of andere kanalen wordt misleid om vertrouwelijke informatie te delen of om schadelijke software te installeren.*

Noord-Korea

Noord-Koreaanse cyberaanvallen dragen voor een groot deel bij aan de politieke, militaire en economische ambities van Noord-Korea. Noord-Korea heeft een offensief cyberprogramma. Zo zijn de aanvallen gericht op het stelen van informatie over politieke en economische standpunten over Noord-Korea, internationale samenwerkingsverbanden, maar ook over hoogwaardige (militaire) technologie. Noord-Koreaanse cyberactoren zijn zeer succesvol in het ontvreemden van *cryptocurrency* en omzeilen met hun aanvallen de opgelegde sancties tegen Noord-Korea. De cyberaanvallen dragen bij aan de financiering van het regime. Hiermee wordt bijvoorbeeld het Noord-Koreaanse cyber- en kernwapenprogramma gefinancierd.

Economische veiligheid

De Nederlandse economische en veiligheidsbelangen staan onverminderd bloot aan een verscheidenheid aan (statelijke) dreigingen. Hierbij gaat het primair om ongewenste kennis- en technologieoverdracht en strategische afhankelijkheden.

De Nederlandse defensieindustrie, bedrijven, kennisinstellingen en wetenschappers zijn een potentieel doelwit van diverse statelijke actoren die (heimelijk) hoogwaardige, al dan niet militair relevante, technologie proberen te verwerven. Nederland heeft unieke hoogwaardige kennis- en technologieposities, onder andere op gebied van halfgeleiders, kwantumtechnologie en lucht- en ruimtevaart, die worden bedreigd door spionagepogingen of (heimelijke) overnames door landen van zorg zoals Rusland, China en Iran. Deze kennis en technologie kunnen bijdragen aan de militaire capaciteitsopbouw in deze landen.

De Nederlandse defensieindustrie is voor een aanzienlijk deel aangewezen op leveranciers uit derde landen en daarom vatbaar voor risicovolle strategische afhankelijkheden. Daarnaast kunnen afhankelijkheden in de Nederlandse vitale infrastructuur een risico vormen voor de Nederlandse economische veiligheidsbelangen.

De MIVD en AIVD hebben de onderzoeken op het gebied van economische veiligheid en strategische afhankelijkheden belegd binnen de gezamenlijke MIVD-AIVD inlichtingenteams. Deze teams dragen tevens bij aan diverse maatregelen die de overheid heeft genomen om de dreiging tegen de Nederlandse economische veiligheid tegen te gaan en de weerbaarheid te vergroten, zoals het Ondernemersloket Economische Veiligheid, het stelsel van investeringstoetsing en het Loket Kennisveiligheid.

1.6 Missieondersteuning en aandachtsgebieden

In 2024 heeft de MIVD de inzet van de Nederlandse strijdkrachten in missiegebieden ondersteund. De MIVD maakt inlichtingenproducten ten behoeve van militaire inzet en de politieke besluitvorming die hiermee gemoeid is. Ook tijdens de inzet blijft de MIVD betrokken door middel van onderzoek naar aspecten die relevant zijn voor de directe dreiging tegen Nederlandse militairen in een inzetgebied en coalitie en bedreigingen voor het succesvol kunnen uitvoeren van de missie, zoals dreiging tegen het nationale politieke draagvlak in het land van inzet of factoren van invloed op het effectief optreden van eenheden.

Westelijke Balkan

De MIVD verrichtte in 2024 onderzoek naar de westelijke Balkan ter ondersteuning van de inzet van de Nederlandse krijgsmacht als onderdeel van *European Union Force Bosnia and Herzegovina* (EUFOR Althea). In Bosnië en Herzegovina hield, ondanks het starten van toetredingsonderhandelingen met de EU, de sterke etno-nationalistische retoriek van vooral Bosnisch-Servische zijde aan. Ook klonken er meer separatistische geluiden vanuit de Servische Republiek, een deelentiteit van Bosnië en Herzegovina. In Kosovo nam in aanloop naar verkiezingsjaar 2025 de onrust toe. De spanningen pasten binnen de toename van de activiteiten van de vaak (Kosovaars-) Servische nationalistische groeperingen. De

Kosovaarse regering heeft geprobeerd, in het kader van de aanpak van corruptie en georganiseerde misdaad, meer politie in te zetten in Noord-Kosovo. De verwachting is dat spanningen periodiek gaan oplaaien. Het normalisatieproces tussen Servië en Kosovo, bemiddeld door de EU, is door de harde opstelling van beide zijden moeilijker geworden. Mede door de aanwezigheid van militaire missies van de EU en de Navo zijn grootschalige incidenten en significante sociale onrust in de regio uitgebleven.

Afrika

Het onderzoek van de MIVD richt zich op het tijdig onderkennen en signaleren van strategische en veiligheidsrelevante ontwikkelingen die een (potentiële) dreiging vormen ten aanzien van de nationale veiligheid, Nederlandse belangen en/of (potentiële) missies van de EU.

Mali, Burkina Faso en Niger behoren tot de minst ontwikkelde landen ter wereld. Door een combinatie van onder andere extreme armoede, zwakke staatscapaciteit, klimaatverandering en een sterke bevolkingsgroei ontstaat steeds vaker schaarste aan primaire levensbehoeften. In alle drie de landen hebben militairen uit frustratie over de slechte (veiligheids-) situatie de macht gegrepen.

In Mali breidden jihadistische organisaties hun operatiegebieden nog steeds uit. Het zwaartepunten van jihadistische activiteiten ligt in Noord- en Centraal-Mali, maar er is sprake van een verschuiving van geweldsincidenten richting het zuiden. Buiten de hoofdstad is de jihadistische dreiging dan ook toegenomen. Maar ook in de hoofdstad sloegen de jihadisten afgelopen jaar toe. In september wist de jihadistische organisatie Jama'at Nusrat al-Islam wal-Muslimin (JNIM) daar het vliegveld en een opleidingsinstituut van de gendarmerie aan te vallen. Het Malinese leger werkt samen met Russische paramilitairen in het bestrijden van de jihadisten.

