Ministerie van Defensie

VOORUITZIEND VERMOGEN VOOR VREDE & VEILIGHEID

De Militaire Inlichtingen- en Veiligheidsdienst
beschermt wat ons dierbaar is
MIVD openbaar jaarverslag 2018

VOORUITZIEND VERMOGEN VOOR VREDE & VEILIGHEID

De Militaire Inlichtingen- en Veiligheidsdienst
beschermt wat ons dierbaar is
MIVD openbaar jaarverslag 2018


POLITIE

INHOUD

VOORWOORD MINISTER

In 2019 is het dertig jaar geleden dat de Berlijnse muur viel. Het begin van een tijdperk met een optimistische ondertoon. Vrede, veiligheid en welvaart leken binnen handbereik in een wereld waarin grote tegenstellingen waren overwonnen. Dat beeld is dertig jaar later gekanteld. De internationale veiligheid staat al langer onder druk. Oude dreigingen steken de kop weer op. Nieuwe dreigingen dienen zich aan. Internationale tegenstellingen verscherpen, terwijl oude bondgenootschappen onder druk komen te staan.
In deze context doet de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) zijn belangrijke werk. Onder de noemer 'vooruitziend vermogen voor vrede en veiligheid' zorgt de MIVD ervoor dat Defensie de informatie krijgt die ze nodig heeft om ons land te kunnen beschermen. Die kennis is onze kracht. Niet zelden is deze letterlijk van levensbelang voor onze militairen. De inlichtingen van de MIVD leveren ook een onmisbare bijdrage aan ons streven naar een informatie gestuurde krijgsmacht, een van de speerpunten uit de Defensienota 2018. Zij zijn bovendien cruciaal voor het Nederlandse veiligheidsbeleid en de nationale veiligheid. De MIVD speelt dus een belangrijke rol in het beschermen wat ons dierbaar is: onze veiligheid, vrijheid en welvaart.

We mogen niet naïef zijn over de toenemende onveiligheid. Nederland heeft meer dan ooit goede inlichtingen nodig. De in 2018 verijdelde cyberoperatie van de Russische militaire inlichtingendienst (GRU) was illustratief voor de veranderende veiligheidsomgeving. Door deze bloot te leggen, gaven wij een duidelijke boodschap af: wij tolereren dit niet in ons land. Samenwerking met onze partners, zowel nationaal als internationaal, was daarbij van groot belang.
Het jaar 2018 stond voor de MIVD ook in het teken van de implementatie van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv2017). Een complexe wet die meer impact had op de MIVD dan bij de totstandkoming van de wet is onderkend. In de tussentijd gaan de werkzaamheden van de dienst, waaronder de ondersteuning van missies, gewoon door. Net als het onderkennen van informatie- en cyberoperaties.

In dit jaarverslag kunt u lezen wat in 2018 de belangrijkste aandachtpunten waren en hoe de MIVD haar taken heeft vervuld.
Elke dag opnieuw in deze snel veranderende wereld de juiste inlichtingen boven tafel krijgen, vraagt vaak het uiterste van de dienst en zijn medewerkers. Ik zie hoe vastberaden de medewerkers van de MIVD zijn om samen met de krijgsmacht, AIVD en onze andere partners in binnen- en buitenland de complexe dreigingen het hoofd te bieden. Het niveau van het Nederlandse inlichtingenpersoneel is hoog. Dit leidt tot concrete successen voor onze veiligheid. Dat vervult mij met trots en ik hoop u als lezer ook.

Minister van Defensie
Ank Bijleveld-Schouten

INLEIDING VAN DE DIRECTEUR MILITAIRE INLICHTINGEN- EN VEILIGHEIDSDIENST

We leven in een wereld die snel onveiliger, complexer en onvoorspelbaarder wordt.
De Nederlandse krijgsmacht staat voor de taak deze complexe en veelzijdige dreigingen het hoofd te bieden in het belang van het Koninkrijk en de internationale rechtsorde. Goede en onafhankelijke inlichtingenondersteuning is hiervoor bittere noodzaak, zeker voor een krijgsmacht die in toenemende mate informatiegestuurd optreedt. De MIVD is voor deze inlichtingenondersteuning van onschatbare waarde. De dienst doet daartoe onderzoek in binnen- en buitenland binnen de kaders van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) en de Wet Veiligheidsonderzoeken.

Er is in de wereld veel aan de hand en de MIVD ervaart daarvan onmiddellijk de gevolgen. De MIVD heeft het afgelopen jaar bij voortduring inlichtingen verstrekt over dreigingen tegen militaire operaties, defensiepersoneel, defensielocaties, de strategische positie van Nederland en het bondgenootschap. De MIVD waarschuwde voor gevaren zoals spionage en cyber-aanvallen en bestreed deze. Ook gaf de dienst informatie over ontwikkelingen in Afrika, het Midden-Oosten en Eurazië die een potentiële dreiging voor de nationale veiligheid vormen en ondersteunde het Nederlandse voorzitterschap van de VN met inlichtingenrapporten.

Ook het belang van de veiligheidsbevorderende taak van de MIVD groeit als gevolg van de veranderde veiligheidscontext. De MIVD heeft tientallen Defensiebedrijven gescreend en hen geholpen bij de beveiliging van strategische informatie. De MIVD voorkomt op deze wijze het weglekken van defensiegeheimen, van groot belang voor het overeind houden van de technologische voorsprong en daarmee slagkracht van de Nederlandse krijgsmacht.

Dit alles doet de MIVD in de regel zonder dat ons werk en dus ook onze successen openbaar worden. Onze analyses zijn meestal staatsgeheim. Als wij zouden vertellen wat we weten en hoe we aan onze informatie zijn gekomen, zijn we onze kostbare inlichtingenpositie in een paar tellen kwijt of stellen we mogelijk de levens van onze bronnen in de waagschaal. Dat maakt het soms lastig om onze boodschap over te brengen. ‘Aansprekend bewijs’ voor een dreiging kunnen en willen wij in de regel niet openbaar maken.

In 2018 hebben we daarop een uitzondering gemaakt met de persconferentie over de verstoring van een hack-operatie van medewerkers van de Russische militaire inlichtingendienst GRU op Nederlandse bodem. Voor onze dienst een ongebruikelijke stap. Toch is het soms nodig, ook om de weerbaarheid in de samenleving te vergroten. Want minder naïviteit betekent betere bescherming van waardevolle informatie en grotere alertheid tegen mogelijke ongewenste beïnvloeding.

In dit jaarverslag wordt op twee landen dieper ingegaan vanwege hun grote invloed op het veiligheidsklimaat. Het betreft de Russische Federatie en China. De aandacht voor deze landen is er ook bij de behandeling van de thema's hybride dreiging, militaire techniek en proliferatie.

In dit jaarverslag laten we ook zien welke wettelijke taken we hebben, hoe wij worden gecontroleerd en hoe wij werken aan de verdere implementatie van de Wiv2017.

Ik ben trots op wat de MIVD doet voor de veiligheid van Nederland en onze militairen in binnen- en buitenland. Ik ben vooral ook trots op de burgers en militairen die in dienst van de MIVD samen hun bijzondere werk doen. Hun professionaliteit, gedrevenheid en integriteit zijn doorslaggevend voor ons succes. Ook in 2018 is dat weer gebleken.

Directeur Militaire Inlichtingen- en Veiligheidsdienst
Generaal-majoor Onno Eichelsheim

De Russische Federatie voert regelmatig long range aviation (LRA) vluchten uit. Hierbij worden strategische bommenwerpers van het type TU-160 BLACKJACK ingezet. Deze toestellen vliegen regelmatig boven de Atlantische oceaan en de Noordzee maar hebben in 2018 ook Venezuela aangedaan. Strategische bommenwerpers zijn de meest zichtbare uiting van het Russische (nucleair) machtsvertoon.

1 RUSSISCHE DREIGING

In de afgelopen jaren is de Europese veiligheidsomgeving en het dreigingsbeeld door het Russische optreden aan de NAVO-periferie ingrijpend gewijzigd. Recente gebeurtenissen - het Russisch optreden in de Zee van Azov maar ook de recente vaststelling door de MIVD dat Rusland het INF-verdrag schendt- zijn manifestaties van een trend die al ruim een decennium gaande is.

Het beeld dat hieruit naar voren komt is zorgelijk. Er is sprake van een toenemende en geïntegreerde Russische dreiging tegen bondgenootschappelijke, Europese en daarmee Nederlandse belangen. Het gaat om een militaire dreiging die op verschillende manieren op ons af komt: via hybride-, spionage- en cyberoperaties maar ook in de vorm van modernisering en uitbreiding van conventionele bewapening.

Russische intenties

Het Russische veiligheidsdenken is gebaseerd op een *zero sum* benadering. Dit betekent dat wanneer de veiligheid van de één verbetert, de veiligheid van de ander verslechtert.

Rusland, het Russisch leiderschap maar ook een deel van de bevolking, voelt zich binnen dit zero sum denken in toenemende mate bedreigd en omsingeld.

Moskou streeft een ingrijpende verzwakking van de Europese veiligheidsstructuur na, waarbij de rol van de NAVO sterk verminderd of uitgespeeld raakt. Een aantal landen in het oosten van Europa, waaronder NAVO-bondgenoten, zou volgens het Kremlin in de exclusieve Russische invloedssfeer moeten liggen.

Het Kremlin zet nu al middelen in, met name op het hybride vlak, om dit doel te realiseren. Er is op dit moment nog geen intentie om deze doelstelling met militaire middelen te bewerkstelligen. Zorgwekkend is echter dat Rusland – anders dan 10 jaar geleden – nu wel beschikt over de militaire middelen om een operatie met beperkte geografische doelstellingen tegen NAVO te initiëren en in eerste instantie succesvol te voltooien.

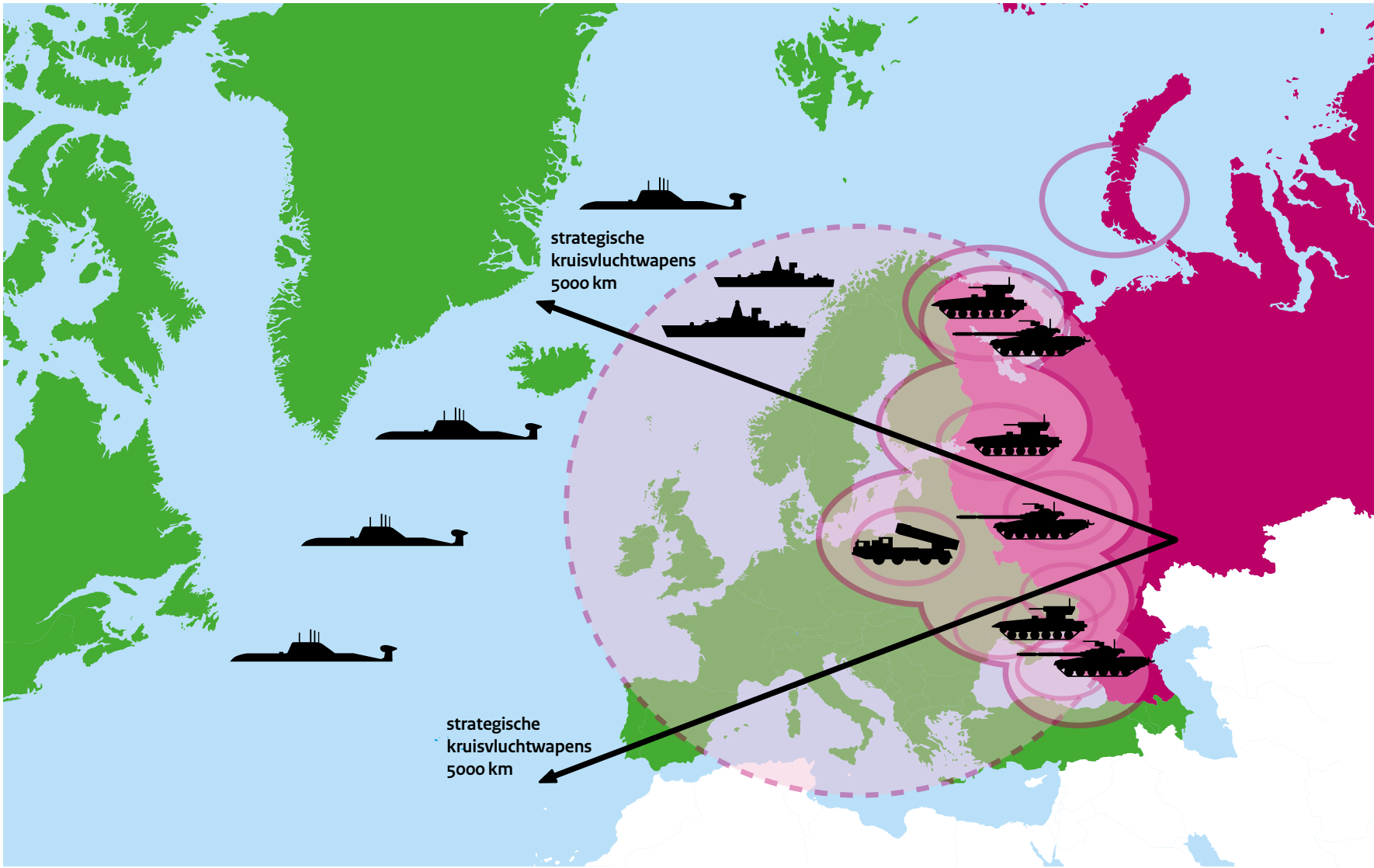
Ontwikkeling Russische militaire capaciteiten

