Ministerie van Defensie

Openbaar jaarverslag 2025

Militaire Inlichtingen- en Veiligheidsdienst

21 april 2026

Openbaar jaarverslag 2025

Militaire Inlichtingen- en Veiligheidsdienst

21 april 2026


D-602

INHOUDSOPGAVE

Voorwoord directeur MIVD

Het jaar 2025 stond in het teken van rivaliserende grootmachten die strijden om politieke, militaire, economische en technologische macht. Internationale samenwerkingsverbanden en afspraken die gebaseerd zijn op gedeelde waarden en regels verliezen kracht. Ingrepen in andere, autonome landen zijn geen uitzonderingen meer. Daarbij zien we dat bestaande afhankelijkheden en technologische innovaties worden uitgebuit.

We bewegen ons steeds meer in een wereld van machtsblokken. Het multilaterale systeem waarop we decennialang hebben vertrouwd, met internationale instituties als hoeders van regels en afspraken, staat onder druk. Juist in die ruimte, waar regels vervagen en macht bepalender wordt, groeit de dreiging. Bondgenootschappen waar we jarenlang op konden vertrouwen, zijn niet meer vanzelfsprekend. Europa moet steeds nadrukkelijker zelf verantwoordelijkheid nemen voor de toekomst. Ongerustheid daarover is begrijpelijk, misschien ook nog wel terecht. Maar onrust alleen maakt ons niet veiliger. Actie, daadkracht en weerbaarheid wel.

Rusland vormt de grootste en meest directe dreiging voor vrede en stabiliteit in Europa, en daarmee onze nationale veiligheid en onze belangen. Dat zien we met de oorlog in Oekraïne. Daarnaast zien we dat Rusland ook cyberaanvallen, desinformatiecampagnes, sabotageacties en spionage inzet om angst, onrust en verdeeldheid te veroorzaken en besluitvorming te beïnvloeden. Acties waarmee Rusland net onder de drempel van een openlijk militair conflict blijft.

In het streven van Rusland om in de nieuwe wereldorde een van de grootmachten te zijn, kan Rusland rekenen op China als bondgenoot. Beide hebben grote geopolitieke ambities en zetten zich af tegen de westerse invloed in de wereld. China hanteert een neutrale houding ten aanzien van de oorlog in Oekraïne, maar Chinese bedrijven leveren wel degelijk steun aan de Russische oorlogsinspanning. China blijft uitgesproken in de wens om Taiwan in te lijven, eventueel met militair ingrijpen. Tegelijkertijd is China actief met spionage, cyberaanvallen en het heimelijk verwerven van technologie en kennis.

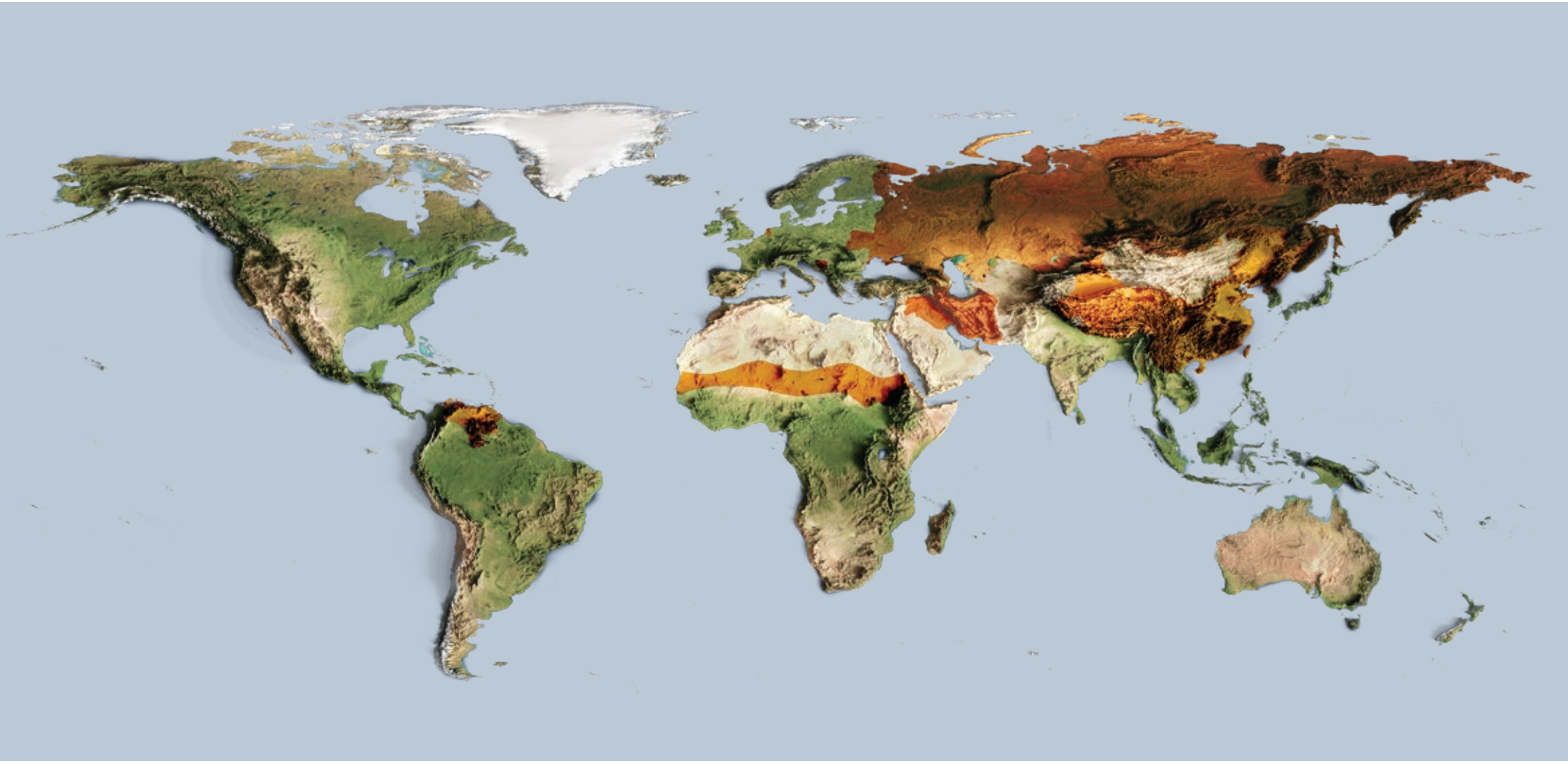
Ook andere landen en regio's in de wereld hadden in 2025 effect op de dreiging tegen Nederland en nationale belangen. In het Midden-Oosten was dat onder meer zichtbaar met de aanvallen van Houthi's op de scheepvaart in de Rode Zee en Golf van Aden en de uitstraling van conflicten in Syrië, Irak, Iran, Libanon en de Palestijnse gebieden. Het Caribische deel van het Koninkrijk werd bedreigd door het conflict tussen de Verenigde Staten en Venezuela.

De tijdelijke wet die in 2024 in werking trad, is uiteindelijk eind 2025 vrijwel volledig uitgevoerd. Daarmee kunnen de mogelijkheden van hackbevoegdheden, kabelinterceptie en bulkdatasets beter worden benut. Er is echter meer nodig om de dreigingen in deze snel veranderende wereld te blijven volgen. De technologische en geopolitieke ontwikkelingen maken een herziening van de Wet op de inlichtingen- en veiligheidsdiensten 2017 noodzakelijk. Daarbij worden de fundamentele waarborgen gehandhaafd.

Nederland moet zich in onzekere tijden staande houden, al dan niet in Europees verband of in andere coalities. Want de vraag is niet óf we worden bedreigd, maar hoe goed we op die dreigingen zijn voorbereid.

De MIVD heeft, samen met de AIVD en andere partners in binnen- en buitenland, de urgente taak om steeds weer een passend antwoord te hebben op de veelheid aan dreigingen. Zo beschermen we Nederland, de krijgsmacht en onze militairen. Zo vergroten we de weerbaarheid van onze bedrijven, universiteiten en onze samenleving. Dat vraagt veel van de medewerkers van de MIVD. Ik vind het dan ook een eer om hun werk, waar dit verslag een goed beeld van geeft, te mogen vertegenwoordigen.

Directeur Militaire Inlichtingen- en Veiligheidsdienst
Vice-admiraal Peter Reesink



1 INLICHTINGEN EN VEILIGHEID VOOR NEDERLAND

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 de MIVD als organisatie en tenslotte geeft hoofdstuk 4 een overzicht van de kengetallen over 2025 weer.

1.1 *De Russische Federatie*

De Russische dreiging

Rusland vormt de grootste en meest directe dreiging tegen vrede en stabiliteit in Europa en brengt daarmee onze nationale veiligheidsbelangen direct in gevaar. De oorlog in Oekraïne, die ondertussen haar vijfde jaar is ingegaan, is onderdeel van een langdurig Russisch streven naar een fundamentele wijziging van de Europese veiligheidsarchitectuur en de internationale rechtsorde. Rusland streeft naar een multipolaire wereldorde waarin het één van de mondiale grootmachten is. Deze context geeft de oorlog in Oekraïne voor het Russische regime een existentieel karakter; het gaat niet (alleen) om territorium, maar bovenal om de Russische positie in de wereld en de toekomst van de Russische natie, cultuur en (toegeëigende) traditionele waarden. Interne en externe veiligheid van de Russische staat zijn onlosmakelijk met elkaar verbonden: het liberaal-democratisch waardensysteem vormt een bedreiging voor de interne stabiliteit en de grip van het Russisch leiderschap op de macht.

Een militair conflict tussen Rusland en de NAVO is niet ondenkbaar, maar zolang Rusland in Oekraïne vecht is een conventionele oorlog tegen de NAVO vrijwel uitgesloten. Tegelijkertijd treft Rusland nu al concrete voorbereidingen voor een mogelijk conflict met de NAVO. De MIVD beoordeelt dat Rusland, in de voor hen meest gunstige omstandigheden, binnen een jaar na beëindiging van de gevechtshandelingen in Oekraïne voldoende gevechtskracht kan genereren om een regionaal conflict tegen de NAVO te initiëren. Het Russische doel van een dergelijk conflict is niet om de NAVO militair te verslaan, maar door beperkte terreinwinst de NAVO politiek uiteen te spelen. Desnoods onder de dreiging van nucleaire wapeninzet.

Anders dan tijdens de Koude Oorlog lijken nu dempende factoren (een overzichtelijke bipolaire wereldorde, een werkende wapenbeheersingsarchitectuur, begrip en kennis over strategische afschrikking en diverse formele en informele overlegstructuren) voor een groot deel afwezig. Bovendien staan we aan de vooravond van een technologische revolutie (met *artificial intelligence*, *quantum computing* en *bio science*) waarvan de gevolgen nog niet te overzien zijn. Rusland zet middelen in die net onder de drempel van een openlijk militair conflict blijven. Het doel is om angst en onrust te veroorzaken, besluitvorming in landen en internationale gremia te beïnvloeden en voor Rusland gunstige voorwaarden te creëren, voor zowel het uitoefenen van druk als het initiëren van militaire operaties. Hierdoor bestaat er een reëel risico op onbedoelde en daarmee moeilijk te beheersen escalatie. De onvoorspelbare koers van het huidige Amerikaanse veiligheidsbeleid kan van invloed zijn op de Russische kosten-batenanalyse.

Ontwikkelingen op het gebied van nucleaire wapens

In 2025 was sprake van een aantal verontrustende ontwikkelingen op nucleair wapengebied. Rusland, dat beschikt over het grootste strategisch- en tactisch-nucleaire arsenaal ter wereld, testte in oktober een tweetal nieuwe wapensystemen; het nucleair aangedreven kruisvluchtwapen 'Burevestnik' en de eveneens nucleair aangedreven torpedo 'Poseidon'. Beide wapensystemen zullen in de toekomst van nucleaire ladingen worden voorzien. Bovendien heeft Rusland de tijdelijke stopzetting van het plaatsen van zogenaamde INF-wapens (grondgelanceerde wapens met een bereik tussen de 500 en 5.500 km) beëindigd en heeft het waarschijnlijk de 'Oreshnik' *Intermediate Range Ballistic Missile* in Belarus gestationeerd. Deze wapens hebben, mede vanwege de extreem korte waarschuwingstijd, tijdens crises een uitermate destabiliserende werking.

Daarnaast heeft ook de substantiële uitbreiding van het Chinese strategisch-nucleaire arsenaal gevolgen voor zowel Rusland als de Verenigde Staten. We bevinden ons in het beginstadium van een nieuwe nucleaire wapenwedloop, waarvan de afloop ongewis is. Het ontbreken van een effectieve wapenbeheersingsarchitectuur, de opkomst van China als potentiële derde nucleaire supermacht en technologische ontwikkelingen (de effecten die met name kunstmatige intelligentie en *quantum computing* in potentie hebben op nucleaire besluitvormingsprocessen) compliceren de veiligheidssituatie dermate, dat deze wedloop moeilijker te beteugelen zal zijn dan tijdens de Koude Oorlog.

Russische Federatie: oorlog in Oekraïne

In 2025 heeft de Russische krijgsmacht de oorlog in Oekraïne onverminderd voortgezet. Rusland blijft in staat om incrementele terreinwinsten te boeken over meerdere assen. De Russische hoofdinspanning is nog steeds gericht op de verovering van de Donbas, in het bijzonder Sloviansk en Kramatorsk. Uit openbare uitingen van onder andere president Poetin blijkt dat de Russische territoriale ambities in Oekraïne verder gaan dan alleen de Donbas en bijvoorbeeld ook de verovering van Zaporizhzhia-stad beogen. Ook werd in het voorjaar een mislukt offensief gelanceerd richting Sumy.

