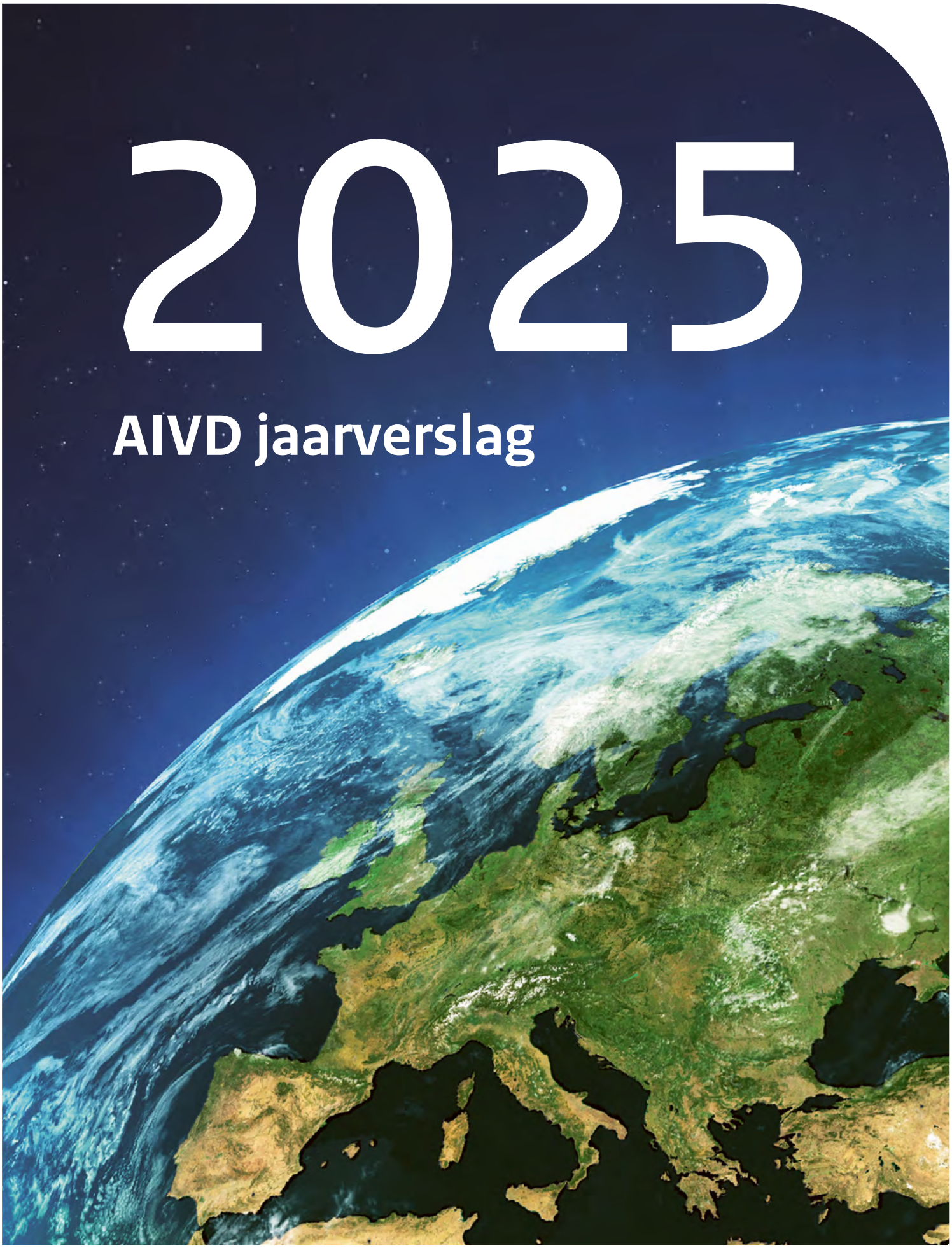
Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

2025

AIVD jaarverslag



Inhoud

Voorwoord

Hoe treed je verstandig op in een wereld vol conflict en botsende belangen, in het bijzonder als je die conflicten niet zelf hebt gezocht? Het is een vraag waarmee Nederland momenteel indringend wordt geconfronteerd.

Het is ook een vraag waarover de AIVD voortdurend nadenkt. Het is immers onze verantwoordelijkheid de nationale veiligheid van Nederland te beschermen. Dat vraagt effectief handelen, ongeacht wat de dreigingen in binnen- of buitenland zijn. In zekere zin is dit jaarverslag te lezen als antwoord op de vraag hoe we dat in 2025 hebben gedaan.

Het handelen van de AIVD begint altijd met het onderzoeken van de feiten, ook als anderen die proberen te verbergen. We duiden de feiten eigenstandig en apolitiek, in alle nuance en ongeacht of ze comfortabel zijn om onder ogen te zien – vaak zijn ze dat niet.

Het is bijvoorbeeld een oncomfortabel feit dat het regime van Rusland zich in 2025 nog aanvallender is gaan opstellen tegen Europese landen. In woorden: het regime schildert onze vrijheden af als pervers en bedreigend en probeert eenheid in en tussen Europese landen te ondermijnen. En in daden: Russische hackers pleegden cyberaanvallen op onder meer de Nederlandse politie en de Signal- en WhatsApp-accounts van onze hoogwaardigheidsbekleders en militairen.