Het afgelopen decennium heeft Rusland de conventionele en nucleaire strijdkrachten in zowel kwantitatief als kwalitatief opzicht zeer sterk verbeterd. Hoewel het strategische vermogen nog altijd in het voordeel is van het verenigde Westen, zijn de conventionele en tactisch nucleaire krachtsverhoudingen in Europa momenteel in het Russisch voordeel, nadrukkelijk ook tegen de NAVO. Het Kremlin beschikt op een regionaal niveau niet alleen over meer middelen, maar vooral ook over een grotere variëteit aan middelen. Daarom zal het voor het Westen moeilijk zijn om een juist antwoord te vinden op Russische acties, primair maar niet uitsluitend in het militaire domein. Hierdoor bestaat het gevaar op *under-responding* (sluipende Russische expansie), of juist *over-responding* (escalatie)

Aan dit militair overwicht, en daarmee het vermogen om ook politiek druk te zetten, ligt een aantal elementen ten grondslag:

- Rusland heeft een zeer snel politiek en militair besluitvormingsproces.
- Rusland is in staat om veel sneller eenheden aan de NAVO-oostflank te concentreren.
- de Russische krijgsmacht beschikt over modern materieel, soms moderner dan dat van de NAVO, en steeds beter opgeleid personeel.

De Russische Federatie heeft de conventionele en nucleaire strijdkrachten in zowel kwantitatief als kwalitatief opzicht sterk verbeterd. De regionale militaire krachtsverhoudingen zijn momenteel in het Russische voordeel. Een aanzienlijk deel van Europa ligt binnen het bereik van strategische raketten die uitgerust kunnen worden met een conventionele en nucleaire lading.



- Rusland kan, in eerste instantie, een deel van Europa afsluiten voor NAVO-versterkingen. De NAVO komt initieel niet door de geavanceerde defensieve en offensieve wapensystemen van Rusland heen (*Anti Access/ Area Denial environment* (A2AD)). Dit geldt specifiek voor de Baltische Zeeregio maar bijvoorbeeld ook voor delen van de Zwarte Zee.
- De rol van tactisch nucleaire wapens is fundamenteel anders dan in het Westen. Tactisch nucleaire wapens worden gebruikt voor regionale afschrikking en voor nucleaire de-escalatie. Het Kremlin kan dreigen met de inzet van tactisch nucleaire wapens en mogelijk zelfs met de demonstratieve inzet daarvan, om de tegenpartij naar de onderhandelingstafel te dwingen en (bondgenootschappelijke) vastberadenheid aan te tasten.

Het Kremlin beseft dat het NAVO vermogen uiteindelijk groter is, maar ook dat de Verenigde Staten daar een cruciale rol in speelt. In de visie van het Kremlin zijn de VS, het Amerikaans militair vermogen en de Amerikaanse veiligheidsgarantie aan Europa, de pijlers waarop het bondgenootschap steunt. Rusland zal dan ook uitsluitend een militaire operatie tegen NAVO initiëren als een essentieel veiligheidsbelang in de Russische perceptie onmiddellijk wordt bedreigd en als het Russisch leiderschap denkt dat een eensgezinde NAVO-reactie kan worden voorkomen. Dit is waar hybride oorlogvoering een belangrijke rol speelt.

Oekraïne
Het risico op escalatie in het oosten van Oekraïne is groter geworden na het incident tussen Rusland en Oekraïne eind november 2018 in de Zee van Azov. Ook in 2018 was er sprake van een gestage opbouw van het Russisch militair vermogen op de geannexeerde Krim. De Russische mogelijkheden om invloed uit te oefenen in de Zwarte Zee regio nemen hierdoor toe.

Toenemende Russische bemoeienis buiten de traditionele aandachtsgebieden

De MIVD zag in 2018 ook een toenemende Russische betrokkenheid bij conflicten buiten de traditionele Russische aandachtsgebieden. Deze trend werd enkele jaren geleden al ingezet. Dit optreden is vooral gericht op de ondersteuning van regimes, partijen en stromingen die de Russische agenda direct of indirect steunen. Hoewel het meest duidelijke voorbeeld de Russische betrokkenheid in Syrië is, was er een toenemende Russische betrokkenheid in Noord-Afrika en Sub Sahara Afrika, het Midden-Oosten, de Westelijke Balkan en de Indo-Pacific. Opvallend was de toenemende aanwezigheid van Russische *Private Military Companies* in diverse conflictgebieden in Afrika en het Midden-Oosten. In Venezuela oefende de Russische strategische luchtstrijdkrachten samen met eenheden van de Venezolaanse krijgsmacht. Deze militaire aanwezigheid onderstreepte de politieke en economische steun van het Kremlin aan het regime Maduro.

De MIVD heeft op 13 april 2018 een hackaanval van de Russische militaire geheime dienst verstoord op de Organisatie voor het Verbod op Chemische Wapens (OPCW) in Den Haag.

Op deze foto zijn de vier Russische inlichtingenofficieren te zien bij aankomst op luchthaven Schiphol.

2 HYBRIDE DREIGING

Hybride oorlog- of conflictvoering is de geïntegreerde inzet van alle beschikbare politiek-diplomatieke, economische, informatie, inlichtingen, cyber, sociaal-culturele en militaire middelen die een staat kan aanwenden voor het bereiken van politiek-strategische doelstellingen, zonder dat er sprake is van een openlijk interstatelijk gewapend conflict. Hybride dreigingen zijn op zich niet nieuw, maar hebben door ontwikkelingen in informatietechnologie een steeds grotere impact gekregen op onze nationale en bondgenootschappelijke veiligheid.

Geopolitieke belangen zijn vaak leidend voor de inzet van cyber spionage- of sabotage-operaties. Internationale organisaties (en hun medewerkers) zoals de NAVO, de OPCW of de EU, of nationale ministeries van Defensie en Buitenlandse Zaken zijn dikwijls doelwit. Maar ook andere instellingen kunnen plots als doelwit worden aangemerkt als zij in de geopolitieke verhoudingen een rol spelen.

Zo werden sportinstellingen en -evenementen bijvoorbeeld niet aangemerkt als hoog risico doelwit; toch is de conclusie nu dat vele tientallen sportfederaties zijn gehackt.

Hybride strategieën vertonen een grote mate van flexibiliteit, waarbij richting, ingezette middelen en zwaartepunten afhankelijk zijn van de actor. Rusland, bijvoorbeeld zet als regionale macht met regionale doelstellingen vooral politieke en economische middelen, militaire intimidatie en beïnvloedingsinstrumenten in om de NAVO-solidariteit en de trans-Atlantische band te ondergraven en nationale en Europese besluitvormingsprocessen te beïnvloeden.

China richt zich op het mondiale speelveld om de economische en politieke randvoorwaarden te creëren voor een vooraanstaande rol op het wereldtoneel en vis-a-vis de VS.

Dergelijke staten bedienen zich daarbij van verschillende hybride middelen.

Spionage en cyber

Staten bedienen zich van verschillende hybride middelen. Het kan gaan om klassieke spionage, maar ook om digitale spionage en, steeds vaker, een combinatie van beide. Hacken biedt mogelijkheden voor sabotage en voor beïnvloeding van politieke en bestuurlijke besluitvorming en de publieke opinie met behulp van de gehackte informatie. Landen die cyber spionage-campagnes uitvoeren zetten ook menselijke bronnen in of gebruiken commerciële activiteiten van (staats-) ondernemingen en technologie voor spionage.

Hack 'n leak

Een nieuwe trend zijn de zogenaamde *hack 'n leak*-operaties door inlichtingendiensten, waarbij gehackte data online wordt geplaatst. Deze data wordt daarna door de media overgenomen. Dat is een vorm van beïnvloeding, te meer omdat de aangeboden data soms gemanipuleerd of bewust selectief wordt aangeboden. Ook heeft de MIVD onderkend dat data werd gebruikt voor chantage tegen instellingen of personen, of werd deze gedeeld met media of advocaten, zonder dat duidelijk wordt dat gegevens afkomstig zijn uit hacks. Digitale spionage kan daarmee eenvoudig overgaan in een informatie-operatie of sabotage.

Het kan ook gaan om cyber. Landen die offensieve cyber spionage-campagnes uitvoeren zetten ook menselijke bronnen in of gebruiken commerciële activiteiten van (staats-) ondernemingen en technologie voor spionage.

China

In het huidige Chinese systeem zijn economische, politieke, militaire, cyber-, veiligheids- en inlichtingenactiviteiten nauw met elkaar verweven. China zet daarbij in op de verwerving en verdere ontwikkeling van innovatieve technologie.

Heimelijk gebeurt dit onder andere door de inzet van (economische) spionage en offensieve cyberprogramma's. Deze offensieve cyberprogramma´s richten zich niet alleen op de Defensie-toeleveranciers of ministeries, maar ook op onze vitale sectoren en organisaties, zoals de telecomsector, universiteiten, onderzoeksinstituten, zorginstellingen, biotechnologie, hightech industrie, startups, handel, en defensieorderbedrijven.

China's *Belt and Road Initiative*, waarbij wereldwijd fysieke infrastructuur zoals havens en spoorwegen worden opgekocht of aangelegd door Chinese (staats)ondernemingen, gaat steeds meer gepaard met de uitrol van een digitale equivalent, de *Digital Belt and Road*.

Russische Federatie

Het offensieve cyberprogramma van de Russische Federatie is zorgwekkend. De operationele risico's die worden genomen zijn groot, en de inzet is geavanceerd. Het Russische cyberarsenaal bestaat uit capaciteiten om digitale spionage, digitale sabotage en informatie-operaties uit te voeren: wereldwijd en ook met een korte planningscyclus. De inlichtingenbehoefte is in belangrijke mate geopolitiek en militair gedreven, en Rusland vormt voor landen wereldwijd een geavanceerde opponent in het digitale domein.