Rusland en Oekraïne hebben hun intensieve luchtcampagnes tegen elkaars kritieke infrastructuur in 2025 voortgezet. De wederzijdse consistente en geconcentreerde drone-, lucht- en raketaanvallen op strategische doelen waren nog niet doorslaggevend, maar hadden wel ingrijpende verstorende effecten. De aanhoudende Russische aanvallen hebben inmiddels een belangrijk deel van de vitale knooppunten in het Oekraïense energienetwerk tijdelijk of permanent uitgeschakeld, met aanzienlijke gevolgen voor de Oekraïense bevolking en economie. Andersom vormden de gerichte Oekraïense aanvallen op olieraffinaderijen, pijpleidingen en olietankers van de schaduwvloot een steeds grotere belasting voor zowel de Russische binnenlandse brandstofvoorziening als de economisch belangrijke petrochemische export. De opbrengsten van olie- en gasproducten zijn van cruciaal belang voor het Russisch Federale budget, financiering van het Militair Industrieel Complex (MIC), de oorlogsinspanning in Oekraïne en de dreiging richting Europa. Middels de schaduwvloot van veelal verouderde olietankers met incorrecte (verzekerings) papieren en (vlaggen)registratie probeert Rusland sanctiebeleid en handhaving vanuit het Westen te omzeilen.

Sinds de Russische invasie van Oekraïne in 2022 schat de MIVD in dat Rusland circa 1,2 miljoen permanente verliezen[1] (waaronder meer dan een half miljoen doden) heeft geleden tegenover ongeveer een half miljoen Oekraïense permanente verliezen. In 2025 is echter een zorgwekkende trend waar te nemen waarbij de verhouding van het aantal dagelijkse gesneuvelden naar elkaar toe beweegt als gevolg van een toenemend aantal Oekraïense permanente verliezen. Deze verhouding is voor Oekraïne ongunstig, omdat het, in tegenstelling tot Rusland, niet of nauwelijks in staat is om de verliezen aan te vullen.

[1] *Dit betreft personele verliezen, te weten: doden, gewonden en vermisten.*

Russische Federatie: uitbreiding krijgsmacht

Ondanks de verliezen in Oekraïne is Rusland ook in 2025 in staat gebleken uitvoering te geven aan wederopbouw en uitbreiding van de krijgsmacht. Daarbij is ingezet op personele werving en opleiding, productie van zware wapensystemen en strategische munitiereserves. Er wordt grootschalig geïnvesteerd in capaciteiten die in de Oekraïne-oorlog cruciaal blijken en naar inschatting van Rusland ook in mogelijk toekomstige conflicten cruciaal zullen zijn, zoals grondgebonden luchtverdediging, langeafstandswapens en bovenal capaciteiten in en gericht tegen het onbemande domein. Het is vooralsnog onbekend of deze plannen op de lange termijn economisch haalbaar zijn. De voortdurende hoge Russische materiële en personele verliezen in de oorlog in Oekraïne kunnen deze geplande groei frustreren. Zolang de Oekraïense verdediging standhoudt, wordt daarmee de opbouw van een potentiële Russische militaire dreiging richting NAVO-grondgebied vertraagd.

De toegenomen militaire dreiging vanuit Rusland komt echter niet uitsluitend voort uit de kwantitatieve toename van de Russische krijgsmacht. De gevechtservaring die de Russische krijgsmacht sinds 2022 opdoet in Oekraïne en de wijze waarop zij deze weet te integreren in de eigen oefencyclus, zorgt ook voor een aanzienlijke kwalitatieve verbetering in het optreden van de Russische krijgsmacht, met name in het onbemande domein.

In september 2025 heeft Rusland samen met Belarus voor het eerst sinds het begin van de oorlog met Oekraïne weer een reguliere vierjarige strategische oefening in westelijke strategische richting georganiseerd: ZAPAD-2025. Zoals verwacht vond deze oefening in vergelijking met voorgaande edities in afgeslankte vorm plaats, omdat Rusland voor een groot deel militair gebonden is aan Oekraïne. Hoewel kleinschalig, zijn de waargenomen oefenactiviteiten indicatief voor prominente ontwikkelrichtingen van de Russische krijgsmacht op een operationeel en tactisch niveau, zoals onder meer de verbetering van commandovoering en de integratie van onbemande systemen op alle niveaus.

Naar oordeel van de MIVD laat de Russische krijgsmacht hiermee een sterk adaptief vermogen zien. De Russische krijgsmacht is niet alleen groter, maar ook effectiever geworden dan voor de oorlog in Oekraïne.

Russische dreiging richting Europa

De MIVD stelde in 2024 al dat Rusland zich in dat jaar agressiever, brutaler en provocerender opstelde tegen Europese landen, op het gebied van spionage maar vooral ook op het gebied van sabotage. Sabotageactiviteiten die aan de Russische inlichtingen- en veiligheidsdiensten kunnen worden toegeschreven, kenden in Europa een (voorlopig) hoogtepunt in de zomer van 2024. Hierna nam het aantal sabotageactiviteiten af. Vooralsnog is onduidelijk waarom de Russische sabotageactiviteiten in Europa destijds zijn afgeschaald. Wel is sinds de zomer van 2025 een voorzichtige toename van activiteiten ter voorbereiding op sabotage zichtbaar. Dit suggereert dat Rusland de mogelijkheid houdt voor escalatie en de-escalatie ten aanzien van de sabotageactiviteiten.

Voor het uitvoeren van deze activiteiten maken de Russische diensten gebruik van een andere modus operandi. Mede als gevolg van de grootschalige uitzetting van Russische inlichtingenofficieren die opereerden onder diplomatiek dekmantel in een groot aantal Europese landen vanaf 2022, en striktere visaregels binnen het Schengengebied, is het voor de Russische inlichtingen- en veiligheidsdiensten moeilijker geworden om activiteiten te ontplooien in Europa. Om dit te ondervangen zijn de Russische diensten andere tactieken gaan gebruiken. Ze zijn zich onder meer gaan toeleggen op het gebruik van gelaagde netwerken. Deze netwerken bestaan uit coördinatoren, facilitators en zogeheten *low-level* agenten die de sabotageacties (zowel fysiek als digitaal) uitvoeren. Deze constructie maakt het voor Rusland gemakkelijker om betrokkenheid bij sabotageoperaties te verhullen.

Russische dreiging richting Nederland

De sabotageacties zijn nog steeds veelal gericht tegen organisaties die betrokken zijn bij de oorlog in Oekraïne, specifiek militaire en logistieke

doelen. In Nederland hebben geen fysieke incidenten plaatsgevonden. Wel blijft Nederland voor Rusland een potentieel doelwit, onder meer omdat Nederland aanzienlijke steun levert aan Oekraïne en omdat Nederland een transport- en informatieknooppunt in Europa is.

Hoewel de nieuwe modus operandi rondom sabotageactiviteiten succesvol blijkt voor de Russische diensten, acht de MIVD het onwaarschijnlijk dat de toename van sabotageactiviteiten de al bestaande modus operandi van de Russische diensten, met bewezen methodes en hogere operationele veiligheid, zullen vervangen. Dit betekent dat westerse inlichtingen- en veiligheidsdiensten aandacht moeten besteden aan sabotageacties, zonder de aandacht te verliezen voor andere dreigingsvormen vanuit de Russische inlichtingen- en veiligheidsdiensten.

De MIVD en AIVD hebben in 2025 een toenemend aantal meldingen ontvangen over waarnemingen van drones, bijvoorbeeld in de buurt van vitale infrastructuur, luchthavens en militaire faciliteiten. Bij dit soort meldingen geldt dat het vaststellen van vermeende Russische betrokkenheid gecompliceerd is en veelal niet kan worden bevestigd.

Spionage blijft een hoofdrol spelen voor de Russische inlichtingen- en veiligheidsdiensten. Via menselijke en technische bronnen proberen de Russische diensten de hand te leggen op strategische geheimen, kennis en technologie om een politiek of militair voordeel te verkrijgen. Russische inlichtingenofficieren zetten diverse dekmantels in voor het verkrijgen van deze informatie.

Verkenningsactiviteiten bij onder andere ambassades in Nederland
Uit onderzoek van de MIVD en de AIVD bleek dat een minderjarige digitale netwerken van ambassades en andere organisaties in Den Haag in kaart bracht. Deze verkenningsactiviteiten werden uitgevoerd op verzoek van een zelfbenoemde pro-Russische hacktivistische groepering. Na een ambtsbericht van de MIVD heeft de politie aanhoudingen verricht. Omdat deze actie op tijd is gestopt en dankzij samenwerking tussen nationale en internationale partners, is erger voorkomen.

De Russische inlichtingen-en veiligheidsdiensten spelen daarnaast een belangrijke rol bij het verwerven van technologie en *dual use* goederen in het buitenland ten behoeve van de Russische defensie-industrie. Deze werkwijze stelt Rusland in staat om het westerse sanctiebeleid deels te omzeilen. Ook Nederlandse bedrijven met kennis van hoogwaardige technologie kunnen onder de aandacht komen van de Russische diensten.

De Oostflank

De Russische inlichtingen- en veiligheidsdiensten zijn actief in de landen aan de oostgrens van het NAVO-bondgenootschap. Daar verzamelen ze informatie over de militaire capaciteiten van de NAVO waarmee ze een spionagedreiging kunnen vormen voor Nederlandse militairen die daar actief zijn. Daarnaast zijn de Russische inlichtingen- en veiligheidsdiensten actief in Oekraïne, waar ze het conflict proberen te beïnvloeden in het voordeel van Rusland. Door de uitzettingen van de Russische inlichtingenofficieren die actief waren onder een diplomatiek dekmantel, zijn de Russische diensten meer gaan werken met online gerekruteerde agenten die informatie verzamelen.

Russische Federatie: militaire techniek

Ondanks sancties en beperkte toegang tot grondstoffen, onderdelen en halffabricaten, weet Rusland nog steeds op grote schaal wapens te produceren. Bovendien is Rusland in staat om de ontwikkeling van nieuwe technieken en wapensystemen door te zetten. De grootschalige inzet van *One Way Attack Unmanned Aerial Vehicles* (OWA-UAV's), waarbij zowel eenvoud als vernuft steeds meer hand in hand gaan, laten bijvoorbeeld zien dat Rusland zowel kwantitatief als kwalitatief in staat blijft een adaptieve wapenindustrie in stand te houden.

ANP / Maxim Shipenkov

Met het onderzoek naar Russische militair-technologische ontwikkelingen ondersteunt de MIVD adequate groei en doorontwikkeling van de Nederlandse krijgsmacht en haar bondgenoten, zodat zij beter voorbereid zijn in geval van een mogelijk door Rusland geïnitieerd grootschalig conflict tegen de NAVO.

Russische Federatie: cyber

Net als voorgaande jaren zijn Russische cyberactoren zeer actief op het gebied van offensieve cyberoperaties richting Europa. Het gaat hierbij zowel om actoren die direct gelieerd zijn aan de Russische inlichtingen- en veiligheidsdiensten, als om pro-Russische aanvallers die verder afstaan van de Russische overheid maar wel worden gesteund door de staat. Het aantal verschillende Russische cyberactoren neemt tevens toe. Hun operaties variëren van relatief eenvoudig *spearphishing*[2] tot het gebruik van geavanceerde *malware* om toegang te krijgen tot systemen van overheden, bedrijven en instanties.

Rusland probeert digitaal te spioneren door in te breken op systemen van de Nederlandse overheid en andere EU- en NAVO-landen. Het doel is om informatie te verkrijgen over bijvoorbeeld de steun aan Oekraïne. Daarnaast investeren sommige Russische actoren in cybercapaciteiten om in een later stadium cybersabotage te kunnen uitvoeren.

Publieke attributie LAUNDRY BEAR

In mei 2025 traden de MIVD en AIVD naar buiten over de Russische cyberactor LAUNDRY BEAR. In 2024 hebben de MIVD en AIVD deze, voorheen publiek onbekende Russische cyberactor, onderkend. Deze actor heeft in Nederland een cyberaanval uitgevoerd waarbij werkgerelateerde contactgegevens van Nederlandse politiemedewerkers zijn buitgemaakt. Sinds deze bekendmaking zijn de activiteiten van de actor niet gestopt. LAUNDRY BEAR voert al sinds tenminste 2024 cyberaanvallen uit op westerse overheden, bedrijven en andere organisaties. Vaak richten de aanvallen van deze cyberactor zich op zaken die relevant zijn voor de Russische oorlogsinspanningen in Oekraïne, zoals ministeries van Defensie van NAVO-landen, krijgsmachtonderdelen en defensie(toe)leveranciers. De Nederlandse politie lijkt om opportunistische redenen doelwit te zijn geweest.

De MIVD signaleert dat de Russische capaciteiten om cyberaanvallen uit te voeren groeien. Russische actoren kunnen hun cyberaanvallen in een hoog tempo uitvoeren. Dit komt mede doordat zij hun aanvallen deels kunnen automatiseren, ook door middel van kunstmatige intelligente.

Cyber op het slagveld

Een fors deel van het Russische offensieve cyberprogramma richt zich op de oostflank van Europa. Net als in voorgaande jaren vervult digitale spionage hierin een hoofdrol. Hierbij ziet de MIVD dat de Russische staat op verschillende manieren buitgemaakte informatie gebruikt. Zo maakt het Russische leger gedurende de oorlog in Oekraïne tijdens militaire operaties gebruik van informatie die afkomstig is uit cyberoperaties, zoals Oekraïense troepenbewegingen of locatiegegevens van militairen.

Chataccounts Nederlandse overheidsmedewerkers doelwit[3]

In 2025 hebben de MIVD en AIVD vastgesteld dat een Russische cyberactor trachtte wereldwijd toegang te krijgen tot een groot aantal Signal- en Whatsapp-accounts van hoogwaardigheidsbeklеders, militairen en ambtenaren. Binnen deze campagne heeft de actor ook toegang gekregen tot de chataccounts van meerdere Nederlandse overheidsmedewerkers. Naast het verkrijgen van toegang is het voor de actor zelfs mogelijk om deze over te nemen. Hierdoor kunnen contactpersonen van het slachtoffer in de veronderstelling zijn dat ze berichten sturen aan het slachtoffer zelf, waar in werkelijkheid de berichten bij de actor belanden.

Prioritering bij sabotageactiviteiten

Ook in het geval van sabotageacties in het cyberdomein geldt Oekraïne nog altijd als de hoogste prioriteit van Russische cyberactoren. Vooral de Oekraïense energie- en logistieke sector zijn hier het doelwit van geweest. Deze prioritering kan veranderen bij een einde van de oorlog. Zo is het

[2] *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*

[3] *http://aivd.nl/documenten/2026/03/09/cyberadvies.-phishing-via-chatapps-signal-en-whatsapp*

mogelijk dat Russische cyberactoren hun capaciteiten dan breder gaan inzetten op NAVO-landen en EU-lidstaten, waaronder Nederland.