De veiligheidssituatie in Burkina Faso is in 2024, net als de jaren daarvoor, achteruitgegaan. Burgers komen steeds vaker klem te zitten tussen de heersende junta van de, in 2022 met een staatsgreep aan de macht gekomen, president Traoré en jihadistische groeperingen. De jihadistische aanvallen worden ook steeds grootschaliger en gebeuren op steeds meer plaatsen in het land. Om de verslechterende veiligheidssituatie het hoofd te bieden heeft de junta, net als in Mali, de hulp ingeroepen van Russische paramilitairen. Zij zijn belast met de persoonlijke beveiliging van juntaleider Traoré en verzorgen trainingen voor de Burkinese strijdkrachten.

De situatie in Niger komt overeen met die in Mali en Burkina Faso. Ook dit land kent een aanhoudend slechte veiligheidssituatie die de in juli 2023 met een staatsgreep aan de macht gekomen regering niet effectief weet te verbeteren. Ook hier vormen aanvallen van jihadisten de grootste dreiging en ook de Nigerese junta heeft de hulp van Russische paramilitairen ingeroepen die vergelijkbare taken uitvoeren als in Burkina Faso.

Irak

De MIVD heeft ook in 2024 onderzoek gedaan naar Irak. Daarbij lag het zwaartepunt op de inlichtingenondersteuning aan de *NATO Mission in Iraq* (NMI). De Nederlandse militaire bijdrage aan missie NMI omvat voor de periode van mei 2024 tot mei 2025 de levering van een Nederlandse commandant, ongeveer vijftien personen aanvullende staf, een *Force Protection* element en drie transporthelikopters inclusief personeel.

In 2024 leidde het conflict tussen Israël en Hamas tot aanvallen door de (veelal) sjiitische aan Iran gelieerde milities op coalitielocaties in Irak en Syrië. Deze aanvallen waren veelal kleinschalig van aard en de menselijke en materiële schade bleef grotendeels beperkt. Sinds begin oktober hebben er geen aanvallen tegen coalitielocaties in Irak plaatsgevonden.

Vanaf medio augustus verlegden de Iraakse, aan Iran-gelieerde milities hun focus. Zij legden zich toe op het uitvoeren van kleinschalige aanvallen

in de richting van Israël. Het aantal aanvallen nam daarbij vanaf medio september 2024 significant toe. Na het staakt-het-vuren tussen Israël en Hezbollah op 27 november afgelopen jaar, werden de aanvallen op Israël opgeschort.

De MIVD heeft in 2024 onderzoek gedaan naar de politiek in Irak. De Iraakse politiek kenmerkte zich in 2024, ondanks het regionale conflict tussen Israël en Iran (inclusief zijn bondgenoten Hamas en Hezbollah), door relatieve stabiliteit. De regering van premier al-Sudani heeft verschillende successen weten te behalen, onder andere door het verbeteren van de infrastructuur. Grootschalige structurele problemen blijven echter onopgelost. Aanhoudende maatschappelijke onvrede door een gebrek aan onder andere voldoende basisvoorzieningen (zoals water en elektriciteit) en werkgelegenheid resulteert regelmatig in demonstraties in geheel Irak.

Iran

De MIVD verrichtte in 2024 onderzoek naar de politieke en militaire invloed van Iran in het Midden-Oosten. Het land steunt in die regio tal van Iran-gezinde milities, zoals Hezbollah en de Houthi's, met wapens, advies en inlichtingen. Zo tracht Iran zijn invloed in de regio te behouden en waar mogelijk te vergroten.

Maar het Iraanse regime kreeg in 2024 een aantal zware klappen te verduren. Ten eerste doordat het sluimerende conflict met Israël ontbrandde. Gedurende het jaar bestookten beide landen elkaar een aantal keer met raketten en UAV's, waarbij de Israëlische aanvallen in militair opzicht vele malen effectiever bleken dan de Iraanse.

Ten tweede doordat Iran moest toezien hoe zijn bondgenoten in de regio onder vuur kwamen te liggen. Hamas en Hezbollah werden hard getroffen door Israëlische aanvallen. In december zag Iran met de val van het Assad-regime in Syrië een belangrijke partner wegvallen, waardoor de geopolitieke positie van Iran kwetsbaarder werd.

Een opmerkelijke politieke gebeurtenis in Iran was het overlijden van president Raisi, die op 19 mei omkwam bij een helikoptercrash. Raisi werd opgevolgd door de relatief gematigde Mahmoud Pezeshkian, die op 5 juli de presidentsverkiezingen won. President Raisi werd beschouwd als de belangrijkste kandidaat om Iran's Opperste Leider, Ali Khamenei, op te volgen. Door Raisi's overlijden ligt deze opvolgingsvraag weer open.

ISIS

Ook in 2024 heeft ISIS in Irak en Syrië personele en materiële verliezen geleden als gevolg van de aanhoudende druk van de verschillende veiligheidstroepen gesteund door de anti-ISIS-coalitie. In 2024 heeft de afname van aanslagen door ISIS in Irak zich verder voortgezet. In 2024 zijn er meerdere weken verstreken zonder dat er aanslagen zijn gepleegd, hetgeen uitzonderlijk was. De aanslagen die ISIS wel uitvoerde waren veelal kleinschalig, waarbij eenvoudige *hit & run*-tactieken werden toegepast. De meeste incidenten komen voor in centraal Irak. Gezien het grensoverschrijdende karakter van de activiteiten van ISIS en (ondersteuning van) inzet van bondgenoten is ook naar activiteiten van ISIS in Syrië gekeken.

1.7 Veiligheidsbevorderende taken

Elektronische veiligheidsonderzoeken

Het Defensie Beveiligingsbeleid (DBB) stelt een aantal veiligheidsnormen die de exclusiviteit, de integriteit en de beschikbaarheid van informatie (van alle rubriceringen) bevorderen. Naast bouwkundige, organisatorische en beveiligings-technische normen, stelt het DBB de eis dat een ruimte waar informatie besproken of verwerkt wordt met de rubricering Stg. GEHEIM en/of hoger aan een Elektronisch Veiligheidsonderzoek (EVO) onderworpen wordt. De MIVD voert onderzoeken uit op dergelijke bestaande ruimten en brengt adviezen uit voor nieuwbouw- of

verbouwprojecten. Dit om vroegtijdig eventuele aandachtspunten omtrent informatieveiligheid te signaleren. De MIVD voert deze onderzoeken uit voor alle defensieonderdelen en werkt, waar mogelijk, samen met Nederlandse collega diensten binnen het vakgebied.