Het is een oncomfortabel feit dat China – een land dat we als handelspartner met open armen ontvangen – al jaren heimelijk en illegaal actief is om de kennis van onze bedrijven en kennisinstellingen te bemachtigen, en dat de dreiging daarvan in 2025 zowel is verbreed als verdiept. Dat bedreigt onze autonomie en het innovatie- en verdienvermogen van bedrijven waar Nederland trots op is.

Zulke activiteiten staan niet op zichzelf. Ze zijn onderdeel van een breder streven van verscheidene landen om in de wereld (China, in mindere mate Rusland) of in een regio (onder meer Iran en Noord-Korea) meer macht naar zich toe te trekken en de wereldorde te vervormen naar eigen autocratische ideologie.

Die dynamiek is de eerste maanden van 2026 verder op scherp gezet. Met overweldigend militair optreden in Venezuela en Iran heeft de Verenigde Staten duidelijk gemaakt dat het zal ingrijpen als het vindt dat andere landen Amerika's positie bedreigen, of als zij Amerika's zwaarwegende belangen in gevaar brengen.

Simone Smit
Directeur-generaal
Algemene Inlichtingen- en Veiligheidsdienst

De langetermijngevolgen daarvan, ook voor de nationale veiligheid van Nederland, zijn nog onduidelijk. Maar we zien met nog meer scherpte dan in de afgelopen jaren een instabiele en onvoorspelbare wereldorde, na decennia waarin stabiliteit en voorspelbaarheid het fundament waren voor groei en vrede.

Dit jaarverslag beschrijft wat we op basis van onderzoek kunnen zeggen over tegen Nederlandse veiligheidsbelangen gerichte activiteiten van andere landen, en wat we op basis van inlichtingenonderzoek hebben ontmaskerd en gestopt. Dat geldt ook voor dreigingen waarbij actoren in binnen- en buitenland zijn verbonden. Zo hebben we meer inzicht gekregen in hoe andere landen soms criminele netwerken in Nederland inzetten.

Het geldt bovendien voor extremistische en terroristische dreigingen. Zo denken we opnieuw (onder meer) jihadistisch geweld te hebben voorkomen. Zeker elf keer bracht de AIVD daarover een ambtsbericht uit, op basis waarvan de politie aanhoudingen kon verrichten. Extra zorgelijk is dat zes van de aangehouden personen jonger waren dan 24, wat duidt op een verdere toename van het aantal pro-ISIS jongeren in Nederland.

De aanhoudingen illustreren nog een kenmerk van het handelen van de AIVD: het is erop gericht om onze partners beter in staat te stellen hun werk te doen voor de veiligheid van Nederland. De AIVD werkt daarom nauw samen met partners in de veiligheidsketen, de MIVD en de NCTV, de politie en het Openbaar Ministerie in het bijzonder. En we werken steeds meer samen met het bedrijfsleven en het openbaar bestuur. Die relaties hebben we in 2025 versterkt en uitgebreid.

Ook internationaal hebben we nog meer de krachten gebundeld. Want het is evident dat we samen sterker staan in de huidige wereldorde. De samenwerking met Europese partnerdiensten hebben we zelfs zo geïntensiveerd, dat het niet overdreven is te spreken van een kantelpunt. Een sprekend voorbeeld is dat de AIVD in 2025 het aantal inlichtingenbijdragen aan de *Single Intelligence Analysis Capacity* van de Europese Unie meer dan verdubbeld heeft.

Buitenlandse diensten werken graag met ons samen omdat de AIVD wat te bieden heeft. We zijn, in alle bescheidenheid, goed in wat we doen. Onze taak vraagt dat van ons. Dat raakt een derde kenmerk van ons handelen – we blijven dichtbij onszelf. We versterken waar we goed in zijn (onder meer onze technologie, waarin we voorop willen lopen), we bewaken onze onafhankelijkheid en we weten wat we te beschermen hebben. We zijn de inlichtingen- en veiligheidsdienst van een vrije en een weerbare democratie. Juist daarom geven onze mensen het beste van zichzelf.

En zo – op basis van de feiten, krachten bundelend met wie onze belangen of waarden deelt en onze veiligheid kan vergroten, dienstbaar aan de samenleving – handelde de AIVD in 2025 in het belang van de nationale veiligheid. Dat is werk om met trots bij stil te staan.

1. De wereld waarin de AIVD werkzaam is

Op 24 en 25 juni werd in Den Haag de NAVO-top gehouden. De top kreeg extra lading wegens de vele conflicten in de wereld. Met onder meer veiligheids-onderzoeken en cyberonderzoeken droeg de AIVD bij aan de veiligheid van het evenement. Ook in de inlichtingenwereld werd internationale samenwerking in 2025 steeds belangrijker. Foto: ANP

1.1

Met inlichtingen effect bereiken: dreigingen voorkomen en wegnemen

De AIVD staat voor de nationale veiligheid. Al sinds onze oprichting, kort na de Tweede Wereldoorlog, beschermen we Nederland tegen nationale en internationale dreigingen. We beschermen daarbij de democratische rechtsorde: de maatschappelijke orde die gebaseerd is op recht en democratie. De democratische rechtsorde is van grote invloed op onze kwaliteit van (samen)leven.

