Ministerie van Defensie

> Retouradres Postbus 20701 2500 ES Den Haag

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

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

Onze referentie

BS2024012669

Bij beantwoording, datum, onze referentie en onderwerp vermelden.

Datum 18 april 2024
Betreft MIVD jaarverslag 2023

Hierbij bied ik u het openbaar jaarverslag van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) over het jaar 2023 aan. In dit verslag legt de MIVD verantwoording af over de werkzaamheden van het afgelopen jaar.

DE MINISTER VAN DEFENSIE

drs. K.H. Ollongren

Ministerie van Defensie

Openbaar jaarverslag 2023

Militaire Inlichtingen- en Veiligheidsdienst

18 april 2024


22:50
23:00

Openbaar jaarverslag 2023

Militaire Inlichtingen- en Veiligheidsdienst

18 april 2024

2 Militaire Inlichtingen- en Veiligheidsdienst

INHOUDSOPGAVE

4 Militaire Inlichtingen- en Veiligheidsdienst

Voorwoord directeur MIVD

Het afgelopen jaar liet wederom vele conflicten op het wereldtoneel zien. De oorlog in Oekraïne ging onverminderd door en er was de terreuraanval van Hamas in Zuid-Israël, met daarop volgend de militaire inval van Israël in Gaza, onrust in het Midden-Oosten en aanvallen van de Houthi-beweging op de koopvaardij in de Rode Zee. Eerder in het jaar was er een oplaaiende strijd in Sudan waardoor in allerijl honderden Nederlanders moesten worden geëvacueerd, de militaire escalatie van Nagorno-Karabach, geweldsincidenten in Kosovo en toenemende militaire assertiviteit van China richting Taiwan. Dit is, helaas, geen limitatieve opsomming. We bleven ook dagelijks geconfronteerd met de veelal onzichtbare acties van statelijke en niet-statelijke tegenstanders. In de *grey zone*, het schemergebied tussen oorlog en vrede, bedreigden tegenstanders met een scala van heimelijke en digitale methoden onze vrede en veiligheid, onze open en vrije samenleving en onze welvaart.

De MIVD staat bij al deze dreigingen, samen met onze partners, aan de frontlijn. In de meer en meer turbulente, onvoorspelbare wereld met dreigingen die steeds naderbij komen, is het essentieel dat de krijgsmacht goed wordt ondersteund in haar optreden. Hiervoor leveren we militair relevante inlichtingen op alle niveaus. Bovendien leveren we strategische inlichtingen voor politieke besluitvormers en waar mogelijk handelingsopties ter verhoging van de weerbaarheid, ook voor andere instituties en bedrijven. Waar nodig treedt de MIVD op, binnen de mogelijkheden die de wet daarvoor biedt.

Om haar wettelijke taken te kunnen uitvoeren en bestaande bevoegdheden te kunnen gebruiken, heeft de dienst een toereikend mandaat nodig, passend bij de democratische rechtstaat die we beschermen. De tijdelijke wet naar landen met een offensief cyberprogramma, die op een nader te bepalen datum in 2024 in werking zal treden, moet de MIVD in staat stellen sneller op te treden om dreigingen van landen met een offensief cyberprogramma het hoofd te bieden. Ook moet de tijdelijke wet de diensten de ruimte geven om gebruik te maken van hun bevoegdheid om op kabelgebonden netwerken relevant berichtenverkeer en malware te onderscheppen, wat voor de nationale veiligheid en cybersecurity van wezenlijk belang is. De nota van wijziging regelt de omgang met bulkdatasets die met bijzondere bevoegdheden zijn verkregen op een betere manier. Deze verbeteringen blijven gepaard gaan met een zeer hoog niveau van waarborgen, onder meer door de invoering van bindend toezicht door de CTIVD tijdens de taakuitvoering. Bovendien is de brede herziening van de Wiv 2017 voor de komende kabinetsperiode nog steeds urgent en noodzakelijk.

Tot slot wil ik markeren dat we onze taken alleen kunnen uitvoeren met de inzet van onze medewerkers. Militairen en burgers die samen in dienst van de MIVD het bijzondere werk verrichten om de snel veranderende dreigingen steeds voor te blijven. Hun inzet voor onze krijgsmacht en de veiligheid van Nederland maakt mij enorm trots om voor deze organisatie te werken.

Directeur Militaire Inlichtingen- en Veiligheidsdienst
Schout-bij-nacht Peter F.M. Reesink

Openbaar jaarverslag MIVD 2023
Met het openbaar jaarverslag geeft de MIVD uitvoering aan artikel 12 van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017). Het openbaar jaarverslag geeft aan op welke onderzoeksopdrachten en veiligheidsbevorderende taken de dienst zich in 2023 heeft gericht. Deze onderzoeksopdrachten en veiligheidsbevorderende taken zijn gebaseerd op de meerjarige inlichtingenbehoefte zoals vastgelegd in de Geïntegreerde Aanwijzing Inlichtingen en Veiligheid (GA I&V) 2023-2026. Deze GA I&V is in nauwe samenwerking tussen de interdepartementale behoeftestellers (de ministeries van Defensie, Algemene Zaken, Buitenlandse Zaken, Binnenlandse Zaken en Koninkrijksrelaties en Justitie & Veiligheid[1]) en de MIVD en AIVD tot stand gekomen.

1 *Justitie & Veiligheid behartigt tevens de belangen van de overige departementen in de GA I&V onderhandelingen.*

1 INLICHTINGEN EN VEILIGHEID VOOR NEDERLAND

De MIVD ondersteunt wereldwijd de inzet van de Nederlandse strijdkrachten in missiegebieden. De MIVD doet dit met inlichtingen die betrouwbaar en actueel zijn; door inlichtingen te verzamelen, te analyseren en te verspreiden. Ter voorbereiding op de ontplooiing van Nederlandse troepen in het buitenland maakt de MIVD inlichtingenproducten, zoals dreigingsappreciaties en inlichtingenberichten, ten behoeve van de militaire inzet en de politieke besluitvorming die daarmee gemoeid is.

De veiligheidsrisico's voor Nederland veranderen snel en dreigingen nemen toe in omvang, variëteit en verwevenheid. Het militaire conflict in Oekraïne en de aanval van Hamas op Israël op 7 oktober 2023 en het daaropvolgende conflict hebben dat duidelijk gemaakt. Ook vonden er in 2023 onder andere staatsgrepen plaats in Niger en Sudan, Azerbeidzjan ontplooide een militaire operatie en hernam Nagorno-Karabach, met een grote vluchtelingenstroom tot gevolg en namen ook de spanningen in Kosovo toe.

Daarnaast werd, door een verhoogde dreiging van jihadistisch terrorisme, op 12 december 2023 het dreigingsniveau voor Nederland verhoogd van niveau 3 (aanzienlijke dreiging[2]) naar niveau 4 (substantiële dreiging[3]) op een schaal van 5. Dit houdt in dat er een reële kans bestaat dat een aanslag in Nederland zal plaatsvinden. Al deze gebeurtenissen onderstrepen het beeld van een onzekere, veranderlijke veiligheidscontext.

De MIVD moet in deze onzekere veiligheidscontext in staat zijn om snel te reageren op crises en tegelijkertijd duurzaam strategisch inlichtingenonderzoek te kunnen verrichten naar bijvoorbeeld de dreiging vanuit China en Rusland. De onzekere en veranderlijke veiligheidscontext vraagt veel van de wendbaarheid van de diensten, omdat crises snel opkomen en dreigingen divers en omvangrijk zijn.

Naast de strategische dossiers, aandachtsgebieden en de ondersteuning aan de krijgsmacht, heeft de MIVD ook veiligheidsbevorderende taken. De MIVD beschermt bijvoorbeeld de militaire geheimen en operaties van Defensie, spoort cyberaanvallen op, ontmaskert buitenlandse inlichtingenofficieren die op heimelijke en soms illegale wijze inlichtingen vergaren. De Nederlandse defensie-industrie, bedrijven, kennisinstellingen en wetenschappers zijn een potentieel doelwit van diverse statelijke actoren die (heimelijk) hoogwaardige, al dan niet militair relevante, technologie proberen te verwerven. De MIVD draagt bij aan de weerbaarheid en veiligheid van Defensie en de defensie-industrie door bijvoorbeeld onderzoek te doen naar de beveiliging van bedrijven die moeten voldoen aan de veiligheidseisen van Defensie.[4]

De grote verscheidenheid aan dreigingen vereist dat de MIVD op een veelheid aan onderwerpen over een relevante en betrouwbare inlichtingenpositie moet beschikken en informatie snel moet kunnen vergaren, verwerken, analyseren en dissemineren. De MIVD werkt hiertoe nauw samen met onder andere de krijgsmacht, de AIVD, de NCTV en met buitenlandse partnerdiensten.

Leeswijzer
Dit jaarverslag behandelt de inlichtingenonderzoeken, missieondersteuning en aandachtsgebieden op basis van een geografische en thematische verdeling. Daarna komen aan de orde de veiligheidsbevorderende taken, de verantwoording naar politiek en samenleving, de MIVD als organisatie en tenslotte de kengetallen van de dienst.

2 *Aanzienlijke dreiging (3): de kans op een aanslag is voorstelbaar.*
3 *Substantiële dreiging (4): de kans op een aanslag is reëel.*
4 *Algemene Beveiligingseisen voor defensieopdrachten 2019 (ABDO 2019).*

1.1 *Inlichtingenonderzoek in 2023*

De Russische Federatie

Russische Federatie: militair-strategische intenties

De Russische invasie van Oekraïne in februari 2022 toont dat dreigingen kunnen omslaan in militair geweld met verstrekkende gevolgen, ook op het Europees continent. Voor zowel Oekraïne als Rusland is dit een existentieel conflict. Voor Oekraïne geldt dit in een zeer letterlijke betekenis. Het militair verliezen van dit conflict betekent dat Oekraïne als soevereine staat feitelijk ophoudt te bestaan. De inspanningen van de Oekraïense staat en bevolking en de essentiële (militaire) steun die door het westen wordt gegeven hebben er toe geleid dat de Russische militaire opmars is gestuit. Hoewel het Oekraïense tegenoffensief, dat in juni 2023 is gestart, heeft geleid tot tactische successen, zijn de Oekraïense strijdkrachten niet in staat gebleken een doorbraak te forceren. Ondertussen heeft Rusland het militair initiatief eind 2023 weer overgenomen.

Hoewel Rusland in 2022 de militaire doelstellingen naar beneden heeft moeten bijstellen, blijft het strategisch doel onveranderd. Het Russische doel is om Oekraïne, als bufferstaat, blijvend te kunnen controleren. Het fundamentele karakter dat deze oorlog in Russische ogen heeft, is ook in 2023 gebleken. Rusland ziet deze oorlog als een breder conflict met het Westen. Hiermee heeft deze oorlog ook in Russische ogen een existentieel karakter; niet alleen de toekomst van de Russische positie in Europa en de wereld staat op het spel, maar ook de toekomst van de Russische natie, cultuur en wat Rusland traditionele waarden noemt. De oorlog in Oekraïne is uiteindelijk een botsing tussen tegengestelde en onverenigbare wereldbeelden. Deze diepgewortelde ideologie, gecombineerd met de Russische status van nucleaire supermacht, zal een politieke oplossing van dit conflict en het vinden van een bestendigde manier om met elkaars verschillen om te gaan uitermate complex maken. Dit betekent ook dat de Russische militaire, politieke en economische dreiging er één van de lange termijn is.

Rusland probeert de Europese veiligheidsarchitectuur ingrijpend te wijzigen door de NAVO en de EU te ondermijnen. De Russische dreigingsperceptie ten aanzien van de NAVO heeft zich in 2023 verdiept, met onder andere als gevolg de toetreding van Finland en de recente toetreding van Zweden tot het bondgenootschap. Een conflict met de NAVO is voorstelbaar geworden. Hoewel Rusland op de korte termijn niet in gewapend conflict met de NAVO wil raken, is er een zeker risico op ongewilde escalatie als gevolg van miscommunicatie en misverstanden.

De eerste contouren voor een hervorming van de Russische krijgsmacht zijn in 2023 waargenomen, waarbij Rusland de geleerde lessen uit de Oekraïne-oorlog tracht toe te passen. Rusland bereidt zich voor op een post-conflict situatie waarin de NAVO de belangrijkste tegenstander is. De Russische conventionele strijdkrachten hebben zware verliezen geleden, maar dat is niet per se een reden tot optimisme. Rusland kan zich hierdoor gedwongen zien op de korte termijn een prominentere rol te gunnen aan tactische kernwapens in zijn defensie- en veiligheidsbeleid.

Wapenbeheersing heeft in 2023 voor Rusland sterk aan relevantie ingeboet. Rusland heeft de deelname aan het strategisch kernwapenverdrag[5] bevroren, waardoor dit verdrag zijn waarde heeft verloren. Daarnaast heeft Rusland de ratificatie van het *Comprehensive Nuclear-Test-Ban Treaty* ongedaan gemaakt. Hoewel dit niet direct betekent dat Rusland kernwapentesten zal hervatten, is het signaal onmiskenbaar en zorgelijk. Rusland heeft in 2023 ook aangegeven tactische kernwapens in Belarus te willen stationeren. Dit past binnen een breder beeld waarin Rusland nucleaire retoriek gebruikt om angst en onzekerheid in het Westen te creëren en besluitvormingsprocessen te frustreren.

Russische Federatie: militair vermogen en militaire activiteiten

De oorlog in Oekraïne in 2023 kenmerkt zich door beperkte gebiedsveroveringen aan beide zijden ten koste van een hoge slijtage. In het afgelopen jaar is gebleken dat Rusland weerbarstiger en veerkrachtiger is dan velen hadden gedacht. Rusland heeft de enorme verliezen

5 *Strategic Arms Reduction Treaty (START).*

weten aan te vullen, veelal met slecht getraind personeel, en heeft nieuwe eenheden kunnen oprichten. Rusland blijkt ook in staat het zware materieel aan te vullen, waarbij kwaliteit wordt ingeruild voor kwantiteit. De inschatting is dat het Russische militair-industrieel complex momenteel de gevolgen van de opgelegde sancties deels kan mitigeren, door een veelvoud aan (korte termijn) maatregelen, zoals opgeschaalde productiecapaciteit en importsubstitutieprogramma's[6]. Deze programma's zijn erop gericht om alternatieve producten te verwerven of produceren die door de sancties niet langer verkrijgbaar waren. Rusland zal voor sommige van deze producten echter nog steeds afhankelijk blijven van westerse onderdelen, waardoor de kans dat de Russische Federatie gaat proberen op heimelijke wijze aan deze onderdelen (uit met name westerse landen) te komen blijft bestaan.

Bij de oorlog in Oekraïne staat 'klassiek' militair vermogen centraal. Hoewel cyber- en hybride oorlogvoering krachtige force multipliers kunnen zijn, blijkt juist het vermogen om eenheden op het slagveld in te zetten en te ondersteunen van doorslaggevend belang te zijn voor het behalen van militair succes. De voortzetting van westerse militaire steun is voor Oekraïne dan ook cruciaal om zich staande te kunnen blijven houden op het slagveld.

In het begin van 2023 heeft Rusland intensieve gevechten gevoerd in het oosten van Oekraïne. Echter dit offensief heeft niet geleid tot de gewenste gebiedsveroveringen. De meest significante overwinning is de vrijwel volledige inname van Bakhmut (en in 2024 Avdiivka) na maanden van Russische aanvallen, voornamelijk door eenheden van de Russische private militaire onderneming Wagner.

In het voorjaar van 2023 begon het Oekraïense tegenoffensief, onder andere met westers getrainde eenheden en westers materieel. Rusland heeft voorafgaand aan dit tegenoffensief zeer uitgebreide verdedigingslinies ingericht. Hoewel Oekraïne bij het tegenoffensief tactische successen boekte, is een operationele doorbraak uitgebleven. De zeer uitgebreide mijnenvelden en een gebrek aan tactische verrassing vanwege de grote hoeveelheid Russische drones aan het front, hebben bijgedragen aan het uitblijven van een doorbraak. Daarnaast hebben moderne capaciteiten zoals onbemande systemen, geavanceerde sensorcapaciteit en elektronische oorlogsvoering een groot remmend effect op de voortgang van offensieve operaties van beide zijden.

Op 24 juni 2023 culmineerde een langslepend conflict tussen de leider van Wagner, Jevgeni Prigozjin, en het leiderschap van het Russische ministerie van Defensie in een mislukte muiterij. Met de dood van Prigozjin als gevolg van een vliegtuigcrash op 24 augustus 2023 was de min of meer zelfstandige status van Wagner definitief voorbij. Het Kremlin heeft na zijn dood het zakelijke en militaire imperium van Prigozjin ontmanteld. Het Russische ministerie van Defensie is erop gebrand de vele private militaire ondernemingen in Rusland strak aan de leiband te houden.

Sinds oktober 2023 zijn de Russische strijdkrachten op diverse plekken opnieuw in het offensief gegaan. In het bijzonder bij het oord Avdiivka voerde Rusland zeer intensieve offensieve acties uit met uitzonderlijk hoge personele verliezen. Het is de verwachting dat ook de komende maanden de Russische krijgsmacht een offensieve houding in zal blijven nemen.

In 2023 is Rusland verder gegaan met veelvuldige langeafstands-aanvallen om de druk op de Oekraïense samenleving, overheid en strijdkrachten op te voeren. Het strategische accent van deze aanvallen verschuift deels met de seizoenen: van voortzetting van de aanvallen op energie-infrastructuur in de eerste wintermaanden, naar verstoring van de Oekraïense graanexport in de zomer, tot aan een hernieuwde campagne tegen energie-infrastructuur in het late najaar. Daarnaast blijft Rusland aanvallen uitvoeren op operationeel belangrijke militaire doelwitten als luchtverdedigingssystemen, vliegbases, hoofdkwartieren en logistieke installaties. Hoewel deze aanvallen veelal verstorend zijn en schaarse Oekraïense capaciteiten binden, heeft Rusland onvoldoende

6 *Importsubstitutie: Overgaan tot het produceren van goederen die voorheen werden geïmporteerd.*

langeafstandswapens om Oekraïne daadwerkelijk strategisch te kunnen verlammen.