Economische veiligheid

Met het oog op het toegenomen belang van inlichtingen en veiligheidsbevorderende maatregelen op het gebied van economische veiligheid, kijkt de MIVD specifiek naar risico's en veiligheidsbelangen ten aanzien van (economische) spionage en ongewenste buitenlandse beïnvloeding in relatie tot defensieorderbedrijven. Hierbij is het van belang dat de open economie en daarmee het verdienvermogen van Nederlandse bedrijven, waaronder defensieorderbedrijven, niet ten koste gaat van de integriteit, veiligheid en operationeel inzetbaarheid van de Nederlandse krijgsmacht.

De Nederlandse economische en veiligheidsbelangen staan onverminderd bloot aan een verscheidenheid aan (statelijke) dreigingen zo ook de Nederlandse defensie-industrie. Hierbij gaat het primair om ongewenste kennis- en technologieoverdracht en strategische afhankelijkheden.

Nederland heeft unieke hoogwaardige kennis- en technologieposities, onder andere op gebied van halfgeleiders, kwantumtechnologie en lucht- en ruimtevaart, die worden bedreigd door spionagepogingen of (heimelijke) overnames door landen van zorg zoals Rusland, China en Iran. Deze kennis en technologie kunnen bijdragen aan de militair opbouw in deze landen.

De Nederlandse industrie is voor een aanzienlijk deel aangewezen op leveranciers uit derde landen en daarom vatbaar voor risicovolle strategische afhankelijkheden. Daarnaast kunnen afhankelijkheden in de Nederlandse vitale infrastructuur een risico vormen voor de Nederlandse (economische) veiligheidsbelangen.

De MIVD en AIVD hebben de onderzoeken op het gebied van economische veiligheid en strategische afhankelijkheden belegd in gezamenlijke inlichtingenteams. Deze teams dragen tevens bij aan diverse maatregelen die het Kabinet heeft genomen om de dreiging tegen de Nederlandse economische veiligheid tegen te gaan en de weerbaarheid te vergroten.

Industrieveiligheid

Het DBB, en in het bijzonder de Industriebeveiliging, schrijft de verplichtingen voor die intern Defensie gelden bij het uitwisselen van Bijzondere Informatie (BI) met het bedrijfsleven, de defensie-industrie of bij de uitvoering van opdrachten met een vitaal karakter. De regeling Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) schrijft de eisen voor waaraan het bedrijfsleven moet voldoen, voordat zij geautoriseerd kunnen worden om in aanraking te komen met BI. Bij aanvang van een opdracht controleert Bureau Industrieveiligheid (BIV) van de MIVD de bedrijven om zeker te stellen dat zij voldoen aan de gestelde eisen uit de ABDO. Doorlopende activiteiten van BIV betreffen het routinematig inspecteren van bedrijven met een ABDO-autorisatie, het uitvoeren van integrale veiligheidscontroles, het adviseren van ABDO-bedrijven en de opdrachtgever (Defensie). In het geval van een incident waarbij BI is betrokken, treft of laat BIV-maatregelen treffen, om (eventuele) compromitteren te voorkomen of te beperken.

Met het oog op het toegenomen belang van inlichtingen en veiligheidsbevorderende maatregelen op het gebied van economische veiligheid, kijkt de MIVD specifiek naar risico's en veiligheidsbelangen ten aanzien van (economische) spionage en ongewenste buitenlandse beïnvloeding in relatie tot defensieorderbedrijven. Hierbij is het van belang dat de open economie en daarmee het verdienvermogen van Nederlandse bedrijven, waaronder defensieorderbedrijven, niet ten koste gaat van de integriteit, veiligheid en operationele inzetbaarheid van de Nederlandse krijgsmacht.

In 2024 beschikte de MIVD over informatie over (voorgenomen) buitenlandse overnames en/of investeringen inzake defensieorder-

bedrijven betrokken bij het leveren van exclusieve diensten of hoogwaardige (militaire) technologie. Daarnaast was een toename van incidenten in het cyberdomein te zien. Ook ABDO-bedrijven worden hierdoor geraakt. In 2024 is de samenwerking met de AIVD geïntensiveerd ter voorbereiding op de omslag van defensieopdrachten naar Rijksbrede opdrachten. In de aankomende periode zal o.l.v. een interdepartementaal programma de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO) worden afgerond. Het BIV zal opgaan in het Nationaal Bureau Industrieveiligheid (NBIV), een gezamenlijk bureau van de MIVD en de AIVD.

Veiligheidsonderzoeken

De Unit Veiligheidsonderzoeken (UVO) van de MIVD en de AIVD kijkt positief terug op 2024, aangezien 93,3% van de veiligheidsonderzoeken binnen de wettelijke norm van acht weken is afgerond. In 2024 rondde de UVO samen met de mandaathouder (Koninklijke Marechaussee) 84.847 veiligheidsonderzoeken af. De behoefte aan veiligheidsonderzoeken blijft stijgen. Deze trend was in 2023 ook al zichtbaar. Dit komt onder meer door een toename van het aantal vertrouwensfuncties in Nederland, onder andere bij Defensie.

De UVO heeft in 2024 structurele maatregelen doorgevoerd om te kunnen voorzien in de behoefte aan veiligheidsonderzoeken. De unit heeft onder andere meer personeel geworven en gewerkt aan digitalisering en (gedeeltelijke) automatisering van veiligheidsonderzoeken. Door automatisering kan de UVO meer medewerkers inzetten op complexe dossiers, waardoor kwalitatief hoogwaardige onderzoeken geleverd kunnen worden. Bovendien heeft automatisering er onder andere voor gezorgd dat de gemiddelde wachttijd is verkort ten opzichte van vorig jaar.