Samenwerking China en Rusland op het gebied van ruimtevaart-technologie

Rusland is niet meer de ruimtemacht die de Sovjet-Unie ooit was en is zelfs genoodzaakt om ruimtevaarttechnologie uit China te verwerven. Sinds 2014 heeft Rusland te maken met economische sancties die het zeer moeilijk hebben gemaakt om technologisch hoogwaardige componenten uit het Westen te verkrijgen. Daarnaast heeft Rusland te maken met een kennisvlucht van hoogopgeleid technisch personeel naar het buitenland. De gevolgen voor de Russische ruimtevaartindustrie zijn groot en de effecten daarvan zijn voor Rusland iedere dag te merken in de oorlog met Oekraïne.

Door een gebrek aan eigenstandig ontwikkelde *Intelligence, Surveillance and Reconnaissance* (ISR) satellieten kan Rusland niet volledig het benodigde tempo van moderne oorlogsvoering behalen. ISR-satellieten zijn onder andere van belang voor het vinden van belangrijke doelwitten die zich ver van de frontlinie bevinden, zoals commandoposten en logistieke centra, die vervolgens kunnen worden aangegrepen met langeafstandswapens. Om het gebrek aan deze ISR-middelen op te vangen, tracht Rusland te zoeken naar creatieve oplossingen waaronder het gebruik van openbare satellietbeelden, het kopen van kant-en-klare satellieten en satellietbeelden van Chinese bedrijven, alsmede het inzetten van alternatieve inlichtingensensoren zoals UAV's als ISR-middelen.

Eén van de alternatieven is het aanschaffen van deze satelliettechnologie in China. Chinese bedrijven schuwen aan de ene kant publieke bekendheid over de samenwerking met Russische ruimtevaartbedrijven, omdat ze beducht zijn voor westerse sancties. Aan de andere kant zoeken deze Chinese bedrijven naar buitenlandse afnemers, waaronder Russische, om producten zoals satellieten en satellietbeelden aan te verkopen. Rusland heeft een grote behoefte aan deze producten en kan dergelijke (kwalitatief goede) producten nergens anders verwerven. De MIVD ziet een verontrustende samenwerking tussen Chinese bedrijven en de Russische staat op het gebied van ruimtevaarttechnologie. De verwachting is dat deze samenwerking in de komende jaren verder zal intensiveren.

1.2 *China*

China bouwt aan een nieuwe wereldorde

Op 3 september 2025 werd in Beijing een grote militaire parade gehouden ter nagedachtenis aan het einde van de Tweede Wereldoorlog, 80 jaar geleden. De parade liet een zelfverzekerde Chinese leider zien en ook de contouren van de wereldorde die hij voor zich ziet: een wereld waarin China het krachtige middelpunt is waarnaar andere staten zich richten.

Daags voor deze parade had de Chinese leider een nieuw mondiaal initiatief afgekondigd: het *Global Governance Initiative* (GGI). Eerder in 2025 vond in Hongkong de oprichting plaats van de door China geïnitieerde *International Organization for Mediation* (IOMed). Beide initiatieven passen in China's beleid om nieuwe internationale structuren op te zetten die de belangen van China beter behartigen en die China in staat stellen om vooral zijn invloed te vergroten in het mondiale zuiden. De wereldorde die China op deze manier tot stand wil brengen is erop gericht de westerse invloed in de wereld, vooral van de Verenigde Staten maar ook van Europa, te verminderen.

China en de relatie met Rusland

China streeft naar verandering van de wereldorde en vindt in Rusland een belangrijke bondgenoot. Beide landen staan namelijk een meer multipolaire wereld voor, waarbij zij een prominentere stem hebben in de regionale- en wereldpolitiek en de rol van de Verenigde Staten en de NAVO teruggebracht wordt.

In de oorlog tussen Rusland en Oekraïne stelt China zich pseudoneutraal op, maar in de praktijk heeft het zijn militaire samenwerking met Rusland in het afgelopen jaar sterk geïntensiveerd. De ervaring van de Russische strijdkrachten in Oekraïne is zeer belangwekkend voor het Volksbevrijdingsleger (*People's Liberation Army,* 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. Ook groeit de Chinese export naar Rusland nog steeds. Sommige Chinese producten kan Rusland gebruiken voor zijn oorlogsindustrie. Andersom is Rusland een belangrijke leverancier van olie en gas voor China, waarmee Rusland zijn oorlogsinspanningen kan financieren. In 2025 werden verschillende Chinese entiteiten, waaronder twee banken, door de EU gesanctioneerd voor medewerking aan sanctieomzeiling door Rusland.

Door China's diverse vormen van steun aan Rusland, die belangrijk zijn voor de Russische oorlogsinspanningen in Oekraïne, heeft China ook invloed op de veiligheidssituatie op het Europese continent.

Het afgelopen jaar heeft de media bericht dat de Chinese minister van Buitenlandse Zaken tijdens een bespreking met de EU naar voren had gebracht dat China het zich niet kan permitteren wanneer Rusland de oorlog tegen Oekraïne zou verliezen, omdat dan de aandacht van het Westen, met name van de Verenigde Staten, zich meer zou gaan richten op China. Gezien China's opstelling ten aanzien van Taiwan en in bredere zin zijn aanspraken in de Indo-Pacific, duidt dit er volgens de MIVD op dat het Chinese leiderschap zo een verbinding legt tussen strijdtonelen in Europa en in Oost-Azië. Dit maakt dat de dreiging die van China uitgaat zich verbreedt en verdiept.

Spanning bouwt op in zeeën rond China

Ook in 2025 is China doorgegaan met de verdere uitbreiding en modernisering van zijn krijgsmacht. Hierdoor is China in staat steeds verder buiten zijn directe periferie te opereren en verstevigt het zijn positie als regionale grootmacht met wereldwijde ambities. Hierbij is de ontwikkeling van de Chinese marine (PLA Navy, PLAN) en kustwacht (*China Coast Guard*, CCG) in het bijzonder van belang. De capaciteitsopbouw die de PLAN en de CCG gedurende de afgelopen twee decennia hebben doorgemaakt, stelt hen steeds meer in staat Chinese economische en veiligheidsbelangen buiten de eigen regio te verdedigen. De recente toevoeging van een derde hypermodern vliegkampschip is exemplarisch voor deze ontwikkeling.

De ontwikkeling naar een hoogwaardige krijgsmacht kan niet los gezien worden van China's onveranderde intentie om Taiwan in te lijven. China beoogt om Taiwan op vredelievende wijze bij de Volksrepubliek te doen sluiten, maar heeft de inzet van militaire middelen om dit doel te bereiken nooit uitgesloten. Met grootschalige militaire oefeningen, zoals STRAIT THUNDER 2025 en JUSTICE MISSION 2025, oefende China vorig jaar militaire druk uit op Taiwan. Ook de voortdurende betreding van de Taiwanese *Air Defence Identification Zone* (ADIZ) door de Chinese luchtmacht draagt hieraan bij. Het aantal keren dat China dit in 2025 deed lag opnieuw hoger dan het voorgaande jaar.

In 2025 werd via een hackerscollectief bekend dat Rusland en China al in 2023 een overeenkomst hebben gesloten aangaande luchtlandings-operaties. In deze overeenkomst is afgesproken dat Rusland enkele tientallen voertuigen zal leveren die door luchtlandingstroepen worden gebruikt en hierbij ook in de bijbehorende training zal voorzien.

China: economische veiligheid

China gebruikt zijn economische macht om geopolitieke druk uit te oefenen. Door de Verenigde Staten afgekondigde handelstarieven werden door China beantwoord met handelstarieven voor Amerikaanse producten en later restricties op de uitvoer van zeldzame aardmetalen. China laat hiermee zien hoe cruciaal het is voor het maken van producten die zowel een civiel als militair doel kunnen hebben. Deze afhankelijkheid

ANP / Xinhua/ABACA

kan risicovol zijn voor de Nederlandse en Europese economie en kan ook het vermogen om autonoom strategische keuzes te maken bedreigen.

China's voortgaande technologische en economische ontwikkeling vereist veel kennis en het doen van hoogwaardig onderzoek. Hiervoor trekt China ook westerse onderzoekers aan en stuurt het Chinese studenten en onderzoekers naar het Westen om kennis op te doen die zij later in China kunnen toepassen of verder ontwikkelen. Op deze wijze krijgt China geavanceerde en soms zeer gevoelige kennis en technologieën in handen, die het kan toepassen in zijn eigen technologische en economische ontwikkeling en de modernisering van zijn krijgsmacht.

China: spionage

Chinese inlichtingen- en veiligheidsdiensten hebben ook in 2025 actief inlichtingenactiviteiten uitgevoerd. Het gaat daarbij om het benaderen van voor China relevante individuen, het op- en uitbouwen van netwerken en het vergaren van informatie en technologie die China in zijn voordeel kan gebruiken. Mensen kunnen hier bewust of onbewust, vrijwillig of onder dwang, aan meewerken. China werkt volgens een *whole of society* approach. Dit houdt in dat alle onderdelen van de samenleving, zowel individueel als georganiseerd, kunnen worden ingezet voor inlichtingen-activiteiten. Omdat alle Chinese staatsburgers, bedrijven en organisaties wettelijk verplicht zijn om hieraan mee te werken, heeft deze *whole of society approach* een wettelijke basis. Deze vorm van inlichtingenactiviteiten is sinds 2025 in Nederland onder de aangepaste nationale spionagewet strafbaar.

Toenemende Chinese cyberdreiging

Het Chinese Volksbevrijdingsleger reorganiseerde in 2024 zijn cybereenheden en bracht daarbij technische capaciteiten samen. Dit stelde Chinese hackers in 2025 in staat hun *tooling* en infrastructuur voortdurend aan te passen en zeer flexibel in te spelen op kansen en veranderende omstandigheden. De MIVD schat in dat China hierdoor offensieve cybercapaciteiten beter kan integreren met militaire operaties. Al met al staat China nu waarschijnlijk op gelijke voet met de Verenigde Staten op het gebied van offensieve cybercapaciteiten.

De MIVD neemt structurele Chinese cyberspionage waar die gericht is tegen de westerse defensie-industrie. De MIVD schat in dat China daarmee inzicht krijgt in de militaire capaciteiten van tegenstanders en de eigen technologische kennis aanvult waar dat nodig is.

Toegang tot kwetsbaarheden

De MIVD verwacht in 2026 een verdere toename in het aantal campagnes gericht op het misbruiken van kwetsbaarheden, waaronder in edge devices zoals routers, firewalls en VPN-oplossingen.

Chinese statelijke actoren hebben toegang tot specialistische kennis over westerse hard- en software dankzij een divers en uitgebreid ecosysteem van Chinese bedrijven en kennisinstellingen die offensieve cyberoperaties faciliteren. Ook het Chinese Volksbevrijdingsleger zoekt naar ingangen in westerse technologie. De MIVD onderkende in 2025 dat meerdere onderdelen binnen dezelfde eenheid zelfs concurreerden om kwetsbaarheden te vinden in een bepaald type edge device.

Chinese cyberactoren stellen de Nederlandse en bondgenootschappelijke weerbaarheid voor een grote uitdaging door hun gebruik van onbekende software-kwetsbaarheden (zero days) en snelle operationalisering van reeds gepubliceerde kwetsbaarheden. De diensten stellen vast dat detectie, respons en mitigatie vaak onvoldoende opgewassen zijn tegen de omvangrijke en professionele Chinese cyberdreiging.

Chinese hackers stellen de Nederlandse en bondgenootschappelijke cyberver-dediging op de proef. Het gaat hierbij zowel om Chinese aanvalsgroepen die zich structureel op de Europese Unie en NAVO richten, alsook groepen die opportunistisch kwetsbare netwerken raken. De MIVD schat in dat waarschijnlijk een beperkt deel van de Chinese cyberoperaties tegen Nederlandse belangen wordt gedetecteerd en vervolgens gemitigeerd.

Ook westerse telecommunicatiebedrijven hadden in 2025 de aandacht van Chinese hackers. Aanvalsgroep SALT TYPHOON verkreeg toegang tot de routers van kleinere Nederlandse hostingproviders.[4]
De MIVD en AIVD openbaarden samen met partners een rapport over de attributie en modus operandi van deze groep.[5] Telecombedrijven zijn prioriteitsdoelwitten van Chinese hackers omdat hier waardevolle informatie buitgemaakt kan worden.

China: militaire techniek en wapensystemen

China blijft bezig met disruptieve technologieën ontwikkelen voor zijn krijgsmacht. Rusland probeert daar steeds meer aansluiting bij te vinden, waarbij op bepaalde vlakken door beide landen wordt samengewerkt. China prioriteert de ontwikkeling van militaire troefkaarten zoals *quantum technology, artificial intelligence* en biotechnologie.

Daarnaast ontwikkelt China ook nieuwe materialen en productie-technologieën om het Westen een stap voor te zijn. Zo kan China met ontwikkelde materialen de weerstand van Chinese onderzeeboten mogelijk significant verlagen, waardoor deze boten efficiënter worden en lastiger detecteerbaar. 3D-printers (in westerse media en wetenschappelijk onderzoek vaak *additive manufacturing* genoemd) kunnen vlak achter de frontlinie reserveonderdelen gaan printen, wat een groot logistiek voordeel op het slagveld kan opleveren. Ten behoeve van deze ontwikkelingen op het gebied van (wapen-) productietechnologie zet China significante stappen in de ontwikkeling en productie van eigen machines, die steeds minder westerse componenten bevatten.

1.3 *Midden-Oosten*

Iran

De MIVD verrichtte in 2025 onderzoek naar de politieke en militaire invloed van Iran in het Midden-Oosten. In januari ondertekende de Iraanse president Pezeshkian in Moskou het langverwachte Overkoepelende Strategische Partnerschap met Rusland. Deze overeenkomst onderstreept de nog altijd intensieve (militaire) samenwerking tussen beide landen. Voor Iran is deze samenwerking gedurende het jaar nog essentiëler gebleken dan eerder gedacht omdat het bijdraagt aan het herstel van de militaire capaciteiten. Het land is in militair opzicht nog altijd verzwakt als gevolg van de 12-daagse oorlog met Israël (juni 2025) en het verlies van bondgenoot Assad in Syrië (december 2024).