De Oekraïense luchtverdediging en langeafstandscapaciteit is het afgelopen jaar verder versterkt met geavanceerde westerse systemen. Hoewel de luchtverdediging hierdoor inmiddels een aanzienlijk deel van de Russische langeafstandswapens kan onderscheppen, zijn er nog steeds onvoldoende middelen om alle doelwitten adequaat te beschermen. Zowel defensief als offensief zijn en blijven de Oekraïense luchtverdediging en luchtstrijdkrachten in zeer belangrijke mate afhankelijk van voortzetting van de westerse militaire steun.

Op zijn beurt werd Rusland in 2023 geconfronteerd met een snel evoluerende luchtdreiging achter de eigen linies. Toenemende complexe aanvallen met korte- en langeafstandsdrones op Moskou en andere prominente locaties in Rusland, brengen de oorlog ook publicitair naar Russisch grondgebied, ver verwijderd van het front. Daarnaast "veroorzaken" ze bij meerdere gelegenheden aanzienlijke materiële schade aan zware bommenwerpers en andere militaire vliegtuigen.

Zowel op het vasteland als op het door Rusland bezette Krim-schiereiland heeft Oekraïne door inzet van recent geleverde westerse precisiegeleide langeafstandswapens (zoals *Storm Shadow* en ATACMS[7]) effectief doelen aan kunnen grijpen die tot dan toe buiten bereik lagen. Het aangrijpen van vooruitgeschoven helikopterbases en munitiedepots, een Russische onderzeeboot, faciliteiten voor scheepsreparatie en het hoofdkwartier van de Zwarte Zeevloot op de Krim, zijn prominente militaire en publicitaire successen van Oekraïne.

Daarnaast heeft Oekraïne het afgelopen jaar in het Zwarte Zeegebied meerdere aanvallen uitgevoerd met *Unmanned Surface Vessels* (USV's). Hierbij zijn verschillende Russische schepen op de Zwarte Zee en in Russische havens aangegrepen. De uitgevoerde USV-aanvallen zijn een aanzienlijke tegenslag voor de Russische marine en de Zwarte Zeevloot in het bijzonder. Door deze tegenslagen heeft Rusland niet langer de mogelijkheid om ongehinderd op te treden in het westelijk deel van de Zwarte Zee en heeft daardoor niet meer de volledige controle over dit gebied.

> **Russen ontduiken westerse sancties via dekmantelbedrijven**
> Russische inlichtingendiensten zijn betrokken bij het ontduiken van westerse sancties. Ze maken daarbij gebruik van dekmantelbedrijven. Russische bedrijven zijn voor hun (militaire) productie in belangrijke mate afhankelijk van westerse technologie en goederen. Mede door de sancties hebben Russische producenten problemen met het verkrijgen van onderdelen en materialen. De Russische diensten worden ingezet om de gesanctioneerde goederen op een heimelijk manier aan te schaffen en naar Rusland te transporteren. Ook Nederlandse bedrijven zijn doelwit.

Rusland: Militaire techniek en wapensystemen

Het Russisch Militair-Industrieel Complex (MIC) is omvangrijk en kenmerkt zich door een focus op productie en *Research & Development* van wapensystemen. Rusland blijft, ondanks steeds zwaardere sancties, wapens en militaire technologie ontwikkelen, produceren en op grote schaal wapens en wapentechniek exporteren. Om de groeiende behoefte aan wapens en munitie als gevolg van de oorlog in Oekraïne in te vullen, vergroot Rusland de productiecapaciteit hiervan. Hierbij lijkt Rusland steeds beter in staat alternatieven te vinden voor gesanctioneerde artikelen, bijvoorbeeld door succesvolle importsubstitutie en heimelijke verwerving. De alternatieven zijn echter vaak van inferieure kwaliteit en bij heimelijke verwerving geldt dat de kosten hoger zijn, de omvang kleiner en doorlooptijd langer is. Bovendien gebruikt Rusland waar nodig geïmporteerde wapensystemen zoals Iraanse drones. Desondanks streeft Rusland een zo groot mogelijke strategische onafhankelijkheid na, waarbij het ook geïmporteerde wapensystemen het liefst vervangt door nationaal ontwikkelde en geproduceerde systemen.

7 *ATACMS: Army Tactical Missile System; tactische ballistische raketten.*

De focus van Russische militaire technologie is zowel defensief als offensief. Te denken valt aan hoogwaardige luchtverdedigingssystemen, maar ook aan ballistische en hypersonische raketten. Ondanks de oorlog in Oekraïne en de toegenomen nationale vraag, worden Russische wapensystemen of hiervan afgeleide systemen wereldwijd verspreid en worden deze op vrijwel elk strijdtoneel ingezet.

De MIVD doet onderzoek naar Russische militair-technologische ontwikkelingen, mede om de Nederlandse krijgsmacht in staat te stellen goed onderbouwde keuzes te maken als het gaat om aanschaf en ontwikkeling van nieuwe militaire systemen voor nu en de toekomst. Uit in 2023 uitgevoerd onderzoek concludeert de MIVD dat de dreiging die uitgaat van de huidige en toekomstige Russische militaire middelen groot is en blijft. Het is daarbij vrijwel zeker dat de Nederlandse krijgsmacht in geval van operaties in aanraking komt met hoogwaardige Russische wapensystemen, mede door de wereldwijde proliferatie (export) van deze systemen door Rusland.

Russische Federatie: sabotagedreiging richting Nederland

De vitale maritieme infrastructuur in het Nederlandse deel van de Noordzee, zoals internetkabels, gasleidingen en windmolenparken, kan kwetsbaar zijn voor sabotage. Rusland brengt deze infrastructuur heimelijk in kaart en onderneemt activiteiten die duiden op spionage en voorbereidingshandelingen voor verstoring en sabotage.

> **Russisch onderzoeksschip wederom actief op Nederlandse deel van de Noordzee.**
> Een Russisch onderzoeksschip was in 2023 wederom actief op het Nederlandse deel van de Noordzee. De MIVD denkt dat de Russen de mogelijkheden voor potentiële toekomstige sabotage wilden onderzoeken, vanwege de activiteiten en het gedrag van het schip. Het Russische schip werd tijdens haar activiteiten op de Noordzee geschaduwd door Nederlandse marine-eenheden.

Russische Federatie: spionage

De dreiging van spionage door Rusland bleef in 2023 actueel, zo constateerde de MIVD in samenwerking met de AIVD. Voor de Russische inlichtingen- en veiligheidsdiensten blijft Nederland namelijk een belangrijk spionagedoelwit, temeer omdat ons land in 2023 wederom veel steun leverde aan Oekraïne, in de vorm van militair materieel en trainingen. Ook is Nederland een belangrijk doorvoerland van militair materieel dat richting Oekraïne en de NAVO-oostflank gaat.
De Russische diensten proberen informatie te verzamelen over het Nederlandse overheidsbeleid ten aanzien van Rusland, over de NAVO en de EU en de *high-tech*-sector. Aandacht is er ook voor de internationale organisaties die gevestigd zijn in Nederland, met name voor de organisaties die onderzoek doen naar mogelijk door Rusland in Oekraïne gepleegde oorlogsmisdaden, zoals de Organisatie voor het Verbod op Chemische Wapens (OPCW) en het *International Criminal Court* (ICC). De Nederlandse krijgsmacht en defensie-industrie zijn eveneens interessante aandachtsgebieden voor Russische inlichtingenofficieren.

In het verleden maakten Russische inlichtingenofficieren vaak gebruik van een dekmantel als diplomaat, waardoor ze in Nederland konden verblijven en een beschermde (diplomatieke) status genoten. Deze dekmantel konden ze in 2023 veel minder goed gebruiken, aangezien Nederland de meeste Russische inlichtingenofficieren met deze dekmantel het land heeft uitgezet. Bovendien voert Nederland een effectief visumbeleid, wat het voor Rusland lastig maakt om nieuwe inlichtingenofficieren in Nederland te plaatsen. De MIVD en de AIVD verwachten echter wel dat de Russische diensten andere dekmantels en andere manieren zullen gebruiken om te spioneren in Nederland. Denk hierbij aan een dekmantel als zakenman of journalist. Dit kan de afname van het aantal inlichtingenofficieren onder diplomatiek dekmantel echter niet compenseren.

Ook in het buitenland vormen de Russische diensten een dreiging voor Nederland en Nederlandse belangen. Nederlandse diplomaten, studenten, militairen of zakenmensen die in het buitenland verblijven kunnen

doelwit zijn van spionage. De Russische diensten hebben immers meer bewegingsvrijheid in landen die niet of terughoudend optreden tegen Russische spionageactiviteiten.

Naast spionage, houden de Russische inlichtingen- en veiligheidsdiensten zich bezig met het heimelijk verwerven van goederen in of via Nederland. Door middel van dekmantelbedrijven proberen de Russische diensten producten aan te schaffen die vanwege internationale sancties niet aan Rusland verkocht mogen worden. Het gaat dan vaak om goederen die Rusland kan gebruiken voor zijn krijgsmacht.

Russische Federatie: economische perspectieven

Het veranderende geopolitieke landschap dwingt Moskou tot keuzes, die soms ongemakkelijk zijn en handelingsvrijheid inperken. Noodgedwongen verschuift Moskou zijn focus richting nieuwe afzetmarkten, alternatieve handelspartners en internationale gremia die een tegenwicht aan het Westen kunnen bieden. De Russische politieke en economische afhankelijkheid van partners, zoals bijvoorbeeld China, is in deze context toegenomen.

Russische Federatie: cyber

- Cyberspionage

Het grootste deel van Russische cyberoperaties is gericht op spionage. Het doel van de operaties is het bemachtigen van militaire, diplomatieke en economische informatie over Oekraïne en NAVO-bondgenoten.

Het uitvoeren van cyberoperaties tegen Oekraïne blijft voor Russische statelijke cyberactoren in 2023 de hoogste prioriteit. De MIVD zag in 2022, het eerste jaar van de *full scale* Russische invasie, veel Russische cyberoperaties gericht op de sabotage van Oekraïense kritieke infrastructuur. Afgelopen jaar is de focus verlegd naar de ondersteuning van Russische grondoperaties door middel van cyberspionage. Russische statelijke cyberactoren proberen middels cyberoperaties bijvoorbeeld locaties van Oekraïens militair materieel en personeel in kaart te brengen om die vervolgens fysiek aan te grijpen. Dergelijke cyberoperaties zijn veelal gericht op de digitale systemen in gebruik bij Oekraïense militairen aan het front.

De inlichtingenbehoefte van Rusland richting de NAVO bestaat onder andere uit het verkrijgen van inzicht in militaire steun vanuit NAVO-landen. Zo proberen Russische statelijke actoren via cyberspionageoperaties zicht te krijgen op de transporten van westerse militaire steun, zowel binnen als buiten Oekraïne. Hierbij zijn landen die onderdeel uitmaken van de aanvoerroute doelwit geworden van dergelijke cyberoperaties, waaronder Nederland. Naast Oekraïne en de NAVO zijn de Nederlandse krijgsmacht, ministeries en ambassades afgelopen jaar direct en indirect doelwit geweest van (onsuccesvolle) cyberspionagepogingen.

De MIVD rapporteerde in 2022 over routers die door de GRU gebruikt worden als aanvalsinfrastructuur en de verstoring van dat netwerk. In 2023 zag de MIVD dat Russische actoren gebruik blijven maken van gehackte infrastructuur van onschuldige gebruikers ten behoeve van digitale spionage-, sabotage- en beïnvloedingsactiviteiten.

Russische cyberoperaties

De MIVD heeft het afgelopen jaar kritieke inlichtingen met Oekraïne gedeeld over Russische cyberoperaties en hierdoor bijgedragen aan het beschermen van Oekraïense overheidsnetwerken en kritieke infrastructuur.
Tevens heeft de MIVD actie ondernomen om de digitale bewegingsvrijheid van Russische statelijke actoren om cyberoperaties uit te voeren tegen Nederland, Europese- en NAVO-bondgenoten en Oekraïne in te perken. De MIVD is voornemens dergelijke acties komend jaar uit te blijven voeren.

- Digitale beïnvloeding

Informatieconfrontatie, waaronder beïnvloeding door misleiding, desinformatie en cyberoperaties, speelt een centrale rol in de Russische

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

wijze van optreden. Dit wordt voor een belangrijk deel uitgevoerd via digitale middelen om onder meer psychologische effecten te veroorzaken. Om hun betrokkenheid te verbergen bij het heimelijk verspreiden van desinformatie en propaganda via digitale kanalen, passen Russische inlichtingendiensten veel technieken toe die zij ook voor cyberoperaties gebruiken. In het geval van de informatieoperatietroepen van de Russische militaire inlichtingendienst GRU zijn het deels dezelfde eenheden die voor zowel cyberoperaties als heimelijke beïnvloeding verantwoordelijk zijn.

In 2023 constateerde de MIVD dat een groter deel van de digitale spionage-, sabotage- en beïnvloedingsactiviteiten uitgevoerd wordt door 'hacktivistische'[8] collectieven. In sommige gevallen gebruiken 'traditionele' Russische cyberactoren deze hacktivistische covers. In andere gevallen gaat het daadwerkelijk om hacktivistische groeperingen die handelen in het verlengde van de Russische staat. Deze groeperingen vallen vaak buiten de traditionele organisatiestructuren van het Russische cyberprogramma.

- Cybersabotage

De Russische cybersabotagecampagne tegen Oekraïne is de meest grootschalige en intensieve uit de geschiedenis. Moskou probeert regelmatig om Oekraïense vitale infrastructuur digitaal te saboteren en voert voortdurend aanvallen uit met *wipermalware* (kwaadaardige software die informatie wist). Bij de uitvoering van de voorbereiding en uitvoering van sabotage wordt ook gebruik gemaakt van pro-Russische *proxies*[9].

Ten opzichte van het eerste jaar van de oorlog in Oekraïne heeft de MIVD in 2023 een toename waargenomen van cyberoperaties door Russische statelijke actoren tegen Europese en NAVO-bondgenootschappelijke doelwitten. De MIVD acht het waarschijnlijk dat sommige van deze cyberoperaties zijn uitgevoerd met als doel een digitale positie binnen kritieke infrastructuur te bemachtigen, om deze op een later moment te kunnen saboteren. Indien succesvol kan dit potentieel verstrekkende maatschappelijk ontwrichtende gevolgen hebben, waardoor de MIVD dit als een zorgwekkende ontwikkeling ziet.

De aanhoudende en zeer hoge druk die Rusland hiermee uitoefent vereist constante waakzaamheid van zowel Oekraïne als het Westen. Daarnaast is samenwerking met de private sector van cruciaal belang om digitale weerbaarheid te behouden en bevorderen. Het succes van de Oekraïense digitale verdediging is niet gegarandeerd. Waarschijnlijk kan dit succes alleen volgehouden worden zolang de westerse steun net zo intensief en adaptief blijft als de cyberoperaties van de Russische inlichtingendiensten en diens *proxies*.

China

Hoewel er op het eind van het jaar een voorzichtige toenadering was tussen de Verenigde Staten en de Volksrepubliek China, zag 2023 vooral een China dat steeds meer zijn eigen strategische belangen liet prevaleren boven het behouden van een goede relatie met het Westen. Gedurende 2023 heeft Xi Jinping zijn grip op de Chinese Communistische Partij (CCP), het Chinese staatsbestel en daarmee de Chinese samenleving nog verder verstevigd. In maart 2023 werd Xi voor de derde keer benoemd tot president. Door de combinatie van zijn functies als president, opperbevelhebber en partijsecretaris en een politbureau[10] met louter loyalisten, heeft Xi nu voor onbepaalde tijd een zeer sterke autoriteitspositie verworven.

Nationale veiligheid is één van de onderwerpen die Xi heeft bestempeld als topprioriteit dit jaar. Dit uitte zich in de vorm van een aantal nieuwe wetten, waar de nieuwe contraspionagewet het voornaamste voorbeeld van is. Deze wet maakt, in theorie, alle Chinezen, ook die buiten China verblijven, verantwoordelijk voor het leveren van een bijdrage aan China's nationale veiligheid. Daarnaast laten ook de wet op de buitenlandse

9 *Proxies zijn organisaties die niet formeel gelieerd zijn aan de Russische overheid maar in de praktijk een vorm van aansturing en/of ondersteuning kennen vanuit de Russische overheid en waarvan de activiteiten bijdragen aan Russische strategische doelen.*

10 *Politbureau (politiek bureau) is het uitvoerend orgaan van de CCP.*

relaties en de dataprotectiewet[11] zien dat de controle van de CCP op de Chinese samenleving en buitenlandse bedrijven in China toeneemt.
In de Zuid-Chinese Zee (ZCZ), een voor de wereldhandel belangrijk economisch corridor, voeren het optreden van de Chinese krijgsmacht en de kustwacht de spanningen verder op. Stabiliteit en vrije doorvaart in deze regio is ook voor de Nederlandse economie van groot belang.
China toonde zich in toenemende mate bereid om zijn soevereiniteits-claims over delen van dit gebied met woord en daad te verdedigen.
Zo verkondigde het Chinese ministerie van Defensie in april 2023 dat China onbetwistbare soevereiniteit heeft over de eilanden in de ZCZ en de omringende wateren. Daarnaast poogden de Chinese kustwacht en daaraan gelieerde civiele schepen meermaals de bevoorrading van Filipijnse eenheden op de *Second Thomas Shoal* (onderdeel van de Spratly eilanden in de ZCZ) te verhinderen door de inzet van waterkanonnen en het doelbewust aanvaren van Filipijnse schepen.