In 2024 is de Mandaatregeling Defensie Wet op de inlichtingen- en veiligheidsdiensten 2017 en de Wet veiligheidsonderzoeken gewijzigd. Door deze wijziging ligt de bevoegdheid van het weigeren of intrekken van een verklaring van geen bezwaar (VGB) niet meer bij de Plaatsvervangend Secretaris-Generaal van Defensie, maar bij de (plaatsvervangend) directeur van de MIVD.

De wijziging van de Wet veiligheidsonderzoeken is in januari 2025 aan de Tweede Kamer aangeboden. De wet beoogt meer flexibiliteit te bieden aan sectoren waar medewerkers die een vertrouwensfunctie bekleden veelvuldig van werkgever wisselen en introduceert een locatie gebonden VGB. Voor de werkgevers is een aan- en afmeldverplichting opgenomen in geval zij een medewerker op een vertrouwensfunctie plaatsen of daaruit ontheffen. Als gevolg van deze verplichting ontstaat er voor de AIVD en MIVD een actueel bestand van vertrouwensfunctionarissen, in de vorm van een register. Er wordt gewerkt aan de ontwikkeling van dit register. De parlementaire behandeling van het wetsvoorstel zal naar verwachting in 2025 worden afgerond, zodat de nieuwe wet in 2026 in werking kan treden.


F803

2 VERANTWOORDELIJK NAAR DE SAMENLEVING

Maatschappelijke steun en vertrouwen van de samenleving in het handelen van de MIVD is essentieel. De dienst heeft de beschikking over verschillende bevoegdheden die de uitvoering van haar taken mogelijk maakt. De Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2027) biedt de grondslag voor de inzet van bijzondere bevoegdheden en de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen (Tijdelijke wet) is hierop een aanvulling. De wet en samenleving stellen hoge eisen aan hoe de dienst haar gegevens verwerft en verwerkt. Het interne systeem van naleving, toezicht en verantwoording wordt gevat onder de naam compliance.

2.1 *Werken aan de Wiv 2017 en de Tijdelijke wet*

De Wiv 2017 beschrijft de taken en bevoegdheden van de MIVD en de AIVD. Al een aantal jaar is duidelijk dat de Wiv 2017 op onderdelen niet voldoet aan de eisen die de moderne operationele praktijk van de diensten stelt. Onafhankelijke onderzoeken door de Evaluatiecommissie Wiv 2017 en de Algemene Rekenkamer bevestigen de tekortkomingen: de diensten zijn niet wendbaar genoeg in het tegengaan van buitenlandse dreigingen en hebben te maken met een grote administratieve lastendruk. Deze lastendruk gaat ten koste van de effectiviteit en de mogelijkheid om te innoveren. De slagkracht door een effectieve inzet van bevoegdheden en de toekomstbestendigheid van de diensten staan hierdoor onder druk. Het kabinet besloot daarom in 2021 dat de Wiv 2017 grondig moest worden herzien.

Het kabinet bood de Tweede Kamer in september 2023 een hoofdlijnennotitie aan. Deze bevat kaders voor de brede herziening van de Wiv 2017. Op 23 oktober 2024 is hierover een commissiedebat gevoerd. Op basis van de hoofdlijnennotitie, de inbreng van de Tweede Kamer en de werking van de Tijdelijke wet zal een nieuwe toekomstbestendige Wet op de inlichtingen- en veiligheidsdiensten worden gemaakt. Beoogd is om het wetsvoorstel eind 2025 voor openbare consultatie aan te bieden.

Op 1 juli 2024 is de Tijdelijke wet in werking getreden. Deze Tijdelijke wet moet de diensten onder meer in staat stellen om op korte termijn Nederland effectiever te verdedigen tegen landen met offensieve cyberprogramma's. Deze wet moet ons beter in staat stellen om Nederland effectiever te verdedigen door bestaande bevoegdheden zoals kabelinterceptie en hacken effectiever in te zetten en de mogelijkheid om verworven datasets langer te kunnen gebruiken. De Tijdelijke wet regelt ook dat de diensten bij de Afdeling Bestuursrechtspraak van de Raad van State beroep kunnen aantekenen tegen bindende oordelen van de Toetsingscommissie Inzet bijzondere Bevoegdheden (TIB) en Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

In 2024 zijn nog niet alle bevoegdheden uit de Tijdelijke wet daadwerkelijk ingezet. De CTIVD heeft aangegeven door huisvestingsproblematiek[24] alle werkzaamheden voor bindend toezicht onder de Tijdelijke wet nog niet volledig uit te kunnen voeren. Dit heeft ertoe geleid dat onder andere de bepalingen omtrent de hackbevoegdheid nog niet zijn ingezet. Op de werking van de Tijdelijke wet in de praktijk wordt een invoeringstoets uitgevoerd. De eerste resultaten worden gepresenteerd aan de Kamer in juni 2025 en worden meegenomen bij de herziening van de Wiv 2017. Ook na die invoeringstoets zal de Tijdelijke wet doorlopend worden gemonitord.

[24] *Kamerbrief: 'Stand van zaken huisvesting CTIVD' 29 november 2024: Ref.4427880*

2.2 *Compliance en risico*

De MIVD werkt met bijzondere gegevens. Hierbij is het van belang dat medewerkers zich bewust zijn van de wettelijke kaders. Bij de verantwoordelijkheid voor compliant werken hoort ook het zorgvuldig onderzoeken van compliance-meldingen. In 2024 heeft de MIVD geïnvesteerd in het vergroten van het compliance-bewustzijn van haar medewerkers en het verbeteren van het incidentenproces. Dit heeft geresulteerd in een toegenomen aantal compliance-meldingen bij het Compliance Office. Het Compliance Office coördineert de behandeling van deze compliance-meldingen, die veelal resulteren in maatregelen zoals het verbeteren van beleid, processen en/of procedures. Doordat medewerkers ervaren dat een compliance-melding leidt tot concrete verbeteringen neemt de meldingsbereidheid toe.

Het afgelopen jaar heeft de MIVD, de CTIVD een aantal keer geïnformeerd over een compliance-incident. Dit volgens de afspraken die zijn vastgelegd in het incidentenprotocol tussen de CTIVD en de diensten. In een aantal gevallen heeft de CTIVD de door het Compliance Office geadviseerde maatregelen naar aanleiding van een compliance-incident onderschreven en de MIVD geadviseerd deze op te volgen. In een enkel geval heeft de CTIVD voor het afronden van de behandeling van het compliance-incident de Tweede Kamer geïnformeerd over het uitblijven van vooruitgang.