Om deze dreigingen goed in beeld te krijgen en te houden en effectieve tegenmaatregelen mogelijk te maken, moet de MIVD de intenties, capaciteiten en doelstellingen van de diverse actoren kunnen vaststellen. Ook moet de MIVD zicht houden op de middelen die deze actoren in kunnen en willen zetten om hun doelen te bereiken. De MIVD doet daarom steeds intensiever inlichtingenonderzoek naar hackers in dienst van andere staten. Het oogmerk van deze onderzoeken is attributie (wie zit er achter een cyberoperatie), het genereren van voorspellend vermogen en het bieden van handelingsperspectief. Vaststellen wie er achter een cyber operatie zit is ingewikkeld, kostbaar en tijdrovend, maar niet onmogelijk. Publieke attributie (door staten, cyber security-bedrijven of -onderzoekers) is meer gangbaar geworden als onderdeel van een aanpak om de kosten voor de aanvaller te verhogen.

MIVD-inlichtingenonderzoek heeft in 2018 diverse digitale spionage-pogingen onderkend.

Militaire sabotage
Voorbereidingen tot digitale militaire sabotage, ook op NAVO-grondgebied, geven aanleiding tot serieuze zorg. Meerdere hackersgroeperingen uit verschillende landen hebben de afgelopen jaren ervaring opgedaan. De kennis en geoefendheid van de hackers groeit, de operaties zijn steeds geavanceerder en men laat zich niet beperken door bepalingen in internationale verdragen. Ook de dreiging van digitale spionage groeit nog altijd.


SanDisk
RBN41GW

Rusland moderniseert zijn strategische nucleaire strijdkrachten en investeert onder meer in moderne, zeer mobiele intercontinentale raketten.

3 MILITAIRE TECHNOLOGIE EN PROLIFERATIE

De MIVD volgt militair-technologische ontwikkelingen om de Nederlandse krijgsmacht op de juiste wijze uit te kunnen rusten tegen dreigingen die uitgaan van bestaande en vooral toekomstige wapensystemen. In 2018 besteedde de MIVD vooral aandacht aan de militair-technologische ontwikkelingen in de Russische Federatie en China alsmede aan de proliferatie van wapensystemen en *dual-use* technologieën naar (potentiële) risicolanden en inzetgebieden. Tevens volgde de MIVD nauwlettend de vooruitgang op het gebied van geïmproviseerde explosieven in missiegebieden.

Technologische ontwikkelingen in de Russische Federatie

Typische militair-technologische ontwikkelingen in de Russische Federatie zijn de ontwikkeling van wapensystemen met een groot bereik en hoge snelheid, de zogenaamde '*hypersone*' wapens. Naast de mogelijkheid om doelen over lange afstanden en in kortere tijd aan te kunnen vallen, kan de Russische krijgsmacht met zulke systemen een (potentiële) tegenstander de toegang tot een regio te ontzeggen, bijvoorbeeld tot de Baltische Zee en de Zwarte Zee. Tevens hebben deze wapens een rol in het beschermen van de Russische nucleaire capaciteit en de intercontinentale ballistische raketten waardoor in combinatie met de in president Poetins toespraak aangekondigde wapens de overlevingskansen van de Russische nucleaire afschrikkingsmacht aanzienlijk toenemen. Deze wapensystemen bevinden zich in nog zeer uiteenlopende stadia van ontwikkeling.

Een andere belangrijke trend binnen de militair-technologische ontwikkelingen in de Russische Federatie, is de ontwikkeling, productie en ingebruikname van wapensystemen die specifiek gericht zijn tegen Westerse C4ISR-systemen [1] zoals satellieten en communicatienetwerken. Het gaat hierbij om onder andere antisatellietwapens en elektronische oorlogsvoeringsystemen.

Naast bovenstaande ontwikkelingen, richt de Russische defensie-industrie zich ook op een nieuwe generatie wapensystemen. Deze vijfde generatie wapensystemen omvatten onder andere nieuwe jachtvliegtuigen en onderzeeboten. De uitbreiding en modernisering van de militaire ruimtevaartprogramma's vallen hier ook onder. Moderne technologieën zoals kunstmatige intelligentie, robotisering, 3D-printen, lasertechnologie en de toepassing van nieuwe hoogwaardige materialen zoals composieten, kunnen daarin ook hun toepassing vinden.

De MIVD onderkende in de afgelopen jaren Russische initiatieven om de impact van de sancties teniet te doen door benodigde componenten zelf te ontwikkelen en te produceren. De nationale defensie-industrie en kennisinstituten zoals universiteiten werken nu intensiever samen om medio volgend decennium pariteit met westerse technologie te behalen. De MIVD blijft ook de komende jaren de (technologische) ontwikkelingen binnen de Russische defensie-industrie en krijgsmacht nauwlettend volgen.

Ondanks de ontwikkelingen van nieuwe, geavanceerde technologieën binnen specifieke domeinen van militair optreden, vormen wapensystemen die conceptueel hun oorsprong vinden tijdens de laatste fase van de Koude Oorlog en de Sovjet-Unie, nog altijd de ruggengraat van de Russische strijdkrachten. Hieronder vallen tanks, pantservoertuigen, grond-luchtverdedigingssystemen, schepen, onderzeeboten en jachtvliegtuigen. Omdat deze relatief goedkope wapensystemen hun weg vinden naar afzetmarkten in het Midden-Oosten, Afrika en Latijns-Amerika, kan de Nederlandse

[1] Afkorting C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance Reconnaissance

Drone's oftewel unmanned aerial systems worden als speelgoed en als hobby in toenemende mate gebruikt. De MIVD heeft waargenomen dat zelfbouw en commerciële vrij verkrijgbare drones ook worden ingezet in missiegebieden door terroristische organisaties als spionage en aanslagmiddel. Daarnaast zijn commercieel verkregen drones kwetsbaar daar de tijdens de vlucht verzamelde data mogelijk door anderen en fabrikanten kunnen worden ingezien. De MIVD heeft gewaarschuwd voor de risico's van drones, ook in Nederland.

krijgsmacht hiermee worden geconfronteerd. De MIVD volgt de ontwikkelingen en de proliferatie van deze wapensystemen als deze in potentie een bedreiging kunnen vormen voor de krijgsmacht of de regionale stabiliteit.

Technologische ontwikkelingen in China

De Chinese defensiemoderniseringen hebben tot doel capaciteiten te ontwikkelen die de Chinese krijgsmacht in staat stellen zogenoemde 'lokale oorlogen onder geïnformatiseerde omstandigheden' te voeren en winnen. De Chinese krijgsmacht beschikt thans over een aantal zogenoemde '*anti access/area denial*' capaciteiten, zoals moderne oppervlakteschepen, onderzeeboten, (ballistische) antischipraketten, lange afstand luchtverdedigingssystemen en offensieve luchtcapaciteiten, waarmee het een potentiele tegenstander tot in het westelijke deel van de Stille Oceaan aan kan grijpen. China investeert in het expeditionair vermogen van de krijgsmacht om zijn groeiende internationale belangen, zoals de verschillende *Chinese and Road Inititiative* (BRI) projecten, en de Chinese burgers buiten het grondgebied te kunnen beschermen.

Met de toename van China's politieke, economische en militaire invloed in Azië, en op termijn in de rest van de wereld, nemen ook de zorgen van andere regionale (groot)machten over deze groeiende invloed toe. Onzekerheid over de Chinese intenties leidt er toe dat andere landen bestaande veiligheidsallianties versterken, en nieuwe allianties aangaan. Deze veranderende veiligheidssituatie kan de regionale vrede en stabiliteit nadelig beïnvloeden.

De Chinese defensie-industrie ontwikkelde zich in de afgelopen jaren verder van een kopieerindustrie van vooral Sovjet-Russisch materieel tot een industrie die in staat is om in grote mate zelfstandig een breed arsenaal aan geavanceerde wapensystemen te ontwikkelen en te produceren. De Chinese defensie-industrie biedt deze wapens ook actief aan op de exportmarkt. Deze trend zette zich in 2018 voort en zal dat de komende jaren nog verder blijven doen. De MIVD constateert een

toenemend en grootschaliger gebruik van moderne technologieën. Mede onder druk van de overheid, de integratie van de defensie- en civiele industrieën en kennisinstituten en de toegenomen kennis en vaardigheid, is China steeds beter in staat moderne wapensystemen te produceren die tenminste gelijkwaardig en waarschijnlijk ook goedkoper zijn dan soortgelijke Russische wapensystemen. Maatgevend hiervoor is dat China op het gebied van (militaire) ruimtevaart, evenals in voorgaande jaren, in 2018 een aanzienlijke ontwikkeling heeft doorgemaakt en op het vlak van *hypersone* wapens waarschijnlijk een koppositie inneemt. Evenals de Russische Federatie, richt ook China zich op de ontwikkeling, productie en ingebruikname van wapensystemen tegen Westerse C4ISR-systemen. De verwachting is dat bovenstaande trends de komende jaren blijven toenemen en dat China eerder dan de Russische Federatie pariteit behaalt met het westen.

Voor sectoren waar nog onvoldoende technische kennis en vaardigheden aanwezig zijn, verwerven Chinese bedrijven of kennisinstituten, soms op heimelijke wijze, hoogwaardige componenten in andere landen. De Chinese interesse in Nederlandse militaire en *dual-use* goederen en kennis blijft een aandachtspunt voor de MIVD.

Technologische ontwikkeling op het gebied van aanslagmiddelen

De MIVD volgt ook actief de technologische ontwikkelingen van geïmproviseerde wapensystemen zoals geïmproviseerde bommen (*Improvised Explosive Devices*, IED's), *home made explosives* (HME) en commercieel verkrijgbare radiografische vliegtuigen en helikopters (*Unmanned Aerial Vehicles*, UAV's) die voor terroristische en/of militaire doeleinden worden gebruikt. Dergelijke wapensystemen spelen een steeds grotere rol, vooral in de strijd tegen niet-statelijke actoren. Voor de meeste terroristische organisaties, die niet aan conventionele wapens kunnen komen, zijn geïmproviseerde wapensystemen de '*weapon of choice*' door dat ze relatief makkelijk beschikbaar en goedkoop zijn. Doordat de MIVD gezamenlijk met andere defensieonderdelen onderzoek verricht naar de nieuwe technische toepassingen die terroristische organisaties gebruiken, kunnen tijdig tegenmaatregelen worden ontwikkeld. Het is hierbij ook belangrijk om vast te stellen hoe deze systemen tijdig kunnen worden gedetecteerd en geneutraliseerd.

Dreiging van massavernietigingswapens

In 2018 is wederom gebleken dat ontwikkelingen rond verschillende wapenprogramma's in landen van 'zorg' een dreiging blijven voor de internationale veiligheid. Zo zijn er in het afgelopen jaar meerdere incidenten geweest waar massavernietigingswapens daadwerkelijk zijn ingezet.

Evenals in de voorgaande jaren, vonden in 2018 in Syrië verschillende aanvallen met chemische wapens plaats. De zwaarste aanval was een aanval met chloorgas op de stad Douma in april. Hierbij kwamen tientallen burgers om en vielen veel gewonden. Ter vergelding voor deze aanval voerden de Verenigde Staten, het Verenigd Koninkrijk en Frankrijk raketaanvallen uit op locaties in Syrië die van belang waren voor het chemisch wapenprogramma van het land. De gezamenlijke Unit Contraproliferatie van de MIVD en AIVD (UCP) rapporteerden in 2018 uitgebreid over de inzet van chemische middelen door het Syrische regime.

Iran blijft ballistische raketten ontwikkelen en verbeteren. Over het Iraanse ballistische raketprogramma is verschillende keren gerapporteerd. Onderzocht werd ook of Iran zich hield aan de afspraken uit het Comprehensive Plan of Action.

Hoewel de felle retoriek tussen Donald Trump en Kim Jong Un sinds hun ontmoeting in juni verminderde, is de opgestarte dialoog weer afgebroken na de mislukte top in februari van dit jaar.