Ook voerde China het afgelopen jaar de druk op Taiwan verder op. Het meest opvallend was het militaire machtsvertoon na de ontmoeting tussen toenmalig voorzitter van het Amerikaanse Huis van Afgevaardigden Kevin McCarthy en de Taiwanese president Tsai Ing-wen in april 2023. Het Volksbevrijdingsleger simuleerde toen een aanval op het eiland. Daarnaast was het aantal Chinese militaire vliegtuigen dat de Taiwanese *Air Defence Identification Zone* (ADIZ) betrad aanzienlijk, maar vergelijkbaar met het voorgaande jaar. Opvallend is wel dat deze luchtoperaties niet langer alleen vanaf het Chinese vasteland worden uitgevoerd, maar in toenemende mate ook vanaf Chinese vliegdekschepen op de Filipijnse Zee.
China en Rusland hebben hun economische, politieke en militaire samenwerking in 2023 voortgezet en verder geïntensiveerd. Met de toenemende strategische wedijver tussen de VS en China aan de ene kant, en tussen NAVO en Rusland aan de andere, vinden Peking en Moskou elkaar als partner. Beide landen ambiëren een meer multipolaire wereld, waarbij de rol van de VS (en NAVO) teruggebracht wordt en waarbij China en Rusland een prominentere stem hebben in de regionale en wereldpolitiek. Om de economische, diplomatieke en militaire relatie te bestendigen vonden in 2023 meermaals op het hoogste niveau ontmoetingen plaats, waaronder tussen de staats- en regeringshoofden.

China's versterkte relatie met Rusland droeg in 2023 direct en indirect bij aan het in stand houden van de Russische oorlogsinspanningen in Oekraïne. Daarmee verzwakt China Nederlandse en bondgenootschappelijke maatregelen tegen Rusland. De toenemende militaire samenwerking biedt China en Rusland een mogelijkheid de kracht van hun strategische partnerschap verder uit te dragen, en biedt het Volksbevrijdingsleger een kans om te leren van het Russische militaire optreden in Oekraïne. Het is twijfelachtig of Peking een substantiële bijdrage kan (of wil) leveren aan vredesonderhandelingen die recht doen aan de Oekraïense soevereiniteit. Echter, ondanks de groeiende samenwerking en gedeelde belangen is van een natuurlijke alliantie geen sprake. China worstelt hiermee, hetgeen zich sterk uit in China's pseudoneutraliteit en veelal door eigenbelang gedreven beleid ten aanzien van het Oekraïneconflict. De oorlog in Oekraïne en sancties tegen Rusland hebben gezorgd voor een nieuwe dynamiek in de samenwerking waarin het 'ongelimiteerde partnerschap' op de proef wordt gesteld.
Zo resulteert de oorlog in een ingewikkelde dynamiek waarin Rusland in hogere mate afhankelijk is van China en Peking deze afhankelijkheid (succesvol) poogt uit te buiten. Tegelijkertijd dient Peking een balans te vinden tussen zijn ambities als 'verantwoordelijke grootmacht', steun aan partner Rusland, en zijn handelsbelangen in met name Europa.

China: Militaire techniek en wapensystemen

China blijft veel investeren in mensen en middelen om qua militaire capaciteiten en militaire technologie op of boven het niveau te komen van het Westen. China heeft inmiddels een uitgebreide ontwikkel- en productiecapaciteit opgebouwd. De laatste jaren zijn binnen het Chinees militair-industrieel complex grote conglomeraten[12] gevormd waarbinnen enorm veel kennis en middelen beschikbaar zijn. Deze conglomeraten houden zich bezig met de ontwikkeling, productie en innovatie van

11 *Personal Information Protection Law. Inwerking getreden op 1 nov 2021.*

12 *Een geheel van bedrijven, bestaande uit meerdere divisies, die wat activiteiten betreft zeer verschillend zijn en vrijwel zelfstandig opereren (diversificatie van activiteiten).*

militaire wapensystemen en technologieën. Hierbij wordt dusdanig intensief samengewerkt met het bedrijfsleven en kennisinstituten dat de scheidslijn tussen militaire en niet-militaire technologieontwikkeling vervaagt of zelfs afwezig is. Zo zijn er op het gebied van kwantumtechnologie Chinese universiteiten die onderzoek doen voor de Chinese krijgsmacht. Nederlandse samenwerking met bijvoorbeeld Chinese onderwijsinstellingen komt hiermee niet exclusief ten goede aan de internationale technologische vooruitgang, maar aan de ontwikkeling van de capaciteiten van de Chinese krijgsmacht.

De MIVD constateert dat China een groot aantal satellieten in banen om de aarde heeft. Deze satellieten hebben in principe een wereldwijde dekking (maar China legt een duidelijke nadruk op regionale focus) en kunnen bijdragen aan zaken als aardobservatie, detectie van elektronische signalen (bijvoorbeeld om maritiem verkeer te kunnen volgen), spionage en het genereren van waarschuwingen over bijvoorbeeld lanceringen van geleide wapens. Het aantal en de kwaliteit van de Chinese ruimtecapaciteiten is inmiddels dusdanig dat aan de dominantie van de VS in de ruimte wordt getornd. Zo zijn een deel van de Chinese aardobservatiesatellieten van absolute wereldklasse[13]. China bouwt niet alleen aan voornoemde klassieke ruimtecapaciteiten, maar bijvoorbeeld ook aan een ruimteveer met specifieke militaire toepassingen. Ook ontwikkelt China een kwantumcommunicatiesatelliet constellatie[14]. Hierin is het land wereldwijd koploper.

De MIVD doet onderzoek naar Chinese militair-technologische ontwikkelingen, mede om de Nederlandse krijgsmacht in staat te stellen goed onderbouwde keuzes te maken als het gaat om aanschaf en ontwikkeling van nieuwe wapensystemen voor nu en de toekomst. Uit het in 2023 uitgevoerde onderzoek heeft de MIVD kunnen concluderen dat de dreiging die uitgaat van de huidige en toekomstige Chinese militaire capaciteiten groot is. De kans dat de Nederlandse krijgsmacht in aanraking komt met Chinese wapens wordt ook steeds groter, mede door de wereldwijde proliferatie (export) van deze systemen door China.

China: spionage

In 2023 heeft de MIVD, in samenwerking met de AIVD, het onderzoek naar de activiteiten van de Chinese inlichtingendiensten voortgezet. Daarbij heeft de MIVD in aanvulling op het onderzoek van voorgaande jaren, geconcludeerd dat Chinese actoren een breed palet aan activiteiten uitvoeren om in de Chinese inlichtingenbehoefte te voorzien.

Net als de afgelopen jaren heeft China in 2023 de ambitie nagestreefd zich verder te ontwikkelen tot een grootmacht, zowel economisch, politiek als militair. Om dit doel te bereiken wil China een hoogwaardige kenniseconomie opbouwen die niet afhankelijk is van westerse kennis en technologie. China wil een krijgsmacht opbouwen die zich kan meten met iedere andere krijgsmacht. Voor deze doelstellingen heeft China geavanceerde technologie nodig die het nog niet allemaal zelf bezit. Deze ontbrekende kennis en technologie probeert China in het buitenland te verwerven. Daarvoor heeft China naast veel legale middelen zoals wetenschappelijk onderzoek en bedrijfsinvesteringen, ook in 2023 zijn inlichtingendiensten ingezet.

Vooral in de halfgeleiderindustrie, lucht- en ruimtevaart, en de maritieme industrie vormt Nederland voor China nog steeds een aantrekkelijk spionagedoelwit van Chinese inlichtingenactoren, dit vanwege de goede kennispositie van bedrijven en kennisinstellingen in deze sectoren. Ook beschikt de Nederlandse krijgsmacht, net als de krijgsmachten van onze bondgenoten, over kennis van modern materieel en over militair-operationele expertise die China kan gebruiken om zijn eigen krijgsmacht verder op te bouwen. Daarom vormen ook defensiematerieelprojecten, operationele eenheden en (voormalig) defensiepersoneel van Nederland en onze bondgenoten doelwitten van Chinese spionage. In 2023 heeft de

13 *Een grondresolutie van minder dan 25 cm is inmiddels bere kt. Dit houdt in dat een significant hoger detailniveau gehaald is dan de meeste commercieel beschikbare beelden die tegenwoordig vaak in de media te zien zijn.*

14 *Een kwantumcommunicatiesatellietconstellatie is een groep communicatiesatellieten die samenwerkt als een systeem en doormiddel van kwantumtechnologie ve lige informatiedeling mogelijk maakt.*

MIVD daarom, samen met de AIVD, het onderzoek voortgezet naar de Chinese spionagedreiging tegen deze sectoren en Defensieonderdelen en waar nodig geadviseerd om mitigerende maatregelen te treffen.
De MIVD doet onderzoek naar het weglekken van gevoelige en militair relevante kennis via academische samenwerking door bijvoorbeeld Chinese promovendi aan Nederlandse universiteiten. In 2023 heeft de MIVD in aanvulling hierop onderzoek gedaan naar andere Chinese modi operandi om gevoelige Nederlandse kennis te vergaren. Daarbij heeft China een zeer breed spectrum aan methoden gebruikt, variërend van openlijke en legale activiteiten van bedrijven tot heimelijke activiteiten van de Chinese inlichtingendiensten. Als China in Nederland (of andere westerse landen) militair relevante technologische kennis vergaart, dan kan dit China helpen om zijn krijgsmacht verder op te bouwen. Dat kan een negatief effect hebben op de mondiale machtsbalans en de Nederlandse internationale veiligheidsbelangen.

De MIVD heeft in samenwerking met de AIVD onderzoek gedaan naar de Chinese spionagedreiging tegen de Nederlandse halfgeleidersector. Hierbij constateren de diensten dat van de Chinese inlichtingendiensten een brede spionagedreiging uitgaat richting de halfgeleiderindustrie in verscheidene landen, waaronder Nederland. Partijen in de Nederlandse halfgeleiderindustrie moeten daarbij rekening houden met zowel een digitale-dreiging als een zogenaamde *human intelligence*-[15] of *insider threats*[16].

China: Cyber

In 2023 waren Nederlandse en bondgenootschappelijke (defensie) bedrijven en overheidsinstellingen veelvuldig doelwit van diverse Chinese cybereenheden. Deze eenheden richtten zich waarschijnlijk primair op de collectie van onder andere intellectueel eigendom, persoonsgegevens en voorkennis omtrent politiek-bestuurlijke beleid- en besluitvorming. Het tempo van Chinese cyberoperaties op westerse doelwitten ligt hoog en Chinese inlichtingendiensten schroeven de capaciteiten om westerse doelwitten aan te vallen steeds verder op.

> **Politiek gemotiveerde cyberspionage in Europa**
> De actuele digitale spionagedreiging tegen westerse overheden en instellingen vanuit China is op dit moment hoog. Een een groot deel van de EU-lidstaten heeft in 2023 te maken gehad met een cyberaanval van een Chinese statelijke hackersgroep. De doelwitten lijken gericht uitgekozen met als doel inlichtingen te vergaren over politieke besluitvorming. Om deze doelwitten binnen te dringen, voeren Chinese hackersgroepen ook ondersteunende operaties uit, waaronder op telecomproviders en leveranciers van ICT-diensten.

Hoewel Chinese statelijke hackersgroepen al geruime tijd grootschalige en persistente cyberspionagecampagnes uitvoeren tegen Nederlandse en bondgenootschappelijke belangen, zag de MIVD in 2023 een toename van de intensiteit, omvang en het technische niveau van deze cybercampagnes. Zo hebben de MIVD en de AIVD waargenomen dat Chinese aanvalsgroepen:

- Zich nadrukkelijk richten op *edge devices*[17], zoals VPN-apparatuur.
- Met hoog operationeel tempo kwetsbaarheden uitbuiten, soms al op de dag van publicatie.
- Tevens vaker gebruik maken van onbekende kwetsbaarheden.

De MIVD nam in 2023 voornamelijk grootschalige scanactiviteit waar tegen kwetsbare systemen van een breed scala aan doelwitten, waaronder ABDO-bedrijven[18] en defensieorganisaties. Het patroon is dat aanvallers geautomatiseerde toegang proberen te verkrijgen tot netwerken van doelwitten en in een later stadium bepalen of deze *access*-posities relevant zijn voor China. Tijdens een van deze campagnes wist een Chinese statelijke hackersgroep binnen enkele maanden 20.000 slachtoffers te infecteren. Chinese cyberactoren professionaliseerden hun operaties in 2023 verder door vaker gebruik te maken van gehackte

15 *Human intelligence: het verzamelen van inlichtingen door interpersoonlijk contact in alle vormen en m.b.v diverse middelen.*
16 *Insider threats: dreigingen die vanuit de eigen organisatie komen, bijv. rancuneuze voormalige of huidige werknemers of kwaadwillende zakenpartners en contacten die beschikken over interne of gevoelige bedrijfsgegevens.*
17 *Edge devices: een apparaat wat een toegangspunt (gateway) biedt tot (kern)netwerken van ondernemingen of service providers zoals routers, routing switches etc.*
18 *ABDO-bedrijven die de uitvoering op zich nemen van gerubriceerde of vitale defensieopdrachten en gehouden zijn aan de regeling Algemene Beve ligingseisen voor Defensieopdrachten (ABDO).*

infrastructuur, waaronder consumentenapparatuur. Dit bemoeilijkt effectieve verdediging, detectie en attributie.

Geavanceerde Chinese spionagemalware onthuld
Defensie werd zelf ook slachtoffer van Chinese statelijke hackers. In 2023 konden aanvallers binnenkomen bij een defensienetwerk. Een defensie-onderdeel gebruikte het netwerk voor samenwerking met derde partijen op het gebied van R&D. De MIVD publiceerde in februari 2024 een openbaar technisch rapport[19] met details op de website van het Nationaal Cyber Security Centrum (NCSC) over de bij het incident aangetroffen malware.

China beschikt over een significante cybercapaciteit met een grote hoeveelheid en verscheidenheid aan betrokken actoren. Uit inlichtingen van de MIVD en AIVD blijkt bijvoorbeeld dat tientallen Chinese bedrijven offensieve cyberoperaties ondersteunen met softwarekwetsbaarheden, malware, (semi-)anonieme aanvalsinfrastructuur en specialistische soft- en hardware voor digitale aanvallen. De hoge mate van professionalisering en strategische clustering van Chinese hackerseenheden in combinatie met de samenwerking met Chinese (staats)bedrijven geven China hoogwaardige capaciteiten om aanvallen op Nederland en bondgenoten uit te voeren.

Ook Chinese universiteiten dragen bij aan de opbouw van offensieve capaciteiten. Inlichtingen tonen aan hoezeer het Chinese offensieve cyberprogramma gestoeld is op samenwerking tussen bedrijfsleven, universiteiten en Chinese inlichtingendiensten. De scheidslijnen tussen organisaties zijn daarbij onduidelijk: personen vervullen soms zowel een wetenschappelijke rol als een rol in het Chinese veiligheidsapparaat en werken daarbij samen met Chinese (staats)bedrijven. De MIVD acht het zeer waarschijnlijk dat dergelijke samenwerkingsverbanden resulteren in een spionagerisico.

Chinese prepositionering voor sabotage op Amerikaanse doelwitten
In 2023 onthulden Microsoft en de VS het bestaan van een grootschalig Chinees cybersabotageprogramma. Dat is onder meer gericht op prepositionering in Amerikaanse militaire en civiele vitale infrastructuur, in de vorm van de VOLT TYPHOON-campagne. Hiermee probeert China inzetopties voor tijdens een potentieel gewapend conflict te creëren. Vooralsnog zijn geen activiteiten uit dit programma tegen Europa bekend. De Chinese capaciteit op dit gebied groeit echter hard en kan binnen betrekkelijk korte tijd overal ter wereld ingezet worden. Hierdoor kan dit Chinese cybersabotageprogramma de komende jaren in potentie een dreiging voor Defensie en ook Nederland worden.

China: Economische veiligheid
De MIVD en de AIVD signaleerden in 2023 een aanhoudende dreiging tegen onder andere de Nederlandse halfgeleiderindustrie. China probeert op diverse wijzen in Nederland technologie te verwerven. China maakt daarbij gebruik van een combinatie van (cyber)spionage, *insiders* binnen Nederlandse bedrijven, (strategische) overnames van halfgeleiderbedrijven, het omzeilen van geldende exportrestricties en het *reverse engineering*[20] van vergunningsvrije technologie. Naarmate legale en openlijke verwerving van technologie moeilijker wordt, door onder andere screening van investeringen en exportcontroles, neemt het risico op illegale, heimelijke verwerving toe. Dit vormt een dreiging voor de Nederlandse economische veiligheid.

Caribisch gebied
De MIVD en de AIVD doen gezamenlijk onderzoek naar politieke en militaire ontwikkelingen in Venezuela en mogelijke uitstralingseffecten richting het Koninkrijk der Nederlanden en in het bijzonder Aruba, Bonaire en Curaçao.

Het Maduro-regime probeert zijn positie te consolideren en zich optimaal voor te bereiden op de presidentsverkiezingen in 2024. Op 3 december werd een referendum gehouden over de status van Essequibo; het gebied ten westen van de Essequiborivier dat deel uitmaakt van Guyana. Op basis van de uitslag van dit referendum riep het regime het gebied uit als Venezolaans grondgebied. Hoewel de spanning hierdoor sterk opliep, hebben de leiders van beide landen uitgesproken het dispuut niet met militaire middelen te willen beslechten. Wel gaat het dispuut gepaard met (beperkte) Venezolaanse

19 *Rapport Coathanger 'a stealthy Chinese FortiGate RAT'.*
20 *Reverse engineering is het onderzoeken van een product om daaruit af te leiden wat de specificaties en eisen zijn en/of om de werking te achterhalen.*

defensieve militaire activiteiten in het grensgebied. Interne tegenstanders van het regime worden gemarginaliseerd en de oppositie wordt onderling uitgespeeld. Hoewel de onderhandelingen tussen regime en oppositie beperkte successen hebben geboekt, zijn er geen aanwijzingen dat het regime bereid is tot substantiële concessies die bijdragen aan eerlijke en vrije verkiezingen. Daarnaast ontbeert het de oppositie de middelen om druk op het regime uit te oefenen. Zij zijn daarbij volledig afhankelijk van de Verenigde Staten, die ook direct met het regime onderhandelt.