Koninklijke
Marechaussee

3 EEN ORGANISATIE IN BEWEGING

3.1 MIVD Toekomstperspectief 2024 - 2030

In oktober 2024 heeft de MIVD een intern perspectief voor de periode 2024-2030 vastgesteld. Dit perspectief is het resultaat van een continu proces van strategievorming, waarbij zowel interne als externe actoren worden betrokken. Het perspectief schetst de veiligheidscontext, de daaruit voorvloeiende doelstellingen voor de organisatie en een aantal operatielijnen waarlangs deze worden verwezenlijkt. De doelstellingen beschrijven waar we in 2030 willen staan:

- De MIVD speelt snel in op geopolitieke veranderingen: De MIVD reageert snel op opkomende crisissituaties, anticiperen op geopolitieke veranderingen en onderzoeken zowel de gekende als de ongekende dreiging. Hiertoe bundelen we onze krachten met onze partners, kunnen we snel schakelen tussen onze inlichtingenposities en richten we met behulp van nieuwe technologische mogelijkheden onze organisatie slim en flexibel in.

- De MIVD is een cruciaal instrument in de *grey zone*: de MIVD heeft een essentiële rol in de *grey zone*. Daarbij beschikt de MIVD over unieke bevoegdheden, middelen en expertise om Nederland en Defensie te beschermen en afschrikking te bieden. De MIVD biedt handelingsopties aan voor anderen en treft vanuit de eigen contra-inlichtingentaak en de veiligheidsbevorderende taken in samenwerking met andere instanties, proactief maatregelen tegen dreigingen. We werken hierbij samen met onze (inter-)nationale partners.

- De MIVD is gereed voor een grootschalig gewapend conflict: de MIVD helpt de krijgsmacht te versterken en afschrikking op te bouwen om te voorkomen dat de NAVO en Nederland bij een grootschalig gewapend conflict betrokken raken. De MIVD realiseert een gezaghebbende inlichtingenpositie en vergroot daarmee de slagkracht van het Nederlandse militaire inlichtingen- en veiligheidssysteem. We zorgen hierbij dat we goed zijn aangesloten op het Operationeel Hoofdkwartier.

- De MIVD duidt, gebruikt en beschermt nieuwe technologische ontwikkelingen, voor onze afnemers en onze operaties: we benutten de kansen die nieuwe technologische ontwikkelingen bieden, hebben de implicaties van disruptieve technologieën scherp en beschermen militair relevante technologie om te voorkomen dat statelijke actoren sensitieve technologieën weten te bemachtigen.

3.2 Veranderen en groeien

Een goede ondersteuning op het gebied van Human Resources (HR) is essentieel voor de invulling van de visie van de dienst. De MIVD is een organisatie met zowel een kwalitatieve als kwantitatieve groeiopgave waarbij moet worden geanticipeerd op de groeiende militaire dreiging en de benodigde kennis die hiervoor nodig is. Doorontwikkeling op het gebied van strategische personeelsplanning en strategisch talentmanagement maakt dat de MIVD invulling geeft aan opvolgingsvraagstukken en kan investeren in duidelijkere en betere loopbaanperspectieven.

Daarnaast is de MIVD continu bezig een aantrekkelijke werkgever te zijn voor zowel ons zittend personeelsbestand als toekomstige collega's. De MIVD doet dit onder andere door het continu investeren in leiderschap en het bieden van opleidings- en ontwikkelmogelijkheden. Met name ten behoeve van het werven van schaarse capaciteit benadert de MIVD actief potentiële kandidaten om hen kennis te laten maken met het Inlichtingen en Veiligheidsdomein. Dit waar mogelijk in samenwerking met onze partners binnen Defensie en de AIVD.

3.3 Een datagedreven inlichtingendienst

Het onderzoeksproces is in hoge mate afhankelijk van het snel en doelgericht verwerken van grote hoeveelheden data en de IV-voorzieningen die onze analisten in staat stelt dit te doen. Om ook in de toekomst relevant te blijven, is de MIVD bezig om het inlichtingenproces en de besluitvorming meer datagedreven te maken. De dienst werkt daarbij continu aan vernieuwing en verbetering van de informatietechnologie voor verwerving, opslag, processing, bewerking, analyse en verspreiding van onze inlichtingen. Daarnaast investeert de MIVD in het benodigde maar schaarse menselijke kapitaal.

Het belang van continuïteit en bedrijfszekerheid van de IV-voorzieningen neemt bij oplopende spanning alleen maar toe. De dienst investeert daarom extra in het verstevigen van het fundament.

Tot slot investeert de dienst in een aantal programma's en projecten die het datagedreven werken mogelijk maken en de kwaliteit van de informatiehuishouding verhogen. Hieronder vallen ook programma's op het gebied van infrastructuur, dataprocessing en het versterken van de samenwerking en de connectiviteit met de krijgsmacht. Strategieën op het gebied van algoritmen en Cloud zijn verder uitgewerkt. Samen met de AIVD heeft in 2024 de afronding van een gezamenlijke opgerichte afdeling plaatsgevonden. In deze afdeling zijn de kennis en kunde op het gebied van IT, applicaties, data, informatiehuishouding en kaders en architectuur bijeengebracht. Hiermee is de MIVD beter geëquipeerd om strategische prioritering en uitvoering op het gebied van data en IV op een zodanige wijze in te richten dat er invulling gegeven kan worden aan een datagedreven toekomst voor beide diensten.

3.4 Samenwerking

Verbonden met de krijgsmacht

De prioritering van Hoofdtaak 1 vraagt om een versterkte samenwerking tussen de MIVD en de krijgsmacht. In 2024 heeft de MIVD verdere stappen gezet om de krijgsmacht bij een grootschalig conflict beter en langdurig te kunnen ondersteunen. De noodzaak daartoe was er altijd al, maar de werkzaamheden en prioritering in het kader van Hoofdtaak 1 hebben vanwege de voortdurende verslechtering van de internationale veiligheidssituatie een nog grotere urgentie gekregen.