Niettemin heeft Noord-Korea nog geen raketlanceringen of nucleaire tests uitgevoerd. Er is echter nog geen zicht op een permanente oplossing voor het conflict. In 2018 is onderzoek gedaan naar het ballistische raketprogramma en het nucleaire wapenprogramma van Noord-Korea.

Ook is door de MIVD en AIVD inhoudelijke ondersteuning geleverd aan onderzoeken naar de dreiging die uitgaat van biologische en chemische wapenprogramma's van niet-statelijke actoren (bijvoorbeeld ISIS) en de risico's hiervan voor Nederland.

In 2018 was Nederland lid van de VN veiligheidsraad. Ter ondersteuning van deze rol hebben de MIVD en AIVD de Nederlandse overheid veelvuldig van informatie voorzien over casussen waar een relatie was met massavernietigingswapens.

Tegengaan van verwerving van kennis, technologie en goederen

Landen als Rusland, China, Iran, Syrië Pakistan en Noord Korea blijven in Nederland en andere westerse landen op zoek naar kennis en goederen voor gebruik in hun eigen wapenprogramma's. De MIVD en AIVD doen onderzoek naar de wijze waarop deze landen proberen de benodigde kennis en goederen te verkrijgen. Omdat deze kwestie vaak grensoverschrijdend is, wordt daarbij intensief samengewerkt met buitenlandse collega-diensten.

Ook wordt veelvuldig samengewerkt met Nederlandse partijen die een rol spelen bij de exportcontrole, zoals het ministerie van Buitenlandse Zaken (BZ) en de Douane. De MIVD en AIVD worden regelmatig om informatie gevraagd bij de beoordeling van een exportvergunning. Daarnaast is meerdere keren, door middel van een ambtsbericht, informatie met BZ gdeeld over verwervingspogingen die zijn geïdentificeerd. Het gaat dan om goederen die ook gebruikt kunnen worden voor de ontwikkeling of productie van massavernietigingswapens of overbrengingsmiddelen daarvan. Meerdere verwervingspogingen zijn zo voorkomen.

Nederlandse bedrijven moeten zich ervan bewust zijn dat landen interesse kunnen hebben in technologisch hoogwaardige producten en diensten die kunnen worden gebruikt voor de vervaardiging van massavernietigingswapens of onderdelen daarvan. De Unit Contra Proliferatie van MIVD en AIVD (UCP) geeft daarom voorlichting aan relevante partijen, zoals bedrijven en kennisinstellingen, over de risico's van proliferatie en wat zij kunnen doen om verdachte transacties te identificeren. De MIVD en AIVD leveren bijvoorbeeld een actieve bijdrage aan de seminars over exportcontrole die door het ministerie van Buitenlandse Zaken worden gegeven.

4 MILITAIRE MISSIES

Ter voorbereiding van een besluit tot inzet van Nederlandse militairen brengt de MIVD inlichtingenproducten uit over betreffend land en regio. De producten van de MIVD ondersteunen de politiek-militaire besluitvormers. Als de missie eenmaal is ontplooid, ondersteunt de MIVD de commandanten ter plaatse met operationele inlichtingenproducten. Deze producten dragen bij aan de *situational awareness* en de *situational understanding* van de commandanten ter plaatse en bieden hen handelingsperspectief.

Operation Inherent Resolve (Midden-Oosten)

Net als in de voorgaande jaren waren in 2018 Syrië en Irak primaire aandachtsgebieden voor de MIVD, vooral vanwege de Nederlandse betrokkenheid bij de strijd tegen ISIS. Nederland droeg het afgelopen jaar bij aan *Operation Inherent Resolve* (OIR) door Iraakse en Koerdische militairen te trainen en met de inzet van F-16's boven Irak en Oost-Syrië. De MIVD heeft aan nationale en internationale afnemers inlichtingenproducten verstrekt, om zo de besluitvorming over de militaire inzet en de daadwerkelijke defensie-operaties te ondersteunen.

Mede dankzij de Nederlandse inzet, heeft ISIS in Irak en Syrië geen controle meer over stedelijke gebieden en grote, aaneengesloten terreindelen. Dat wil niet zeggen dat de organisatie is verslagen. De groepering is goeddeels overgegaan op een *insurgency* en is in staat om in grote delen van Irak aanslagen te plegen. In Syrië werd ISIS verder teruggedrongen, zodat de groepering eind 2018 nog één *pocket* bezit in het uiterste oosten van het land. Daarnaast is ISIS elders actief in Syrië, echter zonder daar gebiedscontrole te kunnen uitoefenen. Al met al heeft de Coalitie de terreurgroep de afgelopen jaren weliswaar een ferme slag toegebracht, maar beschikt ISIS nog steeds over aanzienlijke capaciteiten en zijn de onderliggende problematieken nog onvoldoende geadresseerd. Zo blijft er een voedingsbodem voor radicalisering, omdat veel Iraakse soennieten zich gemarginaliseerd voelen.

De capaciteiten van de Iraakse strijdkrachten zijn flink verbeterd, hoewel zij nog altijd met tekortkomingen en problemen kampen die hun effectiviteit in de strijd tegen ISIS hinderen. De Koerdische veiligheidstroepen zijn goed in staat om de veiligheid in de Koerdische autonome regio te garanderen. Hun capaciteiten zijn verbeterd door internationale steun. Er is sprake van enige coördinatie tussen de Koerdische en Iraakse troepen.

Resolute Support (Afghanistan)

De missie Resolute Support (RSM) ondersteunt de verdere opbouw van een professioneel veiligheidsapparaat in Afghanistan, waaronder leger en politie. Nederlandse militairen adviseren samen met bondgenoten het hogere kader van het leger en de politie. Verder leveren Nederlandse *special forces* een bijdrage aan de opleiding en inzet van de speciale politie-eenheid ATF 888, die wordt aangestuurd door het Afghaanse ministerie van Binnenlandse Zaken.

De politieke inlichtingenanalyses van de MIVD gaan onder meer over het machtsspel tussen de regering van nationale eenheid (NUG) en *powerbrokers* in Noord-Afghanistan. Daarnaast werd in 2018 onderzoek gedaan naar de intenties, capaciteiten en activiteiten van de Taliban en *Islamic State Khorasan Province* (ISKP).

De MIVD heeft in 2018 beleidsmakers en commandanten tijdig voorzien van relevante inlichtingen, waardoor zij goed geïnformeerde besluiten konden nemen. Voor militair commandanten boden de inlichtingen van de MIVD een toetssteen voor het eigen veiligheidsbeeld in de planning van operaties.

MINUSMA (Mali)

Nederlandse militairen namen in 2018 deel aan de *Mission Multidimensionelle Intégrée des Nations Unies pour la Stabilisation au Mali* (MINUSMA) en de *European Training Mission* (EUTM) in Mali. Binnen MINUSMA verzamelen, verwerken en analyseren deze militairen inlichtingen voor de Verenigde Naties, die hierdoor effectiever kunnen optreden.

Het blijft onrustig in Mali. De onvrede wordt versterkt door verschillende maatregelen die de nieuwe regering sinds september heeft genomen. De laatste maanden van 2018 werden dan ook gekenmerkt door regelmatige (vreedzame) demonstraties van de oppositie en een golf van stakingen in diverse sectoren. Terroristische organisaties vormen de grootste bedreiging voor MINUSMA-troepen.

Het grensgebied van Noord-Mali met Niger werd het afgelopen jaar gekenmerkt door een geïntensiveerde strijd tussen terroristische groeperingen enerzijds en contraterreurtroepen gesteund door lokale gewapende groeperingen anderzijds. De veiligheidssituatie in Centraal-Mali werd in 2018 in toenemende mate gekenmerkt door zowel etnisch als radicaalislamitisch geweld. Het gebrek aan effectief overheids-optreden tegen het aanhoudende etnische geweld kan tot gevolg hebben dat de bevolking ter bescherming zijn heil zoekt bij niet-statelijke gewapende actoren, zoals zelfverdedigingsmilities of terroristische groeperingen.

Baltische staten en Polen

De vooruitgeschoven militaire aanwezigheid van de NAVO in de drie Baltische staten en Polen, *enhanced Forward Presence* (eFP), draagt bij aan de versterking van de Europese veiligheid, aan een geloofwaardige afschrikking tegen Russische agressie en toont bondgenootschappelijke solidariteit. De aanwezigheid van deze eenheden is beperkt in omvang en defensief van aard.


UN

De MIVD volgt de politieke en militaire ontwikkelingen aan de NAVO-oostflank en genereert inlichtingen ter ondersteuning van deze inzet.

UNTSO en UNIFIL (Israel/Libanon)
Nederland neemt deel aan de VN-missies UNTSO (*United Nations Truce Supervision Organisation*) die toezicht houdt op de bestanden in de regio tussen Israël en de omringende landen en UNIFIL (*United Nations Interim Force in Lebanon*) die toeziet op de beëindiging van vijandelijkheden in het grensgebied tussen Israël en Libanon en het ondersteunen van de inzet van de *Lebanese Armed Forces* (LAF). Er is een nauwe relatie van Libanon met Syrië.

Het voortdurende conflict in Syrië sorteert een negatief effect op de veiligheidssituatie in Libanon. De MIVD richt zich op zowel de politieke als de veiligheidssituatie in Libanon, waarbij aandacht wordt besteed aan onder meer Hezbollah. Deze organisatie speelt een belangrijke rol in de binnenlandse politiek van Libanon en strijdt in Syrië aan de zijde van de Syrische regeringstroepen.

UNMISS (Zuid-Soedan)
De *United Nations Mission in South Sudan* (UNMISS) ziet toe op de veiligheids-situatie in Zuid-Sudan. De militairen van UNMISS, waaronder Nederlandse militairen, beschermen de bevolking en onderzoeken mensenrechten-schendingen. Weken van intensieve onderhandelingen onder leiding van buurland Soedan hebben in september 2018 geleid tot een vredesakkoord tussen de strijdende partijen in Zuid-Soedan. Mede doordat niet alle partijen het vredesakkoord hebben getekend vinden er, ondanks een hernieuwd staakt-het-vuren, met regelmaat gevechten plaats in diverse delen van het land. Daarnaast blijft in grote delen van Zuid-Soedan de voedselonzekerheid erg groot. De komende maanden zullen in het teken staan van de implementatie van het vredesakkoord.

5 LANDEN VAN AANDACHT

In een snel veranderende en onvoorspelbare wereld met gekende en ongekende dreigingen groeit de behoefte aan militair relevante inlichtingen over bepaalde landen van aandacht ten behoeve van conflict-beheersing en –preventie.

Iran

In 2018 werd onderzoek verricht naar de (militaire) verhoudingen in de Golf-regio vanwege het strategische belang en de vitale economische betekenis hiervan voor het Westen in het algemeen en Nederland in het bijzonder. Iran hanteert het concept van strategische afschrikking voor de veiligheid in de Perzische Golf / Straat van Hormuz, maar ook vanwege de politiek-militaire controverse tussen Iran en Saudi-Arabië. Aandacht was er voor de Iraanse krijgsmacht en vooral zijn betrokkenheid bij de strijd in Syrië en Irak. Deze militaire steun is gericht op het bestrijden van ISIS als onderdeel van het nationale Iraanse veiligheidsbeleid en op het aan de macht houden van het Syrische regime. Ook streeft Iran naar permanente invloed in Syrië en Irak. Teheran zal ook doorgaan met het gecalculeerd leveren van militaire steun aan zijn zogenoemde 'strategische sjiitische bondgenoot', Hezbollah. De MIVD is van oordeel dat Iran aan de zijde van de Libanese Hezbollah een directe militaire confrontatie met Israël vermijdt.