Irak

Afgelopen jaar onderzocht de MIVD eveneens de Iraakse politiek en de aan Iran gelieerde Iraakse milities (*Iran Aligned Militia Groups*, IAMGs). Hoewel de omliggende regio beheerst werd door instabiliteit als gevolg van het regionale conflict tussen Israël en Iran (inclusief zijn bondgenoten), bleef het in Irak op politiek- en veiligheidsgebied relatief rustig. De IAMG's stonden in 2025 onder grote druk om zich terughoudend op te stellen in het conflict tussen Israël en Iran. Ook werden de milities gemaand zich te ontwapenen of verder te integreren in het Iraakse staatsbestel. Vooralsnog blijven enkele IAMG's zich verzetten tegen ontwapening. Een deel van de Iraakse milities lijkt zijn focus te hebben verlegd naar het politieke domein. Verder hebben er verscheidene aanvallen plaatsgevonden tegen de vitale infrastructuur in de Koerdische Autonome Regio sinds de 12-daagse oorlog tussen Israël en Iran. Hoewel deze aanvallen door geen enkele partij zijn opgeëist, worden de incidenten wel aan de Iraakse milities geattribueerd.

De Iraakse politiek was in 2025 in de ban van de parlementaire verkiezingen die op 11 november werden gehouden. De zittende minister-president Mohammed Shia' al-Sudani heeft de verkiezingen gewonnen. Ondanks deze overwinning lukte het al-Sudani niet om buiten het *Shia Coordination Framework*

[4] *https://www.aivd.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon*
[5] *https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a*

(SCF) voldoende steun te vinden bij andere partijen om een regering te vormen en daarmee een tweede termijn als minister-president zeker te stellen. Daarop heeft al-Sudani zich weer terug aangesloten bij de andere sjiitische partijen, verenigd in het *Shia Coordination Framework*. Hiermee werd het SCF opnieuw het grootste blok in het Iraakse parlement en behoudt het zijn invloed. De verwachting is dat de eerste maanden van 2026 in teken zullen staan van onderhandelingen tussen de verschillende Iraakse politieke partijen over de verdeling van de belangrijkste politieke functies (de parlementsvoorzitter, president en minister-president) en de benoeming van de nieuwe ministers.

Syrië

De stabiliteit van Syrië en de ontwikkelingen van de veiligheidssituatie heeft in 2025 eveneens de aandacht gehad van de MIVD. Hoewel de nieuwe regering onder leiding van president Ahmed Hussein al-Sharaa stappen heeft gemaakt met de opbouw van het staats- en veiligheidsapparaat en met de ontwikkeling van betrekkingen met relevante regionale en internationale partners, oefent het niet in alle delen van het land een machtsmonopolie uit. Dit geldt in het bijzonder voor het noordoosten waar de Koerdische SDF zich verzet tegen integratie in de nieuwe Syrische krijgsmacht, en in het zuiden waar de door Israël gesteunde druzische minderheid zich verzet tegen de nieuwe regering. Ook trachten aanhangers van het voormalige Assad-regime de nieuwe regering te destabiliseren. Daarnaast kampt president Sharaa met interne kritiek van radicaalislamitische en jihadistische elementen binnen zijn voormalige rebellencoalitie, de Hay'at Tahrir al-Sham.

ISIS in Irak en Syrië

In 2025 heeft ISIS in Irak slechts een beperkt aantal aanvallen uitgevoerd. Veelal betrof het kleinschalige aanvallen waarbij eenvoudige hit & run-tactieken werden toegepast. De meeste incidenten komen voor in centraal Irak. Om het grensoverschrijdende karakter van de activiteiten van ISIS te beperken, heeft Irak de grensbewaking richting Syrië verder versterkt. In september 2025 hebben de Verenigde Staten, zoals overeengekomen met Irak, een begin gemaakt met het afbouwen van de Amerikaanse bijdrage aan de anti-ISIS-coalitie in Irak. De Iraakse regering is ervan overtuigd dat zij de nog resterende ISIS dreiging in Irak zelf kunnen bedwingen.

Voorafgaand en tijdens de val van het Syrische regime van Assad in december 2024, heeft de anti-ISIS coalitie een groot aantal aanvallen uitgevoerd op ISIS om een heropleving te beteugelen. Desondanks heeft ISIS door de ontwikkelingen in Syrië meer bewegingsvrijheid gekregen. Hoewel de meeste aanslagen nog steeds in het noordoosten van Syrië plaatsvinden, heeft ISIS ook de capaciteit om aanslagen uit te voeren in andere delen van het land.

Palestijnse Gebieden

In 2025 zette de MIVD zijn onderzoek naar de activiteiten van Hamas in de Gazastrook en de Westelijke Jordaanoever voort. Gedurende het jaar heeft Hamas door het Israëlische offensief aan kracht ingeboet, maar is nog steeds in staat gebleken de controle te behouden in delen van de Gazastrook.

Libanon

In vergelijking met 2024 was 2025 een relatief rustig jaar in Libanon, maar de oorlog tussen Israël en Hezbollah heeft desondanks de veiligheids-situatie sterk beïnvloed. Ondanks een staakt-het-vuren voert Israël vrijwel dagelijks luchtaanvallen uit op vermeende Hezbollah-doelwitten in Libanon. De huidige Libanese regering probeert ondertussen de complexe taak van ontwapening van Hezbollah tot uitvoering te brengen en stelt dit in het directe grensgebied met Israël voltooid te hebben. Israël heeft meermaals aangegeven dat ontwapening niet snel genoeg gaat en dat Hezbollah zich juist herbewapent, onder meer met wapens uit Iran. Of Hezbollah zich in de rest van Libanon zal laten ontwapenen of zich hiertegen verzet, heeft directe gevolgen voor de veiligheidssituatie in het land.

Jemen

In 2025 heeft de MIVD onderzoek gedaan naar de Houthi-beweging (hierna: de Houthi's) in Jemen en de veiligheidssituatie in de Rode Zee. Van maart tot en met mei 2025 hebben de Verenigde Staten in het kader van OPERATION ROUGH RIDER grootschalige aanvallen uitgevoerd op Houthi-doelen in Jemen. Desondanks zijn de Houthi's doorgegaan met aanvallen op schepen in de Rode Zee en in de Golf van Aden die in hun ogen een link hebben met Israël. Op 23 en 29 september hebben de Houthi's aanvallen uitgevoerd op de Nederlands gevlagde MV MINERVAGRACHT, waarbij twee Filipijnse bemanningsleden gewond zijn geraakt van wie er een later is overleden aan zijn verwondingen. Ook hebben de Houthi's, tot aan het staakt-het-vuren tussen Israël en Hamas in oktober, vrijwel dagelijks aanvallen uitgevoerd op Israël met OWA UAV's en ballistische raketten. Sinds het staakt-het-vuren in Gaza zijn er, ondanks herhaaldelijk dreigen door de Houthi's, geen aanvallen meer geconstateerd in 2025.

1.4 Caribisch gebied

Venezuela

De ontwikkelingen in Venezuela in 2025, en de oplopende spanningen tussen de Verenigde Staten en Venezuela, leiden tot zorgen in en over het Caribische deel van het Koninkrijk. De MIVD en AIVD doen gezamenlijk onderzoek naar de politieke en militaire ontwikkelingen in Venezuela en de mogelijke uitstralingseffecten richting het Koninkrijk der Nederlanden en houden de situatie daarom nauwgezet in de gaten. Het Venezolaanse regime leek eind 2025 de Venezolaanse oppositie effectief buitenspel te hebben gezet.

De Verenigde Staten heeft in januari 2025 de druk op Venezuela opgevoerd. Zo was er vanaf de zomer van 2025 sprake van een grootschalige Amerikaanse troepeninzet in het Caribisch gebied. Doel was volgens de Amerikanen de bestrijding van drugshandel, maar in Venezuela werd gevreesd voor een militaire actie tegen het land. Internationaal werd Venezuela gesteund door een aantal partners, waaronder Rusland, China en Iran.

Gevolgen voor het Caribische deel van het Koninkrijk

Het Koninkrijk is niet betrokken bij de nationaal aangestuurde operaties van de Verenigde Staten in Venezuela en het Caribisch gebied. Oplopende spanningen in Venezuela (of tussen Venezuela en de Verenigde Staten) kunnen gevolgen hebben voor Aruba, Curaçao en Bonaire. Zo kunnen nieuwe militaire activiteiten opnieuw leiden tot een tijdelijke sluiting van het luchtruim. Ook kan de aanvoer van goederen, waaronder dagelijkse boodschappen, over zee bemoeilijkt worden. Daarnaast valt niet uit te sluiten dat er bij verdere escalatie een vluchtelingenstroom richting de benedenwindse eilanden op gang komt.

1.5 Contraproliferatie

Rusland

De diensten beoordelen dat Rusland blijft investeren in zijn chemische en biologische programma's. Tevens gaat Rusland door met de inzet van chemische wapens in Oekraïne. Het gaat hierbij niet alleen om het gebruik van traangas, maar ook om de chemische stof chloorpicrine[6]. De MIVD en AIVD hebben op 4 juli 2025 samen met de Duitse *Bundesnachrichtendienst* (BND) een nieuwsbericht gepubliceerd over de intensivering van het gebruik van chemische wapens door Rusland in Oekraïne.[7] Inzet van chemische stoffen is in strijd met het Verdrag Chemische wapens.

[6] *Chloorpicrine heeft een vergelijkbaar, maar sterker effect dan traangas. Bij hoge concentraties kan de stof dodelijk zijn, vooral als men blootgesteld wordt in afgesloten ruimtes. Chloorpicrine valt onder de categorie verstikkende chemische wapens en staat vermeld op Chemical Weapons Convention (CWC) Verificatielijst 3. Inzet van middelen die genoemd worden op de Verificatielijsten is onder geen enkel beding toegestaan*

[7] *www.rijksoverheid.nl/actueel/nieuws/2025/07/04/rusland-intensiveert-het-gebruik-van-chemische-wapens-in-oekraine*

Iran

In juni 2025 hebben Israël en de Verenigde Staten aanvallen uitgevoerd op Iran, gericht op het Iraanse nucleaire programma en Iraanse capaciteiten om een kernwapen te ontwikkelen. Hoewel er over de exacte omvang van de schade (mede door uiteenlopende politieke belangen) tegenstrijdige beweringen bestaan, staat vast dat deze op meerdere terreinen aanzienlijk is. Iran zal veel tijd en middelen moeten investeren voordat het terug is op het punt van voor de aanvallen. Daarnaast zijn door het activeren van het *Snapback-mechanisme*[8] veel VN-sancties weer van kracht, evenals de bepaling dat het verrijken van uranium door Iran gelimiteerd wordt. Iran legt zich hier echter niet zomaar bij neer en vindt in Rusland en China twee machtige partners die bereid zijn om Iran in internationale gremia een hand boven het hoofd te houden.

Na de aanvallen op Israël in 2024, als vergelding op de uitschakeling van Nasrallah en het bombardement van het Iraanse consulaat in Damascus, heeft Iran in 2025 zijn ballistische raketarsenaal verder ontwikkeld. Iran toonde in 2025 voor het eerst een ballistische raket met een bereik van meer dan 1000 kilometer die gebruik maakt van een doelzoekkop. Hiermee kan Iran bijvoorbeeld schepen aangrijpen op een grotere afstand van de kustlijn. In juni 2025 vond een escalatie plaats in het conflict tussen Iran en Israël. Gedurende deze 12-daagse oorlog voerden Israël en de Verenigde Staten aanvallen uit op de nucleaire- en raketfaciliteiten van Iran waarbij belangrijke (nucleaire) wetenschappers van beide programma's werden uitgeschakeld. Als reactie voerde Iran meerdere raketaanvallen uit op Israël waarbij honderden ballistische raketten zijn gelanceerd. Sinds de 12-daagse oorlog maakt Iran grote stappen in het herstellen van de toegebrachte schade en poogt hiervoor benodigde materialen en apparatuur uit andere landen te verwerven. Iran heeft in 2025 de samenwerking met Rusland op het gebied van ruimtevaart verder uitgebreid. Daarnaast heeft Iran wederom korteafstandsraketten geleverd aan Rusland voor de oorlog in Oekraïne.

Noord-Korea

Het jaar 2025 was het laatste volledige jaar waarin Noord-Korea enkele van de strategische doelen, bijvoorbeeld de ontwikkeling van een intercontinentale ballistische raket met gebruik van vaste brandstof, uit het vijfjarenplan dat in 2021 gepubliceerd is, kon bewerkstelligen. Het land heeft verder ingezet op de uitbreiding van het nucleaire arsenaal met het tonen van faciliteiten voor de verrijking van uranium. Daarnaast gaat Noord-Korea door met de ontwikkeling van nieuwe intercontinentale ballistische raketten, zoals de nieuw aangekondigde Hwasong-20. Ook blijft het land werken aan de ontwikkeling van *hypersonic glide vehicles*[9].

Noord-Korea toonde zich in 2025 prominent aanwezig op het mondiale toneel. Noord-Koreaanse troepen liepen mee in een militaire parade in Moskou en Kim Jong-Un bezocht Beijing voor een militaire parade. Op de achtergrond blijft Noord-Korea de samenwerking met Rusland intensiveren om de eigen (wapen-)industrie te moderniseren. Ook blijft het korteafstandsraketten leveren die door Rusland worden gebruikt om doelen in Oekraïne aan te grijpen.

Verwerving

De MIVD signaleert dat landen als Rusland, Iran, China en Noord-Korea steeds intensiever onderling samenwerken bij de verwerving van goederen en kennis die kunnen worden gebruikt bij de vervaardiging en verdere ontwikkeling van massavernietigingswapens.