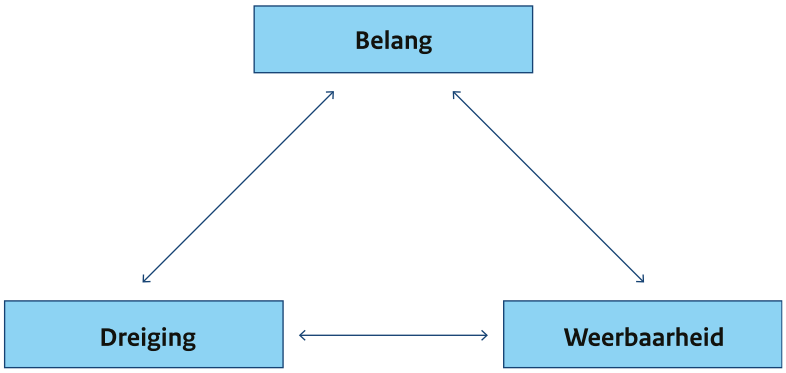
Een veelvoud aan dreigingen

Er waren in 2025 veel dreigingen tegen de nationale veiligheid en de democratische rechtsorde. Vanuit de jihadistische beweging kwam een aanhoudende terroristische dreiging voort. Uit anti-institutioneel extremistische hoek ontvingen onder anderen journalisten en rechters regelmatig bedreigingen. Het rechts-extremistisch gedachtegoed vormt een voedingsbodem voor geweld. Er is sprake van verwevenheid tussen statelijke actoren en criminele netwerken. Via spionage proberen andere landen op heimelijke wijze informatie te verkrijgen over en invloed uit te oefenen in Nederland. De dreiging van landen met een offensief cyber-programma bleek dit jaar nog groter dan voorheen werd ingeschat. Rusland bereidt zich voor op een langdurige confrontatie met het Westen. De Chinese dreiging verbreedt en verdiept. De ontwikkelingen in Venezuela leiden tot zorgen in en over het Caribische deel van het Koninkrijk. Instabiliteit in het Midden-Oosten zet Nederlandse veiligheidsbelangen onder druk. En landen zoals Iran, Rusland en Noord-Korea proberen voor de (door)ontwikkeling en productie van hun massavernietigingswapens kennis en goederen te verwerven in het Westen. Het veelvoud aan dreigingen wordt in meer detail besproken in dit jaarverslag.

Belangen en weerbaarheid

Iedere dreiging moet steeds gezien worden in relatie tot twee andere aspecten: de ‘te beschermen belangen’[1] en de Nederlandse weerbaarheid tegen deze dreigingen. Bij een hoge weerbaarheid, heeft een dreiging minder impact op de belangen. Het omgekeerde is ook waar. Zo maakt bijvoorbeeld verdeeldheid binnen de samenleving Nederland kwetsbaar voor statelijke inmenging en extremistische bewegingen die daar munt uit willen slaan. Dit verlaagt de weerbaarheid van de samenleving.

[1] De zes nationale veiligheidsbelangen zijn: territoriale, fysieke, economische en ecologische veiligheid, sociale en politieke stabiliteit, en internationale rechtsorde en stabiliteit. Ook organisaties hebben hun eigen te beschermen belangen.



Geopolitieke verschuivingen kunnen zorgen voor veranderingen in iedere hoek van deze 'dreigingsdriehoek'. Ook de steeds verdergaande technologisering van de wereld, en op de langere termijn klimaatverandering, hebben hier bijvoorbeeld invloed op.

Landen en thema's van onderzoek

Naar welke landen en thema's de AIVD en MIVD onderzoek doen, wordt vastgelegd in de Geïntegreerde Aanwijzing Inlichtingen en Veiligheid (GA I&V). De GA I&V wordt vastgesteld door de ministers van Binnenlandse Zaken en Koninkrijksrelaties, Defensie en Algemene Zaken na overleg met de minister van Justitie en Veiligheid en de minister van Buitenlandse Zaken. Daarnaast biedt de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) ruimte om onderzoek te doen naar dreigingen tegen de nationale veiligheid die niet in de GA I&V worden genoemd. De huidige GA I&V geldt tot en met eind 2026. De inhoud ervan is geheim.
De onderzoeksprioriteiten van de AIVD zijn wel openbaar en worden beschreven in een Jaarplanbrief, die in december wordt gepubliceerd.

Wettelijk kader

Om de democratische rechtsorde te beschermen, is het van groot belang dat de AIVD en de MIVD ook zelf binnen een wettelijk kader functioneren: een kader dat de democratie beschermt en burgers het vertrouwen geeft dat de diensten hun taken vervullen met fundamentele waarborgen, zoals onafhankelijk toezicht.

De zes wettelijke taken van de AIVD die zijn vastgelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv) zijn:

- Onderzoek doen naar organisaties en personen die een dreiging vormen (a-taak);
- Veiligheidsonderzoeken uitvoeren (b-taak);
- Veiligheidsmaatregelen bevorderen (c-taak);
- Inlichtingen over het buitenland inwinnen (d-taak);
- Dreigings- en risicoanalyses opstellen (e-taak);
- Naslag doen naar bepaalde personen en organisaties (f-taak).