Libië

De politieke situatie en de veiligheidssituatie in Libië bleven in 2018 in vele opzichten fragiel. Libië was en blijft o.a. op het gebied van terrorisme, mensen-, wapen-, brandstof- en narcoticasmokkel een risico voor een flink deel van de Afrikaanse regio en voor landen van de Europese Unie. Libië blijft nog steeds grofweg verdeeld in minstens twee politieke kampen met ieder hun eigen diffuse militaire verbanden. Ondanks diverse initiatieven van de Ondersteuningsmissie van de Verenigde Naties in Libië (UNSMIL) verwacht de MIVD dat het houden van in 2019 geplande presidentiële en parlementaire verkiezingen problematisch wordt. De belangen van de diverse partijen in Libië lopen teveel uiteen en er is geen partij die de veiligheid van verkiezingen kan garanderen.

Na in 2017 grotendeels onder de radar te hebben geopereerd, vertoonde ISIS-Libië in 2018 tekenen van herstel met diverse assertieve operaties. Tekenend voor dit herstel waren de relatief hoge aantallen succesvolle aanslagen in zowel rurale als verstedelijkte gebieden in Libië.

Ondanks de rivaliteit tussen strijdende partijen en het ontbreken van een sterk centraal gezag is in 2018 de migratiestroom richting Europa sterk afgenomen ten aanzien van 2017. Deze daling is grotendeels het gevolg van diverse Italiaanse initiatieven samen met de GNA en diverse aan de GNA gelieerde partijen. Ongeveer 21.000 irreguliere migranten arriveerden in 2018 via de centrale Middellandse zeeroute in Europa. Ondanks deze lagere aantallen zitten naar schatting nog tenminste 700.000 irreguliere migranten vast in Libië.

Latijns-Amerika en de Caribische regio

In een gezamenlijk team (Team Caribisch Gebied) vergaren de MIVD en AIVD informatie over het Caribisch gebied en Zuid-Amerika, ter ondersteuning van de het buitenlands beleid en defensiebeleid van het Koninkrijk der Nederlanden. Daarom worden ontwikkelingen die van invloed kunnen zijn op de veiligheid en buitenlandse belangen van het Koninkrijk en op de Nederlandse militaire presentie in de Caribische delen van het Koninkrijk door de diensten gevolgd.

De situatie in Venezuela is zeer zorgelijk. Het land heeft te lijden onder een combinatie van grootschalige politieke en sociaaleconomische crises. In 2018 is de economische en veiligheidssituatie in Venezuela verder verslechterd en is de democratie verder uitgehold.

Maduro had internationaal nog steun van een aantal landen, waaronder de Russische Federatie en China. In ruil voor wapenleveranties, leningen en goederen hebben deze landen de afgelopen jaren aanzienlijke belangen verkregen in de Venezolaanse economie, voornamelijk in de oliesector. Als blijk van de goede betrekkingen met Venezuela, heeft de Russische Federatie aan het einde van 2018 twee strategische bommenwerpers voor oefeningen naar Venezuela gevlogen. Turkije heeft de banden met Venezuela aangehaald.

Als gevolg van de economische crisis en hyperinflatie kampt de Venezolaanse bevolking met tekorten aan eerste levensbehoeften en een zeer slechte veiligheids- en gezondheidssituatie. Inmiddels hebben miljoenen Venezolanen hun land verlaten. De meesten van hen zijn naar landen in de regio vertrokken, waaronder ook de Caribische delen van het Koninkrijk.

De verwachting is dat Venezuela komend jaar een bron van instabiliteit in de regio zal blijven. De instabiele situatie heeft een negatief effect op de regionale veiligheidssituatie, vanwege de potentiële uitstralingseffecten blijven de MIVD en AIVD de ontwikkelingen nauwlettend volgen.

Venezuela beschikt over geavanceerde luchtafweersystemen van Russische makelij. Zoals het kaartje duidelijk maakt, zouden deze systemen het luchtruim boven de Caribische delen van het Nederlands koninkrijk kunnen bestrijken. De Venezolaanse strijdkrachten hebben een defensieve doctrine en dus geen offensief oogmerk. De instabiele situatie in het land geeft echter reden om de situatie nauwlettend te volgen.

6 WEERBAAR EN ALERT

Om dreigingen tegen de Nederlandse Defensiebelangen tijdig te ontdekken en onschadelijk te maken, levert de MIVD contra-inlichtingen.

Spionage

Bij ongeoorloofd vergaren van informatie of ongewenste beïnvloeding door landen dan wel niet-statelijke actoren is sprake van spionage. De MIVD voert onderzoek uit naar spionage wanneer deze een bedreiging kan vormen voor het optreden van de krijgsmacht, voor de Nederlandse defensie-industrie of voor bondgenootschappelijke organisaties. Naast spionage kunnen staten zich ook voor andere doeleinden met heimelijke activiteiten bezighouden, bijvoorbeeld voor de beïnvloeding van de politieke besluitvorming of de manipulatie van de beeldvorming en de media. De dreiging doet zich niet alleen voor in Nederland, maar ook in de Caribische delen van het Koninkrijk en in missiegebieden.

Rusland en China zijn de twee voornaamste actoren waarnaar onderzoek wordt gedaan. Russische inlichtingendiensten zijn heimelijk aanwezig en actief in Nederland, net als in andere westerse landen. De Chinese inlichtingendiensten vergaren actief militaire inlichtingen in Nederland. De dreiging die uitgaat van deze activiteiten tegen Nederlandse defensiebelangen wordt onderzocht en daar waar mogelijk worden maatregelen getroffen. De dreiging tegen Defensie richt zich tevens op de verwerving van militair technologische kennis en specifieke *dual-use* technologie. Deze technologie kan zowel civiel als militair worden gebruikt, zoals satelliettechnologie.

Het afgelopen jaar is door toegenomen dreiging het belang en de prioriteit van contra-inlichtingenonderzoek naar spionage verder toegenomen.

Extremisme en radicalisering

De MIVD verricht onderzoek naar verschijnselen van radicalisering en extremisme, van welke vorm dan ook, onder Defensiepersoneel. Feitelijke gedragingen zijn daarbij altijd leidend. De ontwikkelingen in de samenleving en de invloed hiervan op Defensie worden door de MIVD vanzelfsprekend in de gaten gehouden.

Salafisme

Feitelijke gedragingen die hun oorsprong vinden in een salafistische geloofsovertuiging kunnen een dreiging vormen voor Defensie en de nationale veiligheid.

In voorkomende gevallen zal worden bezien of, en zo ja welke, maatregelen dienen te worden getroffen. Dit is tot op heden niet nodig geweest.

De MIVD heeft in 2018 onderzoek verricht naar de jihadistisch terroristische dreiging tegen belangen van Defensie om deze tijdig te signaleren en te neutraliseren. De activiteiten concentreerden zich zowel op het onderkennen van (vermeende) radicalisering binnen Defensie als op het onderkennen van jihadistisch terroristische dreiging tegen Defensie. De MIVD waarschuwt defensieonderdelen en externe organisaties over mogelijke dreigingen, wat hen in staat stelt om passende maatregelen te treffen. Dit is tot op heden niet nodig geweest. De MIVD heeft evenmin aanwijzingen dat buitenlandse terreurcellen contacten onderhouden of onderhielden met Nederlandse militairen.

Extremisme

Acties tegen Defensie vanuit links-activistische en/of links-extremistische groepen en individuen zijn voornamelijk gericht op de thema's

wapenhandel, nucleaire wapens, betrokkenheid van Defensie bij de uitvoering van het asielbeleid en de werving van Defensiepersoneel. Deze acties hebben voor het overgrote deel een activistisch karakter en leverden slechts in een enkel geval schade of hinder voor de krijgsmacht op.

De rechts-extremistische scene in Nederland focust zich de afgelopen jaren vooral op de islam. Het rechts-extremisme kent een opleving in Nederland. Rechts-extremisme binnen de defensieorganisatie kan de interne veiligheid van de krijgsmacht ondermijnen. Het gaat bijvoorbeeld om interne onrust als gevolg van discriminatie van militairen, waardoor zowel de hiërarchische structuur binnen een eenheid als de onderlinge samenwerking onder druk kunnen komen te staan.

Het is daarom van belang personen of groepen binnen de defensieorganisatie, die het extremistische gedachtegoed aanhangen dan wel (actief) steun verlenen aan extremistische partijen en organisaties, tijdig te onderkennen. Een rechts-extremistische geweldsdreiging richting Defensie is vooralsnog niet onderkend.

Defensie heeft in 2018 drie onderzoeken ingesteld naar aanleiding van signalen over racistische uitingen met verwijzingen naar Nazi-Duitsland. De AIVD-rapportage over rechts-extremisme meldt onder andere dat binnen rechts-extremistische kringen een polariserend discours over de islam wordt gevoerd. Hiervoor zijn binnen Defensie geen aanwijzingen. Evenmin heeft de MIVD op dit moment indicaties dat binnen de krijgsmacht sprake is van rechts-extremistische netwerken.

Veiligheidsonderzoeken

Per 1 oktober 2018 is de ministeriële Regeling Unit Veiligheidsonderzoeken in werking getreden. Met deze regeling is het kader geschapen om het Bureau Veiligheidsonderzoeken Defensie en Bureau Veldorganisatie van de MIVD en de Businessunit Veiligheidsonderzoeken van de AIVD in een nieuwe unit samen te laten gaan. Vooruitlopend op deze samenwerking is per maart 2018 geharmoniseerd.

De MIVD heeft in 2018 17.250 veiligheidsonderzoeken uitgevoerd naar personen die een vertrouwensfunctie (wilden gaan) vervullen. Dat aantal wijkt percentueel gezien weinig af van het totaal aantal verrichte veiligheidsonderzoeken (17.106) in 2017. Het aantal DCPL-onderzoeken (sollicitanten) is gestegen ten opzichte van dezelfde periode vorig jaar, 5.025 tegenover 4.639 (2017).

Uitgangspunt is dat 90% van de veiligheidsonderzoeken die de MIVD uitvoert binnen de maximale wettelijke beslistermijn van 8 weken moet zijn afgerond. Voor 2018 is het aantal door de MIVD uitgevoerde onderzoeken in 93% van de gevallen binnen 8 weken afgerond.

Onderzoeken	Positieve besluiten	Negatieve besluiten	Totaal aantal besluiten
A-niveau door MIVD	1.924	3	1.927
B-niveau door MIVD	10.431	17	10.448
C-niveau door MIVD	4.872	3	4.875

Bezwaar en beroep

Naar aanleiding van de besluiten tot weigering of intrekking van de VGB hebben verschillende mensen bezwaar aangetekend en/of zijn in (hoger) beroep gegaan. Onderstaand in de tabel een overzicht van de afhandeling van bezwaar- en (hoger)beroepsprocedures naar aanleiding van besluiten veiligheidsonderzoeken.

2018	Ingediend in 2018	Afgedaan in 2018	Ongegrond	Gegrond	Niet-ontvankelijk	Ingetrokken	Afgewezen
Bezwaren	3	2	-	-	2	-	-
Beroepen	1	2	2	-	-	-	-
Hoger beroep	3	2	2	-	-	-	-
Voorlopige voorziening	-	-	-	-	-	-	-
Totaal	7	6	4	-	2	-	-

Industrieveiligheid

In het kader van de Industrieveiligheid adviseert en controleert de MIVD de integrale beveiliging van de defensieorderbedrijven, die onder de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) vallen, de zogeheten ABDO-bedrijven. Hier gaat het om bedrijven die zijn belast met de uitvoering van gerubriceerde of vitale defensieopdrachten voor Nederland of voor buitenlandse opdrachtgevers door de Nederlandse defensie-industrie. Alleen geautoriseerde ABDO-bedrijven mogen gerubriceerde opdrachten voor Defensie uitvoeren.

Het aantal bedrijfsbezoeken, het aantal audits en het aantal voorlichtingssessies is in dit jaar geïntensiveerd. Net als andere jaren zijn defensie-orderbedrijven gecontroleerd op het voldoen aan de ABDO regelgeving.