Rusland, Iran, China, Pakistan, Syrië en Noord-Korea zijn voor de (door) ontwikkeling en productie van hun massavernietigingswapens ook nog steeds afhankelijk van kennis en goederen uit het Westen. Gezien de huidige geopolitieke situatie heeft onderzoek naar Iraanse en Russische verwerving de prioriteit. Het tegengaan van de verspreiding van massavernietigingswapens blijft onverminderd belangrijk; ze vormen een serieuze dreiging voor Nederland en de internationale rechtsorde en wanneer Nederlandse kennis en goederen voor dergelijke wapens worden gebruikt, kan dat ons

[8] *De clausule uit het JCPOA (het nucleaire akkoord met Iran uit 2015) die voorschrijft dat bepaalde opgeschorte sancties terug ingevoerd kunnen worden als Iran zich niet aan het akkoord houdt*

[9] *Raketten die met hypersonische snelheden binnen de atmosfeer opereren*

ANP / Maxim Shipenkov

land imagoschade opleveren. In 2025 hebben de MIVD en AIVD een aantal keer voorkomen dat bepaalde apparatuur landen van zorg bereikte. Dit betrof apparatuur waarmee deze landen technisch onderzoek kunnen doen dat betrekking heeft op massavernietigingswapens. De MIVD en AIVD werken hierbij samen met veel verschillende organisaties in binnen- en buitenland, zoals douaneorganisaties en inlichtingendiensten.

Ook in het afgelopen jaar hebben Rusland en Iran hun activiteiten voortgezet om in Nederland en Europa strategische goederen te verwerven. Met het opleggen en uitbreiden van internationale sancties tegen Rusland en Iran zijn handelsnetwerken verschoven en is er meer noodzaak voor omleiding. Voorbeelden van landen die worden gebruikt voor omleiding zijn de Verenigde Arabische Emiraten, Turkije, Kazachstan en China.

1.6 *Contra-inlichtingen (CI) en ongekende dreigingen*

Eén van de taken van de MIVD is het verrichten van onderzoek naar dreigingen van spionage, extremisme en terrorisme, in het bijzonder in relatie tot de krijgsmacht.

Zo heeft de MIVD in 2025 onderzoek gedaan naar rechts-extremisme en anti-institutioneel extremisme. De focus van het onderzoek lag op dreigingen tegen Defensie en op dreigingen vanuit (aspirant-)defensie-medewerkers 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.

Daarnaast heeft de MIVD in 2025 onderzoek gedaan naar de dreiging van spionage- (inlichtingen)activiteiten van landen zoals Iran en Noord-Korea. Deze landen trachten hierbij de positie van de Nederlandse krijgsmacht binnen multilaterale samenwerkingsverbanden te bepalen of proberen specifieke kennis over Defensie en de defensie-industrie te bemachtigen.

Rechts-extremisme

De MIVD onderzoekt en constateert de dreiging(en) die uitgaan van rechts-extremisme voor Defensie. Deze dreigingen worden via briefings, berichten en analyses binnen de krijgsmacht verspreid. Het handelings-perspectief ligt daarmee primair bij de verschillende defensieonderdelen. Daar waar nodig zijn op basis van inlichtingen van de MIVD passende maatregelen getroffen door het bevoegd gezag tegen deze personen.

De MIVD stelt vast dat Defensie aantrekkingskracht blijft uitoefenen op rechts-extremisten. Zo heeft de MIVD ook in 2025 rechts-extremistische (aspirant-)defensiemedewerkers onderkend die bij Defensie (wilden) werken. De MIVD heeft verschillende handelingsopties waaronder:

- De MIVD kan een ambtsbericht uitbrengen gericht aan de commandant van een defensiemedewerker waarna deze maatregelen kan treffen.
- Daarnaast kan de MIVD, onder andere op basis van inlichtingen, een Verklaring van Geen Bezwaar (VGB) weigeren of intrekken. Op deze manier kan worden voorkomen dat rechts-extremisten hun baan bij Defensie starten of voortzetten.
- Bij (een vermoeden van) strafbare feiten kan de MIVD een ambtsbericht delen met het Openbaar Ministerie. Dit is een zwaarwegend middel wat enkel ingezet wordt wanneer de nationale veiligheid in het geding is.

De onderzoeken van de MIVD naar rechts-extremisme spelen zich voor een belangrijk deel af in het online domein. Een kleiner aantal personen neemt daarnaast deel aan rechts-extremistische bijeenkomsten of ontplooit rechts-extremistische activiteiten in het fysieke domein. Rechts-extremisten beschouwen de krijgsmacht over het algemeen niet als tegenstander en zien Defensie niet als een legitiem doelwit. Ook heeft de MIVD momenteel geen indicaties van een geweldsdreiging vanuit

rechts-extremistische defensiemedewerkers richting de samenleving. De MIVD ziet wel een risico voor de defensieorganisatie van normalisering van racistische, antisemitische en discriminerende uitingen door (aspirant-)defensiemedewerkers ten koste van minderheden. Daarbij hoeft iemand niet per se een rechts-extremistische intentie te hebben om uitingen met een rechts-extremistische connotatie te doen.

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 kan een dreiging opleveren voor de defensieorganisatie en de democratische rechtsorde.

De MIVD heeft in 2025 onderkend dat meerdere defensiemedewerkers het kwaadaardige-elite-narratief aanhangen en daarnaar handelden. In een aantal gevallen was een pro-Russisch sentiment onderdeel van het gedachtegoed van deze medewerkers. De loyaliteit van defensiemedewerkers aan (de taken van) Defensie en de rechtsstaat kan op het spel staan als zij een anti-institutionele levensovertuiging hebben. Opvallend genoeg wordt dit spanningsveld niet altijd door henzelf zo ervaren. Ondanks hun overtuigingen zien deze defensiemedewerkers het niet als problematisch om voor een organisatie te werken die onderdeel is van het huidige systeem. Tegelijkertijd verklaart een aantal van hen niet bereid te zijn om voor Defensie ingezet te worden bij een oorlogssituatie of grootschalige crisis.

Ook bij anti-institutioneel extremisme geldt dat de MIVD ambtsberichten kan uitbrengen –waarna bevoegd gezag maatregelen kan treffen. Zo heeft de MIVD 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. Hierop zijn maatregelen getroffen. De onderzoeken die in 2025 zijn uitgevoerd gaven de MIVD op dat moment geen aanwijzingen voor gewelddadig anti-institutioneel extremisme richting de krijgsmacht.

Iran

De MIVD voerde in 2025 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. Dit onderzoek heeft onder andere het inzicht opgeleverd dat Iraanse activiteiten tegen Defensie, op opportunistische basis, plaats blijven vinden in binnen- en buitenland. Daar waar nodig heeft de MIVD mitigerende maatregelen getroffen en zal dit ook in de toekomst blijven doen.

Onderzoek in 2025 heeft opgeleverd dat het Iraanse regime inzet op zijn offensieve cyberprogramma om zijn doelstellingen te bevorderen. Iraanse cyberactoren ondernemen onder andere beïnvloedings-operaties, digitale sabotage en digitale spionage. Iraanse cyberactoren richten zich hierbij vooral op Israël maar ook op andere landen, waaronder landen in het Westen.

In 2025 blijft Iran onverminderd inzetten op cyberspionagecampagnes richting in het Westen verblijvende critici van het Iraanse regime, waaronder dissidenten en journalisten. Iran zet onder andere geavanceerde malware in. Iraanse actoren proberen op deze wijze digitale toegang te verkrijgen tot de persoonlijke apparatuur en/of accounts (mail, sociale media) van deze personen. Wanneer succesvol verkrijgt Iran hiermee zicht op persoonlijke informatie van slachtoffers.

De MIVD en AIVD constateren dat de Iraanse cyberdreiging continueert richting experts die zich met het Midden-Oosten bezighouden. Naast experts toonde Iran in 2025 ook interesse in overheidspersoneel. Iran doet dit waarschijnlijk met het doel om zicht te krijgen op voor Iran relevante informatie en gebruikt hiervoor verregaande *spearphishing* en *social engineering*[10] technieken.

De MIVD en AIVD constateerden in 2025 ook dat Iran zijn offensieve cyberprogramma inzette tijdens de 12-daagse oorlog tussen Iran en Israël in juni 2025. Het beperkte effect dat Iran bereikte met militaire capaciteiten motiveerde waarschijnlijk Irans keuze voor de inzet van het offensieve cyberprogramma jegens Israël. Tevens constateerden de MIVD en AIVD dat Iran tijdens de oorlog in staat was om zijn reguliere cyber-activiteiten naar andere doelwitten te continueren.

Noord-Korea

De Noord-Koreaanse digitale spionagedreiging manifesteerde zich in 2025 in staatsgeleide sanctieomzeiling door de inzet van Noord-Koreaanse hackers die onder valse identiteit en voorwendselen (heimelijke) IT-werkzaamheden verrichten. Deze activiteiten zijn gericht op financieel gewin en/of digitale spionage voor het regime. Het offensieve cyberprogramma van Noord-Korea draagt zeer waarschijnlijk bij aan de financiering van het Noord-Koreaanse (nucleaire) wapenprogramma. De belangrijkste doelen van dit cyberprogramma zijn financieel gewin en cyberspionage gericht op hoogwaardige (militaire) technologie, (geo-) politieke en wetenschappelijke informatie over het Koreaans Schiereiland.

De dreiging vanuit Noord-Koreaanse IT'ers was eerst voornamelijk gericht op de Verenigde Staten. Deze dreiging heeft zich echter ontwikkeld richting Europa. De MIVD en AIVD hebben verschillende cyberaanvallen tegen Nederlandse bedrijven en personen waargenomen. Een aantal van deze cyberaanvallen is zeer waarschijnlijk uitgevoerd door of met behulp van Noord-Koreaanse IT'ers. Deze aanvallen waren voornamelijk gericht op het ontvreemden van cryptocurrency en mogelijk ontvreemden van bedrijfsinformatie.

Digitale oplichting

Noord-Koreaanse IT'ers laten zich onder valse identiteit inhuren door buitenlandse organisaties om IT-werkzaamheden te verrichten. Zij voeren hun werkzaamheden als voltijdsmedewerker of contractant op afstand uit. Doorgaans voeren zij uitsluitend hun contractuele taken uit en werken vaak tegelijkertijd voor meerdere bedrijven. Het primaire doel van deze werkwijze is financiering van het regime door (een groot deel van) hun inkomen af te staan. Noord-Korea probeert zeer waarschijnlijk op deze wijze buitenlandse valuta te verkrijgen. Naast deze Noord-Koreaanse IT'ers zijn er ook IT'ers die legitiem werk verrichten en tevens cryptocurrency of data stelen.

Noord-Koreaanse IT'ers lichten online personen en organisaties op. Het primaire doel is stelen van cryptocurrency. Zij gaan opportunistisch te werk, een mogelijkheid tot het ontvreemden van sensitieve data laten zij niet onbenut. De oplichting is met name gericht op de cryptocurrency en blockchain sector, waardoor zij zich waarschijnlijk ook richten op relevante IT-gerelateerde kennis.

Daarnaast heeft een Noord-Koreaanse cyberactor cyberaanvallen uitgevoerd tegen de Nederlandse ambassade in Seoul, via *spearphishing* en impersonatie van overheidsmedewerkers. Ze gebruikten hiervoor een nep Buitenlandse Zaken e-mailaccount. *Spearphishing* en impersonatie zijn bekende modus operandi van Noord-Koreaanse cyberactoren. De aanvallen waren zeer waarschijnlijk onderdeel van een grotere cybercampagne. Meerdere ambassades zijn doelwit en slachtoffer geweest.

1.7 Missieondersteuning en aandachtsgebieden

Het afgelopen jaar heeft de MIVD de inzet van de Nederlandse strijdkrachten in diverse missiegebieden ondersteund. De MIVD maakt inlichtingenproducten ten behoeve van militaire inzet en de politieke besluitvorming die hiermee gemoeid is. Zowel in de planningsfase als tijdens de inzet blijft de MIVD betrokken door middel van onderzoek naar

[10] *Bij Social engineering zetten (cyber) criminelen manipulatietechnieken in om gegevens te winnen of een gewenst resultaat te behalen*

mogelijke dreiging gericht tegen Nederlandse militairen en eenheden van bondgenoten in een inzetgebied. Ook wordt onderzoek verricht naar mogelijke bedreigingen voor de succesvolle uitvoering 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

Het jaar 2025 werd gekenmerkt door politieke en civiele onrust in meerdere landen op de Westelijke Balkan. In Bosnië en Herzegovina liepen de politieke spanningen hoog op nadat de toenmalig president Milorad Dodik van de Servische Republiek (RS), een deelentiteit van het land, werd veroordeeld voor het niet opvolgen van besluiten van de internationale Hoge Vertegenwoordiger die toeziet op naleving van het Dayton-vredesakkoord. De sterk etno-nationalistische retoriek van vooral Bosnisch-Servische zijde hield aan en het leiderschap van de Servische Republiek ging wederom door met haar pogingen om het centrale Bosnische gezag en de invloed van de Hoge Vertegenwoordiger in te perken. Hoewel Dodik in eerste instantie weigerde het vonnis te erkennen, veranderden hij en de RS-top toch van koers: Dodik trad gedwongen af, benoemde een interim-president en de RS-autoriteiten troffen een aantal de-escalerende stappen, wat onder andere het opheffen van de Amerikaanse sancties tot gevolg had. Echter vertaalden de politieke spanningen zich niet in (grootschalige) veiligheidsincidenten in Bosnië en Herzegovina.

In Kosovo vonden in 2025 lokale verkiezingen en tweemaal parlementsverkiezingen plaats. De verkiezingen verliepen zonder grote incidenten, maar de maatschappelijke spanningen hielden wel aan. Deze passen binnen de trend van de vaak Kosovaars-Servische activiteiten die als doel hebben de rechtmatigheid van de Kosovaarse overheid te ondermijnen. De Kosovaarse regering probeerde, ondanks de politieke instabiliteit en internationale kritiek, om vanuit Pristina haar autoriteit in Noord-Kosovo te doen gelden en haar invloed te consolideren. Vanuit Kosovaars-Servische zijde worden deze activiteiten vooral opgevat als onevenredig en gericht op de Kosovaars-Servische gemeenschap. De verwachting is dat dergelijke spanningen periodiek zullen blijven oplaaien nu een duurzaam vergelijk, bemiddeld door de EU in de Belgrado-Pristina dialoog, voorlopig uit zicht is geraakt door de harde opstelling van beide zijden.

Servië bleef regionaal gezien ook in 2025 grote invloed hebben op de politieke- en de veiligheidssituatie in de omringende landen, zoals Bosnië en Herzegovina en Kosovo. In Servië zelf balanceerden de autoriteiten tussen het Westen, Rusland en China in het kader van het beleid om neutraliteit uit te willen stralen. Door sterke conflicterende belangen van geopolitieke actoren is dat beleid verder onder toenemende druk komen te staan. Ook vanuit de eigen bevolking nam de druk op president Vučić en de regering toe, mede omdat significante concessies aan de anticorruptie- en antiregeringsdemonstranten uitbleven. Met diverse repressieve maatregelen slaagden de autoriteiten erin om de macht in handen te houden.