Het Venezolaanse regime is steeds succesvoller in het uitonderhandelen van sanctieverlichting. In 2023 zijn onder andere de restricties op de olie-export (tijdelijk) opgeheven. Het Maduro-regime heeft dit voor elkaar gekregen zonder het eigen machtsmonopolie aan te tasten. Ondanks de gestegen olie-inkomsten blijft het regime ver van ingrijpende hervormingen van de economie. Hierdoor blijft de sociaaleconomische situatie voor de meeste Venezolanen kwetsbaar.

In 2023 vierde de Venezolaanse marine haar 200ste verjaardag. De viering hiervan ging gepaard met een renovatie van de vloot. Voor veel schepen betekende dit slechts cosmetische ingrepen, maar enkele *Guaiqueri*-klasse *Ocean-going Patrol Vessels* zijn bewapend met nieuwe antischeepsraketten. Ook zijn er nieuwe oppervlakte-eenheden aangeschaft, waaronder een nieuw kustwacht patrouillevaartuig, een logistiek ondersteuningsschip en enkele snelle aanvalsboten met antischeepsraketten. De overige Venezolaanse krijgsmachtonderdelen maakten minder grote ontwikkelingen door dit jaar. Ondanks dat er meer financiële middelen beschikbaar zijn voor investeringen in de krijgsmacht ten opzichte van voorgaande jaren, blijft de Venezolaanse krijgsmacht kampen met personeelstekorten, gebrekkige opleiding en achterstallig onderhoud. Gemiddeld genomen blijft het gereedstellingsniveau daarom laag. Venezuela blijft ook op het gebied van militaire samenwerking toenadering zoeken tot partnerlanden als Iran, Rusland en China .
Het Venezolaanse regime heeft al jaren geen volledige controle meer over het gehele grondgebied en luchtruim. Naast de politie en het leger kent het land een conglomeraat van allerlei irreguliere gewapende groeperingen met uiteenlopende loyaliteiten, zoals guerrillagroeperingen, paramilitairen en overige criminele bendes die met geweld de macht hebben overgenomen in bepaalde wijken, steden en regio's.

Contraproliferatie

De Unit Contraproliferatie (UCP) van de MIVD en de AIVD vierde in 2023 zijn vijftienjarig jubileum. Sinds 2008 doet de UCP onderzoek naar massavernietigingswapenprogramma's in zogeheten landen van zorg (Russische federatie, Iran, China, Noord-Korea, Syrië) en levert een bijdrage om dit te voorkomen. Deze landen blijven zoeken naar manieren om westerse technologie en kennis te verwerken in hun programma's. 2023 kenmerkt zich door de verharding van eerdergenoemde landen ten opzichte van internationale controleorganen, zoals het Internationaal Atoomagentschap (IAEA) en de Organisatie voor het Verbod op Chemische Wapens (OPCW), en dysfunctie in exportcontroleregimes, zoals de *Nuclear Suppliers Group* (NSG) en de *Missile Technology Control Regime* (MTCR). Dit ondermijnt de internationale verdragen over non-proliferatie, zorgt voor blokvorming tussen verschillende landen en resulteert in verdere internationale polarisatie.

Internationale controleorganen

Internationale controleorganen zijn ervoor om de proliferatie van massavernietigingswapens te voorkomen en/of in te perken, zonder dat dit ten koste gaat van de ontwikkeling van civiele programma's. Het IAEA, een onafhankelijke VN-organisatie, voert bijvoorbeeld inspecties uit in landen die nucleaire activiteiten ontplooien. De OPCW in Den Haag voert wereldwijde inspecties uit om te controleren of verdragstaten de bepalingen van de *Chemical Weapons Convention* hebben geïmplementeerd en naleven. Beide organisaties streven bevordering van vreedzaam gebruik in civiele programma's na. Voor het BTCW (*Biological Toxin Weapons Convention*) bestaat vooralsnog geen organisatie zoals de IAEA en OPCW.
Om vreedzaam gebruik te bevorderen maken landen afspraken in meerdere exportcontroleregimes. De NSG maakt afspraken over exportcontrole

van nucleaire *dual-use* technologie. De MTCR doet dit voor raketten en rakettechnologie en de AG (*Australia Group*) voor voor *dual-use* op het chemische en biologische vlak. Middels het Wassenaar Arrangement worden conventionele militaire en *dual-use*-goederen gecontroleerd.

Toename gelegenheidscoalities

Nederland is producent van hoogwaardige goederen en kennis en doet mee in de kopgroep van landen die inzetten op de ontwikkeling van nieuwe technologieën. Om deze technologieën te bemachtigen zetten landen van zorg complexe verwervingsstructuren op. Waar export-controleregimes onder druk staan, wordt er meer op nationaal en bilateraal niveau in gelegenheidscoalities gewerkt aan verscherpte controles en uitbreiding van sancties. Ondanks deze maatregelen zijn landen van zorg nog steeds in staat technologie te importeren.

Zo ziet de UCP dat sinds de EU-sancties op Rusland zijn opgelegd en uitgebreid, strategische (*dual use*) goederen steeds meer via omleidingslanden, zoals de Verenigde Arabische Emiraten, China, Turkije, India en Kazachstan, alsnog naar Rusland gaan, wat het tegenhouden van deze handel enigszins bemoeilijkt. In sommige gevallen betreffen dit ook goederen uit Nederland.

De UCP heeft het afgelopen jaar middels inlichtingenberichten en ambtsberichten andere overheidsinstanties op de hoogte gebracht van het bestaan van verschillende Iraanse en Russische verwervings-netwerken. Dit heeft geresulteerd in diplomatieke, bestuursrechtelijke en strafrechtelijke maatregelen.

Iran

Het nucleaire programma van Iran is ook in het afgelopen jaar een punt van aandacht geweest, onder andere door de moeizame samenwerking tussen Iran en het kernenergie-agentschap van de VN (het IAEA). Zo verwijt Iran het IAEA ervan politiek gemotiveerd te handelen en perkt het de controlemogelijkheden van het agentschap steeds verder in.

Zo beperkt Iran de toegang van het IAEA tot relevant geachte locaties, wordt data van IAEA-monitoringsapparatuur niet toegankelijk gemaakt en werd de accreditatie van een groep inspecteurs ingetrokken. Deze ontwikkelingen hebben ertoe geleid dat het IAEA in september heeft aangegeven zonder samenwerking van Iran niet in staat te zijn om te verifiëren dat het nucleaire programma van Iran uitsluitend vreedzame doeleinden dient.

In 2023 heeft Iran haar ballistische raketcapaciteiten verder uitgebreid met onder andere de *Fattah II* raket, door Iran omschreven als een hypersone ballistische raket. Op 18 oktober zijn de restricties op het importeren en exporteren van rakettechnologie door Iran verlopen. Deze restricties zijn in 2015 ingesteld als onderdeel van het *Joint Comprehensive Plan of Action*, de "nucleaire deal". EU heeft deze restricties (unilateraal) wel voortgezet. Op 17 oktober 2023, een dag daarvoor, stelde het Russische ministerie van Buitenlandse Zaken dat handel op rakettechnologie nu volgens de daarvoor geldende Russische richtlijnen mocht plaatsvinden, zonder betrokkenheid van de VN-Veiligheidsraad. Dergelijke handel zou een verdere stap zijn in de militaire samenwerking tussen Rusland en Iran.

Noord-Korea

Ook Noord-Korea heeft felle kritiek geuit op het IAEA en het orgaan ervan beschuldigd een spreekbuis van Washington te zijn. Net als in het voorgaande jaar heeft Noord-Korea zich daarnaast ook dit jaar weer bediend van vergaande nucleaire retoriek. Dit ging verder dan woorden alleen: in maart 2023 presenteerde Noord-Korea middels foto's aan de buitenwereld een nieuw ontwikkelde kernkop, die bedoeld zou zijn voor tactische nucleaire inzet.

Noord-Korea heeft daarnaast in 2023 voor het eerst een intercontinentale ballistische raket gelanceerd die gebruikmaakt van vaste brandstof. Daarmee zet het stappen naar een geavanceerder arsenaal aan raketten dat de NAVO kan bedreigen. Tevens heeft Noord-Korea een nieuwe onderzeeër voor tactische nucleaire wapens gepresenteerd en heeft

daarnaast twee onsuccesvolle pogingen gedaan om een militaire satelliet te lanceren. In de tussentijd heeft Noord-Korea ook de banden met Rusland aangehaald middels bezoeken van Kim Jong-un aan Rusland en van de Russische minister Sjojgoe van Defensie en minister Lavrov van Buitenlandse Zaken aan Noord-Korea.

Syrië en Rusland

Het bezitten en de ontwikkeling van chemische wapens voor offensieve doeleinden is een directe schending van de *Chemical Weapons Convention*. De Unit Contraproliferatie heeft in het afgelopen jaar het onderzoek naar Syrië en Rusland op dit thema voortgezet. De UCP onderzocht de huidige intenties en capaciteiten van het Syrische regime met betrekking tot chemische wapens. Hiertoe wordt onderzocht hoe diverse methodes voor de productie van chemische agentia[21] gebruikt kunnen worden om de herleidbaarheid naar een actor te beperken. Daarnaast is onderzocht hoe Syrië omgaat met OPCW-inspecties. Onderzoeken van de OPCW stagneren door een toenemende polarisatie tussen lidstaten en de moeizame samenwerking tussen Syrië en de OPCW. Ondanks dat de OPWC concludeert dat het Syrische regime verantwoordelijk is voor meerdere gifgasaanvallen, zijn er internationaal beperkt mogelijkheden om de verantwoordelijken hiervoor te berechten.

In het onderzoek naar het Russische chemische wapenprogramma is veel aandacht uitgegaan naar het scherper in kaart brengen van de huidige en in ontwikkeling zijnde Russische chemische wapencapaciteiten. Dat Rusland blijft investeren in onderzoek naar chemische wapens blijkt onder andere uit de constante stroom aan (wetenschappelijke) publicaties en de investeringen die Rusland doet in zijn chemische wapen gerelateerde (onderzoeks-)faciliteiten. Daarnaast onderzocht de UCP de inzet van *riot control agents*[22] in de oorlog tussen Rusland en Oekraïne. De inzet van deze stoffen als onderdeel van oorlogsvoering is verboden onder de *Chemical Weapons Convention*.

Dual-use karakter van biologische capaciteiten

Het bezit en de ontwikkeling van biologische wapens voor offensieve doeleinden is een directe schending van het Biologische en Toxine Wapenverdrag (BTWC). Onderzoek naar de schending van dit verdrag is complex omdat biologische capaciteiten over het algemeen *dual-use* zijn. Dit houdt in dat de capaciteiten die voor regulier defensief biologisch onderzoek gebruikt worden, ook gebruikt kunnen worden wanneer er offensieve intenties zijn.

Daarnaast volgen de ontwikkelingen in de biotechnologie en synthetische biologie elkaar snel op. Hiermee nemen de mogelijkheden voor *dual-use*-gebruik van deze technieken toe en verandert het perspectief op traditionele biologische wapens. De UCP onderzoekt hiertoe de capaciteiten en activiteiten van zowel Rusland als China. Dit is een uitbreiding op het lopende onderzoek naar het militaire biologische programma van Rusland.

Contra-inlichtingen (CI) en spionage

Extremisme en terrorisme in relatie tot de krijgsmacht

Eén van de taken van de MIVD is het verrichten van onderzoek naar dreigingen van extremisme en terrorisme in relatie tot Defensie. In 2023 heeft de MIVD dit onderzoek vooral gericht op rechts-extremisme en anti-institutioneel extremisme. De focus van het onderzoek ligt op dreigingen tegen Defensie en op dreigingen vanuit defensiemedewerkers richting de democratische en internationale rechtsorde. Op basis van dit onderzoek heeft de MIVD belanghebbenden in staat gesteld om maatregelen te treffen, zowel tegen specifieke personen als op het gebied van beleidsontwikkeling.

Rechts-extremisme

De MIVD heeft in 2023 wederom onderzoeken opgestart naar mogelijke rechts-extremisten. Het aantal onderzoeken naar mogelijke rechts-extremisten die voor Defensie wilden werken (sollicitanten, etc.) is in 2023

21 *Chemische agens: elk chemisch element of elke chemische verbinding zoals deze in natuurlijke staat voorkomt of het resultaat is van een productie.*

toegenomen ten opzichte van 2022. Daarnaast is het aantal onderzoeken naar mogelijk rechts-extremistische defensiemedewerkers (reeds in dienst) in 2023 juist afgenomen. De aard van het gedachtegoed van de personen in onderzoek bij de MIVD verschilt. Bij sommigen blijkt daadwerkelijk sprake te zijn van rechts-extremisme. In andere gevallen is soms eerder sprake van meeloopgedrag, ernstige normvervaging. De MIVD heeft bij geen van de onderzoeken indicaties dat hier personen tussen zitten met terroristische intenties.

De MIVD heeft sinds begin 2022 meer zicht gekregen op kritische geluiden uit rechts-extremistische kringen over Defensie. Dat beeld zet zich in 2023 voort. De kritiek van sommigen richt zich bijvoorbeeld op het door Defensie gevoerde diversiteitsbeleid. Ondanks deze kritiek op Defensie als werkgever ziet de MIVD geen afname van het aantal personen uit rechts-extremistische kringen dat een baan bij de krijgsmacht ambieert. De krijgsmacht oefent dan ook een blijvende aantrekkingskracht uit op rechts-extremisten. Zo blijkt vaak dat ze een baan bij de krijgsmacht in algemene zin goed voor hun ontwikkeling vinden, bijvoorbeeld vanwege de discipline en/of de fysieke training die militairen ondergaan.

Anti-institutioneel extremisme

Anti-institutioneel extremisten geloven dat er een kwaadaardige elite aan de macht is die het volk ernstig onderdrukt. Deze kwaadaardige elite zou hiervoor instituties gebruiken zoals de overheid, de media en de wetenschap. Sommige anti-institutioneel extremisten zien Defensie als onderdeel van de kwaadaardige elite of doen een beroep op militairen om in actie te komen en het volk tegen die elite te beschermen. Dit levert een dreiging op voor de krijgsmacht, de rechtstaat en de democratische rechtsorde. De MIVD heeft in 2023 defensiemedewerkers onderkend die dit gedachtegoed aanhangen en uitdragen. Waar nodig zijn op basis van inlichtingen van de MIVD passende maatregelen getroffen door het bevoegd gezag tegen deze medewerkers.

Spionage statelijke actoren

De MIVD voert onderzoek uit naar de (heimelijke) activiteiten van Iraanse militaire- en civiele inlichtingendiensten gericht op de verwerving van kennis en middelen die een dreiging vormen voor de veiligheid, paraatheid en inzetbaarheid van de krijgsmacht in nationaal of internationaal verband, voor de defensie-industrie en voor militaire bondgenootschappelijke organisaties als de NAVO. Onderzoek in 2023 heeft opgeleverd dat Iraanse activiteiten tegen Defensie op opportunistische basis plaats blijven vinden. Afhankelijk van actuele ontwikkelingen, specifieke activiteiten en aanwezigheid van de Nederlandse krijgsmacht in aandachtsgebieden van Iran is sprake van verhoogde interesses en activiteiten van Iraanse inlichtingendiensten richting Defensie en NAVO-bondgenoten.

Ook in 2023 deed de MIVD onderzoek naar de dreiging van spionage (inlichtingen)activiteiten van andere landen anders dan de hiervoor specifiek beschreven landen. Deze landen trachten hierbij de positie van de Nederlandse krijgsmacht binnen multilaterale samenwerkingsverbanden te bepalen of proberen specifieke kennis over Defensie of de defensie-industrie te bemachtigen.

De Noord-Koreaanse cyberspionagedreiging richting Nederland is primair gericht op organisaties in de crypto-sector, hoogwaardige technologie met militaire toepassing en onderzoekers gespecialiseerd in Noord-Korea. Het stelen van cryptovaluta is interessant voor Noord-Korea om de opgelegde sancties te kunnen omzeilen en het Noord-Koreaanse cyber- en kernwapenprogramma te financieren.

22 *Traangassen gebruikt om tegenstanders tijdelijk uit te schakelen door irritatie van de ogen, mond, keel, longen en huid.*

1.2 *Missieondersteuning en aandachtsgebieden*

De MIVD ondersteunt wereldwijd de inzet van de Nederlandse strijdkrachten in missiegebieden. In 2023 heeft de MIVD de volgende missies ondersteunt:

- Irak: *Operation Inherent Resolve* (OIR) en aan de *NATO Mission Iraq* (NMI).
- Perzische Golf en de Straat van Hormuz: *European-led Maritime Awareness Mission in the Strait of Hormuz (EMASOH).*
- Sudan: evacuatieoperatie uit Sudan.
- Inzetlocaties met een beperkte omvang:
  - Libië, Libanon, VN-missie Golan en Bosnië.
- Nederlandse inzet in het kader van de bescherming van het NAVO-grondgebied (Litouwen, Roemenië, Bulgarije, Oostelijk Middellands Zeegebied en de Baltische staten).
- Inzet op Nederlands grondgebied ter ondersteuning van de NAVO.
- Ondersteuning van overige *non-foreseeable Operations.*

Ter voorbereiding op de ontplooiing van Nederlandse troepen in het buitenland maakt de MIVD inlichtingenproducten, zoals dreigings-appreciaties, ten behoeve van de militaire inzet en de politieke besluitvorming die daarmee gemoeid is. Tijdens de missie verricht de MIVD onderzoek naar aspecten die relevant zijn voor *threat to the force* (de directe dreiging tegen Nederlandse militairen in een inzetgebied en coalitie) en *threat to the mission* (bedreigingen voor het succesvol kunnen uitvoeren van de missie, zoals dreiging tegen het nationale politieke draagvlak in het land van inzet of factoren van invloed op het effectief optreden van eenheden). Het oogmerk is het tijdig en volledig informeren van de militaire commandant en de verantwoordelijke besluitvormer over relevante dreigingen die uitgaan van statelijke en niet-statelijke actoren in de zogeheten *Area of Responsibility* (gebied waarvoor men verantwoordelijk is).