Het wettelijk kader moet de dienst in staat stellen om deze verschillende taken goed te blijven uitvoeren – ook bij alle technologische en geopolitieke ontwikkelingen die elkaar in een snel tempo opvolgen, en die van grote invloed zijn op de dreigingen die de AIVD probeert te voorkomen en weg te nemen. Daarom is de wetgeving voor de dienst momenteel aan verandering toe. De Wiv wordt herzien.

Met inlichtingen effect bereiken

Met hoogwaardige en unieke inlichtingen geeft de AIVD zijn nationale partners, zoals de ministeries en het Openbaar Ministerie (OM), inzicht in allerlei soorten dreigingen en vergroot daarmee hun handelingsvermogen. Zo kan het OM op basis van een zogeheten ambtsbericht van de AIVD actie ondernemen. In 2025 bracht de AIVD 93 ambtsberichten uit aan nationale en lokale partners. Dat zijn er 20 meer dan in 2024.

> Lees meer op aivd.nl/ambtsbericht

Ook heeft de AIVD in 2025 een groot aantal cyberadviezen uitgebracht, onder andere vanwege de NAVO-top in Den Haag. De AIVD heeft bijvoorbeeld, voorafgaand aan de top, samen met het Nationaal Cyber Security Centrum (NCSC) tien cyberadviezen uitgebracht over tactieken, technieken en procedures die veel worden gebruikt door statelijke actoren. Het doel van een cyberadvies is om de ontvangers van de informatie, zoals de organisatie van deze top, handelingsperspectief te bieden zodat zij beveiligingsmaatregelen kunnen nemen. Hiermee draagt de AIVD bij aan de weerbaarheid tegen statelijke actoren.

Een ander type product dat de AIVD uitbrengt voor het taakveld bewaken en beveiligen is het dreigingsproduct. In 2025 heeft de AIVD meer dreigingsproducten uitgebracht dan in 2024. Deze toename is onder meer het gevolg van een toegenomen vraag vanuit de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het OM, en van nieuwe casussen die zich in 2025 aandienden. Ook is geïnvesteerd in extra capaciteit voor het taakveld. Op basis van deze dreigingsproducten kunnen de NCTV, het OM en lokaal bestuur beveiligingsmaatregelen nemen of aanpassen. Dit doen zij voor belangendragers van de democratische rechtsorde, zoals politici, journalisten of wetenschappers.

Nu Europa in toenemende mate de verantwoordelijkheid neemt voor de eigen veiligheid, is Europese samenwerking, ook voor de diensten, belangrijker dan ooit. Daarom heeft de AIVD in 2025 het aantal inlichtingenbijdragen aan de *Single Intelligence Analysis Capacity* (SIAC) van de Europese Unie meer dan verdubbeld. Deze bijdragen versterken de inlichtingenpositie van onder andere de Europese Commissie, de Europese Dienst voor Extern Optreden en de Raad van de Europese Unie.

Naast het vergroten van het handelingsvermogen van onze partners, is de AIVD ook zelf een handelende dienst. Op basis van inlichtingen, en door ook zelf actief op te treden, probeert de dienst te voorkomen dat statelijke actoren, organisaties of personen onze (inter)nationale veiligheidsbelangen bedreigen, de democratische rechtsstaat ondermijnen of instituties aanvallen. In samenwerking met nationale en internationale partners kan de AIVD ervoor kiezen om een handeling actief te verstoren als ze zien dat deze de (inter)nationale veiligheid bedreigt.

De dienst treedt naar buiten met inlichtingen. Dit doet de AIVD om de overheid, bedrijven en burgers te informeren over dreigingen en zo de weerbaarheid te verhogen. Zo bracht de AIVD samen met de MIVD en de Duitse inlichtingendienst Bundesnachrichtendienst (BND) in 2025 naar buiten dat Rusland intensiever gebruik heeft gemaakt van chemische wapens in Oekraïne. Ook informeert de dienst de samenleving via thematische analyses, brochures en (cyber)adviezen.

> **Lees meer op aivd.nl/beveiligingsadviezen**

Samenwerking cruciaal

Binnen ieder onderzoeksgebied is samenwerking cruciaal om dreigingen te voorkomen of weg te nemen, de te beschermen belangen inzichtelijk te hebben en te houden, en de Nederlandse weerbaarheid en die van zijn partners te vergroten. De AIVD zet volop in op Europese samenwerking. De dienst is actief in vele nationale en internationale samenwerkingsverbanden, en speelt hierin regelmatig een leidende rol. Dit doet de dienst als een gecombineerde dienst. De AIVD is onder andere een inlichtingen-, veiligheids- en sigintdienst. Dat is een unieke combinatie in de wereld. Juist in internationale samenwerking is dat van grote meerwaarde. Om onze krachten te bundelen, werkt de AIVD nauw samen met de MIVD. En met tal van partners, waaronder bedrijven en kennisinstellingen. De samenwerking met private partijen kan alleen verder worden versterkt als het wettelijk kader van de dienst dit mogelijk maakt.

1.2

Ontwikkeling: technologie als kroonjuweel, wapen en schild

Technologische ontwikkelingen hebben een grote impact op de huidige, veranderende wereldorde en geven deze mede vorm. Deze ontwikkelingen zijn eveneens van invloed op het inlichtingen- en veiligheidsdomein. Dit hoofdstuk gaat aan de hand van de aspecten 'belang, dreiging, weerbaarheid' hierop in.