Bureau Industrieveiligheid constateerde in 2018 dat bedrijven voldoen aan de oude regelgeving, maar dat er nog wel beveiligingsmaatregelen getroffen moeten worden om aan de nieuwe regelgeving te kunnen voldoen. De nieuwe regelgeving is ingevoerd op 1 juni 2017 ingevoerd. Deze regelgeving was nodig gezien de toegenomen dreiging tegen de Nederlandse defensie-industrie. De ABDO bedrijven is gevraagd om incidenten nauwkeuriger te melden. Dit heeft geleid tot een hoger aantal incidenten in 2018.

Screenen bedrijfsleven/Industrieveiligheid

671 bedrijven in portefeuille

185 afgegeven ABDO-autorisaties

27 geweigerde ABDO-autorisaties

108 meldingen incidenten

75 behandelde aanvragen niet-Nederlanders op vertrouwensfuncties bij ABDO opdrachten

Cijfers Facility Security Clearance (FSC)
Met buitenlandse National en Designated Security Authorities (NSA/DSA) is contact onderhouden om Facility Security Clearances (FSC) aan te vragen en af te handelen.

Op verzoek van het buitenland wordt in verband met de eventuele gunning van een buitenlandse defensieorder aan een Nederlands bedrijf gevraagd een FSC af te geven.

FSC

55	door buitenland aangevraagde FCS's
52	aan buitenland afgeven FSC's
51	in buitenland door NL aangevraagde FSC's
49	uit buitenland voor NL ontvangen FSC's

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

Met de AIVD is afgesproken om de Request for Visit samen uit te voeren.

RfV

2377	uitgaande aanvragen
651	inkomende aanvragen
3038	totaal aanvragen

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. Afgelopen jaar heeft de MIVD vier keer een dreigingsinschatting gemaakt.

De MIVD kan ook een dreigingsanalyse maken. Dat is een uitgebreide analyse van concrete en voorstelbare dreigingen vanuit het perspectief van de bedreigde, zoals een politicus of diplomaten. Afgelopen jaar heeft de MIVD twee keer een dreigingsanalyse gemaakt.

Tapstatistieken

Afgelopen jaar heeft de regering besloten de tapstatistieken van de AIVD en MIVD voortaan jaarlijks openbaar te maken in de jaarverslagen. Het gaat dan om de cijfers van het aantal taps van de diensten per jaar. In 2018 zijn door de MIVD 309 taps geplaatst. Voorbeelden zijn een telefoontap 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.

Melding bijzondere voorvallen

Jaarlijks ontvangt de MIVD meldingen van bijzondere voorvallen. Dit zijn voornamelijk voorvallen vanuit de defensieorganisatie en meldingen van partnerorganisaties of burgers. In 2018 ontving de MIVD 5119 meldingen. De meldingen die de MIVD ontvangt (zowel uit Nederland als de missiegebieden) zijn zeer divers. Een deel van deze meldingen houdt een mogelijke bedreiging voor de veiligheid van de krijgsmacht in. Daarbij valt te denken aan opvallende belangstelling voor kazernes, defensiepersoneel of het thuisfront.

Indien noodzakelijk kan de MIVD een derde partij over de (mogelijke) dreiging informeren zodat passende maatregelen kunnen worden genomen. Belangrijke partners binnen Defensie zijn de Beveiligingsautoriteit Defensie en de Koninklijke Marechaussee, buiten Defensie zijn dat de AIVD, NCTV en de Nationale Politie.

De CI-analyses van dreigingen in (potentiële) missiegebieden worden uiteraard meegenomen in de inlichtingenproducten zoals die worden opgesteld voor de afnemers. Met het uitvoeren van deze taken levert de MIVD een belangrijke bijdrage aan de veiligheid van Defensie en de defensie-industrie, zowel in Nederland als in de missiegebieden.


Mem[1027/12007MB]
Swp[
Tasks: 75, 20
Load average:
Uptime: 1 day,
PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
2321 root 20 0 99M 84812 460 S 4.0 0.7 1:35.60 rsync -r -u
2319 root 20 0 99M 85572 948 D 3.3 0.7 1:15.00 rsync -r -u
7497 root 20 0 26092 2352 1444 R 1.3 0.0 0:06.03 htop
7414 root 20 0 26000 2040 1452 S 0.7 0.0 0:01.11 bmon
1595 20 0 481M 48824 6712 S 0.0 0.4 0:40.17 /usr/sbin/mysq
1631 20 0 481M 48824 6712 S 0.0 0.4 0:04.91 /usr/sbin/mysq
1617 20 0 481M 48824 6712 S 0.0 0.4 0:02.70 /usr/sbin/mysq
1579 root 20 0 19268 740 508 S 0.0 0.0 0:08.70 /usr/sbin/irqb
1618 20 0 481M 48824 6712 S 0.0 0.4 0:02.71 /usr/sbin/mysq
1614 20 0 481M 48824 6712 S 0.0 0.4 0:02.69 /usr/sbin/mysq
7466 20 0 103M 2100 1028 S 0.0 0.0 0:00.04 sshd: thijs@pt
2120 20 0 103M 2512 1116 S 0.0 0.0 0:02.58 sshd: thijs@pt
1632 20 0 481M 48824 6712 S 0.0 0.4 0:07.74 /usr/sbin/mysq
1620 20 0 481M 48824 6712 S 0.0 0.4 0:02.70 /usr/sbin/mysq
1619 20 0 481M 48824 6712 S 0.0 0.4 0:02.70 /usr/sbin/mysq
1621 20 0 481M 48824 6712 S 0.0 0.4 0:02.71 /usr/sbin/mysq
1615 20 0 481M 48824 6712 S 0.0 0.4 0:02.73 /usr/sbin/mysq
1613 20 0 481M 48824 6712 S 0.0 0.4 0:02.70 /usr/sbin/mysq
1612 20 0 481M 48824 6712 S 0.0 0.4 0:02.70 /usr/sbin/mysq
1064 root 20 0 186M 2804 1508 S 0.0 0.0 0:01.78 nmbd -D
1995 root 20 0 269M 15152 9748 S 0.0 0.1 0:01.64 /usr/sbin/apach
7561 root 20 0 21268 2356 1660 S 0.0 0.0 0:00.03 bash
7544 20 0 103M 2020 1028 S 0.0 0.0 0:00.11 sshd: thijs@pts
1616 20 0 481M 48824 6712 S 0.0 0.4 0:02.69 /usr/sbin/mysq
7344 20 0 103M 2100 1028 S 0.0 0.0 0:00.12 sshd: thijs@pts
770 root 20 0 266M 7828 5960 S 0.0 0.1 0:01.34 smbd -F
7559 root 20 0 64532 1836 1376 S 0.0 0.0 0:00.01 su
7545 20 0 22468 3608 1708 S 0.0 0.0 0:00.04 -bash
7495 root 20 0 103M 4236 3252 S 0.0 0.0 0:00.02 sshd: [accepted
1 root 20 0 33620 2916 1460 S 0.0 0.0 0:05.88 /sbin/init
446 root 20 0 19476 652 452 S 0.0 0.0 0:00.14 upstart-udev-br
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice - F8Nice + F9Kill F10Qui

7 WET OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN 2017

Op 1 mei 2018 is de Wet op de inlichtingen en veiligheidsdiensten 2017 (Wiv 2017) in werking getreden. Wijziging van de wet was nodig omdat nieuwe technologische ontwikkelingen hebben geleid tot verandering in de manier waarop mensen met elkaar communiceren. Om ongekende dreigingen tijdig te kunnen onderkennen, moeten we toegang hebben tot die digitale gegevensstromen. Naast het gericht op een persoon of organisatie zoeken (wat onder de oude wet al kon), maakt de nieuwe wet het mogelijk dat onderzoeksopdrachtgericht op een kenmerk te doen. Zo kan de MIVD haar essentiële taak in de toekomst blijven vervullen. Inzet van deze nieuwe bevoegdheid wordt nog voorbereid. In 2018 is er dus nog geen gebruik van gemaakt.

De Wiv 2017 kent niet alleen nieuwe bevoegdheden, maar ook versterking van de waarborgen voor de privacy. Zo blijft de wet in balans. Er worden nieuwe eisen gesteld aan de MIVD op het gebied van zorgplicht voor gegevens en datareductie. Ook striktere regels over bewaartermijnen en het terstond vernietigen van niet-relevante gegevens maken de inbreuk op de persoonlijke levenssfeer van onschuldige burgers zo klein mogelijk.

Nieuw in de wet is de oprichting van een onafhankelijke toetsende instantie, de Toetsingscommissie Inzet Bevoegdheden (TIB). Deze commissie toetst bij bijzondere bevoegdheden vooraf of de inzet ervan rechtmatig is. Ter inhoudelijke voorbereiding van de TIB op de toetsing heeft de MIVD briefings gegeven.

In het voorjaar van 2018 zijn naar aanleiding van het referendum over de Wiv 2017 door het kabinet extra waarborgen toegezegd. Er komt een wijziging van de Wiv waardoor expliciet in de wet komt te staan dat inzet van een bevoegdheid ‘zo gericht mogelijk’ gebeurt. Dit naast de al in de wet opgenomen vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Ook zijn er aanvullende beleidsregels gemaakt en zijn er vervroegd wegingsnotities gemaakt voor de bestaande samenwerkingsrelaties met buitenlandse partnerdiensten. Op 1 januari 2019 waren niet al deze wegingsnotities van de MIVD gereed. De samenwerking met partners zonder wegingsnotities is opgeschort.

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft de implementatie van de Wiv 2017 onderzocht en schatte voor een aantal waarborgen het risico op toekomstig onrechtmatig handelen door de MIVD als gemiddeld of hoog in. Dit betreft geen oordeel dat daarmee onrechtmatig is gehandeld.

De implementatie van de wet vergt veel van de diensten. Tegelijkertijd moet de operationele taakuitvoering van de diensten gewoon doorgang vinden. Deze combinatie vormt een uitdaging.


FREDERIKKAZERNE

8 MENSEN, MIDDELEN, MANIEREN

Werving personeel

De MIVD was in 2018 niet volledig gevuld. Er is een Task Force opgericht om de vulling en de verdere groei van de organisatie in samenspraak met alle ketenpartners te plannen, te begeleiden en te controleren.

Informatietechnologie

Het belang van hoogwaardige informatie- en communicatietechnologie voor de MIVD is nauwelijks te overschatten. De dienst ontwikkelt zich meer en meer tot een datagedreven organisatie; *(big) data analytics* maakt zowel target gericht onderzoek mogelijk als het achterhalen van ongekende dreigingen. Continue verbetering van de informatie-technologie voor verwerving, opslag, ontsluiting, analyse en verspreiding van gegevens is daarmee zeer belangrijk. Een deugdelijke gegevens-huishouding is ook vanuit de optiek van de Wiv 2017 van essentieel belang.

In 2018 heeft de MIVD eerste stappen gezet om de ICT-achterstand in te lopen. Ook de CTIVD heeft zorgen geuit over de ICT-infrastructuur bij de MIVD. Het wegwerken van de ICT-achterstand kost tijd en vraagt om investeringen. Defensie investeert daarom de komende jaren in de ICT bij de MIVD, oplopend tot 20 miljoen euro structureel.
In 2018 heeft, mede door de situatie op de arbeidsmarkt, een beperkte groei van de personele capaciteit in de ICT plaatsgevonden.

Infrastructuur

Gezien de groei van de MIVD vanaf 2018 tot eind 2020 is aan het Rijksvastgoedbedrijf opdracht gegeven delen van de Frederikkazerne te verbouwen. De verbouwing is medio 2018 gestart. De bestaande huisvesting wordt daarmee vanaf medio 2018 op norm gebracht en gehouden.