Balkan

Na de Russische invasie in Oekraïne is het Westen beducht op een additionele Europese brandhaard in de Balkan. In Bosnië en Herzegovina bleven ondanks de sterke etno-nationalistische retoriek van vooral Bosnisch-Servische zijde, grootschalige incidenten en sociale onrust uit. Het niet starten van toetredingsgesprekken tot de EU, omdat er niet aan vastgestelde criteria wordt voldaan, leidt bij de bevolking tot frustratie en daar wordt in de retoriek van Bosnisch-Servische zijde dankbaar gebruik van gemaakt. Ook tekent zich een verharding af in de (vaak separatistische) retoriek en handelingen van Republika Srpska-president Milorad Dodik. Zo bekrachtigde hij in 2023 een aantal wetten in de Republika Srpska (RS) die het centrale Bosnische gezag en de invloed van de Hoge Vertegenwoordiger (HV) Christian Schmidt moeten inperken.

In Noord-Kosovo blijft het onrustig. De spanningen passen binnen een trend waarbij ondermijnende activiteiten vanuit Servische (en/of Kosovaars-Servische) zijde toenemen en waar de Kosovaarse regering vanuit Pristina probeert, in het kader van de aanpak van corruptie en georganiseerde misdaad, zijn autoriteit in Noord-Kosovo te doen gelden. De verwachting is dat dergelijke spanningen periodiek oplaaien totdat Kosovo en Servië in het kader van de Belgrado-Pristina dialoog (door de EU geleid) tot een duurzaam vergelijk komen.

Afrika

Nederland was in 2023 betrokken bij de Sahel-regio met onder meer militaire, politie- en civiele bijdragen aan VN- en EU-missies. Defensie was met een aantal staffunctionarissen en trainingsmissies actief in het gebied. De MIVD heeft deze inzet ondersteund met strategische analyses over de politieke stabiliteit en actuele dreigingsbeelden. Het onderzoek van de MIVD richt zich op het tijdig onderkennen en signaleren van strategische en veiligheidsrelevante ontwikkelingen die een (potentiële) dreiging vormen ten aanzien van de nationale veiligheid, Nederlandse belangen en/of (potentiële) missies van de EU.

Mali, Burkina Faso en Niger behoren tot de minst ontwikkelde landen ter wereld. Extreme armoede, zwakke staatscapaciteiten, corruptie, oude kastestructuren en etnische spanningen, onder andere door achterstelling van bevolkingsgroepen, komen veel voor. Door een combinatie van klimaatverandering en een sterke bevolkingsgroei ontstaat steeds vaker schaarste aan primaire levensbehoeften. In alle drie de landen hebben militairen de macht gegrepen.

In 2023 kenmerkte de politieke situatie in de Sahellanden zich, net als in 2022, door grote instabiliteit. In Mali verslechterde de veiligheids-situatie verder toen gevechten tussen de alliantie van Noord-Malinese separatistische milities en de Malinese strijdkrachten in september oplaaiden. In november slaagden de Malinese veiligheidstroepen erin, met essentiële steun van de Russische *private military company Wagner*, de stad Kidal, de officieuze hoofdstad van de milities, in te nemen.

In Burkina Faso bleef de veiligheidssituatie slecht en de politieke situatie instabiel. De in 2022 met een staatsgreep aan de macht gekomen president Traoré slaagde erin in 2023 aan de macht te blijven, maar niet om de situatie in het land op enigerlei vlak te verbeteren. Ook in Burkina Faso zochten de machthebbers naar mogelijkheden in samenwerking met Rusland. Zo vond er op 31 augustus een officieel bezoek plaats van een Russische militaire delegatie.

In juli 2023 vond in Niger een staatsgreep plaats. In de ochtend van 26 juli blokkeerden Nigerese militairen van de Presidentiële Garde de toegang tot het Presidentiële Paleis. In de nacht van 26 op 27 juli kondigde een groep militairen onder de naam *Counsel Nationale pour la Sauvegarde de la Patria* (CNSP) aan dat de regering van Mohamad Bazoum wordt beëindigd. De regering onder Bazoum was georiënteerd op het Westen. Al snel na de staatsgreep bleek dat de Nigerese juntaleiders, net als eerder in Mali en Burkina Faso, sterke anti-Franse sentimenten koesteren en pro-Russisch georiënteerd zijn.

Midden-Oosten

Bij de inlichtingenondersteuning voor de missies in het Midden-Oosten ligt het zwaartepunt in Irak, waar Nederland bijdraagt aan *Operation Inherent Resolve* (OIR) en aan de *NATO Mission Iraq* (NMI). Op 15 december 2022 is door het kabinet besloten om de Nederlandse missie in Irak tot ten minste eind 2023 te verlengen. De MIVD bijdrage aan OIR is inmiddels grotendeels afgebouwd ten behoeve van een grotere deelname in NMI. Het kabinet heeft besloten tot een aanvullende militaire bijdrage aan NMI van mei 2024 tot mei 2025 die bestaat uit een Nederlandse commandant, ongeveer vijftien personen aanvullende staf, drie transporthelikopters inclusief personeel en 145 militairen t.b.v. *force protection*.

Daarnaast heeft de MIVD dit jaar inlichtingenondersteuning verleend aan de Nederlandse bijdrage aan de missie *European-led Maritime Awareness Mission in the Strait of Hormuz* (EMASOH) in de Perzische Golf en de Straat van Hormuz. De bijdragen voor kleinere missies in het Midden-Oosten, zoals de inzet in VN-missies op de Golan en in Libanon, geschiedt in de vorm van dreigingsappreciaties, met een focus op veiligheid van het Nederlandse personeel in deze missies.

ISIS

Ook in 2023 heeft ISIS in Irak en Syrië personele en materiele verliezen geleden als gevolg van de aanhoudende druk van de verschillende veiligheidstroepen gesteund door de anti-ISIS-coalitie. In 2023 heeft de afname van aanslagen door ISIS in Irak zich verder voortgezet. In de maanden oktober, november en december 2023 zijn er zelfs meerdere weken verstreken zonder dat er aanslagen zijn gepleegd. De aanslagen die ISIS wel uitvoerde waren veelal kleinschalig, waarbij eenvoudige hit & run-tactieken werden toegepast. De meest incidenten komen voor in Centraal Irak. Gezien het grensoverschrijdende karakter van de activiteiten van ISIS en (ondersteuning van) inzet van bondgenoten kijkt de MIVD ook naar Syrië.

Politiek

Na de regeringsformatie in oktober 2022 werd de Iraakse politiek gekenmerkt door een periode van relatieve stabiliteit. Premier Al-Sudani wist enkele kleinschalige successen te behalen, grootschalige structurele problemen blijven echter onopgelost. Aanhoudende maatschappelijke onvrede door een gebrek aan onder andere voldoende basisvoorzieningen en werkgelegenheid resulteert geregeld in demonstraties in geheel Irak.

Sinds oktober 2023 wordt de Iraakse buitenlandse politiek met name bepaald door de oorlog tussen Israël en Hamas. Iraakse hoogwaardigheidsbekleders, zoals premier Al-Sudani, grootayatollah Al-Sistani en afgevaardigden van het grootste politieke blok, het *Shia Coordination Framework* (SCF), riepen vrijwel direct na de aanval op tot solidariteit met het Palestijnse volk. De meest zichtbare steunbetuiging werd georganiseerd door de sjiitische politicus Muqtada al-Sadr, in de vorm van een grote demonstratie op het Tahrirplein in Bagdad. Muqtada al-Sadr is in 2023 niet teruggekeerd in de Iraakse politiek, maar demonstraties van zijn aanhangers droegen bij aan aanhoudende zichtbaarheid van zijn beweging.

> Op 29 juni en 20 juli hebben honderden aanhangers van Al-Sadr gewelddadige betogingen gehouden bij de Zweedse ambassade in de Internationale Zone (IZ) in Bagdad. Aanleiding was de verbranding van een Koran door een Iraakse vluchteling in de Zweedse hoofdstad Stockholm. Bij de demonstratie in juli wisten betogers zich toegang te verschaffen tot het ambassadeterrein en richtten vernielingen aan in het ambassadegebouw.

Veiligheid i.r.t. de missie in Irak

In de periode januari – september 2023 hebben er zich geen noemenswaardige geweldsincidenten voorgedaan tegen de westerse militaire presentie in Irak en Syrië. Aan Iran gelieerde milities gaven de voorkeur hun macht te verstevigen op het Iraakse politieke toneel. In oktober 2023 is hier een kentering in gekomen. Mede in reactie op de opstelling van de Verenigde Staten in de oorlog tussen Israël en Hamas hebben aan Iran gelieerde milities hun aanvallen op coalitiebases in Irak en Syrië hervat. Vanaf 18 oktober 2023 vonden er op bijna dagelijkse basis aanvallen plaats.

Premier Al-Sudani heeft deze drone- en raketaanvallen meermaals veroordeeld. Ook bevestigt de Iraakse regering de steun voor de aanwezigheid van buitenlandse troepen ter versterking van de Iraakse veiligheidssector. De opstelling van Al-Sudani raakt de reeds bestaande politieke spanningen over de aanwezigheid van Amerikaanse- en coalitietroepen in Irak. De aanwezigheid van Amerikaanse-en coalitietroepen wordt door Al-Sudani nog steeds publiekelijk gesteund, maar ook uitgesproken tegenstanders maken deel uit van de regering. De huidige ontwikkelingen dragen bij aan toenemende interne spanningen in de Iraakse politiek en een verhoogde dreiging voor de westerse militaire en diplomatieke presentie.

Iran

Hoewel er afgelopen jaar binnen Iran vrijwel wekelijks sprake was van kleinschalige tegen het regime gerichte demonstraties en het land nog onverkort kampt met economische tekorten, blijft Iran een dominante machtsfactor in het Midden-Oosten. Zo speelden het Iraanse regime en daaraan gerelateerde instituties en milities in 2023 op politiek en veiligheidsgebied een belangrijke rol in Irak, Syrië en Libanon. Deels via deze landen ondersteunt Iran ook vanuit de Gaza-strook en de Westoever opererende milities zoals Hamas en de Palestijnse Islamitische Jihad (PIJ).

Mede dankzij de bemiddeling van China zijn de diplomatieke banden tussen Iran en Saoedi-Arabië sinds het voorjaar van 2023 iets verbeterd. Niettemin blijven de contacten tussen deze landen vooralsnog fragiel. Ook de pogingen van Iran om de samenwerking met regionale economische instituties zoals *Gulf Cooperation Council* (GCC) te verbeteren waren in 2023 nog niet erg succesvol. Op veiligheidspolitiek gebied probeerde Iran tot medio september, met propaganda, intimidatie en diplomatie een toenadering tussen Israël en diverse landen uit de regio,

waaronder Saoedi-Arabië, te voorkomen. De aanval door Hamas op Israël op 7 oktober en de heftige publieke reacties in vele landen in de regio op de voortgaande Israëlische militaire inzet op de Gazastrook hebben er voor gezorgd dat het voorgenomen akkoord tussen Saudi Arabië en Israël, waarbij de relatie tussen beide landen genormaliseerd zou worden, voorlopig uitblijft.

Iraanse invloed in Irak en Syrië

Iran heeft nog steeds op vele gebieden grote invloed op de (veiligheids-) politieke ontwikkelingen in Irak. Iran vormt daarnaast nog steeds een cruciale steunpilaar voor het Syrische (Assad)-regime. Iran ondersteunt de bijna dagelijkse drone- en IDF-aanvallen door sjiitische milities die sinds 18 oktober 2023 op en nabij Amerikaanse en coalitiebases in Irak en Syrië worden uitgevoerd.

Iraanse banden met Rusland

Iran werkt op diverse gebieden (o.a. op diplomatiek en veiligheidsgebied) samen met Rusland. Zo is het aanleveren van diverse door Iran geproduceerde Unmanned Aerial Systems (UAS) en componenten daarvan ten behoeve van de Russische aanvallen op Oekraïne verder geïntensiveerd.

Maritiem

Sinds het voorjaar van 2023 waren er diverse keren spanningen tussen Iran en de Verenigde Staten omtrent de vrije doorgang van de Perzische Golf, de Straat van Hormuz en de Golf van Oman. Zo zijn er meerdere incidenten geweest waarbij de *Islamic Republic of Iran Navy* (IRIN), dan wel *Islamic Revolutionary Guard Corps Navy* (IRGCN), Iran koopvaardijschepen met Amerikaanse banden en/of Israëlische banden, hebben bedreigd en soms in beslag heeft genomen. Enkele van deze tankers hebben, volgens Iran, zonder Iraanse toestemming binnen Iraanse territoriale wateren gevaren.

Na de start van de oorlog in Gaza is de Houthi-beweging vanuit Jemen begonnen met het uitvoeren van aanvallen op Israëlische doelen. Sinds 19 november 2023 valt de Houthi-beweging koopvaardijschepen in de Rode Zee en de Golf van Aden aan met een veronderstelde Israëlische link. De Houthi's beschikken over een uitgebreid arsenaal aan wapens om aanvallen op maritieme of landdoelen uit te voeren. De Houthi-beweging maakt gebruik van verschillende drones, ballistische anti-schipraketten en antischipkruisvluchtwapens om aanvallen uit te voeren op doelen in het Rode Zeegebied. Iran onderhoudt al jarenlang contacten met de Houthi's en ondersteunt hen onder andere met wapenleveranties en technische expertise.

Current Intel

Naast de strategische dossiers van de specifieke teams heeft de MIVD ook aandacht voor gebieden die buiten de GA vallen. Gedurende 2023 is de hiervoor opgezette Current Intelligence Unit (CIU) ingezet voor inlichtingen-ondersteuning van binnen- en buitenlandse inzet (oefeningen en operaties) van Defensie. De CIU ondersteunde onder meer de evacuatie-operatie uit Sudan.

> Kort na de uitbraak van gevechten tussen rivaliserende delen van het veiligheidsapparaat in Sudan in april 2023, werd duidelijk dat een evacuatie van ca. 250 Nederlanders op korte termijn noodzakelijk was. De MIVD heeft tijdens de evacuatie ondersteuning geboden door het in kaart brengen van vijandige activiteiten, capaciteiten en intenties teneinde de besluitvorming en uitvoering van actuele informatie te voorzien. Daarbij is gebleken dat de MIVD binnen korte tijd in staat was tijdige, relevante en tactische inlichtingen te genereren. Hierdoor heeft de MIVD actief bijgedragen aan de veiligheid van Nederlanders in Sudan en het succes van de evacuatieoperatie.

De CIU is nauw betrokken bij de inlichtingenvoorziening aan de departementen inzake conflictgebieden en gebieden waar een dreiging zich manifesteert voor de Nederlandse belangen. De CIU blijft tevens betrokken bij de informatievoorziening aan de Nederlandse commerciële lucht- en scheepvaart alsmede de briefings voor de Directie Operaties (DOPS).

1.3. *Veiligheidsbevorderende taken*

Naast de strategische dossiers, aandachtsgebieden en de ondersteuning aan de missiegebieden, heeft de MIVD ook veiligheidsbevorderende taken. Nederlandse bedrijven, kennisinstellingen en wetenschappers zijn een potentieel doelwit van diverse statelijke actoren die (heimelijk) hoogwaardige, al dan niet militair relevante, technologie proberen te verwerven. Ook de vitale processen in Nederland zijn kwetsbaar voor sabotage door statelijke actoren middels (de gevolgen van) ongewenste investeringen en overnames. Staten kunnen door overnames van bedrijven die hoogwaardige technologie ontwikkelen of door investeringen in vitale infrastructuur, ongewenste afhankelijkheden creëren met risico's voor het functioneren van de Nederlandse economie en de nationale veiligheid. Daarmee is de continuïteit van onze vitale processen in het geding en dreigt het weglekken van kennis en vertrouwelijke of gevoelige informatie. In dit kader is ook de defensie-industrie kwetsbaar voor (economische) spionage, zowel in het fysieke als digitale domein. De MIVD draagt bij aan de weerbaarheid en veiligheid van Defensie en de defensie industrie.

Elektronische veiligheidsonderzoeken
Vanuit het Defensiebeveiligingsbeleid (DBB) wordt een aantal veiligheids-bevorderende normen gesteld die de exclusiviteit van informatie (met rubricering Stg. GEHEIM en hoger) bevorderen. Naast bouwkundige, organisatorische en beveiligingstechnische normen, stelt het DBB tevens de eis dat een ruimte waar dergelijke informatie besproken of verwerkt wordt, eens per twee jaar aan een Elektronisch Veiligheidsonderzoek (EVO) moet worden onderworpen. De MIVD voert niet alleen onderzoeken uit op bestaande ruimten maar brengt ook adviezen uit op 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 nationale partnerorganisatie binnen het vakgebied.

Economische veiligheid en strategische competenties
De Nederlandse economische- en veiligheidsbelangen zijn de afgelopen jaren toenemend blootgesteld aan een verscheidenheid van (statelijke) dreigingen. Hierbij gaat het met name om ongewenste kennis- en technologieoverdracht en strategische afhankelijkheden. Door de unieke hoogwaardige kennispositie die Nederland bezit op het gebied van onder andere halfgeleiders, kwantumtechnologie en lucht- en ruimtevaart blijft Nederland voor andere landen een interessant doelwit voor spionage en heimelijke overnames. Veel van deze hoogwaardige kennis en technologie zijn *dual-use* inzetbaar. Het weglekken van deze gevoelige kennis en technologie naar niet-bondgenoten vormt een risico voor de nationale veiligheid en de slagkracht van de Nederlandse krijgsmacht in het bijzonder.