Belang: technologie als kroonjuweel

In Nederland hebben bedrijven, kennisinstellingen en de overheid bijzondere kennis en technologie in huis die nergens anders op de wereld op dat niveau te verkrijgen is. In deze unieke kennis en hoogtechnologische producten zijn statelijke actoren geïnteresseerd.

Statelijke actoren proberen deze kennis en technologie openlijk en heimelijk te verwerven, bijvoorbeeld door middel van samenwerkingen, investeringen en overnames. Hoe meer deze unieke kennis door Nederland en de EU wordt beschermd tegen legale (maar onwenselijke) verwerving, hoe meer statelijke actoren gebruikmaken van heimelijke manieren: ze ontplooien concrete inlichtingenactiviteiten om deze kennis en technologie te verkrijgen. De AIVD draagt samen met de MIVD en nationale en internationale partners bij aan de weerbaarheid tegen deze ongewenste kennis- en technologieoverdracht.

Dreiging: technologie als wapen

Statelijke actoren zetten technologie in als wapen. Zo kunnen zij van over de hele wereld cyberaanvallen aansturen. Met generatieve kunstmatige intelligentie (AI) wordt het mogelijk om met beperkte technische kennis een steeds groter deel van deze aanvallen te automatiseren, en deze daardoor sneller en op grotere schaal uit te voeren.

Technologie kan ook een geopolitiek machtsmiddel zijn: landen kunnen toegang tot technologieën beperken en op die manier druk uitoefenen. Daardoor is het voor ieder land van strategisch belang om zelfstandig te (blijven) beschikken over technologie, of over kritische controlepunten in de gehele productie(keten) hiervan.

Niet alleen bij cyberdreiging spelen technologische ontwikkelingen een rol: technologie is relevant voor alle soorten dreigingen die in dit jaarverslag beschreven staan. Technologie maakt aanvalsmanieren laagdrempeliger en dreigingen complexer.

Voor kleinere landen, zoals Nederland, is het essentieel om strategische afhankelijkheden te onderkennen en hier zorgvuldig mee om te gaan. En bovenal: om hierbij samen te (blijven) werken met andere landen en om effectieve partnerschappen te sluiten met de private sector.

Identificeer de te beschermen belangen
Om ongewenste kennis- en technologieoverdracht te voorkomen wordt het steeds essentiëler om te beschermen belangen aan te wijzen. Welke kennis, technologische ontwikkeling en/of intellectueel eigendom mag koste wat kost niet buiten de eigen controle vallen? Wat zijn de 'kroonjuwelen' en hoe zou ongewenste toegang tot deze belangen de (ambitie voor een) koploperspositie kunnen ondermijnen?

De AIVD en de MIVD hebben in 2025 wederom een aantal ongewenste pogingen verstoord om kennis of technologie te verwerven. Inlichtingenonderzoek naar ongewenste verwerving van geavanceerde Nederlandse technologieën heeft in 2025 bovendien verschillende inzichten opgeleverd, onder andere over verhulde investeringen, omzeiling van exportrestricties en het verkrijgen van bedrijfsgeheimen via (cyber)spionage.

Weerbaarheid: technologie als schild

De veelheid aan complexe en met elkaar verweven dreigingen vraagt om weerbaarheid (inclusief bijbehorende veerkracht) van de gehele samenleving. Een onderdeel van de algehele weerbaarheid van een maatschappij is haar digitale weerbaarheid. Slim ingezette technologische toepassingen kunnen daarbij helpen. Zo kan eerdergenoemde generatieve AI een steeds groter deel van de verdediging tegen cyberdreigingen automatiseren.

Technologisch vooroplopen is essentieel voor de AIVD om de wettelijke taken toekomstbestendig te kunnen uitvoeren. Daarom heeft de dienst zich als doel gesteld om al in een vroeg stadium relevante technologieën te benutten. De organisatie wordt erop ingericht om dit mogelijk te maken. Hierbij is het versterken van internationale en nationale samenwerking met bedrijven, kennisinstellingen en andere overheidsdelen een speerpunt. Er is een Chief Science & Technology Office (CSTO) opgericht om hieraan sturing te geven. Ook investeert de AIVD met de MIVD in een gezamenlijke digitale infrastructuur.

1.3

Belangrijker dan ooit: internationale samenwerking

Internationale ontwikkelingen hebben toenemende impact op de Nederlandse nationale veiligheid. Om de belangen die daarmee gepaard gaan effectief te beschermen is internationale samenwerking cruciaal. De AIVD heeft een groot internationaal netwerk van collega-diensten waarmee wordt samengewerkt. Door samen te werken kan de AIVD gebruikmaken van de kennis en expertise van deze diensten, en daarnaast ook eigen kennis en expertise delen. Bij iedere vorm van samenwerking staan het anticiperen op, wegnemen of voorkomen van dreiging en het vergroten van de weerbaarheid van Nederland en partnerlanden centraal.

De AIVD streeft ernaar om hierin een actieve, betrouwbare en efficiënte samenwerkingspartner te zijn. Ook probeert de dienst de impact van onze inlichtingen steeds zo groot mogelijk te maken via zogeheten inlichtingendiplomatie en door het versterken van relaties met bepaalde landen, dan wel concreet bij te dragen aan bijvoorbeeld sanctiehandhaving. Zo versterkte de AIVD in 2025 de inlichtingensamenwerking met de Europese Unie en de NAVO. Dit ter bevordering van geopolitieke besluitvorming en ter ondersteuning van het Nederlandse buitenland- en veiligheidsbeleid.