Samenwerking met AIVD

De bestaande samenwerking tussen de MIVD en AIVD op het gebied van uitwisseling van informatie en rapportages is gecontinueerd. De implicaties van de nieuwe WIV voor de werkwijze van beide diensten is onderwerp geweest van veelvuldig overleg en samenwerking. De MIVD heeft tot taak om veiligheidsonderzoeken uit te voeren, zoals bedoeld in de Wiv en in de Wet veiligheidsonderzoeken (Wvo). Sinds 1 oktober 2018 werken de AIVD en MIVD samen in de Unit Veiligheidsonderzoeken (UVO). Daarmee is uitvoering gegeven aan de aanbeveling van de commissie-Dessens om een gemeenschappelijke organisatie voor veiligheidsonderzoeken te vormen. De voorbereiding van een geïntegreerde Unit Veiligheids Onderzoeken is afgerond waardoor er nu sprake is van een werkwijze, het gebruik van een informatiesysteem voor nieuwe onderzoeken en samenwerking op een locatie. In verband met beschikbare ruimte is huisvesting op een locatie nog niet volledig gerealiseerd. Door de AIVD en MIVD zijn met Defensie en het Rijksvastgoedbedrijf opties voor herhuisvesting en colocatie in een gebouw uitgewerkt.


NLD
UN

9 VOORUITKIJKEN: WAT WE DOEN IN 2019

Ook in 2019 staat de MIVD voor de taak inlichtingenondersteuning te bieden om de vele complexe en veelzijdige dreigingen het hoofd te bieden.

De onderzoeken van de MIVD richten zich niet alleen op het inzichtelijk maken van bestaande, reeds gekende dreigingen, maar ook op het tijdig onderkennen en duiden van nog ongekende dreigingen. In 2019 heeft de implementatie van de Wet op de inlichtingen en veiligheidsdiensten 2017 (Wiv 2017) hoge prioriteit voor de MIVD. De eerste voortgangsrapportage van de CTIVD liet zien dat er nog veel werk te verrichten is om risico's op onrechtmatig handelen te verkleinen. Bijzondere aandacht zal er zijn voor zorgplicht, datareductie en OOG-interceptie (inclusief geautomatiseerde data-analyse) De komende jaren wordt bovendien geïnvesteerd in de ICT-infrastructuur. Dit moet leiden tot zichtbare vermindering van de geconstateerde risico's in de vervolgrapportages van de CTIVD.

Hieronder worden per aandachtsgebied de hoofdlijnen beschreven van het MIVD onderzoek.

Landenonderzoek

Ook in 2019 doet de MIVD in 2019 onder meer onderzoek naar Afghanistan, Mali, Syrië en Irak. Tevens wordt de inzet van Nederlandse militairen in het kader van *enhanced Forward Presence* (eFP) ondersteund. Daarnaast doet de MIVD samen met de AIVD onderzoek naar de politieke en sociaaleconomische crisis in Venezuela en de mogelijk uitstraling-seffecten richting het Koninkrijk.

Contraproliferatie en proliferatie van militaire technologie

Massavernietigingswapens vormen een grote bedreiging voor de internationale vrede en veiligheid. Nederland heeft verdragen ondertekend die erop gericht zijn om de proliferatie van dergelijke wapens tegen te gaan. De AIVD en de MIVD doen gezamenlijk onderzoek naar landen die ervan worden verdacht dat zij, in strijd met die verdragen, werken aan het ontwikkelen van massavernietigingswapens en hun overbrengingsmiddelen of daar al over beschikken.

De MIVD doet tevens onderzoek naar militair technologische ontwikkelingen in andere landen en de proliferatie van hoogwaardige militaire technologie en wapensystemen naar crisisgebieden, zodat de Nederlandse krijgsmacht op de juiste wijze kan worden uitgerust tegen bestaande en toekomstige dreigingen.

Spionage en beïnvloeding

Een combinatie van klassieke en digitale spionage, beïnvloeding en sabotage zullen ook in de nabije toekomst een ernstige en groeiende dreiging vormen voor Nederland en zijn bondgenoten. Hacken biedt mogelijkheden voor sabotage en beïnvloeding van politieke en bestuurlijke besluitvorming of de publieke opinie door het gebruik van gehackte informatie. Ook door middel van overnames of investeringen trachten landen informatie te bemachtigen of strategische afhankelijkheden te creëren.

Attributie blijft een belangrijk middel, onder meer omdat het de kosten voor de daders verhoogt. Een doordachte, gecoördineerde en overheid brede inzet van instrumenten is van belang. Daartoe richten MIVD, AIVD, NCSC, Politie en OM onder meer een cel op waarin de cyberonderzoeken bij elkaar worden gebracht en waarbij gezamenlijk wordt nagedacht over effectieve vervolgstappen. Deze cel geldt als aanvulling van het succesvol opererend afstemmingsoverleg Cyber, dat wordt voorgezet door de Landelijk Officier van Justitie.

Radicalisering en extremisme
Het onderzoek naar verschijnselen van radicalisering, van welke vorm dan ook, onder Defensiepersoneel wordt gecontinueerd in 2019. Oogmerk van dit onderzoek is ongewenst gedrag tijdig te signaleren. De MIVD adviseert over te treffen maatregelen om deze dreigingen te signaleren en het hoofd te bieden. Het bevorderen van awareness en understanding vereist permanente aandacht.

Hoofdlijnen andere taken en doelstellingen 2019
Naast de hierboven beschreven prioriteiten en accenten, wordt hieronder inzicht gegeven in de overige taken en doelstellingen voor 2019.

Veiligheidsonderzoeken
In 2019 wordt invulling gegeven aan het advies van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) om het beleid van veiligheidsonderzoeken van de AIVD en de MIVD te harmoniseren.

Regeling algemene beveiligingseisen Defensieorderbedrijven (ABDO)
De ABDO-regeling schrijft voor dat Defensieorderbedrijven worden gescreend. Voor de implementatie van omvangrijke materieelprojecten en de uitvoering van bepaalde diensten is Defensie afhankelijk van derden. Naast de vereiste screening zal de MIVD in 2019 eveneens onderzoek doen naar spionage- en cyberactiviteiten die vreemde mogendheden mogelijk tegen de Defensie industrie ontplooien. Een belangrijk aandachtspunt daarbij zijn de bedrijven die actief betrokken zijn bij de vervangingstrajecten van defensiematerieel. Het ministerie van Defensie gaat met de Stichting Nederlandse Industrie voor Defensie en Veiligheid (NIDV) intensiever samenwerken op het gebied van cybersecurity, met als doelstelling de (digitale) beveiliging van de Nederlandse defensie-industrie te versterken en de defensiebedrijven bewuster te maken van de dreiging.

Samenwerking met AIVD
Ook in 2019 blijft het onze ambitie om de samenwerking tussen de AIVD en de MIVD over de volle breedte van het werk in het veiligheidsdomein te versterken. De verslechterde veiligheidssituatie en de effecten daarvan op het dreigingsbeeld maken het noodzakelijk te blijven zoeken naar verbeteringen, die ervoor zorgen dat de diensten op de meest effectieve en efficiënte wijze blijven functioneren.
Mensen, middelen, manieren

Werving Personeel
De MIVD zal ook in 2019 kampen met achterstanden in personele vulling. Tegelijkertijd groeit de organisatie. 2019 staat dan ook in het teken van het werken aan oplossingen voor de achterstanden in de vulling en het mogelijk maken van de groei van de organisatie.

In 2019 wordt, in het licht van deze verdere groei, het pallet aan maatregelen om de arbeidsmarkt in Nederland te bereiken verder geprofessionaliseerd. De opgerichte Task Force zal de verdere groei van de organisatie in samenspraak met alle ketenpartners plannen, begeleiden en controleren. Daarnaast wordt sturing op de personele keten verder geïntensiveerd om deze keten optimaal te laten werken.

ICT en Informatievoorziening
In 2019 en de komende jaren zet de MIVD intensivering op het gebied van ICT en informatievoorziening versterkt door. Hiermee zal verbetering en vernieuwing plaatsvinden, waarbij de volgende speerpunten worden gehanteerd:

- Wiv-conforme gegevenshuishouding. Een verantwoorde uitvoering van de wet vereist een up-to-date ICT-landschap, vernieuwingen op het gebied van de verwerking van data en het aanpassen van werkprocessen. Dat kost tijd en vraagt om investeringen; hier wordt prioriteit aan gegeven.

- Versterken technische operationele voorzieningen. Dit betreft de IT-voorzieningen om 24x7, wereldwijd, in samenwerking met partners of zelfstandig, gegevens te verzamelen, te verwerken en te verspreiden.
- Verhogen voortzettingsvermogen en wendbaarheid door onder andere het wegwerken van technologische achterstand, aanvullende security voorzieningen en toepassing van schaalbare en modulaire basisinfrastructuur.
- Investeren in innovatie. Om de capaciteiten van de dienst, mede gezien de snelle technologische en operationele ontwikkelingen, blijvend aan te laten sluiten bij de I&V-processen is structureel innoveren noodzakelijk.
- Organisatorische doorontwikkeling. Met als doel het realisatie-vermogen en de adaptiviteit te vergroten, komen IT-trajecten met een lange aanloopfase en realisatieduur minder voor; activiteiten worden meer en meer opgedeeld in kleinere stappen met een kortere realisatieduur. De organisatie maakt gebruik van agile methodieken, uitvoering geschiedt in multidisciplinaire IT-teams, waarbij de baten centraal staan en kort-cyclisch bijsturen de regel is.

Infrastructuur

Momenteel zijn de ministeries van Defensie en Binnenlandse Zaken en Koninkrijksrelaties met elkaar in gesprek over de wijze waarop co-locatie van de MIVD en de AIVD het beste kan worden gerealiseerd.


Amersfoort

10 MET WIE WIJ SAMENWERKEN

Nationale samenwerking

Binnen Defensie

Defensie Inlichtingen en Veiligheidsnetwerk
Een succesvolle militaire operatie is ondenkbaar wanneer de commandant van een eenheid niet over een goede inlichtingenpositie beschikt. Om die inlichtingenpositie te kunnen realiseren, is het belangrijk dat alle inlichtingen- en veiligheidsmedewerkers van Defensie nauw samenwerken. In het Defensie Inlichtingen en Veiligheidsnetwerk wordt die samenwerking ingevuld. Cruciale partners hierin zijn onder meer het JISTARC en Defensie Cyber Commando.

Nederlandse Defensie Academie
Ook met de Nederlandse Defensie Academie is samenwerking op het gebied van wetenschappelijk onderzoek en onderwijs over Inlichtingen & Veiligheid.

Met de AIVD

Nationaal werkt de MIVD hecht en intensief samen met de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). De AIVD en MIVD hebben een aantal gezamenlijke teams (Unit Contraproliferatie, Team Caribisch Gebied), de *Joint Sigint Cyber Unit* (JSCU): een gezamenlijke afdeling op het gebied van *Signals Intelligence* en *Cyber*. Daarnaast hebben de AIVD en MIVD een gezamenlijke Unit Veiligheidsonderzoeken (UVO). AIVD en MIVD werken ook samen in het kader van het convenant delen van dreigingsinformatie voor de burgerluchtvaart.

Met binnenlandse partners

Een andere belangrijke nationale partner is de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De NCTV coördineert beveiligingsmaatregelen op basis van informatie die onder meer door de MIVD wordt aangeleverd. Een onderdeel van de NCTV waarin de MIVD participeert, is het Nationaal Cyber Security Centrum voor samenwerking op het gebied van *cyber security*. Het gaat om operationele overleggen waarbij informatie wordt uitgewisseld bij cyberincidenten of –dreigingen.
Ook is de NCTV voorzitter van een aantal overlegfora, waarin de MIVD zitting heeft. Zo neemt de MIVD deel aan het Afstemmingsoverleg Bewaking en Beveiliging (ABB), de Stuurgroep Bewaken en Beveiligen en het (pre-) Gezamenlijk Comité Terrorismebestrijding. De MIVD draagt daarnaast bij aan het Dreigingsbeeld Terrorisme Nederland (DTN).