De Nederlandse industrie is voor een aanzienlijk deel aangewezen op leveranciers uit derde landen. Dit kan risicovolle strategische afhankelijkheden met zich meebrengen. Een voorbeeld hiervan is de manier waarop Rusland de Europese energieafhankelijkheid gebruikt als (politiek) drukmiddel in de oorlog in Oekraïne. Ook kunnen bepaalde afhankelijkheden binnen de Nederlandse vitale infrastructuur een risico vormen voor de Nederlandse economische veiligheidsbelangen. Hoewel op dit moment nog geen daadwerkelijke sabotage van Nederlandse vitale infrastructuur heeft plaatsgevonden, is wel geconstateerd dat statelijke actoren actief zijn met het in kaart brengen van vitale processen. Een voorbeeld hiervan zijn de onderzeekabels en pijpleidingen die onderdeel uitmaken van onderzeese infrastructuur in het Nederlandse deel van de Noordzee.

In 2023 intensiveerden de MIVD en de AIVD de samenwerking op het gebied van economische veiligheid. De MIVD en de AIVD dragen vanuit de wettelijke taken bij aan het beschermen van de Nederlandse overheid, krijgsmacht, (defensie)industrie, vitale infrastructuur en kennisinstellingen tegen dreigingen die een risico vormen voor de

23 *De MIVD heeft zitting in de back-office van het Loket Kennisveilgheid.*

Nederlandse economische- en veiligheidsbelangen. De diensten hebben daarbij als doel het handelend vermogen van de Nederlandse overheid, krijgsmacht, (defensie)industrie, vitale infrastructuur en kennisinstellingen tegen spionage, ongewenste strategische afhankelijkheden en ongewenste kennis- en technologieoverdracht (van *dual-use* goederen) te vergroten.

Het kabinet heeft in 2023 verschillende maatregelen in gang gezet om de dreigingen tegen de economische veiligheid van Nederland tegen te gaan. De diensten hebben in 2023 in dat kader een bijdrage geleverd aan onder andere de Nationale Technologiestrategie, het Ondernemersloket Economische Veiligheid, de wet Veiligheidstoets Investeringen, Fusies en Overnames en het wetsvoorstel 'Screening Kennisveiligheid'[23] van het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).

Industrieveiligheid

Defensie is afhankelijk van een stabiele basis van kennisinstellingen en bedrijven die ervoor zorgen dat Defensie de juiste kennis, technologie en capaciteiten in huis heeft, om invulling te geven aan haar drie hoofdtaken.[24] De ontwikkelingen in de geopolitieke situatie hebben gezorgd voor een extra impuls voor Defensie en daarmee de Nederlandse defensie-industrie.

Bedrijven die de uitvoering op zich nemen van gerubriceerde of vitale defensieopdrachten, zijn gehouden aan de regeling Algemene Beveiligingseisen voor Defensieopdrachten (ABDO). De MIVD toetst bij deze bedrijven of de, in de ABDO gestelde, beveiligingseisen op orde zijn, voordat zij mogen starten met een gerubriceerde opdracht voor Defensie. Als de beveiliging voldoet aan de eisen, wordt een ABDO-autorisatie afgegeven voor die specifieke opdracht.

In 2023 is, net als in voorgaande jaren, een toename zichtbaar van het aantal afgegeven ABDO autorisaties voor bedrijven dat door verwervende instanties binnen Defensie, bedrijven, en buitenlandse partners worden aangevraagd. Om tot een autorisatie te komen begeleidt de MIVD de uitvoering van veiligheidsbevorderende maatregelen en houdt toezicht bij defensieorderbedrijven gedurende de looptijd van opdrachten ter beveiliging van gerubriceerde informatie en te beschermen belangen. Toezicht door de MIVD bij defensieorderbedrijven op de naleving van de beveiligingseisen wordt gedaan door het uitvoeren van audits en inspecties.

Gedurende de looptijd van de opdrachten onderhoudt de MIVD de relaties met de bedrijven waar deze opdrachten worden uitgevoerd. Bij nieuwe dreiging richting de defensie-industrie informeert de MIVD deze bedrijven en adviseert over additioneel te nemen maatregelen. Daarnaast houdt de MIVD nauw contact met de bedrijven wanneer er onverhoopt een incident optreedt en er mogelijk een gerubriceerde defensieopdracht geraakt is. De MIVD werkt daarbij samen met onder andere de AIVD, het Ministerie van Economische Zaken en Klimaat en het Nationaal Cyber Security Centrum (NCSC).
Internationaal heeft de MIVD haar positie als *Designated Security Authority* (DSA)[25] versterkt, met een focus op de mogelijkheden en onmogelijkheden binnen de (inter)nationale keten. Hierbij is rekening gehouden met de huidige geopolitieke ontwikkelingen, het dreigingsbeeld en de technologische vooruitgang. Hiermee heeft de MIVD de (inter)nationale positie van de Nederlandse defensie-industrie versterkt en de internationale *supply chain* veiliger en weerbaarder gemaakt.

In 2023 is de MIVD, in samenwerking met de AIVD, gestart met de transitie van de ABDO naar de ABRO, de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten. Vanuit een gezamenlijke unit zullen de MIVD en de AIVD industrieveiligheid vanuit een gemeenschappelijk eisenkader gaan uitvoeren voor de hele Rijksoverheid, het Ministerie van Defensie en de Nationale Politie. 2024 zal in het teken staan van het

24 *Drie hoofdtaken van Defensie: Beschermen van het eigen grondgebied en dat van bondgenoten; bevorderen van de (internationale) rechtsorde en stab liteit; ondersteunen van civiele autoriteiten en leveren van bijstand bij rampen en crises.*

25 *DSA: Toezichthouder op de beveiliging van internationale gerubriceerde informatie.*

oprichten van een Joint Unit Industrieveiligheid en het verder ontwikkelen van het nieuwe eisenkader.

Veiligheidsonderzoeken

Met de gezamenlijke Unit Veiligheidsonderzoeken (UVO) geven de MIVD en de AIVD uitvoering aan de taken op het gebied van de aanwijzing van vertrouwensfuncties en de uitvoering van veiligheidsonderzoeken als bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) en de Wet veiligheidsonderzoeken (Wvo).

De UVO doet veiligheidsonderzoeken naar (kandidaat-)vertrouwensfunctionarissen. Deze personen hebben door hun werkzaamheden toegang tot gerubriceerde informatie, of zijn in een positie waarin zij de nationale veiligheid kunnen schaden. Bijvoorbeeld bij de Rijksoverheid, Defensie, de burgerluchtvaart en bedrijven die aan vitale processen werken. Afhankelijk van de aard van de vertrouwensfunctie, die is gebaseerd op de mogelijke schade die de (aspirant) vertrouwensfunctionaris kan aanrichten aan de nationale veiligheid, wordt de diepgang van het veiligheidsonderzoek bepaald: A-, B-, of C-onderzoek. Een A-onderzoek is het meest diepgaand en wordt slechts ingesteld voor de meest kwetsbare vertrouwensfuncties. Een C-onderzoek is het minst diepgaande onderzoek. Na een positief afgerond onderzoek krijgt de kandidaat een Verklaring van Geen Bezwaar (VGB).

In 2023 heeft de UVO (inclusief mandaathouders[26]) in totaal 85.622 veiligheidsonderzoeken uitgevoerd en een beslissing genomen over het al dan niet verlenen van een VGB. Ten opzichte van het jaar 2022 betekent dit een volumetoename van 20,0% (t.o.v. 71.343 in 2022). De wettelijke termijn voor het veiligheidsonderzoek is acht weken (56 dagen). De UVO (incl. mandaathouders) heeft in 2023 86,6% van de gevallen besluiten genomen binnen de wettelijke termijn van acht weken. Het streven van 90% binnen acht weken is hiermee niet behaald[27]. Dit onder meer als gevolg van onverwachte groei van aanvragen en beperkte mogelijkheid van de UVO om snel capaciteit op te schalen. Van het totale aantal onderzoeken in 2023 zijn 41.548 onderzoeken uitgevoerd door de UVO zelf (19.671 door de AIVD en 21.877 door de MIVD) en 44.074 door de mandaathouders.

Deze groei is vooral te verklaren door de hogere instroom van personeel met name in de burgerluchtvaart en bij Defensie, en de algehele groei van het aantal vertrouwensfuncties. Daarnaast is de complexiteit van het veiligheidsonderzoek toegenomen, mede als gevolg van het buitenlandbeleid dat in 2021 is ingevoerd (Beleidsregel veiligheidsonderzoeken 2021) dat in circa tien procent van de onderzoeken een rol speelt.

Om in 2024 weer te voldoen aan de norm, heeft de UVO drie belangrijke maatregelen genomen: In de eerste plaats zet het doorlopend in op het vergroten van de capaciteit door werving en behoud van personeel. Ten tweede worden de afspraken met inzenders verduidelijkt om meer grip te krijgen op vraag en aanbod. In de derde plaats streeft de UVO naar een optimaal en uniform werkproces door het programma Modernisering Veiligheidsonderzoeken. Dit programma moet de MIVD en de AIVD in staat stellen adequaat te reageren op de reeds verwachte toenemende vraag naar veiligheidsonderzoeken, vooral door verregaande automatisering waardoor schaarse menselijke capaciteit kan worden ingezet voor complexe dossiers.

De unit is al langer bezig de werkprocessen te verbeteren om ook op de lange termijn de toenemende vraag naar veiligheidsonderzoeken aan te kunnen. In 2023 is daarom de elektronische Opgave Personele Gegevens (eOPG) uitgebreid. In 2023 heeft de UVO 66 procent van de aanvragen via eOPG ontvangen. Dankzij geautomatiseerde onderdelen en aangepaste processen kan de VGB-aanvraag sneller worden behandeld.

26 *Maandaathouders uitvoering Veiligheidsonderzoeken: Nationale Politie en de Koninklijke Marechaussee* **25** *DSA: Toezichthouder op de beveiliging van internationale gerubriceerde informatie.*
27 *De minister van Defensie en de minister van BZK hebben de Tweede Kamer, via een Kamerbrief, op 19 december geïnformeerd over het niet voldoen aan de norm.*

In het derde kwartaal van 2023 is Defensie aangesloten op automatisch alerteren (AA). Een systeem dat de UVO op de hoogte brengt als er bij een vertrouwensfunctionaris wijzigingen zijn in het Justitieel Documentatiesysteem, of als er nieuwe inlichtingeninformatie is over hem of haar die kan leiden tot intrekken van de VGB. Zo nodig doet de UVO dan een nieuw onderzoek. Met de aansluiting van Defensie is naar schatting inmiddels 85 procent van alle vertrouwensfunctionarissen aangesloten op AA.

In het vierde kwartaal van 2023 is begonnen met het geautomatiseerd opvragen bij externe instanties (o.a. Dienst Justitiële Inrichtingen (DJI)) van informatie die relevant is voor een VGB-onderzoek. De personele capaciteit die hiermee in de toekomst vrijkomt, wordt ingezet op complexere onderzoeken.

Herziening Wet veiligheidsonderzoeken (Wvo)
Deze wetswijziging draagt bij aan een toekomstbestendig veiligheids-onderzoek, bijvoorbeeld door het invoeren van een register voor vertrouwensfunctionarissen en van een locatiegebonden VGB voor de burgerluchtvaart en de vracht- en toeleveringsketen. Het wetsvoorstel ondersteunt de diensten bij het voldoen aan hun wettelijke verplichtingen met betrekking tot de doorlooptijden van veiligheidsonderzoeken.

De afdeling advisering van de Raad van State heeft in november 2023 advies uitgebracht over het wijzigingsvoorstel van de Wet veiligheids-onderzoeken. Het advies wordt verwerkt in het wetsvoorstel, dat in 2024 aan de Tweede Kamer ter behandeling wordt aangeboden.


EUROSTAR
KONINKLIJKE
MARECHAUSSEE

2 VERANTWOORDELIJK NAAR POLITIEK EN SAMENLEVING

De MIVD is verankerd in de democratische rechtsstaat. Om zo goed mogelijk zicht te krijgen op de intenties, capaciteiten en activiteiten van bepaalde landen, groeperingen en actoren die een (potentiële) dreiging kunnen vormen, heeft de MIVD de beschikking over verschillende bevoegdheden. De Wiv 2017 biedt de grondslag voor de inzet van die (bijzondere) bevoegdheden. De inmiddels aangenomen 'tijdelijke wet cyberoperaties' voor landen met een offensief cyberprogramma biedt een aanvulling op het wettelijk kader zoals in de Wiv 2017 is opgesteld en beoogt de meest urgente knelpunten op te lossen, vooruitlopend op een brede herziening van de Wiv 2017. De Tijdelijke wet is voor de dienst noodzakelijk in het licht van de toegenomen dreiging van landen met een offensief cyberprogramma. Politieke en maatschappelijke steun voor het werk van de MIVD en een breed gedragen vertrouwen in het verantwoord handelen van alle medewerkers zijn daarbij van essentieel belang. Waar mogelijk gaf de dienst in 2023 dan ook zo veel mogelijk openheid van zaken.

2.1 Leiding en toezicht

Bestuur en verantwoording

De MIVD valt onder directe verantwoordelijkheid van de secretaris-generaal (SG) van het ministerie van Defensie. De minister van Defensie legt verantwoording af aan het parlement over het werk van de MIVD. Wanneer dat in de openbaarheid kan, gebeurt dit in de Vaste Kamercommissie Defensie. Wanneer dat achter gesloten deuren moet, legt de minister verantwoording af aan de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD).

2.2 Een werkende wet voor een open en vrije samenleving

Algemeen

De Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) beschrijft de taken en bevoegdheden van de MIVD en de AIVD. Al een aantal jaar is duidelijk dat de wet niet toereikend is voor de moderne operationele praktijk van de diensten.

De MIVD en de AIVD brachten in 2023 een verslag uit over het functioneren van de diensten (AIVD/MIVD 2018-2023). Het verslag is een vereiste van de Wiv 2017 en beschrijft hoe de diensten de afgelopen vijf jaar zijn omgegaan met de veranderde dreigingen tegen Nederland en het nieuwe wettelijk kader waarbinnen ze werken.

Tijdelijke wet

Een effectief wettelijk kader dat aansluit bij de operationele inlichtingen-praktijk is essentieel voor de MIVD. In de uitvoering van de Wiv 2017 is de wet in een aantal gevallen onvoldoende duidelijk gebleken. In de praktijk leidt deze onduidelijkheid tot knelpunten bij de uitvoering. Om de meest prangende knelpunten weg te nemen is eind 2022 de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen naar de Tweede Kamer gestuurd. De Tijdelijke wet moet de diensten in staat stellen bestaande bevoegdheden effectiever en sneller in te zetten tegen cyberdreigingen. In oktober 2023 is het wetsvoorstel aangenomen door de Tweede Kamer, die op een nader te bepalen datum in 2024 in werking zal treden.

Onderzoeken van de diensten in het digitale domein hebben mede als doel het onderkennen van verborgen dreigingen. De diensten weten in zo'n geval dat er sprake is van een dreiging, maar nog niet precies hoe die dreiging zich manifesteert. Vaak komen deze dreigingen vanuit landen met een offensief cyberprogramma richting Nederland. Deze landen maken gebruik van veel verschillende onderdelen van de digitale infrastructuur en wisselen daar ook snel tussen. Om zicht te krijgen en te behouden op deze dreiging moeten de diensten daarom gelijktijdig verschillende soorten operaties starten en verschillende bevoegdheden inzetten.

De Tijdelijke wet moet de diensten in staat stellen hun bestaande bevoegdheden doeltreffend in te zetten, met bijbehorende effectieve waarborgen, om zo het zicht op landen met een offensief cyberprogramma gericht tegen Nederland te herstellen of op te bouwen. Bij de totstandkoming van de Tijdelijke wet is doorlopend aandacht geweest voor de uitvoerbaarheid.

Nota van wijziging op de tijdelijke wet t.b.v. bulkdatasets

Evenals in 2022 moesten de diensten bulkdatasets vernietigen terwijl deze nog operationele waarde hadden. Het staat niet ter discussie, ook niet voor de CTIVD, dat het gebruik van bulkdatasets door de AIVD en MIVD noodzakelijk is. Bulkdatasets stellen de AIVD en de MIVD in staat om bredere patronen en netwerken te onderkennen en daardoor nieuwe dreigingen in beeld te krijgen. Het oordeel van de afdeling klachtbehandeling van de CTIVD is vooral een bevestiging dat het huidige wettelijke kader van de Wiv 2017 onvoldoende ruimte laat voor een passende omgang met bulkdatasets door de AIVD en MIVD. In september 2023 is daarom een aanvulling op de Tijdelijke wet aangaande regeling betreffende bulkdata middels een nota van wijziging aan de Tweede kamer aangeboden. Deze nota van wijziging maakt inmiddels integraal deel uit van het wetsvoorstel dat de Eerste Kamer op 12 maart 2024 heeft aangenomen.

Met de nota van wijziging wordt beoogd een regeling te introduceren die de diensten de mogelijkheid biedt om jaarlijks de minister te verzoeken een bulkdataset, die met bijzondere bevoegdheden is verworven, langer te behouden. De CTIVD krijgt daarbij een bindende bevoegdheid om te oordelen over de rechtmatigheid van een eventuele verlenging. In de nota van wijziging wordt daarnaast een regeling voorgesteld voor een voorafgaand bindende toets door de Toetsingscommissie Inzet Bevoegdheden (TIB) op een door de minister verleende toestemming tot het *real time* verzamelen van verkeers- en locatiegegevens van personen waarnaar de dienst onderzoek verricht; de zogeheten 'stomme tap'. Het voorstel voor een nota van wijziging op de Tijdelijke wet is ter advisering aan de Afdeling Advisering van de Raad van State voorgelegd. Bij brief van 21 december 2023 is de Tweede Kamer geïnformeerd dat de CTIVD heeft aangegeven dat zij het vooruitlopend op de inwerkingtreding van de Tijdelijke wet vanuit haar toezichthoudende taak onder voorwaarden aanvaardbaar acht om bulkdatasets waarvan de termijn dreigt te verlopen, reeds te verwerken in lijn met de bepalingen in de Tijdelijke wet. De MIVD heeft hier reeds tweemaal gebruik van gemaakt. De Kamer is hierover geïnformeerd[28].