Vertrouwen en zorgvuldigheid

Vertrouwen is essentieel in de samenwerking tussen inlichtingen- en veiligheidsdiensten. Ook is zorgvuldigheid van groot belang bij de keuze voor de aard en intensiteit van iedere samenwerking. Daarom ‘weegt’ de AIVD collega-diensten op een aantal criteria: democratische inbedding, eerbiediging van mensenrechten, professionaliteit en betrouwbaarheid, wettelijke bevoegdheden en technische mogelijkheden en het niveau van gegevensbescherming. Deze weging is een wettelijke verplichting en vindt plaats in gezamenlijkheid met de MIVD. De wegingsnotities worden aangepast als de AIVD en MIVD daar aanleiding voor zien.

De AIVD gaat strategische partnerschappen aan met diensten waarbij het belang om samen te werken groot is, en waarbij de AIVD het resultaat van deze samenwerking als zeer waardevol beschouwt. Dit vraagt een continue investering in de relatie met deze diensten. Bij alle samenwerkingen heeft de AIVD aandacht voor de *quid pro quo*: de wederkerige ‘voor wat, hoort wat’-balans. Tegelijkertijd zorgt de AIVD ervoor te allen tijde en binnen de wettelijke kaders met iedere collega-dienst te kunnen samenwerken als de situatie daarom vraagt.

Naast bilaterale samenwerking met andere diensten, werkt de AIVD ook samen met partners in multilateraal verband. Multilaterale samenwerking vindt onder meer plaats in EU-verband.

Ter illustratie: EU-samenwerking

Op basis van inlichtingen kunnen beleidsmakers zorgen voor beter gewogen beleid. Dat geldt ook op EU-niveau – onder meer voor het Gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) en het Gemeenschappelijk veiligheids- en defensiebeleid (GVDB) van de EU. Deze twee beleidskaders hebben onder andere als doel om de internationale veiligheid te vergroten. Om de EU hiervoor goed onderbouwde keuzes te laten maken, delen lidstaten ook inlichtingen in EU-verband.

INTCEN en SIAC: inlichtingen met mondiale impact

Voor het delen van inlichtingen in EU-verband hecht de AIVD grote waarde aan INTCEN, het *Intelligence and Situation Centre*, en de overkoepelende samenwerkingsvorm SIAC, de *Single Intelligence Analysis Capacity*, van de Europese Unie. SIAC is het exclusieve toegangsportaal voor het delen van strategische inlichtingen met Europese instellingen: het maakt inlichtingenproducten voor EU-beleidsmakers op basis van vrijwillige inlichtingenbijdragen door EU-lidstaten. SIAC en INTCEN verwerven niet eigenstandig inlichtingen. De bescherming van de nationale veiligheid is namelijk een exclusieve ‘competentie’ van de EU-lidstaten.

De AIVD draagt bij aan de versterking van SIAC. In 2025 heeft de AIVD het aantal inlichtingenbijdragen aan SIAC meer dan verdubbeld ten opzichte van 2024. Deze bijdragen versterkten de inlichtingenpositie van onder andere de Europese Commissie, de Europese Dienst voor Extern Optreden en de Raad van de Europese Unie. In een aantal gevallen leidden deze bijdragen tot concrete EU-maatregelen, waaronder sancties.

Versterking liaisonnetwerk

De AIVD heeft op een aantal plaatsen in de wereld liaisons. Hun belangrijkste taak is om de samenwerking met collega-diensten en multilaterale organisaties verder te brengen. Daarnaast voorzien zij Nederlandse ambassades van advies op veiligheidsdossiers. In 2025 heeft de AIVD deze buitenlandse presentie verder uitgebreid.

2. Een veelvoud aan dreigingen die met elkaar samenhangen

Een medewerker van de Dienst Speciale Interventies. Ambtsberichten van de AIVD stelden de politie afgelopen jaar in staat verschillende arrestaties te verrichten. Daarmee zijn hoogstwaarschijnlijk geweldsdreigingen weggenomen. De AIVD bracht onder meer ambtsberichten uit over jihadistische, anti-institutionele en rechts-extremistische dreigingen. Foto: ANP

2.1 Extremisme

De AIVD onderzoekt personen en organisaties die – door de doelen die zij nastreven, dan wel door hun activiteiten – aanleiding geven om te vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de (fysieke) veiligheid of voor andere gewichtige belangen van de staat. Vanwege de aard van hun doelen en activiteiten, duidt de AIVD een deel van deze bewegingen aan als extremistische bewegingen. De AIVD verstaat onder extremisme: het uit ideologische motieven bereid zijn om niet-gewelddadige en/of gewelddadige activiteiten te verrichten die de democratische rechtsorde ondermijnen.