Mede door het stabiliserende effect van de aanwezige (militaire) missies van de EU en de NAVO zijn grootschalige incidenten en significante sociale onrust in de Westelijke Balkanregio uitgebleven.

Afrika

Het onderzoek van de MIVD naar Afrika richtte zich op het tijdig onderkennen en signaleren van strategische en veiligheidsrelevante ontwikkelingen die een (potentiële) dreiging vormen ten aanzien van Nederland, de NAVO en/of (potentiële) missies van de EU.

Afrika is momenteel het wereldwijde zwaartepunt van jihadistisch terrorisme. Op verschillende locaties op het continent zijn meerdere aan al-Qaida en ISIS gelieerde terroristische groeperingen actief die aanvallen plegen tegen lokale overheden, de lokale bevolking en tegen elkaar. De toename van jihadistisch terrorisme is vooral waarneembaar in Mali, Burkina Faso, Niger, Nigeria en Somalië, maar ook in landen aan de Golf van Guinee, in de Democratische Republiek Congo en in Mozambique.

De jihadistische dreiging is het grootst in de buitengebieden, maar in de hoofdsteden zijn de effecten van de jihadistische opstanden ook merkbaar. Zo kreeg de Malinese hoofdstad Bamako te maken met ernstige brandstoftekorten nadat jihadisten blokkades opwierpen. Daarnaast neemt het risico op ontvoeringen van buitenlanders door jihadisten toe.

Rusland is er in verschillende Afrikaanse landen (Mali, Niger, Burkina Faso, Libië, de Centraal Afrikaanse Republiek en Equatoriaal-Guinea) in geslaagd met zijn (para)militaire presentie grote invloed te winnen en tegelijkertijd het Westen militair, economisch en politiek te ondermijnen. De toenemende Russische (para)militaire presentie in Afrika kan op termijn mogelijk een dreiging vormen voor de zuidflank van de NAVO, door gedeeltelijk de Russische internationale isolatie te doorbreken en door Rusland toegang te geven tot cruciale grondstoffen terwijl die tegelijkertijd worden onthouden aan het Westen.

De Russische aanpak was aanvankelijk hybride en ambigu, maar vindt steeds meer in de openbaarheid plaats. Tegen relatief lage kosten weet Rusland gewapende of politieke conflicten in Afrika te gebruiken om kwetsbare regimes te hulp te schieten en aan zich te binden. Rusland maakt daarbij geen punt van de schending van democratische standaarden en mensenrechten, waardoor het land in gaten kan springen die westerse landen laten vallen. Met heimelijke beïnvloedingscampagnes tracht Rusland antiwesterse of (gepercipieerde) antikoloniale sentimenten op het continent te vergroten. Tot slot maakt Rusland gebruik van het feit dat veel landen in het mondiale zuiden momenteel hun internationale betrekkingen diversifiëren.

Voorts is er sprake van een groot aantal actieve conflicten in Afrika. Een voorbeeld is de burgeroorlog in Soedan, die onder andere in de vorm van enorme aantallen vluchtelingen sterke grensoverschrijdende effecten heeft op de bredere regio. Daarmee hebben dergelijke conflicten een destabiliserende werking op landen in, of grenzend aan, de zuidflank van de NAVO. De toenemende strategische competitie in Afrika, onder meer voor toegang tot cruciale grondstoffen, vormt een risico voor het uitbreken van nieuwe conflicten op het continent. Het samenspel van verschillende destabiliserende effecten zorgt daarnaast voor een verhoogd risico op staatsgrepen.

1.8 *Veiligheidsbevorderende taken*

Digitale veiligheid

Tijdens de NAVO-top 2025 zijn er, in lijn der verwachting, voornamelijk laagwaardige cyberaanvallen waargenomen. De cyberaanvallen hadden waarschijnlijk beïnvloeding of verstoring als doel. Het is een opvallend laag aantal in vergelijking met voorgaande toppen. De cyberaanvallen die waargenomen zijn, werden tijdig gemitigeerd door organisaties betrokken bij de cyberbeveiliging van de NAVO-top.

De zomer van 2025 stond in het teken van de aanvallen (door misbruik van onbekende kwetsbaarheden) in Citrix NetScaler, waardoor onder andere het Openbaar Ministerie is getroffen. De opvolging van de incidenten bij Nederlandse overheidsorganisaties toont aan dat de cybersecuritymaatregelen bij veel organisaties binnen de Rijksoverheid ontoereikend zijn. Deze cyberaanvallen vormen een dreiging voor de nationale veiligheid, onder andere door de ontregelende werking die *incident response* kan hebben op de bedrijfsvoering van een organisatie. Het onvermogen van de overheid om zich adequaat te beschermen tegen deze cyberaanvallen kan bij herhaling het algemene vertrouwen van burgers in de overheid schaden.

In 2025 zijn naar aanleiding van meldingen meer incidenten onderzocht waarbij telefoons zijn aangevallen. Mogelijk focussen actoren zich in toenemende mate op telefoons omdat er minder bewustwording is over de risico's en telefoons vaak minder intensief worden gemonitord ten opzichte van computers en servers. Het gebruik van laagdrempelige en

minder geavanceerde methodes zoals social engineering blijkt naast de inzet van geavanceerde malware een effectief middel voor verschillende actoren en leidde tot impactvolle incidenten.

Het aantal statelijke actoren met een offensief cyberprogramma was ook in 2025 onverminderd hoog. Het is de verwachting dat er bij dit brede scala aan statelijke actoren een verdere professionalisering plaatsvindt door investeringen in de ontwikkeling van eigen capaciteiten en de aanschaf van commercieel verkrijgbare middelen. Het is voor landen relatief makkelijk om (nieuwe) digitale aanvalscapaciteiten in te zetten. Geavanceerde spyware is commercieel te koop, en landen kunnen daarmee op veel apparaten of netwerken binnenkomen en meekijken.

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 partners binnen de rijksoverheid.

Ook in 2025 heeft de MIVD invulling gegeven aan deze taak door onderzoeken uit te voeren bij de Operationele Commando's van Defensie en bij partners binnen de rijksoverheid, in binnen- en buitenland. Nieuwe technologische ontwikkelingen bieden mogelijkheden tot het beter uitvoeren van de onderzoeken, maar introduceren ook nieuwe dreigingen binnen het vakgebied. Om deze reden is innovatie en kennisopbouw een cruciaal onderdeel van dit specialisme.

Economische veiligheid

De MIVD verricht onderzoek naar dreigingen gericht tegen de economische veiligheid en nationale economische afhankelijkheden. De Nederlandse economische veiligheidsbelangen staan in 2025 onverminderd onder druk door een verscheidenheid aan (statelijke) dreigingen. Landen van zorg zijn onder andere Rusland, China en Iran. Hierbij gaat het primair om ongewenste kennis- en technologie-overdracht en afhankelijkheden die raken aan onze nationale strategische veiligheid. Deze kennis en technologie kunnen bijdragen aan de militaire capaciteitsopbouw in deze landen.

Ook in 2025 waren de Nederlandse defensie-industrie, bedrijven, kennisinstellingen en wetenschappers een potentieel doelwit van diverse statelijke actoren die (heimelijk) hoogwaardige, al dan niet militair relevante, technologie probeerden te verwerven. De Nederlandse defensie-industrie is voor een aanzienlijk deel aangewezen op leveranciers uit andere landen en daarom vatbaar voor risicovolle strategische afhankelijkheden. Deze afhankelijkheden in de Nederlandse vitale infrastructuur kunnen een risico vormen voor de Nederlandse economische veiligheidsbelangen. Daarnaast heeft Nederland een unieke hoogwaardige kennis- en technologiepositie, onder andere op het gebied van halfgeleiders, kwantumtechnologie en lucht- en ruimtevaart, die wordt bedreigd door spionagepogingen of (heimelijke) overnames door landen als Rusland, China en Iran.

Het onderzoek naar de economische veiligheid heeft in 2025 bijgedragen aan overheidsmaatregelen om de dreiging tegen de Nederlandse economische veiligheid tegen te gaan en de weerbaarheid van ons land tegen deze dreiging te vergroten.

Industrieveiligheid

Op 24 maart 2025 is het Nationaal Bureau Industrieveiligheid (NBIV) opgericht. Het NBIV heeft tot taak het bevorderen van maatregelen ten aanzien van de beveiliging van gegevens en materiaal bij het bedrijfsleven

waarvan bescherming in het kader van de nationale veiligheid geboden is. Deze taak wordt uitgevoerd voor alle departementen, agentschappen, de politie en internationale verdragspartners. Het NBIV is ontstaan uit een samenvoeging van de industrieveiligheidsentiteiten van de MIVD en de AIVD.

Voor het Ministerie van Defensie gold tot begin 2026 de regeling Algemene Beveiligingseisen voor Defensieopdrachten (ABDO). De ABDO schrijft eisen voor waaraan het bedrijfsleven moet voldoen, voordat zij geautoriseerd kunnen worden om in aanraking te komen met bijzondere informatie. Bij aanvang van een opdracht controleert het NBIV de bedrijven om zeker te stellen dat zij voldoen aan de gestelde eisen uit de ABDO. Doorlopende activiteiten van het NBIV betreffen het routinematig inspecteren van bedrijven met een ABDO-autorisatie, het uitvoeren van integrale veiligheidscontroles, het adviseren van ABDO-bedrijven en de opdrachtgevers. In het geval van een incident waar bijzondere informatie bij betrokken is, treft of laat NBIV maatregelen treffen, om (eventuele) compromittering te voorkomen of te beperken.

In 2025 is gewerkt aan het realiseren van de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO). Op 21 november 2025 is het ABRO-stelsel goedgekeurd door de Ministerraad. Met ingang van januari 2026 kunnen departementen, agentschappen en de politie de ABRO toepassen. Deze opdrachtgevers zullen gefaseerd aansluiten in 2026 en 2027.

Het NBIV heeft in 2025 gekeken naar risico's en veiligheidsbelangen ten aanzien van cyberdreigingen, (economische) spionage en ongewenste buitenlandse beïnvloeding in relatie tot toeleveranciers. 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.

Veiligheidsonderzoeken

De dreigingen die worden belicht in de voorgaande hoofdstukken zijn direct merkbaar bij de Unit Veiligheidsonderzoeken (UVO), een gezamenlijke unit van de MIVD en AIVD. Zo wierf het ministerie van Defensie in 2025 meer personeel dan in voorgaande jaren en deed het dus ook meer aanvragen voor veiligheidsonderzoeken bij de UVO. Deze toename is tevens merkbaar voor andere gerelateerde (vitale) sectoren.

De UVO doet veiligheidsonderzoeken naar mensen die door hun werk toegang krijgen of hebben tot staatsgeheim gerubriceerde informatie, of die in een positie komen of zijn waarin ze de nationale veiligheid kunnen schaden. Bijvoorbeeld bij de Rijksoverheid, Defensie, de burgerluchtvaart of bij bedrijven die aan vitale processen werken. Ook doet de UVO veiligheidsonderzoeken naar Nederlanders die een NAVO- of EU-clearance nodig hebben.

NAVO-top: meer dan 500 extra veiligheidsonderzoeken

Voorafgaand aan de NAVO-top heeft de UVO ruim 500 veiligheidsonderzoeken uitgevoerd. Dit waren onderzoeken naar personen die geselecteerd waren om te werken binnen diverse beveiligde zones bij de top. Bij 11 van deze onderzoeken heeft de UVO een negatief besluit genomen. De personen die dit betrof kwamen dan ook niet te werken in deze zones.

Een tijdelijk MIVD- en AIVD-projectteam, buiten de UVO, heeft bovendien extra naslagen verricht voor de NAVO-top. Een naslag is een fundamenteel andere en lichtere procedure dan een veiligheidsonderzoek: hierbij wordt gekeken of (en zo ja hoe) iemand voorkomt in de systemen van de AIVD. Voorafgaand aan de NAVO-top heeft de AIVD, op verzoek van het ministerie van Buitenlandse Zaken en de NAVO, in korte tijd 6.430 personen nageslagen die de top wilden bezoeken. Over 4.090 personen kon direct uitslag worden gegeven, de 2.340 andere personen moesten nader worden beoordeeld. Op basis van deze naslagen heeft de AIVD over één persoon een ambtsbericht uitgedaan.

In totaal heeft de UVO 85.637 besluiten genomen in 2025. Dit is een lichte stijging ten opzichte van 2024. Van dit totaal zijn 32.862 besluiten genomen door de mandaathouder, de Koninklijke Marechaussee. Ondanks de niet afnemende vraag naar veiligheidsonderzoeken, heeft de UVO 92,6% van de veiligheidsonderzoeken binnen acht weken afgerond. Aanvragen die buiten deze termijn zijn afgerond betroffen veelal complexe gevallen. Het gehele overzicht is te vinden in hoofdstuk vier.

Meer A- en B-onderzoeken

Afhankelijk van de aard van functie en de mogelijke schade die de (kandidaat-)functionaris aan de nationale veiligheid kan aanrichten, wordt een A-, B-, C- of Burgerluchtvaart- (BL-) onderzoek ingesteld. Een A-onderzoek is het meest diepgaand en is bedoeld voor de meest kwetsbare vertrouwensfuncties. Hoe zwaarder het veiligheidsmachtigingsniveau, hoe uitgebreider het onderzoek is. De UVO deed in 2025 17 procent meer A- en B-onderzoeken dan in 2024, met name door een grotere aanvraag van veiligheidsonderzoeken bij het Ministerie van Defensie.

Voldoen aan de groeiende vraag

Om te beantwoorden aan de groeiende vraag naar veiligheidsonderzoeken, heeft de UVO in 2024 een aantal structurele maatregelen genomen. Deze zijn in 2025 verder uitgewerkt en uitgevoerd. Zo worden systemen en processen verder geautomatiseerd. Een voorbeeld hiervan is het proces voor het elektronisch aanvragen van veiligheidsonderzoeken voor de sector burgerluchtvaart. Dit proces zal in 2026 verder worden uitgebreid. De voorgenomen groei van Defensie en de intensivering van de samenwerking met het bedrijfsleven en specifiek de defensie-industrie zal naar verwachting leiden tot een toenemende vraag naar veiligheidsonderzoeken. Om te kunnen voldoen aan deze vraag zal de MIVD extra personeel aannemen voor de UVO.