Om de krijgsmacht beter te kunnen ondersteunen is in 2024 allereerst de samenwerking met joint organisatiedelen zoals het Defensie Cyber Commando en het *Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Commando* (JISTARC) bestendigd. Daarnaast kan de krijgsmacht binnen het wettelijk kader, met bijvoorbeeld de MQ-9, onder het mandaat van de MIVD data verwerven en verwerken en tegelijkertijd ook eigen taken uitvoeren (*dual hatted*).

De processen van de MIVD en de krijgsmacht moeten goed op elkaar zijn afgestemd om te kunnen samenwerken. De MIVD sluit nu dichter aan op het plannings- en gereedstellingsproces van de krijgsmacht en is de MIVD nauw betrokken bij de ontwikkeling en inrichting van het operationeel hoofdkwartier *NLD Joint Force Command*. Tenslotte zijn er verdere stappen gezet om meer inlichtingen te delen met NAVO- en EU-bondgenoten, onder andere door meer prioriteit te geven aan het beantwoorden van *Requests for Information* (RFI's).

Tot slot heeft de MIVD in 2024 het voortouw genomen om het strategisch personeelsmanagement binnen het inlichtingen- en veiligheidsdomein van Defensie te versterken. Inlichtingen- en veiligheidspersoneel is schaars en het is van belang dat het personeel optimaal kan worden ingezet, juist ook met het oog op het voorbereiden voor Hoofdtaak 1. Strategisch personeelsmanagement kan helpen toekomstige medewerkers een interessant loopbaan- en ontwikkelperspectief te bieden, waardoor medewerkers kunnen worden behouden voor inlichtingen- en veiligheidsfuncties binnen de krijgsmacht en de MIVD.

Samenwerking met de AIVD

Afgelopen jaar is de samenwerking tussen de MIVD en de AIVD verder geïntensiveerd. De diensten hebben onderzocht hoe nog efficiënter en effectiever kan worden samengewerkt om gezamenlijk de weerbaarheid en veiligheid van Defensie en Nederland te versterken. Op bijna alle niveaus van de organisaties wordt samengewerkt, in gezamenlijke organisatieonderdelen, dan wel in onderlinge afstemming.

Samenwerking private sector & academische partners

De MIVD werkt in een ecosysteem samen met bedrijven en kennisinstellingen aan de nieuwste technologieën, producten, diensten en expertise. Het versterken van deze partnerschappen is een belangrijke pijler in de toekomstvisie.

In 2024 trad de MIVD nadrukkelijker in de openheid en zocht verbinding met de academische wereld, in het bijzonder universiteiten, hogescholen en kennisinstituten. De dienst faciliteerde academisch onderzoek, stelde medewerkers in staat te publiceren en verzorgde gastcolleges. Een voorbeeld is het verzorgen van de eerste Arthur Docters van Leeuwen lezing door de directeur MIVD aan de Universiteit Leiden op 10 december. Voorts is '*Lifting the Fog*' door Bob de Graaff nu ook in het Engels verkrijgbaar waarvoor hij destijds toegang heeft gekregen tot MIVD-archieven. Relevante kennisontwikkeling en kennisdeling op het gebied van inlichtingen en veiligheid houdt de MIVD '*fit for purpose*'. Transparantie draagt bovendien bij aan een beter begrip over inlichtingen binnen de maatschappij.

Marktpartijen zijn in toenemende mate van belang voor de MIVD. Met aldaar aanwezig talent, technologie, data en kapitaal is het innovatievermogen van sommige bedrijven groot. Ook is in het hedendaagse informatietijdperk de toegang van bedrijven tot gegevens sterk vergroot. Commerciële diensten en informatieproducten zijn daarom in toenemende mate relevant voor de dienst. De MIVD zet stappen om het zicht op de mogelijkheden van de markt te vergroten en deze op een doeltreffende, doelmatige en rechtmatige wijze te benutten.

3.5 *Space*

De krijgsmacht en de maatschappij zijn niet alleen zeer afhankelijk van het ruimtedomein, maar er is ook in toenemende mate sprake van militair optreden in de ruimte. Zo toont het conflict in Oekraïne aan dat moderne oorlogsvoering zich uitstrekt tot alle domeinen van militair optreden, inclusief het ruimtedomein. Zo hebben onder andere aardobservatiecapaciteiten en satellietcommunicatie, bijvoorbeeld via Starlink, grote meerwaarde voor de Oekraïense krijgsmacht.

Het afgelopen jaar onderzocht de MIVD ruimtecapaciteiten van landen van zorg en een breed scala aan dreigingen jegens satellietcapaciteiten. Deze dreigingen variëren van onder meer satellietsignaal-verstorende activiteiten tot de ook in open bronnen gerapporteerde ontwikkeling van een nucleair antisatellietwapen door de Russische Federatie. Het uitschakelen, storen of anderzijds negatief beïnvloeden van satellietinfrastructuur zal niet alleen op militair gebied implicaties hebben, maar zal ook ontwrichtende gevolgen hebben voor de maatschappij.

Een eigenstandige inlichtingenpositie op dreigingen in en vanuit het ruimtedomein is van groot belang. Met het attribueren en duiden van dergelijke dreigingen verschaft de MIVD-handelingsperspectief op nationaal en multilateraal niveau. De Defensienota 2024 onderstreept de noodzaak tot het vergroten van het vermogen van de MIVD om gebruik te maken van het ruimtedomein en de inlichtingenpositie op space als het vijfde domein voor militair optreden. De MIVD intensiveert sinds 2023 op space, in nauwe samenwerking met het Defensie *Space Security Center* van de Koninklijke Luchtmacht, in bilaterale samenwerking en in NAVO en in EU-verband. Investeringen in het ruimtedomein op korte termijn zijn noodzakelijk om voorbereid te zijn op een grootschalig conflict en om bij te kunnen blijven met en gebruik te maken van de snelle technologische ontwikkelingen in de ruimtevaartsector.