De democratische rechtsorde kan worden ondermijnd op niet-gewelddadige en gewelddadige manieren. Voorbeelden van niet-gewelddadige manieren zijn systematisch haatzaaien, doelbewust desinformatie verspreiden, en demoniseren en intimideren. Onder gewelddadige methodes vallen bijvoorbeeld mishandelingen, brandstichtingen of ernstigere vormen van geweld. Een uiterste vorm van extremisme is terrorisme: uit ideologische motieven (dreigen met het) plegen van op mensenlevens gericht geweld of op het aanrichten van maatschappij-ontwrichtende schade met als doel (een deel van) de bevolking ernstige vrees aan te jagen, maatschappelijke verandering te bewerkstelligen en/of politieke besluitvorming te beïnvloeden.

In 2025 richtten de onderzoeken van de AIVD zich op beide vormen van dreigingen, binnen met name het islamitisch extremisme, anti-institutioneel extremisme, links-extremisme en rechts-extremisme. De eerstvolgende hoofdstukken gaan hierop in.

> Lees meer op aivd.nl/extremisme

- **De belangrijkste terroristische dreiging komt nog altijd voort uit het jihadisme.**
- **ISIS probeert aanhangers via propaganda te inspireren tot aanslagen of deze, ondanks de wereldwijde druk op de organisatie, zelf te organiseren.**
- **De jihadistische beweging in Nederland bestaat voornamelijk uit ISIS-aanhangers.**
- **Opvallend aan 2025 is de verdere toename aan jongeren (tot 24 jaar) en het aantal personen over wie de AIVD een ambtsbericht heeft uitgebracht.**

2.1.1 Islamitisch extremisme

Ook in 2025 komt de belangrijkste terroristische dreiging voort uit het jihadisme. In december 2025 werd dit geïllustreerd door een grote aanslag in Sydney, Australië bij Bondi Beach, gericht op Joodse deelnemers aan een Chanoeka-viering.

Jihadisme

De jihadistisch-terroristische dreiging tegen Nederland komt vrijwel geheel vanuit ISIS. Deze dreiging komt deels van (aspirant-)aanslagplegers die verbonden zijn met en aangestuurd worden door ISIS. Het andere deel van deze dreiging komt van ISIS-aanhangers die zonder contact met ISIS geïnspireerd worden tot aanslagplanning, of die in sommige gevallen via online contact met ISIS-leden daartoe worden aangezet.

Aangestuurde dreiging ISIS

De toenemende dreiging vanuit ISIS heeft de afgelopen jaren geleid tot versterkte offensieve activiteiten tegen ISIS. Zo pleegden lokale autoriteiten in samenwerking met internationale partners verschillende interventies in onder meer Pakistan en Syrië. Ook startte in Puntland, Somalië, een militair offensief tegen ISIS. Daarmee namen de capaciteiten van ISIS af. Maar ISIS is veerkrachtig en beschikt over een groot aanpassingsvermogen. Op het moment dat de druk op ISIS minder wordt, zal de dreiging van door hen aangestuurde aanslagen relatief snel weer toenemen.

Daarnaast houdt de AIVD aandacht voor de dreiging die uitgaat van netwerken en personen in Europa die aan ISIS zijn gelieerd. De afgelopen jaren hebben verschillende leden van deze netwerken plannen ontwikkeld voor een aanslag. Een Tadzjieks ISKP-lid dat in Nederland woont, is op 21 juli 2025 veroordeeld tot een gevangenisstraf van vijfenhalf jaar voor lidmaatschap en financiering van ISIS.

In de zomer van 2024 werden verschillende personen aangehouden in België, Duitsland en Oostenrijk vanwege mogelijke aanslagplannen. Het merendeel van deze personen is inmiddels vrijgelaten of uitgezet naar landen van herkomst. Door de aanhoudingen, uitzettingen en druk op ISIS buiten Europa is de terroristische dreiging die uitgaat van deze netwerken op dit moment afgenomen. Op termijn kunnen deze netwerken weer actief worden, als ISIS in staat is zijn capaciteiten te vergroten en plannen te ontwikkelen om aanslagen aan te sturen in Europa.

Daarnaast blijven er sporadisch (oud-)ISIS-leden uit Syrië opduiken in Nederland en andere Europese landen. De AIVD zet met nationale en internationale partners in op onderkenning en verstoring van deze individuen en netwerken. Op 26 mei 2025 zijn twee Syrische mannen aangehouden naar aanleiding van een ambtsbericht van de AIVD, die verdacht worden van deelname aan ISIS in Syrië.

ISIS-aanhangers in Nederland

Hoewel de druk op ISIS wereldwijd in 2025 is toegenomen, heeft dat zich niet vertaald in een afname van de dreiging van aanhangers in Nederland, of van de aantrekkingskracht of bereikbaarheid van ISIS online. In 2025 heeft de AIVD over negentien individuen ambtsberichten uitgebracht in het kader van jihadisme. Bij elf van hen had de AIVD aanwijzingen voor een op handen zijnde geweldsdreiging. De politie heeft hen naar aanleiding van deze ambtsberichten aangehouden. Zes van hen waren op dat moment jonger dan 24.

De toename van het aantal pro-ISIS jongeren (tot 24 jaar) die in onderzoek zijn bij de AIVD is verder toegenomen. Jongeren vormen inmiddels een derde van de jihadistische onderzoekspopulatie. Op socialemediaplatformen is het jihadistisch gedachtegoed breed beschikbaar en eenvoudig toegankelijk. Dit komt mede door de activiteiten van jonge jihadisten die op grote schaal jihadistische content online plaatsen, beheren en/of verder verspreiden. Deze platforms zijn daarnaast de belangrijkste verzamelplaats voor jonge jihadisten. Zij kunnen daar op laagdrempelige wijze gelijkgestemden ontmoeten. In veel gevallen blijven deze contacten oppervlakkig en vertalen deze zich niet door in verdiepte contacten of fysieke netwerkvorming.