Gewijzigde Wet Veiligheidsonderzoeken

Nadat de Wet verbetering uitvoering Wet veiligheidsonderzoeken door beide Kamers is aangenomen, is deze op 30 oktober 2025 bekendgemaakt in het Staatsblad. De wet, die onder andere meer flexibiliteit zal bieden aan sectoren waar medewerkers die een vertrouwensfunctie bekleden veelvuldig van werkgever op dezelfde locatie wisselen, treedt gefaseerd in werking per 1 april 2026 en 1 juli 2026.


KONINKLIJKE
MARECHAUSSEE

2 VERANTWOORDING NAAR DE SAMENLEVING

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

Het werk van de diensten is aan toezicht onderhevig. Binnen de Wiv 2017 en de Tijdelijke wet is een effectief toezichtstelsel geregeld op de werkpraktijk van de diensten. Intern gebeurt dit door de compliance- en riskfunctionarissen van de MIVD. Extern door het parlement, openbaar waar het kan, vertrouwelijk waar het moet. Daarnaast is er de Toetsingscommissie inzet bevoegdheden (TIB) en de Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten (CTIVD). De TIB is een onafhankelijke commissie die vooraf toetst of de inzet van de meest ingrijpende bijzondere bevoegdheden door de MIVD rechtmatig is. Het oordeel van de TIB is bindend. De CTIVD doet onderzoek tijdens en na onderzoeken en beoordeelt of de MIVD zich aan de wet houdt. Ook kunnen burgers en organisaties die menen in hun belangen te zijn geschaad, een klacht indienen bij de afdeling Klachtenbehandeling van de CTIVD.

Tijdelijke wet

Hoewel de Tijdelijke wet op 1 juli 2024 volledig in werking is getreden heeft de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) eerder laten weten, wegens huisvestingsproblematiek, slechts beperkt bindend toezicht te kunnen houden. Om die reden kon de wet nog niet volledig toegepast worden. De CTIVD heeft laten weten dat zij sinds 1 oktober 2025 klaar is voor een zo goed als volledige uitvoering van de Tijdelijke wet.

De MIVD en AIVD hebben positieve ervaringen opgedaan met de toepassing van de onderdelen waarvan wel gebruik kon worden gemaakt. Concreet betreft het de inzetmogelijkheden op kabelinterceptie en de regeling rondom de verlenging van de eindtermijn van bulkdatasets.

Daarnaast heeft de MIVD gebruik gemaakt van de mogelijkheid tot het instellen van beroep bij de Afdeling Bestuursrechtspraak van de Raad van State met het oog op definitieve geschilbeslechting tussen de diensten en de Toetsingscommissie Inzet Bevoegdheden (TIB). Er is een invoeringstoets uitgevoerd waarvan de resultaten zijn verstuurd aan de Eerste- en Tweede Kamer. De benoemde knelpunten die naar voren komen in de invoeringstoets worden betrokken bij de herziening van de Wiv 2017.

Brede herziening

In 2025 is er verder gewerkt aan de voorbereiding van het wetsvoorstel dat ziet op een brede herziening van de Wiv 2017. Het streven is om in de eerste helft van 2026 een concept wet in consultatie te brengen. Beoogd wordt om het wetsvoorstel uiterlijk 1 juli 2028 in werking te laten treden, aangezien de Tijdelijke wet dan komt te vervallen.

Er wordt ingezet op een werkbare wet die de benodigde operationele slagkracht en wendbaarheid biedt. Zo kunnen de diensten adequaat reageren op technologische en geopolitieke ontwikkelingen, zonder afbreuk te doen aan fundamentele waarborgen zoals onafhankelijk toezicht. Hoe groter de inbreuk, hoe zwaarder de waarborgen. Tegen die achtergrond wordt ook gekeken naar het actualiseren van benodigde grondslagen voor samenwerking met partners, medeoverheden, kennisinstellingen en bedrijven. Gezien de huidige geopolitieke ontwikkelingen en dreigingen waar Nederland en zijn bondgenoten mee worden geconfronteerd, zal in de wetsherziening uitdrukkelijk aandacht worden besteed aan het effectiever kunnen ondersteunen van de krijgsmacht.

Ook wordt er onder meer gekeken naar hoe de MIVD en AIVD militaire gegevens kunnen verwerven op een wijze die past bij de noodzaak

voor deze gegevens en de inbreuk die plaatsvindt op grondrechten. Daarbij werken we in het kader van de wendbaarheid en operationele slagkracht een raamwerk uit dat differentieert in de van toepassing zijnde voorwaarden en waarborgen voor onderzoeken gericht op militaire en andere evidente dreigingen. Hiermee wordt de lijn voortgezet die met de Tijdelijke wet is ingezet.

2.2 *Compliance*

Bij het beschermen van de democratische rechtstaat is het belangrijk dat de MIVD verantwoordelijk omgaat met de bevoegdheden die zij heeft. De wet en samenleving stellen hoge eisen aan hoe de dienst haar gegevens verwerft en verwerkt. Hiervoor is intern toezicht ingericht in de vorm van een compliancestelsel. Dit compliancestelsel zal de komende jaren verder worden ontwikkeld en bestendigd binnen de organisatie. Afgelopen jaar heeft het *Compliance Office* bijgedragen aan het traject van de brede herziening van de Wiv 2017. Hierbij is in het bijzonder aandacht besteed aan werkbare waarborgen voor het nieuwe wettelijke kader.

Het is van belang dat er een cultuur bestaat van verantwoordelijkheid voor compliant werken voor zowel medewerkers als management. In 2025 heeft het *Compliance Office* geïnvesteerd om de kaders voor de organisatie helder en doorzoekbaar beschikbaar te stellen.

Ook heeft de MIVD in 2025 geïnvesteerd in het vergroten van het compliance-bewustzijn van haar medewerkers, onder meer door het bijdragen aan opleidingen en betrokkenheid bij veranderinitiatieven in de organisatie. Dit heeft geresulteerd in een toename in compliance-meldingen. Deze meldingen resulteren vaak in maatregelen zoals het verbeteren van beleid, processen en/of procedures. Doordat medewerkers ervaren dat een compliance-melding leidt tot concrete verbeteringen blijft de meldingsbereidheid toenemen.

Het *Compliance Office* heeft de compliance-incidenten zorgvuldig onderzocht en over verschillende incidenten is de CTIVD volgens het incidentenprotocol geïnformeerd.


F803

3 EEN ORGANISATIE IN BEWEGING

3.1 MIVD Toekomstperspectief 2024 - 2030

De veiligheidsomgeving heeft zich de afgelopen jaren sterk ontwikkeld. De MIVD heeft in 2024 de organisatievisie hierop bijgesteld in het MIVD-perspectief 2024-2030. De volgende doelstellingen staan centraal in de doorontwikkeling van de MIVD;

- De MIVD speelt snel in op geopolitieke veranderingen: de MIVD reageert snel op opkomende crisissituaties, anticipeert op geopolitieke veranderingen en onderzoekt zowel de gekende als de ongekende dreiging. Hiertoe bundelt de MIVD haar krachten met partners, kan er snel geschakeld worden tussen inlichtingenposities en richt de MIVD met behulp van nieuwe technologische mogelijkheden de 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. We werken hierbij samen met (inter-)nationale partners. De MIVD biedt handelingsopties en treft vanuit de eigen contra-inlichtingentaak en de veiligheidsbevorderende taken in samenwerking met andere instanties, proactief maatregelen tegen dreigingen.
- 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. De MIVD is hierin goed aangesloten op het operationeel hoofdkwartier *Joint Force Command* (JFC).
- De MIVD duidt, gebruikt en beschermt nieuwe technologische ontwikkelingen, voor onze afnemers en onze operaties: de MIVD benut de kansen die nieuwe technologische ontwikkelingen bieden, duidt de implicaties van disruptieve technologieën en beschermt militair relevante technologie om te voorkomen dat statelijke actoren sensitieve technologieën bemachtigen.

3.2 Veranderen en groeien

De MIVD is een organisatie met zowel een kwalitatieve als een kwantitatieve groeiopgave waarbij moet worden geanticipeerd op de groeiende dreiging en de benodigde kennis die hiervoor nodig is. Verder zal er worden doorontwikkeld op het gebied van strategische personeels-planning en strategisch talentmanagement. Hiermee investeert de MIVD in betere loopbaanperspectieven.

Daarnaast is de MIVD continu bezig een aantrekkelijke werkgever te zijn voor zowel het zittend personeelsbestand als toekomstige collega's. De MIVD doet dit onder andere door continu te investeren in leiderschap en het bieden van opleidings- en ontwikkelmogelijkheden. Met name ten behoeve van het verwerven 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 partners binnen Defensie en de AIVD.

Als wendbare organisatie kijkt de MIVD constant naar de veranderende wereld om zich heen. Om ons adaptief vermogen te vergroten voert de MIVD regelmatig organisatorische veranderingen door, bij zowel de eenheden die de kerntaken uitvoeren als de ondersteunende eenheden.

3.3 Een datagedreven inlichtingendienst

De wereldorde is aan het veranderen en dit uit zich in een toenemende strijd om technologische dominantie. Deze strijd wordt gevoerd door technologische voorsprong te behalen en anderen deze te ontzeggen, waarbij landen zowel hard power als soft power inzetten om de eigen positie te versterken. Ook is er een toenemende verwevenheid van buitenlandse en binnenlandse dreigingen die geïntensiveerd wordt door de snelle opmars van technologieën zoals kunstmatige intelligentie. Nederland was in 2025 steeds vaker het doelwit van (digitale) spionage, sabotage en beïnvloeding in de *grey zone*.

Om te voldoen aan opgaven die voortkomen uit de gereedstellings-opdracht en voorbereidingen op een grootschalig conflict zijn er technische maatregelen genomen. In het kader van continuïteit van de dienstverlening zijn in 2025 de eerste stappen gezet in het robuust maken en uitbreiden van de eigen infrastructuur. Er is een nieuwe visie op data, *data lineage* en waarborgen nodig zodat de MIVD sneller verworven data kan verwerken en delen. In combinatie met de toenemende groei van AI-toepassingen vraagt dit om een professionalisering van het MIVD data- en AI-landschap. Het centraliseren van dataverwerking werpt hierbij zijn vruchten af. Zo is de verwerking versneld en is er een datacatalogus ingericht. De eerste interne AI-toepassingen worden op basis hiervan ingericht. Deze toepassingen maken het mogelijk om de dataverwerkingen steeds effectiever en efficiënter vorm te geven.

3.4 Samenwerking

Samenwerking met de NAVO

Het belang van een gedegen, kwalitatieve en kwantitatieve inlichtingensamenwerking met en binnen de NAVO is het afgelopen jaar toegenomen. De militaire alliantie van 32 lidstaten zag met een succesvolle top in Den Haag haar relevantie bevestigd. Waar mogelijk en binnen de wettelijke kaders ondersteunt de MIVD NAVO-inlichtingenorganisaties met tijdige en kwalitatieve inlichtingen-bijdragen, kennis en personeel. Hiermee draagt de MIVD bij aan NAVO-beleid en militaire plannen en stelt daarmee het bondgenootschap in staat te anticiperen op bestaande en snel opkomende nieuwe dreigingen in een complexe multidimensionale wereld.

Samenwerking met de EU

In het licht van de aanhoudende onrust en geopolitieke ontwikkelingen op het wereldtoneel, is de Europese Unie het afgelopen jaar een steeds grotere rol gaan spelen op het gebied van veiligheid en Defensie. Daarbij beschikt de EU over complementaire instrumenten die de Europese veiligheid, en daarmee ook de Nederlandse, kunnen versterken. De MIVD heeft de EU het afgelopen jaar binnen de wettelijke kaders in toenemende mate gesteund met inlichtingen ten behoeve van besluitvorming op strategisch niveau. Het ging daarbij om zowel tijdige en kwalitatieve inlichtingenbijdragen als inhoudelijke expertise.

Samenwerking met de krijgsmacht

Als gevolg van actuele geopolitieke ontwikkelingen en de prioritering van Hoofdtaak 1 van de krijgsmacht, te weten het beschermen van het eigen grondgebied en dat van bondgenoten, heeft de MIVD in 2025 een programma gestart om in geval van een grootschalig conflict vanuit de MIVD de krijgsmacht en de NAVO beter- en langdurig te kunnen ondersteunen. Dit programma zorgt onder andere voor de verbinding tussen het gereedstellingsproces van de krijgsmacht voor een grootschalig

conflict en de gereedstelling van de MIVD. Op deze wijze maakt de MIVD integraal onderdeel uit van het plannings- en gereedstellingsproces van de krijgsmacht.

De processen van de MIVD, de krijgsmacht en de NAVO moeten goed op elkaar zijn afgestemd om in alle fasen van een voorstelbaar conflict individueel en collectief weerbaar te zijn en te kunnen samenwerken. Om de krijgsmacht in de toekomst beter te kunnen ondersteunen heeft de MIVD de samenwerking met het in 2025 opgerichte operationeel hoofdkwartier *Joint Force Command* (JFC) opgezet.

Als onderdeel van de verdere versterking van de samenwerking tussen de krijgsmacht en de MIVD is in 2025 gewerkt aan de technische randvoorwaarden om relevante data, informatie en inlichtingen te kunnen delen. De MIVD heeft in 2025 geïnvesteerd in informatie-gestuurd optreden (IGO). Dit draagt bij aan de integratie en gezamenlijke ontwikkeling van de IGO waardeketens en datagedreven inlichtingen- en veiligheidsprocessen waarmee ketenbrede samenwerking verder is versterkt.

Tot slot heeft de MIVD in 2025 stappen gezet om, samen met de krijgsmachtonderdelen, strategische personeelsplanning voor inlichtingen en veiligheid defensiebreed vorm te geven. Met strategische personeels-planning I&V wordt toegewerkt naar een gecoördineerde en gesynchro-niseerde defensie I&V-keten. In de huidige geopolitieke context wordt het I&V-domein steeds belangrijker, vanwege de signalerende, alerterende en handelende perspectieven die hieruit voortkomen. Strategische personeelsplanning I&V is hiervoor cruciaal, want zo zorgen we dat we in de hele I&V-keten van Defensie voldoende personeel met de juiste kwaliteiten hebben en behouden. De stappen die in 2025 zijn gezet richten zich op het inzicht krijgen in het huidige en toekomstige defensiebrede I&V-bestand.