Wetswijziging

De Tijdelijke wet laat de noodzaak tot een bredere wijziging van de Wiv 2017 onverlet. In september 2023 is een hoofdlijnennotitie brede herziening Wiv 2017 naar de Tweede Kamer gestuurd. Hierin wordt een eerste richting gegeven aan de brede herziening, zo worden aanpassingen van de wet naar aanleiding van de aanbevelingen van de Evaluatiecommissie WIV 2017 (ECW)[29] uiteen gezet en verschillende opties gepresenteerd hoe toezicht in de toekomst effectiever georganiseerd kan worden.

De ECW concludeerde dat de Wiv 2017 onvoldoende aansluit op de technologische complexiteit en dynamiek van de operationele praktijk van de diensten. De Algemene Rekenkamer (AR) stelt dat de effectiviteit van de inlichtingendiensten onder druk staat door de effecten van de

28 *Betreft kamerstuk: Kamerstukken 36 263, nr. 37 en 36 263, nr. 38.*

29 *Kamerstukken 34 588, nr. 88.*

wet op de operationele slagkracht. Hierdoor kunnen de diensten hun wettelijke bevoegdheden onvoldoende effectief inzetten om dreigingen, met name in het cyberdomein, te onderkennen. De ECW en de AR hebben in hun rapporten aanbevelingen gedaan. Deze aanbevelingen worden meegenomen in de brede herziening van de Wiv 2017.

Toezicht

De Toetsingscommissie Inzet Bevoegdheden

De Toetsingscommissie Inzet Bevoegdheden (TIB) toetst bij de inzet van een aantal bijzondere bevoegdheden, nadat de minister daarvoor toestemming heeft verleend, of die toestemming rechtmatig is verleend. Het oordeel van de TIB is bindend. Indien de TIB van oordeel is dat de toestemming niet rechtmatig is verleend, kan een nieuw aangepast verzoek aan de minister en, na toestemming van de minister, opnieuw aan de TIB worden voorgelegd. Of dit wordt gedaan en wanneer, is afhankelijk van de onderbouwing van het oordeel van de TIB en de noodzaak van een inzet.

In 2023 is 6,1% van de bijzondere bevoegdheden die zijn beoordeeld door de TIB niet rechtmatig bevonden. In het onrechtmatigheidsoordeel van de TIB komt geregeld naar voren dat de noodzaak van de inzet ontbreken zou. Daarnaast zijn er juridische verschillen van inzicht met de TIB op wezenlijke gebieden zoals hack- en kabelbevoegdheid. Met de inmiddels aangenomen Tijdelijke wet wordt een belangrijk deel van deze onderwerpen verduidelijkt, opdat over de bedoeling van de wetgeving geen twijfel kan ontstaan. In het afgelopen jaar is de zelfstandige leesbaarheid van de toestemmingsverzoeken, die mede door de steeds grotere mate van technische en operationele details onder druk stond, verder verbeterd.

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD)

De CTIVD is een onafhankelijke commissie die de rechtmatige uitvoering van de Wiv 2017 door de MIVD en de AIVD beoordeelt. De commissie bestaat uit twee afdelingen; de afdeling Toezicht en de afdeling Klachtbehandeling. Deze laatste afdeling behandelt klachten over de MIVD en de AIVD en meldingen van een vermoeden van een misstand bij de MIVD of de AIVD.

De CTIVD trok in 2023 conclusies over hoe de MIVD en de AIVD omgaan met zogeheten kabelinterceptie: het onderzoeken van het dataverkeer dat door een specifieke internetkabel stroomt. De CTIVD hield in 2021 en 2022 verscherpt toezicht op die interceptie, omdat het toen om een relatief nieuwe bevoegdheid ging. Op 23 januari 2024 bood de CTIVD de uitkomsten van het onderzoek aan, aan de Eerste en Tweede Kamer. Volgens de CTIVD hebben de diensten laten zien dat zij de verzamelde gegevens in de eerste fase van het onderzoek behoorlijk en zorgvuldig kunnen verwerken. Ook oordeelt de toezichthouder dat de *compliance* zodanig op orde is dat de diensten klaar zijn voor uitbreiding van kabelinterceptie. De diensten moeten volgens de CTIVD wel nog meer inspanningen leveren voor de verdere verwerking van gegevens. De MIVD en de AIVD hebben daar het afgelopen jaar significante stappen in gezet. Parallel aan de uitbreiding van kabelinterceptie werken de diensten voortdurend aan het verder verbeteren van de processen.

De *pilot* inzake een afwegingskader waarmee aanschaf en inzet van *tooling* voor het verwerven van data kan worden beoordeeld, als gevolg van rapport 72 van de afdeling Toezicht van de CTIVD is in 2023 afgerond. De ministers van Binnenlandse Zaken en Koninkrijksrelaties en Defensie hebben de Tweede Kamer per brief van 24 oktober 2023 geïnformeerd over de uitkomsten ervan.[30]

De MIVD en de CTIVD hebben in 2023 op verschillende momenten op constructieve wijze contact gehad over de totstandkoming en implementatie van de Tijdelijke wet, erop gericht om de CTIVD zo goed mogelijk te faciliteren bij de uitvoering van haar toezichtstaak.

Algemene Rekenkamer en de Auditdienst Rijk

Het handelen van de dienst wordt op verschillende manieren onafhankelijk gecontroleerd. Onder meer door instanties als de Algemene Rekenkamer

30 *Betreft Kamerstuk 29 924, nr. 254.*

(AR) en de Auditdienst Rijk (ADR). De bevindingen van de AR en de ADR worden o.a. gedeeld met de CIVD.

Compliance- en risicomanagement

De Wiv 2017 stelt hoge eisen aan de manier waarop de MIVD op integere wijze haar gegevens verwerft en verwerkt. Dit is de zogeheten zorgplicht. Op de naleving hiervan moet worden toegezien en verantwoording kunnen worden afgelegd. Dit vergroot de transparantie en draagt bij aan het maatschappelijk vertrouwen. Het hele systeem van naleving, toezicht en verantwoording wordt ook wel het compliancestelsel genoemd. Een goed werkend compliancestelsel faciliteert bovendien de CTIVD in het uitvoeren van dynamisch (systeem)toezicht. De MIVD werkt samen met de AIVD aan een gemeenschappelijk compliancestelsel voor beide diensten. De diensten werken immers beiden volgens dezelfde wet en hebben dezelfde toezichthouder.

Het jaar 2023 stond voor een belangrijk deel in het teken van uitbreiding en versterking van de compliance- en risicofunctie van de dienst. Er is nieuw personeel aangetrokken en ingewerkt. Dit zal ook in het komende jaar nog plaatsvinden. Daardoor is het mogelijk om compliance- en risicomanagement beter te integreren in de dagelijkse werkprocessen van de dienst.

Een belangrijk onderdeel van het compliant werken is het kunnen onderkennen van en handelen naar situaties van non-compliance. In 2023 is de MIVD gestart met het afhandelen van deze meldingen volgens een vaste procedure. Dit leidt tot een hogere meldingsbereidheid bij medewerkers, omdat zij ervaren dat een melding sneller wordt opgevolgd en leidt tot een verbetering van de werksituatie. In 2024 zal de procedure worden verbeterd en aangevuld, om sneller te kunnen acteren op meldingen. Ook dient de procedure nog beter aan te sluiten op de afspraken die zijn gemaakt met de toezichthouder CTIVD in het in 2022 overeengekomen incidentenprotocol.

Compliance- en risicomanagement is een fenomeen binnen de dienst dat sinds 2019 gestaag is ingevoerd, maar nog niet bij iedereen bekend is. Ook de hoge instroom van nieuw personeel betekent dat er continue aandacht moet zijn voor het creëren van bewustzijn bij medewerkers en leidinggevenden. De al bestaande instrumenten hiervoor zullen in 2024 daarom worden geïntensiveerd en uitgewerkt.


L800

3 EEN ORGANISATIE IN BEWEGING

Er wordt, in het belang van Nederland en het koninkrijk, veel van de MIVD verwacht. De MIVD wil als *excellent intelligence & security provider* niet dat bewindspersonen, commandanten en eenheden worden verrast in een wereld die complexer en helaas ook minder veilig wordt. Een wereld waarin het vermogen van de MIVD en de AIVD om grote hoeveelheden data te verwerken steeds bepalender wordt.

3.1 Veranderen en groeien

Organisatieverandering

Ook in 2023 was de MIVD een organisatie in beweging. De MIVD werkt middels verschillende reorganisatiesporen verder aan de optimalisering van de Dienst. Hiermee kan de uitbreiding van de MIVD, ten gevolge van de toekenning van aanvullende budgetten geaccommodeerd worden. Dit maakt het mogelijk om structureel te investeren in de toekomstbestendigheid van de organisatie waarbij flexibiliteit behouden wordt. We blijven hierbij ook vooruit kijken om strategische prioritering en uitvoering op het gebied van data en IV op een zodanige wijze in te richten dat er invulling gegeven kan worden aan een data gedreven toekomst voor beide diensten.

De mens centraal in een groeiende dienst

Een goede ondersteuning op het gebied van Human Resources (HR) is essentieel voor de invulling van de visie van de dienst als '*excellent intelligence & security provider*', '*team of teams*' en '*great place to work*'. In 2023 is de HR capaciteit verder versterkt voor de ondersteuning bij de invulling van de groei en ambitie van de dienst, waarbij sprake is van zowel een kwalitatieve als kwantitatieve groeiopgave en meer data gedreven werken. Verbetering van de werving en selectieprocedure en het gericht en proactief benaderen van de arbeidsmarkt heeft positief effect gehad op de vullingsgraad. Dit met name op het gebied van de werving van schaarse IT-expertise. Hierbij wordt de samenwerking met zowel de rest van Defensie als de AIVD opgezocht.

Het vullen van militaire functies bij de MIVD blijft lastig, dit in relatie met de algemene vullingsgraad van militaire functies defensiebreed. De MIVD overlegt met de Operationele Commando's (OPCO's) van de krijgsmacht om daar verbetering in te krijgen.

Ter ondersteuning van een '*great place to work*' heeft de MIVD ook expliciete aandacht voor de ontwikkeling en innovatie binnen het HR-domein. Zo wordt er op alle niveaus binnen de MIVD intensief geïnvesteerd op leiderschap. Ook de aandachtsgebieden Strategische Personeelsplanning en inzet op Strategisch Talentmanagement zijn in 2023 nog meer tot wasdom gekomen. Daarnaast is er aandacht voor zowel persoonlijke als teamontwikkeling in zowel de vorm van trainen en opleiden als in team- en individuele coaching.

Innovatie

De MIVD heeft in 2023 verder ingezet op innovatie. Eind 2021 is de Innovatie Agenda vastgesteld. De Innovatie Agenda geeft inhoudelijke focus aan de innovatie inspanning voor de MIVD en beschrijft de randvoorwaarden die ingericht moeten worden om de innovatiefunctie van de dienst te versterken in de vorm van sleutelinterventies. 2023 heeft in het teken gestaan van het creëren van de juiste randvoorwaarden om

binnen de organisatie innovatief vermogen te ontwikkelen. In 2023 is door de MIVD veel geïnvesteerd in de partnerschappen met de Defensie Innovatiegemeenschap en TNO. In 2023 heeft de MIVD onder andere verschillende externe proposities behandeld waaruit enkele innovatie-trajecten zijn voortgekomen.

In 2023 is ook gewerkt aan het aanwenden van extra capaciteit voor de dienst om innovaties uit te voeren. Met de introductie van een Innovatie Makelaar beschikken de afdelingen voor het eerst over *dedicated* medewerkers wiens taak het is innovatie te bespoedigen. De verwachting is dat hierdoor in 2024 het aantal innovatietrajecten vanuit de afdelingen significant zal stijgen.

Multidomein- en Informatie gestuurd optreden

De veranderende aard van oorlogvoeren en de snel toenemende digitalisering en technologische mogelijkheden noodzaken Defensie tot het ontwikkelen van nieuwe manieren van optreden, gereedstellen, ondersteunen en besturen. De twee uitgangspunten voor deze transformatie zijn Multidomein Optreden (MDO)[31] en Informatie Gestuurd Optreden (IGO)[32]. Door het doorvoeren van MDO en IGO toepassingen bouwt de MIVD aan het fundament om zich te ontwikkelen tot een *excellent intel provider* voor de krijgsmacht, bestuurders, politici en andere relevante (overheids) organisaties en instellingen op het gebied van slimme dataverwerking, verrijking, correlatie, analyse en verspreiding van data, informatie en inlichtingen. Dit om (on)gekende dreigingen tijdig te signaleren en de juiste handelingsopties te bieden. Op deze manier kan de MIVD in het operationeel tempo relevante informatie en inlichtingen op het juiste niveau beschikbaar stellen.

Infrastructuur, werkplekken en goede, veilige werkomstandigheden

Voor de AIVD en de MIVD is het uitgangspunt samenwerken en samenwonen op verschillende locaties (Zoetermeer, Leidschendam en de Frederikkazerne in Den Haag) om de nationale veiligheid te beschermen. In de huidige bestaande panden die door de diensten in gebruik zijn, wordt reeds intensief samengewerkt door verschillende gezamenlijke organisatieonderdelen.

Eind 2023 hebben de secretarissen-generaal van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Defensie gezamenlijk besloten om het zogeheten programma 'Samenwonen AIVD-MIVD' (SAM) op de Frederikkazerne in Den Haag te stoppen, aangezien uit de uitwerking van het voorlopig ontwerp is gebleken dat niet kan worden voldaan aan de gestelde randvoorwaarden ten aanzien van kwaliteit, tijd en geld. Er zou sprake zijn van een verwachte overschrijding van de investeringskosten. Deze hogere investeringskosten zijn met name het gevolg van duurdere grondstoffen, de complexiteit van het project, de eisen aan de beveiliging en de afwezigheid van marktwerking bij de gunning.

Ook met aanpassingen kan deze verwachte overschrijding niet binnen het vooraf gestelde financiële kader worden teruggebracht. De komende periode zal worden bekeken hoe de toekomstbestendige huisvestings-behoefte op de locatie Frederikkazerne zijn beslag zal krijgen. De ambitie, de ideeën en de plannen om de samenwerking tussen beide diensten te versterken staat nog steeds overeind en blijft leidend. Het vervolgtraject voor de FRK zal vanzelfsprekend voortborduren op de tot nu toe opgedane kennis en ervaring ten gunste van de verdere voortgang daarvan.

Begin 2023 is door het Rijksvastgoedbedrijf een pand in Leidschendam ter beschikking gesteld aan de AIVD en MIVD. Het streven is om dit pand eind 2027 in gebruik te nemen voor gezamenlijke huisvesting. Om de groei van de MIVD te faciliteren komen er ook werkplekken beschikbaar in het TNO gebouw op de Waalsdorperweg te Den Haag. Het afgelopen jaar stond op het gebied van huisvesting tevens in het teken van benodigde renovaties, zowel in Den Haag als op de verschillende buitenlocaties van de dienst.

31 *MDO: het gelijktijdig, gesynchroniseerd bereiken van meerdere effecten in meerdere domeinen (Land, zee, lucht, ruimte en cyber).*

32 *IGO: In staat zijn sneller de juiste informatie te verzamelen, analyseren teneinde de situatie beter te begrijpen, zodat snellere en betere besluiten genomen kunnen worden om met de beschikbare middelen de gewenste effecten te bereiken.*

3.2 Een datagedreven inlichtingendienst

Om ook in de toekomst relevant te blijven is het nodig de transformatie naar een datagedreven dienst steeds meer inhoud en vorm te geven. De MIVD werkt continue aan vernieuwing van IT, technologie en het verbeteren van processen. Daarnaast is het investeren in het benodigde maar schaarse menselijke kapitaal noodzakelijk. Het inlichtingenproces is in hoge mate afhankelijk van het snel en doelgericht verwerken van grote hoeveelheden data en de hard- en software die medewerkers in staat stelt dit te doen. Continue verbetering van de informatie-technologie voor verwerving, opslag, processing, bewerking, analyse en verspreiding is daarom een voorwaarde voor een succesvol opererende inlichtingen- en veiligheidsdienst.

Naast het bieden van continuïteit van de huidige toepassingen investeert de dienst in programma's en projecten die het datagedreven werken mogelijk maken en de kwaliteit van de informatiehuishouding verhogen. De MIVD is in ontwikkeling om tot een datagedreven dienst te komen. Kennis en kunde op het gebied van IT, applicaties, data, informatiehuishouding en kaders en architectuur is bijeen gebracht om beter inhoud en vorm te kunnen geven aan prioritering en sturing, samenwerking met de AIVD en besturing passend bij het inlichtingen-proces van de toekomst.

3.3 Samenwerking

De MIVD voorziet Defensie, bestuurders, politici, bedrijven en andere relevante (overheids) organisaties en instellingen gevraagd en ongevraagd van informatie, zodat zij tijdig maatregelen kunnen nemen. De MIVD heeft een belangrijke rol te vervullen bij het versterken van de weerbaarheid en veiligheid van Defensie en de technologische industriële basis van Defensie, Nederland en onze partners. Samenwerking met nationale en internationale ketenpartners en instanties krijgt een steeds belangrijkere plaats bij het werk van de dienst.

Defensie en de MIVD

In 2023 heeft de MIVD zich ingezet om de slagvaardigheid van het Nederlandse Inlichtingen- en Veiligheidssysteem (I&V-systeem) verder te verbeteren door de samenwerking met de krijgsmacht te intensiveren. Dit krijgt vorm zowel bij inlichtingenteams, als in het beleidsdomein. Een sterk en integraal I&V-systeem, waarin processen op elkaar zijn afgestemd en kennis en ervaring wordt gedeeld, is nodig om de krijgsmacht tijdig van bruikbare I&V-diensten te kunnen voorzien. Niet alleen in vredestijd of in tijden van oplopende spanning, maar ook in oorlogsomstandigheden. De noodzaak daartoe die was er altijd al, maar heeft in 2023 een impuls gekregen vanwege de voortdurende verslechtering van de internationale veiligheidssituatie. En dat vraagt om het opnieuw doordenken van de weerbaarheid van de MIVD, de krijgsmacht en de samenleving.