Ook de politie en het ministerie van Buitenlandse Zaken zijn belangrijke binnenlandse partners. Ook in 2018 heeft de dienst gevraagd en ongevraagd inlichtingenappreciaties aan het ministerie van Buitenlandse Zaken verstrekt. Door de zetel in de VN Veiligheidsraad was sprake van een grotere spreiding van onderwerpen en aandachtsgebieden. De inspanningen ten aanzien van de samenwerking en afstemming met de Nationale Politie op zowel operationeel, tactisch en strategisch vlak zijn in 2018 geïntensiveerd.

Overige nationale samenwerkingsverbanden waarin de MIVD participeert zijn:

Defensie Computer Emergency Response Team (DefCERT)
DefCERT werkt samen met de MIVD om de netwerken van Defensie veilig te houden. Zo wordt onder meer gezamenlijk onderzocht wie achter de digitale aanvallen op het defensienetwerk zitten.

Dreigingsmanagement Potentieel Gewelddadige Eenlingen (PGE)
De MIVD participeert in de interdepartementale stuurgroep Dreigingsmanagement Potentieel Gewelddadige Eenlingen (PGE) onder coördinatie van de NCTV. Deze stuurgroep geeft richting aan de activiteiten die in Nederland worden ondernomen om de (mogelijke) dreiging hiervan te kunnen beheersen.

Contra Terrorisme (CT) Infobox
De CT Infobox is een samenwerkingsverband van de MIVD, de AIVD, de Landelijke Eenheid van de Nationale Politie, de Immigratie- en Naturalisatiedienst (IND), de Fiscale Inlichtingen en Opsporingsdienst (FIOD), de *Financial Intelligence Unit* (FIU), het Ministerie van Sociale Zaken en Werkgelegenheid (SZW), de Koninklijke Marechaussee (KMar), het OM en de NCTV. De CT Infobox draagt bij aan de bestrijding van terrorisme en doet dat door informatie, over netwerken en personen die betrokken zijn bij terrorisme en daaraan te relateren radicalisering, op een centraal punt bij elkaar te brengen en te analyseren.

Platform Interceptie Decryptie en Signaal analyse (PIDS)
Dit is een interdepartementaal platform voor onderzoek en advies. PIDS is tevens intermediair tussen aanbieders van telecommunicatie-diensten en -netwerken en de behoeftestellende autoriteiten zoals het OM, opsporingsdiensten, AIVD en MIVD.

Platform 13
Platform 13 is een overlegorgaan tussen telecommunicatiediensten en overheidspartijen. De naam van het platform is een verwijzing naar artikel 13 van de telecommunicatiewet. Hier staan de voorwaarden beschreven waaraan de overheid en telecomaanbieders moeten voldoen bij het aftapbaar maken van openbare telecomnetwerken en -diensten. De MIVD dient een verzoek tot tappen van een telefoon in bij de AIVD.

Afstemmingsoverleg Cyber (AOC)
Aan het Afstemmingsoverleg Cyber nemen naast de MIVD en AIVD, NCSC, het OM en de Landelijke Eenheid van de Nationale Politie deel. Het overleg staat onder leiding van de Landelijke Officier van Justitie. In het AOC worden operationele onderzoeken, waar nodig, afgestemd.

Internationale samenwerking

De MIVD werkt nauw samen met partners in Nederland en daarbuiten. Het versterken van de internationale veiligheidssamenwerking, zowel bilateraal als multilateraal, is een een speerpunt van de Nederlandse defensiestrategie, vastgelegd in de Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022.

Bilatrale samenwerking

Voor een relatief kleine dienst als de MIVD is een effectieve samenwerking met buitenlandse partners van essentieel belang voor de taakuitvoering. In de wereld van inlichtingendiensten is het gebruikelijk om informatie uit te wisselen. Door van elkaars informatie gebruik te maken, wordt de inlichtingenpositie van beide diensten versterkt.

De kaders voor uitwisseling van informatie staan beschreven in de Wiv2017.

Multilaterale samenwerking

Relevante en tijdige inlichtingen spelen een cruciale rol in gezamenlijke besluitvorming. Daarom werkt de MIVD binnen de inlichtingenlijnen nauw samen met de NAVO, EU en de VN. De eerder ingezette beweging van internationale samenwerking op inlichtingengebied, zette zich in 2018 verder voort. Deze ontwikkeling wordt vanuit de MIVD onderschreven en krachtig ondersteund.

Noord-Atlantische Verdragsorganisatie (NAVO)

Het hoogste inlichtingenbestuursorgaan van de NAVO is het *Military Intelligence Committee* (MIC). Binnen dit bestuursorgaan wordt de strategische koers op inlichtingengebied uitgezet. Namens Nederland heeft directeur MIVD zitting in dit comité. Daarnaast beschikt de NAVO op tactisch/operationeel niveau over entiteiten die bijdragen aan de inlichtingenpositie en *situational awareness* van de alliantie.

De MIVD levert binnen de wettelijke kaders personeel en producten aan de NAVO en draagt bij aan de strategische inlichtingenproducten ten behoeve van de Noord-Atlantische Raad en de *Military Council*.

Europese Unie (EU)

Met de Top van Bratislava in 2016 heeft het buitenland- en veiligheidsbeleid van de EU een stevige impuls gekregen. Dit heeft ook gevolgen voor de intensiteit van inlichtingensamenwerking tussen de EU en MIVD. De toenemende vraag loopt voor de MIVD voornamelijk via het *European Union Military Staff Intelligence Directorate* (EUMS INT). Directeur MIVD heeft namens Nederland zitting in de *Directors Board van de Cooperation Framework Arrangement for intelligence support to the European Union* (CFAIS). De MIVD deelt ook inlichtingen om de digitale netwerken van de EU en haar instellingen en personeel veilig te houden.

NAVO-EU-samenwerking

In het Europees Defensie Actieplan van 2017 is onder meer vastgelegd de EU-NAVO samenwerking de komende jaren op te voeren. Op het gebied van inlichtingen speelt deze samenwerking zich vooral af op het gebied van *Counter Hybrid*. In 2018 kreeg deze samenwerking verder invulling. De MIVD participeerde in deze samenwerking.

Verenigde Naties (VN)

Nederland was in 2018 lid van de VN-veiligheidsraad waarover in maart het voorzitterschap gevoerd werd. De MIVD heeft het lidmaatschap en voorzitterschap via de *Task Force VN Veiligheidsraad* van het Ministerie van Buitenlandse Zaken, actief ondersteund.

BICES

Nederland participeert samen met andere landen in een gerubriceerd netwerk voor informatie-uitwisseling, het *Battlefield Information Collection and Exploitation System* (BICES). Door dit systeem is het mogelijk om on line gerubriceerde informatie te delen met aangesloten landen in internationale coalities. Dit kan ook als deze landen geen lid zijn van de NAVO of EU. De directeur MIVD is voorzitter van de BICES *Board of Governors and Directors*, het bestuursorgaan van de BICES organisatie.


TWEEDE KAMER DER STATEN-GENERAAL

11 GOVERNANCE: BESTUUR, TOEZICHT EN VERANTWOORDING

Bestuur

De MIVD wordt aangestuurd door de secretaris-generaal van het ministerie van Defensie. De minister van Defensie draagt de ministeriele verantwoordelijkheid voor de MIVD.

Besluitvorming over het beleidsterrein van Veiligheid en Inlichtingen wordt ambtelijk voorbereid in de ***Commissie Veiligheids- en Inlichtingendiensten Nederland*** (CVIN).
De besluitvorming gaat vervolgens naar de ***Raad Veiligheid en Inlichtingen*** (RVI). De RVI is een onderraad van de Ministerraad.

Definitieve besluitvorming vindt plaats in de ministerraad.

Verantwoording

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). De directeur MIVD is aanwezig bij de vergaderingen van de CIVD als adviseur van de minister van Defensie.

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 2018 ruim 2200 publieksvragen en meldingen rechtstreeks.
In 2018 ontving de MIVD ruim 150 vragen van de media. Meer dan de helft van deze vragen ging over spionage en de verstoring door de MIVD van een hack-operatie door Russische inlichtingenofficieren, gericht op de OPCW. Een kwart van de vragen betrof de Wet op de Inlichtingen- en Veiligheidsdiensten. De overige vragen hadden betrekking op diverse onderwerpen waaronder veiligheidsonderzoeken.

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 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.

Toezicht

Toetsingscommissie Inzet Bevoegdheden (TIB)

De TIB toetst de rechtmatigheid bij de inzet van een aantal bijzondere bevoegdheden waarvoor de minister toestemming heeft verleend. Het oordeel van de TIB is bindend.

Op 29 oktober 2018 heeft de TIB haar voortgangsrapportage aangeboden aan de Tweede Kamer der Staten-Generaal over de eerste zes maanden. Daarnaast heeft de TIB gezamenlijk met de CTIVD in 2018 drie rechtseenheidsbrieven gestuurd aan de Eerste en Tweede Kamer der Staten-Generaal in het kader van gelijke uitleg van de wet. Dit betreft rechtsbescherming advocaten en journalisten in het buitenland,

geautomatiseerde data-analyse en de reikwijdte van de rechtmatigheid-stoetsing TIB.

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

De CTIVD is een onafhankelijke commissie die beoordeelt of de MIVD en de AIVD rechtmatig opereren. Tevens behandelt de CTIVD klachten over het optreden van de MIVD en AIVD en meldingen van een vermoeden van een misstand bij de MIVD en AIVD.

In 2018 zijn er drie CTIVD-rapporten over de MIVD aan de Eerste en Tweede Kamer der Staten Generaal gestuurd. Dat betrof in februari het rapport over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en MIVD (rapport nr. 55). In juni werd het rapport over uitvoering inzageverzoeken bestuurlijke aangelegenheden door AIVD en MIVD (rapport nr. 58) openbaar. Als derde kwam de voortgangsrapportage inzake de werking van de Wiv 2017 (rapport nr. 59).

Notificatie en klachten

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 2018 zijn vier personen geïnformeerd dat ten aanzien van hen bijzondere bevoegdheden zijn ingezet.

In het vorige jaarverslag is n.a.v. het onderzoeksrapport van de CTIVD over de uitvoering van de notificatieplicht door de AIVD en de MIVD melding gemaakt van achterstanden. De uitvoering van de verplichting geschiedt nu tijdig.

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 2018 kwamen bij de MIVD twee klachten binnen. In beide gevallen heeft de MIVD tot tevredenheid van de indiener de klacht informeel kunnen afdoen.

Er zijn geen meldingen binnengekomen over misstanden in 2018.

Inzageverzoeken

Een ieder 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 2018	Aantal verzoeken	Afgedaan	Gehonoreerd**	Nog lopend	Bezwaar	Afgedaan***	Beroep	Afgedaan	Hoger beroep	Afgedaan
Persoonsgegevens	11	10	-	1	1	1	-	-	-	-
Naar overleden familie	15	5	1	10	-	-	-	-	-	-
Bestuurlijke aangelegenheden	7	3	1	24	13	16	2	1	-	3
Totaal	33	18*	2	35	14	17	2	1	-	3*

* Deels verzoeken van jaren vóór 2018
** Gehonoreerd betekent dat aan verzoeker één of meer documenten zijn verstrekt.
*** Bezwaarzaken bij inzageverzoeken worden behandeld door het Dienstencentrum Juridische Dienstverlening van het Defensie Ondersteuningscommando

Dit openbaar jaarverslag 2018 is een uitgave van
de Militaire Inlichtingen- en Veiligheidsdienst,
april 2019

Layout | X-media, Media Centrum Defensie, Den Haag

Foto's | Media Centrum Defensie, Den Haag, ANP