Samenwerking met de AIVD

De MIVD en AIVD hebben afgelopen jaar intensief samengewerkt aan het veilig houden en weerbaarder maken van het Koninkrijk der Nederlanden, het bevorderen van de internationale rechtsorde en het gereedstellen van de krijgsmacht. Waar het meerwaarde oplevert werken de diensten samen, om zo tijdig de best mogelijke inlichtingen te leveren.

Samenwerking private sector & academische partners

Het verder uitbouwen van samenwerkingen met bedrijven en kennisin-stellingen is een prioriteit voor de MIVD. Bedrijven beschikken met hun talent, technologie, data en kapitaal over een sterk innovatievermogen, dat relevant is voor de dienst. Daarom heeft de MIVD in 2025 concrete stappen genomen om haar strategische partnerschappen naar een hoger niveau te tillen. Er is gewerkt aan de ontwikkeling van een visie en strategie voor dergelijke samenwerkingen en er zijn gesprekken gestart met nieuwe potentiële strategische partners. De resultaten hiervan zullen naar verwachting in 2026 zichtbaar zijn.

In 2025 bleef de MIVD verbinding zoeken met de wetenschappelijke wereld, in het bijzonder universiteiten, hogescholen en kennisinstituten. Een voorbeeld is voortzetting van actieve Nederlandse deelname aan het Intelligence College Europe (ICE). Dit Europese initiatief brengt de inlichtingengemeenschap samen met academische partners. Het doel is het bevorderen van een Europese inlichtingencultuur. Ook faciliteerde de MIVD academisch onderzoek, stelde medewerkers in staat te publiceren en verzorgde gastcolleges. Dergelijke 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.

3.5 *Technologisch koploperschap*

Technologische voorsprong wordt in de komende jaren steeds meer bepalend voor vergroten van onze slagkracht. Grootmachten strijden om technologisch leiderschap om een voorsprong op te bouwen, te behouden en anderen deze te ontzeggen.

De MIVD dient, zeker als inlichtingen- en veiligheidsdienst, slimmer en beter te zijn dan haar tegenstanders. Samen met de AIVD streeft de MIVD daarom naar technologisch koploperschap. Daarvoor moeten de diensten beschikken over de mogelijkheid om nieuwe technologieën te kunnen ontwikkelen en gebruiken. Door de innovatiekracht van de organisatie te vergroten, versterken we de capaciteiten van de diensten, de slagkracht van de krijgsmacht en vergroten we de maatschappelijke weerbaarheid. In 2025 hebben de MIVD en de AIVD focus aangebracht in alle initiatieven op het gebied van kwantumtechnologie en een strategie geformuleerd om sturing te geven aan de doorontwikkeling. Ten aanzien van data science & kunstmatige intelligente is onverkort invulling gegeven aan de versnelde adoptie van de Defensie Strategie Data Science en AI 2023-2027.

Space

Zoals de NAVO in haar *Commercial Space Strategy*[11] en de Adviesraad Internationale Vraagstukken (AIV)[12] onderschrijven, is er een noodzaak om militair-civiele synergie te bevorderen om dreigingen in het ruimtedomein te adresseren. Ook de MIVD werkt in toenemende mate samen met private partijen uit de ruimtesector om haar inzicht in het ruimtedomein te vergroten. Dit inzicht is noodzakelijk om de intenties, capaciteiten en activiteiten van landen van zorg te kunnen monitoren in de ruimte. Tevens kan conformiteit aan in multilateraal verband vastgestelde normen met betrekking tot het ruimtedomein worden geverifieerd, zoals het verbod op het plaatsen van nucleaire wapens in de ruimte.

In 2025 onderzocht de MIVD wederom een scala aan dreigingen in en jegens het ruimtedomein, met gevolgen voor moderne krijgsmachten op strategisch, operationeel en tactisch niveau. Naast continuerende GPS-verstoringen met nadelige gevolgen voor bijvoorbeeld luchtvaartverkeer worden in toenemende mate ook zogeheten nabijheidsoperaties door satellieten uitgevoerd, waarbij satellieten van landen van zorg inlichtingen kunnen vergaren of kunnen saboteren. Zoals de AIVD ook in haar rapport benadrukt, vrezen deskundigen dat als gevolg van dergelijke acties Russische of Chinese *dual use* satellieten in de ruimte worden geplaatst (onder het mom van 'ruimtepuinruimen' en 'wetenschappelijk onderzoek') om op een later moment ingezet te worden om Westerse satellieten uit te schakelen. Ook de Duitse Minister van Defensie en het hoofd van het Britse *Space Command* spraken zich in 2025 uit over de dreiging van anti-satellietcapaciteiten. Om de hiervoor beschreven fenomenen in de toekomst tijdig te kunnen onderkennen heeft de MIVD het afgelopen jaar eveneens geïnvesteerd in nieuwe capaciteiten.

In juni 2025 is de eerste operationele *Synthetic Aperture Radar* (SAR)-satelliet gelanceerd om de inlichtingencapaciteit van de Nederlandse krijgsmacht te versterken. Deze satelliet geeft een eerste invulling aan eigenstandige operationele aardobservatiecapaciteit, die ook de internationale samenwerking ten goede zal komen. Het *Defense Space Security Center* van het sinds 1 juli hernoemde Commando Lucht- en Ruimtestrijdkrachten (CLRS) werkt samen met de MIVD om zo effectief mogelijk invulling te geven aan deze capaciteit. Deze samenwerking strekt zich uit van gezamenlijke inrichting van de verwerkingsketen voor satellietbeelden tot afstemming inzake ruimtebeleid, cyberveiligheid, toekomstige capaciteiten en internationale vertegenwoordiging.

[11] *NAVO (13 februari 2025). NATO Commercial Space Strategy. Geraadpleegd via: nato.int/en/about-us/official-texts/2025/02/13/nato-commercial-space-strategy*

[12] *Adviesraad Internationale Vraagstukken (23 juni 2025). Regie op veiligheid in de ruimte. Geraadpleegd via: www.adviesraadinternationalevraagstukken.nl/documenten/2025/06/23/regie-op-veiligheid-in-de-ruimte*

3.6 Infrastructuur en huisvesting

Het Rijksvastgoedbedrijf heeft opdracht gekregen een nieuw en eigentijds kantoorcomplex te realiseren voor de MIVD. Het huidige onderkomen op de Frederikkazerne is verouderd en bovendien niet meer geschikt voor de (nieuwe) wettelijke taken van de MIVD. Daarnaast is nieuwe huisvesting nodig om de groei van het personeel op te vangen en te voldoen aan de huidige wet- en regelgeving, veiligheidseisen en hedendaagse standaarden voor een werkomgeving.

De bouw- en sloopwerkzaamheden werden in 2025 steeds meer zichtbaar. Met deze werkzaamheden maakt de Frederikkazerne ruimte voor het nieuwe MIVD-kantoorcomplex. Als alles volgens planning verloopt zal dit kantoorcomplex medio 2031 klaar zijn, waarna de dienst gefaseerd gaat inhuizen. In dit complex zal, net als op de AIVD-locaties Zoetermeer en Leidschendam, door de diensten worden samengewerkt in gezamenlijke teams. De oplevering van het voor de diensten te renoveren pand in Leidschendam wordt eind 2027 verwacht, inhuizing zal in 2028 plaatsvinden. Voorts is er een traject gestart om de huisvesting op de Frederikkazerne beschikbaar te houden en een ongestoorde bedrijfsvoering en veilige werkomgeving voor de MIVD te borgen.

4 KENGETALLEN

Kengetallen Nationaal Bureau Industrieveiligheid (NBIV):
Bedrijven in portefeuille; **2.327** waarvan:
1.770 Nederlandse bedrijven
557 buitenlandse bedrijven

Intake autorisatie:
In 2025 zijn er in totaal **918** nieuwe autorisaties aangevraagd, waarvan:
500 nieuwe autorisatieaanvragen door een Nederlandse opdrachtgever (Defensie of bedrijf) voor een Nederlands bedrijf
143 nieuwe autorisatieaanvragen door een Nederlandse opdrachtgever (Defensie of bedrijf) voor een buitenlands bedrijf
156 nieuwe autorisatieaanvragen door een buitenlandse opdrachtgever (Defensie of bedrijf) voor een Nederlands bedrijf
119 nieuwe autorisatieaanvragen niet in behandeling zijn genomen, omdat het bedrijf niet aan de gestelde eisen van de kwaliteitstoets voor intake voldeed.

Afhandeling autorisaties:
In 2025 zijn er in totaal **1.174** autorisaties afgehandeld, waarvan:
580 definitieve autorisaties;
82 teruggetrokken autorisaties door de opdrachtgever;
63 geweigerde autorisaties;
104 aan het buitenland afgegeven FSC's;
121 door het buitenland afgegeven FSC's.

Context voor *Facility Security Clearances* (FSC)

Met buitenlandse *National* en *Designated Security Authorities* (NSA/DSA)[13] 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 2025 zijn er in totaal twee audits uitgevoerd bij twee bedrijven.

Meldingen en incidenten

In 2025 zijn er in totaal **256** incidenten gemeld en zijn er **232** afgehandeld.

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 vollediger beeld te krijgen van (trends in) reis- en reizigersgedrag van Defensie gerelateerde reizen.

In 2025 zijn er voor gerubriceerde bezoeken **7.321** RfV's afgegeven:
- Voor bezoeken aan de Nederlandse Defensie **2.848**:
- Voor bezoeken aan buitenlandse Defensies **3.069**.
- Voor bezoeken aan de Nederlandse industrie zijn er **296** RfV's afgegeven.
- Voor bezoeken aan de buitenlandse industrie **1.108**.

Kengetallen veiligheidsonderzoeken
De UVO is een gezamenlijke unit van de MIVD en de AIVD. De unit doet veiligheidsonderzoeken naar (kandidaat-)vertrouwensfunctionarissen: 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).

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

Toelichting bij kengetallen veiligheidsonderzoeken

Van het totale aantal onderzoeken in 2025 zijn er 52.775 uitgevoerd door de UVO zelf en 32.862 door de Koninklijke Marechaussee (mandaathouder). Afhankelijk van de aard van de vertrouwensfunctie en de mogelijke schade die de (kandidaat-) vertrouwensfunctionaris 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	7.136	46	7.182
B-niveau door UVO	27.485	269	27.754
C-niveau door UVO	6.627	55	6.682
BL-niveau door UVO overgenomen van KMar	7.279	1.570	8.849
NAVO Top 2025	516	10	526
E-BL-niveau[1]	1.774	8	1.782
Totaal door UVO	50.817	1.958	52.775
BL-niveau door de KMar	32.862	0[2]	32.862
Totaal aantal onderzoeken	83.679	1.958	85.637

[1] E-BL veiligheidsonderzoeken worden digitaal rechtstreeks bij de UVO ingediend via eOPG.

[2] De KMar geeft geen negatieve besluiten af. Bij twijfel bij een veiligheidsonderzoek op BL-niveau dragen ze het veiligheidsonderzoek over aan de UVO. Eventuele negatieve besluiten worden dan meegerekend bij de negatieve besluiten van de AIVD. Dat verklaart de o hier.

2025		Ingediend in 2025	Afgedaan in 2025	Ongegrond	Gegrond	Niet-ontvankelijk	Ingetrokken	Afgewezen
	Bezwaren	206	167	121	16	7	24	-
	Beroepen	11	11	9	2	1	-	
	Beroep niet-tijdig	1	-	-	-	-	-	-
	Hoger beroep	6	3	3	-	-	-	-
	Voorlopige voorziening	2	2	-	1	-	-	1

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[14]. 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 2025 zijn geen notificaties gedaan. Conform artikel 59 lid 2 van de Wiv is de CTIVD hierover geïnformeerd.

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 desgewenst informatie 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 15 dreigingsappreciaties geschreven.

Tapstatistieken

In 2025 zijn er door de MIVD 4916 taps geplaatst. Het betreft hier de daadwerkelijke inzet van alle vormen van taps. Voorbeelden zijn een telefoontap, IP-tap of het plaatsen van een microfoon. Een target (persoon of organisatie) kan op verschillende manieren en op meerdere apparaten afgeluisterd worden. Deze worden afzonderlijk meegeteld in de statistieken.

Validatie-onderzoek

In 2025 heeft de MIVD 480 meldingen en signalen geregistreerd waarbij sprake was van een mogelijke dreiging voor de veiligheid of inzetbaarheid van de krijgsmacht. Na validatie van deze meldingen en signalen zijn vervolgens 51 meldingen overgegaan in een duidingsonderzoek. De meldingen en signalen zijn divers van aard. Zoals bijvoorbeeld verdachte situaties rondom defensieobjecten met betrekking tot spionage of sabotage, maar ook zorgen over individuen met vermeende radicalisering in verschillende vormen van extremisme. De MIVD ontvangt niet alleen meldingen vanuit (ketenpartners in) Nederland, maar ook vanuit het buitenland. Deze zijn voornamelijk gerelateerd aan militaire inzet, oefeningen en vertegenwoordigers van Defensie in het buitenland.

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

Inzageverzoeken 2025	Aantal verzoeken ingediend in 2025	* Aantal afgedane verzoeken	** Gehonoreerd	Geweigerd	Nog lopend	Bezwaar	Beroep	Hoger beroep
Persoonsgegevens	27	29	6	23	5	2 ingediend 1 afgedaan*	1 ingediend 0 afgedaan	0 ingediend 0 afgedaan
Naar overleden familie	3	4	0	4	0	0 ingediend 0 afgedaan	0 ingediend 0 afgedaan	0 ingediend 0 afgedaan
Bestuurlijke aangelegenheden	5	5	1	4	1	2 ingediend 0 afgedaan	0 ingediend 1 afgedaan*	0 ingediend 1 afgedaan*
Totaal	35	38	7	31	6	4 ingediend 1 afgedaan*	1 ingediend 1 afgedaan*	0 ingediend 1 afgedaan*

* *Deels verzoeken van jaren vóór 2025.*
** *Gehonoreerd betekent dat aan verzoeker één of meer documenten zijn verstrekt.*


F-035