3.6 Infrastructuur en huisvesting

De ministers van Defensie en Binnenlandse Zaken en Koninkrijksrelaties hebben de gezamenlijke ambitie om ten behoeve van de nationale veiligheid de samenwerking tussen de MIVD en de AIVD over de volle breedte van het werk in het veiligheidsdomein te blijven versterken. Deze versterkte samenwerking is eerder ingezet en vindt plaats op inhoud, door middel van gezamenlijke teams en ook door gezamenlijke huisvesting. Gezamenlijke huisvesting zal plaatsvinden op drie locaties; de bestaande locatie Zoetermeer, de te verbouwen locatie Leidschendam en de te realiseren nieuwbouw op de locatie Frederikkazerne. De Tweede Kamer is hier op 28 oktober 2024 over geïnformeerd middels de verzamelbrief '*ontwikkelingen in vastgoed, leefomgeving en ruimtelijke ordening*'.[25]
De locaties Zoetermeer en Leidschendam worden beheerd door de AIVD en de te realiseren nieuwbouw op de Frederikkazerne door de MIVD. Het Rijksvastgoedbedrijf (RVB) verwacht de verbouwde locatie Leidschendam eind 2027 te kunnen opleveren.

Inmiddels werken er al honderden mensen in gezamenlijke teams op de bestaande locaties van de AIVD en de MIVD. Vooruitlopend op de uiteindelijke situatie werken de MIVD en de AIVD in 2025 verder aan gezamenlijke afspraken op diverse bedrijfsvoering onderdelen die behulpzaam zijn voor de verdere intensivering van de samenwerking in het primaire proces.

Om de personele groei van de MIVD de komende jaren te kunnen accommoderen tot aan de oplevering van de additionele huisvesting is een aantal trajecten in gang gezet om de huisvesting op de Frederikkazerne beschikbaar te houden en een ongestoorde bedrijfsvoering en een veilige werkomgeving voor de dienst te borgen. Aanvullend wordt gewerkt aan een tweetal interimvoorzieningen.

[25] *Verzamelbrief ontwikkelingen in vastgoed, leefomgeving en ruimtelijke ordening (BS2024031462) d.d 28 oktober 2024.*


F-015

4 KENGETALLEN

Kengetallen Bureau Industrieveiligheid (BIV):

Bedrijven in portefeuille; 2069 waarvan:
1.566 Nederlandse bedrijven
503 buitenlandse bedrijven

Intake autorisatie:
In 2024 zijn er in totaal 968 nieuwe autorisaties aangevraagd, waarvan:
507 nieuwe autorisatieaanvragen door een Nederlandse opdrachtgever (Defensie of bedrijf) voor een Nederlands bedrijf
181 nieuwe autorisatieaanvragen door een Nederlandse opdrachtgever (Defensie of bedrijf) voor een buitenlands bedrijf
211 nieuwe autorisatieaanvragen door een buitenlandse opdrachtgever (Defensie of bedrijf) voor een Nederlands bedrijf
69 nieuwe autorisatieaanvragen niet in behandeling zijn genomen, omdat het bedrijf niet aan de gestelde eisen van de kwaliteitstoets voor intake voldeed.

Afhandeling autorisaties:
In 2024 zijn er in totaal 1174 autorisaties afgehandeld, waarvan:
687 definitieve autorisaties;
101 teruggetrokken autorisaties door de opdrachtgever;
92 geweigerde autorisaties;
136 aan het buitenland afgegeven FSC's;
158 door het buitenland afgegeven FSC's.

Context voor Facility Security Clearances (FSC)
Met buitenlandse National en Designated Security Authorities (NSA/DSA)[25] is contact onderhouden om FSC's aan te vragen en af te handelen. Op verzoek van het buitenland wordt in verband met eventuele gunning van een buitenlandse defensieorder aan een Nederlands bedrijf gevraagd een FSC te overleggen.

Audits
In 2024 zijn er in totaal 22 audits uitgevoerd bij 22 bedrijven.

Meldingen en incidenten
Incidenten gemeld: 153
Incidenten afgehandeld: 161

Beoordeelde aanvragen Niet-Nederlanders op vertrouwensfuncties bij ABDO-opdrachten
In 2024 zijn er in totaal 426 aanvragen voor Niet-Nederlands ingediend:
428 zijn goedgekeurd.
12 zijn afgekeurd.

Requests for Visit
De ABDO schrijft voor dat, naast medewerkers van Defensie, ook bedrijven hun Request for Visit (RFV) moeten indienen bij Bureau Industrieveiligheid. Hiermee is het mogelijk om een volledig beeld te krijgen van (trends in) reis- en reizigersgedrag van defensie gerelateerde reizen.

In 2024 zijn er voor gerubriceerde bezoeken aan de Nederlandse defensie 2413 RfV's afgegeven:
Voor bezoeken aan buitenlandse defensies 3042.
Voor bezoeken aan de Nederlandse industrie zijn er 209 RfV's afgegeven.
Voor bezoeken aan de buitenlandse industrie 897.

[26] *NSA/DSA: Toezichthouder op de beveiliging van inter-(DSA) of nationale(NSA) gerubriceerde informatie.*

Kengetallen veiligheidsonderzoeken

Kader: De UVO is een gezamenlijke unit van de AIVD en de MIVD. De unit doet veiligheids-onderzoeken naar (kandidaat-)vertrouwens-functionarissen: mensen die door hun werk toegang hebben tot geheime informatie, of in een positie zijn waarin ze de nationale veiligheid kunnen schaden. Bijvoorbeeld bij de Rijksoverheid, Defensie, de burgerluchtvaart of bij bedrijven die aan vitale processen werken. Bij een positief afgerond onderzoek krijgt de kandidaat een verklaring van geen bezwaar (vgb).

Toelichting bij kengetallen veiligheidsonderzoeken

Van het totale aantal onderzoeken in 2024 zijn er 46.094 uitgevoerd door de UVO zelf en 38.753 door de mandaathouder. Afhankelijk van de aard van de vertrouwensfunctie en de mogelijke schade die de (kandidaat-)vertrouwensfunctio-naris aan de nationale veiligheid zou kunnen aanrichten, wordt een A-, B- of C-onderzoek ingesteld. Een A-onderzoek is het meest diepgaand en bedoeld voor de meest kwetsbare vertrouwensfuncties.