Het nieuwe NATO Force Model vraagt om een gerichte inspanning van lidstaten om toe te werken naar grootschalige inzet met korte reactietermijnen. Dit betekent dat de gereedheid van alle Nederlandse krijgsmachtdelen omhoog zal moeten en een focus wordt aangebracht op het actuele dreigingsbeeld. Van de MIVD wordt daarom een grotere betrokkenheid gevraagd bij het plannings- en gereedstellingsproces van Defensie.

De constructieve samenwerking binnen de krijgsmacht kreeg mede door toedoen van de MIVD in 2023 o.a. gestalte door deel te nemen aan Defensie brede conceptontwikkeling, de inrichting van een IGO-programma, door workshops te organiseren voor nieuw geplaatst I&V-personeel van de krijgsmacht en door tijdelijk bij de MIVD geplaatst krijgsmacht personeel. De expertise van de krijgsmacht is, ook in 2023, nodig gebleken om snel te kunnen opschalen als de actualiteit daarom vroeg.

De intensivering van de samenwerking tussen de MIVD en andere afdelingen van de krijgsmacht draagt bij aan het optimaal kunnen benutten van inlichtingencapaciteiten van zowel de MIVD als van eenheden van de krijgsmacht. Samenwerking bij de inzet van het MQ-9 Reaper Squadron van de Koninklijke Luchtmacht is hiervan een voorbeeld, hier werd in 2023 een vervolg aan gegeven. Dat geldt ook voor samenwerking met joint organisatiedelen zoals het Defensie Cyber Commando (DCC), Special Operations Command (SOCOM) en het Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Commando (JISTARC).

Samenwerking (buitenlandse) partnerdiensten

Zoals eerder genoemd werkt de MIVD nauw samen met de AIVD. Om het huidige complexe en grensoverschrijdende dreigingsbeeld goed en tijdig in kaart te brengen, is samenwerking met (inter)nationale organisaties van cruciaal belang. De MIVD werkt ook samen met buitenlandse inlichtingen- en veiligheidsdiensten, bijvoorbeeld door informatie uit te wisselen, gezamenlijk onderzoek te doen en door te leren van elkaars ervaringen. Op deze manier verbeteren we onze informatiepositie, dragen we bij aan nationale en internationale veiligheid en doen we kennis op om te blijven innoveren. Buitenlandse partnerdiensten leveren daarmee een belangrijke bijdrage aan de taakuitvoering van de MIVD.

De mogelijkheden en de waarborgen voor het verstrekken van gegevens en andere vormen van samenwerking met buitenlandse diensten, staan beschreven in de Wiv 2017. Daarnaast worden voor iedere buitenlandse partnerdienst de kaders voor samenwerking uitgewerkt in de zogeheten wegingsnotities[33].

Samenwerking met de EU

De MIVD heeft het afgelopen jaar de EU in toenemende mate ondersteund. In lijn met het in 2022 vastgestelde (meerjarig) Strategisch Kompas van de Europese Unie heeft de MIVD zich het afgelopen jaar gericht op intensievere EU-samenwerking op inlichtingengebied. Ook in 2023 onderstreepten de geopolitieke ontwikkelingen op het wereldtoneel, in het bijzonder aan de randen van Europa, het belang van deze samenwerking, ook voor Nederland. Daarbij heeft de MIVD het afgelopen jaar bijgedragen aan de rol van militaire inlichtingen binnen de EU. De MIVD heeft de EU het afgelopen jaar binnen de wettelijke kaders zoveel mogelijk ondersteund met inhoudelijke expertise en tijdige en kwalitatieve inlichtingenbijdragen.

Samenwerking met de NAVO

De MIVD onderschrijft het voortdurende belang van een gedegen, kwalitatieve en kwantitatieve inlichtingensamenwerking met en binnen de NAVO. De militaire alliantie van inmiddels tweeëndertig lidstaten zag in de afgelopen periode haar bestaansrecht uitdrukkelijk bevestigd. Waar mogelijk en binnen de wettelijke kaders ondersteunt de MIVD de NAVO inlichtingenorganisatie met tijdige en kwalitatieve inlichtingenbijdragen, kennis en personeel. Hiermee stelt de MIVD het bondgenootschap in staat te anticiperen op bestaande en snel opkomende en nieuwe dreigingen in een complexe multidimensionale wereld. Bovendien levert de MIVD belangrijke inlichtingenondersteuning in het kader van de NAVO-missies in Litouwen en Irak en aan eventueel militair optreden in het kader van de bondgenootschappelijke verdediging (art.5).

33 *Criteria van de wegingsnotitie zijn: democractische inbedding, mensenrechten, professionaliteit, wettelijke bevoegdheden en gegevensbescherming.*


Inspectie
Leefomgeving en Transport

4 KENGETALLEN

Kengetallen Bureau Industrieveiligheid (BIV):

Bedrijven

Bedrijven in portefeuille: 1840

- 1.396 Nederlandse bedrijven
- 444 buitenlandse bedrijven

Autorisaties

Aanvraag autorisatie:

In 2023 zijn er in totaal 784 nieuwe autorisaties aangevraagd, waarvan:

- 395 nieuwe autorisatieaanvragen door een Nederlandse opdrachtgever (Defensie of bedrijf) voor een Nederlands bedrijf
- 148 nieuwe autorisatieaanvragen door een Nederlandse opdrachtgever (Defensie of bedrijf) voor een buitenlands bedrijf
- 149 nieuwe autorisatieaanvragen door een buitenlandse opdrachtgever (Defensie of bedrijf) voor een Nederlands bedrijf
- 92 nieuwe autorisatieaanvragen niet in behandeling zijn genomen, omdat het bedrijf niet aan de gestelde eisen van de kwaliteitstoets voor intake voldeed.

Afhandeling autorisaties:

In 2023 zijn er in totaal 836 autorisaties afgehandeld, waarvan:

- 492 afgegeven autorisaties, waarvan:
  - 80 autorisaties werden teruggetrokken door de opdrachtgever
  - 66 autorisaties zijn geweigerd

84 aan het buitenland afgegeven Facility Security Clearances (FSC's)
114 door het buitenland afgegeven FSC's.

Auditeren

In 2023 zijn er in totaal zes audits uitgevoerd bij zes verschillende bedrijven.

Meldingen en incidenten

Incidenten gemeld:	172
Incidenten afgehandeld:	162

Afhandeling aanvragen niet-Nederlanders op vertrouwensfuncties bij ABDO-opdrachten:

In 2023 zijn er in totaal 354 aanvragen voor Niet-Nederlands ingediend, waarvan:

Goedgekeurd:	297
Afgekeurd:	41

Facility Security Clearances

Bij een eventuele gunning van een buitenlandse defensieorder aan een Nederlands bedrijf wordt gevraagd een Facility Security Clearance (FSC) af te geven. De MIVD onderhoudt contact met buitenlandse National en Designated Security Authorities (NSA/DSA) om de FSC's aan te vragen en af te handelen.

Cijfers FSC:

Aan buitenland afgegeven FSC:	84
Door buitenland afgegeven FSC:	114

Requests for visit

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

Rfv's aantallen

Rfv – Industrie (bezoeken aan de industrie)

Uitgaande Rfv:	170
Inkomende Rfv:	760

Rfv – Defensie (bezoeken aan NL of buitenland Defensie)

Uitgaande RFV:	1.555
Inkomende RFV:	2.474

Kengetallen UVO

De UVO rondde in 2023 gemiddeld 86,6 procent van de onderzoeken af binnen de wettelijke termijn van acht weken. Daarmee is de norm van 90 procent niet behaald.

Van het totale aantal onderzoeken in 2023 zijn 41.548 onderzoeken uitgevoerd door de UVO zelf (19.671 door de AIVD en 21.877 door de MIVD) en 44.074 door de mandaathouders.
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.


MAERSK LINE

Kengetallen UVO (inclusief mandaathouders)
* Per 1 februari 2023 is, in goed overleg, het mandaathouderschap van de Nationale Politie beëindigd.

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

Bezwaar en Beroep
Naar aanleiding van de besluiten tot weigering of intrekking van de VGB kunnen personen bezwaar aantekenen en/of in (hoger) beroep gaan. Onderstaand een overzicht van de afhandeling van bezwaar- en (hoger) beroepsprocedures naar aanleiding van besluiten veiligheidsonderzoeken.

Onderzoeken	Positieve besluiten	Negatieve besluiten	Totaal aantal besluiten
A-niveau door UVO	5.769	25	5.794
B-niveau door UVO	20.371	49	20.420
B-niveau door UVO overgenomen van KMar en Nationale Politie	8.547	1.681	10.228
C-niveau door UVO	5.095	11	5.106
Totaal door UVO	39.782	1.766	41.548
B-niveau door KMar en Nationale Politie*	44.074	0**	44.074
Totaal aantal onderzoeken	83.856	1.766	85.622

2023	Ingediend in 2023	Afgedaan in 2022	Ongegrond	Gegrond	Niet-ontvankelijk	Ingetrokken	Afgewezen
Bezwaren	5	4	3	1	-	-	-
Beroepen	2	7	6	-	1	-	-
Hoger beroep	4	1	1	-	-	-	-
Voorlopige voorziening	-	-	-	-	-	-	-
Totaal	11	12	10	1	1	-	-

Samenleving en media

De MIVD geeft zo snel en volledig mogelijk antwoord op vragen van de samenleving en de pers, zonder geheime informatie vrij te geven. De MIVD ontving in 2023 ruim 2200 publieksvragen en meldingen rechtstreeks. In 2023 ontving de MIVD ruim 160 vragen van de media. De vragen waren zeer uiteenlopend van aard.

Er is een spanningsveld tussen publieke rapportage en het werk van een inlichtingen- en veiligheidsdienst. Het actuele kennisniveau, de bronnen en de werkwijze mogen niet openbaar worden gemaakt. Dat beperkt de mate van openbaarheid. De MIVD gaat evenmin in op individuele rechtszaken die nog worden behandeld door een rechter, personeelsvertrouwelijk zijn of de privacy van de betrokkene kunnen schaden. Bij overige vragen maakt de MIVD altijd een afweging of beantwoording van de publieks- of persvraag:

- de werkwijze of het actueel kennisniveau van de MIVD kan prijsgeven;
- in strijd is met de wettelijk bepaalde bronbescherming;
- militaire operaties in gevaar kan brengen.

Klachten en misstanden

Met een klacht over (vermeend) optreden van de MIVD kan een persoon zich richten tot de klachtcoördinator van de MIVD. Indien de indiener van een klacht zich niet kan vinden in de afhandeling van de klacht kan hij zich vervolgens wenden tot de CTIVD. In 2023 kwamen bij de MIVD 39 klachten binnen. Tussen de afdeling klachtbehandeling van de CTIVD en de MIVD vindt regelmatig constructief overleg plaats.

Er zijn geen meldingen binnengekomen over misstanden in 2023.

Cijfers klachten

2023	Klachten nog in behandeling op d.d. 1/1/2023	Ingediend in 2023	Ongegrond	Gegrond	Deels gegrond	Ingetroken	Niet in behandeling / doorverwezen	Klachten nog in behandeling op d.d. 31/12/2023
aantal	6	39	1	6	1	10	9	16

Inzageverzoeken
Eenieder heeft de mogelijkheid een aanvraag te doen naar eventueel bij de MIVD vastgelegde gegevens. Wanneer deze gegevens niet langer actueel zijn voor de taakuitvoering van de MIVD en in deze gegevens geen bronnen of werkwijze van de dienst worden onthuld, kunnen deze in aanmerking komen voor openbaarmaking. Tegen weigering tot openbaarmaking kan achtereenvolgens bezwaar bij een onafhankelijke commissie en beroep bij de rechtbank worden aangetekend.

Inzageverzoeken 2023	Aantal verzoeken ingediend in 2023	* Aantal afgedane verzoeken	** Gehonoreerd	Geweigerd	Nog lopend	Bezwaar	Beroep	Hoger beroep
Persoonsgegevens	32	14	-	14	20	-	2	-
Naar overleden familie	12	8	-	8	5	-	-	-
Data on administrative matters	8	3	-	3	7	2	2	1
Total	52	25	0	25	32	2	4	1

* *Deels verzoeken van jaren vóór 2023.*
** *Gehonoreerd betekent dat aan verzoeker één of meer documenten zijn verstrekt.*

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. 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 2023 zijn geen notificaties gedaan.

Dreigingsanalyses personen

Als de MIVD over concrete en/of voorstelbare dreigingsinformatie beschikt, die geduid kan worden, brengt de MIVD een dreigingsinschatting uit. Naast de dreigingsinformatie wordt ook beoordeeld wat het effect is wanneer de dreiging tot uitvoer wordt gebracht en of de bedreiger de wil en mogelijkheden heeft. De MIVD kan de gewenste informatie ook aanleveren in een dreigingsappreciatie of dreigingsanalyse. Dat is een meer uitgebreide analyse van concrete en voorstelbare dreigingen vanuit het perspectief van de bedreigde, zoals een politicus of diplomaten. Het afgelopen jaar zijn er 22 dreigingsappreciaties geschreven.

Tapstatistieken

In 2023 zijn door de MIVD 2666 taps geplaatst. Het betreft hier de daadwerkelijk inzet van alle vormen van taps. Voorbeelden zijn een telefoon, IP-tap of het plaatsen van een microfoon. Eén target (persoon of organisatie) kan op verschillende manieren en op meerdere apparaten afgeluisterd worden. Die worden afzonderlijk meegeteld in de statistieken.

Validatie-onderzoek

In 2023 is de MIVD 115 validatie-onderzoeken gestart naar aanleiding van meldingen en signalen. Het aantal validatie-onderzoeken is daarmee hetzelfde gebleven ten opzichte van het aantal onderzoeken in 2022. Een deel van de ontvangen meldingen en signalen hield een mogelijke bedreiging voor de veiligheid of inzetbaarheid van de krijgsmacht in, waarnaar een onderzoek werd gestart. De meldingen die de MIVD ontvangt kunnen komen van zowel partners uit Nederland als uit het buitenland. Dit kunnen missiegebieden zijn en landen waar de krijgsmacht oefent of is vertegenwoordigd. De meldingen en signalen zijn divers. Daarbij valt te denken aan zorgen over individuen in relatie tot verschillende vormen van extremisme of terrorisme, opvallende belangstelling in- of ongewenste inmenging van statelijke actoren onder Defensiepersoneel, -materieel, -complexen en de –industrie. Indien nodig kan de MIVD een derde partij over de dreiging informeren, zodat passende maatregelen kunnen worden genomen.

Ministerie van Defensie

Aan	MINDEF
Van	MIVD
Afgestemd met	BSG, DGB, CDS, DJZ, HDFC en DCo
In afschrift aan	STAS

TER BESLISSING

Datum
4 april 2024

Onze referentie
BS2024012669

Opgesteld door
[redacted]@mindef.nl

Aantal bijlagen
1

Nota

Aanleiding
Door middel van de gevoegde aanbiedingsbrief wordt het Openbaar Jaarverslag MIVD 2023 aangeboden aan de Tweede Kamer. Het openbaar jaarverslag geeft een overzicht van de dreigingen die de MIVD in 2023 heeft waargenomen en legt in het openbaar verantwoording af over de werkzaamheden die het afgelopen jaar zijn verricht. Een geheim jaarverslag wordt afzonderlijk aangeboden aan de CIVD.

Gevoegd vindt u de Aanbiedingsbrief Openbaar Jaarverslag MIVD 2023 en het Openbaar Jaarverslag MIVD 2023.

Geadviseerd besluit
U wordt geadviseerd in te stemmen met het Openbaar Jaarverslag MIVD 2023. Daarnaast wordt u geadviseerd in te stemmen met de aanbieding van dit jaarverslag aan de Kamer.

Kernpunten
In het openbaar jaarverslag wordt met dezelfde hoofdstukken als vorig jaar ingegaan op:

- Voorwoord: algemene schets van de veiligheidsontwikkelingen in de wereld, de grey zone en de taken op dat gebied van de MIVD. Tevens komt de tijdelijke wet aan de orde en de inzet van het personeel.
- Inlichtingen en veiligheid voor Nederland: een beschrijving van de belangrijkste statelijke en thematische dreigingen, de missieondersteuning en de veiligheidsbevorderende maatregelen.
- Verantwoordelijk naar politiek en samenleving: een beschrijving van de verantwoordelijkheidsstructuur binnen Defensie, de verhouding tot het parlement, de juridische grondslag voor het optreden met de Wiv2017, de tijdelijke wet en de nota van wijziging, alsook de toezichtsstructuur en het compliance- en risicomanagement.
- Een organisatie in beweging: een beschrijving van de (groei)ambitie van de dienst en welke stappen in 2023 zijn genomen om deze te bereiken op het gebied van personeel, innovatie, ICT en vastgoed. De ambities van de MIVD worden waar mogelijk opgelopen met de AIVD.
- Kengetallen: gaat kwantitatief in op onder meer het Bureau Industrieveiligheid, Unit Veiligheidsonderzoeken, klachten en inzageverzoeken.

Toelichting

Financiële overwegingen
Uit het jaarverslag van de MIVD volgen geen financiële consequenties.

Juridische overwegingen
Uit instemming met het voorgestelde jaarverslag van de MIVD volgen geen juridische consequenties.

Communicatie

De publicatie van het openbaar jaarverslag zal gepaard gaan met een nieuwsbericht op defensie.nl en intranet. Ook wordt er tijd voor de Directeur MIVD vrijgemaakt om media te woord te staan.

Informatie die niet openbaar wordt gemaakt

Persoonsgegevens van de steller worden gelakt vanwege de bescherming van de persoonlijke levenssfeer.

Directeur Militaire Inlichtingen- en Veiligheidsdienst