Toelichting bij afhandeling van bezwaar- en (hoger) beroepsprocedures

Naar aanleiding van besluiten tot weigering of intrekking van een verklaring van geen bezwaar kunnen personen bezwaar aantekenen. Als het bezwaar ongegrond wordt verklaard, kunnen zij in (hoger) beroep gaan.

Onderzoeken	Positieve besluiten	Negatieve besluiten	Totaal aantal besluiten
A-niveau door UVO	6.884	30	6.914
B-niveau door UVO	22.769	158	22.927
B-niveau door UVO overgenomen van KMar	9.244	1.607	10.851
NAVO Top 2025	92	0	92
Totaal door UVO	44.283	1.811	46.094
B-niveau door KMar	38.573	0*	38.753
Totaal aantal onderzoeken	83.036	1.811	84.847

*De KMar geeft geen negatieve besluiten af. Bij twijfel bij een veiligheidsonderzoek op B-niveau dragen ze het veiligheids-onderzoek over aan de UVO. Eventuele negatieve besluiten worden dan meegerekend bij de negatieve besluiten van de AIVD. Dat verklaart de 0 hier.

2024	Ingediend in 2024	Afgedaan in 2023	Ongegrond	Gegrond	Niet-ontvankelijk	Ingetrokken	Afgewezen
Bezwaren	170	90	55	11	12	13	-
Beroepen	9	2	2	-	-	-	-
Hoger beroep	0	1	1	-	-	-	-
Voorlopige voorziening	0	0	-	-	-	-	-

Notificatie

Op grond van artikel 59 Wiv 2017 dient te worden onderzocht of vijf jaar na het beëindigen van de uitoefening van bepaalde bijzondere bevoegdheden hiervan melding gedaan kan worden aan degene jegens wie de bijzondere bevoegdheid is ingezet.[27] Het gaat om de bevoegdheid tot:

- het openen van brieven of andere postzendingen;
- het gericht onderscheppen van communicatie, zoals door het tappen van een telefoon, het plaatsen van een microfoon of een internettap;
- het binnentreden in een woning zonder toestemming van de bewoner.

In 2024 zijn geen notificaties gedaan.

Dreigingsanalyses personen

Als de MIVD over concrete en/of voorstelbare dreigingsinformatie beschikt, die geduid kan worden, brengt de MIVD een dreigingsinschatting uit. Naast de dreigingsinformatie wordt ook beoordeeld wat het effect is wanneer de dreiging tot uitvoer wordt gebracht en of de bedreiger de wil en mogelijkheden heeft. De MIVD kan de gewenst informatie ook aanleveren in een dreigingsappreciatie of dreigingsanalyse. Dat is een meer uitgebreide analyse van concrete en voorstelbare dreigingen vanuit het perspectief van de bedreigde, zoals een politicus of diplomaten. Het afgelopen jaar zijn er 19 dreigingsappreciaties geschreven.

Tapstatistieken

In 2024 zijn door de MIVD 5397 taps geplaatst. Het betreft hier de daadwerkelijk inzet van alle vormen van taps. Voorbeelden zijn een telefoontap, IP-tap of het plaatsen van een microfoon. Eén target (persoon of organisatie) kan op verschillende manieren en op meerdere apparaten afgeluisterd worden. Deze worden afzonderlijk meegeteld in de statistieken.

Validatie-onderzoek

In 2024 is de MIVD 70 duidingsonderzoeken gestart naar aanleiding van validatie van meldingen en signalen. Het aantal onderzoeken ligt daarmee ogenschijnlijk lager dan het aantal validatie-onderzoeken (115) in 2023. Een wijziging in definitie en de werkwijze[28] is de voornaamste reden van dit lagere aantal. Het aantal geregistreerde meldingen en signalen is in 2024 ten opzichte van het voorgaande jaar met circa de helft toegenomen.[29] Een deel van de ontvangen meldingen en signalen hield een mogelijke bedreiging voor de veiligheid of inzetbaarheid van de krijgsmacht in, waarnaar een onderzoek werd gestart. De meldingen die de MIVD ontvangt kunnen komen van zowel partners uit Nederland als uit het buitenland. Dit kunnen missiegebieden zijn en landen waar de krijgsmacht oefent of is vertegenwoordigd. De meldingen en signalen zijn divers. Daarbij valt te denken aan zorgen over individuen in relatie tot verschillende vormen van extremisme, opvallende belangstelling in materieel, complexen, industrie en/of ongewenste inmenging van statelijke actoren onder Defensiepersoneel.

[27] *Zie ook brief CTIVD (kenmerk2024/088); de MIVD heeft voldaan aan de verwachting van de CTIVD waardoor de achterstand volledig is weggewerkt.*

[28] *Vanaf 2024 vond eerst een validatieslag plaats alvorens er een duidingsonderzoek werd gestart. Voorheen werd de validatieslag sneller een validatie-onderzoek genoemd.*

[29] *In 2023 bestond dit uit 327 meldingen waar 115 onderzoeken uit voortvloeiden. In 2024 waren er 596 meldingen waar 70 onderzoeken uit voortvloeiden.*

Inzageverzoeken 2024	Aantal verzoeken ingediend in 2024	* Aantal afgedane verzoeken	** Gehonoreerd	Geweigerd	Nog lopend	Bezwaar	Beroep	Hoger beroep
Persoonsgegevens	21	34	10	24	7	7 ingediend 6 afgedaan	0 ingediend 1 afgedaan*	0 ingediend 0 afgedaan
Naar overleden familie	5	9	2	7	1	4 ingediend 4 afgedaan	0 ingediend 0 ingediend	0 ingediend 0 ingediend
Bestuurlijke aangelegenheden	1	4	1	3	1 (3*)	0 ingediend 3 afgedaan*	0 ingediend 1 ingediend*	1 ingediend 1 ingediend*
Totaal	27	47	13	34	9 (12*)	11 ingediend 13 afgedaan*	0 ingediend 2 ingediend*	1 ingediend 1 ingediend*

* *Deels verzoeken van jaren vóór 2024.*
** *Gehonoreerd betekent dat aan verzoeker één of meer documenten zijn verstrekt.*