Incidenteel neemt de AIVD waar dat jonge jihadisten hun online contact omzetten naar (ook) offline contact. Zo ook bij de acht personen die de politie in april 2025 heeft aangehouden. Hoewel in algemene zin onzeker is in hoeverre jonge jihadisten bereid zijn te handelen naar hun zorgwekkende uitspraken, achtte de AIVD een geweldsdreiging mogelijk van een aantal personen binnen dit netwerk. Daarom bracht de AIVD ambtsberichten uit, die mede tot deze aanhoudingen leidden. Hun online radicalisering past in het beeld dat de AIVD schetste in de publicatie *Een web van haat* (april 2025).

De AIVD gaat niet alleen de dreiging van aanslagen tegen. De AIVD probeert de groei van de jihadistische beweging tegen te gaan, door online netwerkvorming en de verspreiding van het gedachtegoed te verstoren. Zo waren de ambtsberichten van de AIVD in zeven gevallen (mede) gericht op het beperken van het opruiende en radicaliserende effect van dergelijke online activiteiten. Daarnaast zet de AIVD in op het voorkomen van uitreizen door jihadisten vanuit Nederland om zich bij ISIS aan te sluiten. Bij het uitbrengen van ambtsberichten in 2025 waren er vier gevallen aanwijzingen over een mogelijke uitreis. Hoewel de planvorming hiertoe slechts sporadisch concrete vormen aanneemt en ISIS op veel plekken in de wereld moeilijk bereikbaar is, lijkt de interesse in uitreizen aan te houden onder de aanhangers. Hetzelfde is het geval bij personen in andere Europese landen.

Hamas

De AIVD doet onderzoek naar de mogelijke dreiging vanuit de terroristische organisatie Hamas tegen de nationale veiligheid. De AIVD heeft twee handelingsvormen onderkend van Hamas in Europa, uiteenlopend van activistisch tot mogelijke voorbereidingen voor terroristische handelingen. Ten eerste is in Europa al jaren een 'politiek' netwerk actief dat financiële steun voor Hamas verwerft en zich in Europa bezighoudt met activisme, lobby- en andere beïnvloedingswerkzaamheden. In Nederland is een tiental personen actief dat aan dit Europese netwerk te verbinden is. Dit Hamas-netwerk in Nederland is ook al jaren actief met propaganda, lobbywerk en fondsenwerving voor Hamas (in Gaza). Ten opzichte van 2024 heeft de AIVD meer duidelijkheid gekregen over de betrokkenheid van het Hamas-netwerk in Nederland bij pro-Palestina- en anti-Israëlprotesten. Zo ziet de AIVD dat dit netwerk betrokken is bij bredere organisaties die demonstraties organiseren namens een groter deel van de Palestijnse gemeenschap. In 2025 hebben deze demonstraties niet geleid tot gewelddadige incidenten. De AIVD constateert wel dat deze demonstraties kunnen leiden tot verdeeldheid in de samenleving.

De tweede handelingsvorm is aan het licht gekomen via een aantal aanhoudingen in Europa: aan Hamas te relateren personen waren – op aansturing van Hamas-leden in Libanon – betrokken bij het (ver)bergen en (ver)plaatsen van vuurwapens en munitie. Het lijkt erop dat Hamas bezig was met het opbouwen van gewelddadige capaciteiten in Europa. Het is echter vooralsnog niet duidelijk met welk doel dit werd opgebouwd en aangestuurd. Enkelen van deze aangehouden personen worden, naast het lidmaatschap van Hamas, ook verdacht van het voorbereiden van aanslagen op Joodse en/of Israëlische doelen. De strafrechtelijke onderzoeken lopen nog.

> **Lees meer op aivd.nl/terrorisme**

2.1.2 Anti-institutioneel extremisme

> **Ambtsberichten van de AIVD hebben in 2024 en 2025 geleid tot de aanhouding van twee grote groepen gewelddadige anti-institutioneel extremisten en de vondst van vuurwapens, grote hoeveelheden munitie en andere potentiële aanslagmiddelen, zoals zwaar vuurwerk, ontstekers en castorbonen. Hiermee is de gewelddadige dreiging die uitgaat van deze twee groepen weggenomen.**

> **Anti-institutioneel extremisme kan leiden tot terrorisme.**

Vuurwapens, een grote hoeveelheid munitie en castorbonen, het hoofdingrediënt voor het gif ricine: zaken die de politie aantrof bij de aanhouding van acht personen in het kader van een onderzoek naar anti-institutioneel extremisme, in juni 2025. Zij zijn aangehouden na ambtsberichten van de AIVD. Een deel van deze groep wordt verdacht van aan terrorisme gerelateerde feiten.

In 2024 was al een andere groep van tien personen aangehouden op verdenking van terrorisme. In november 2025 oordeelde de rechtbank dat er geen sprake was van een terroristische organisatie, maar wel van een criminele organisatie die opruide tot een terroristisch misdrijf. Door te pleiten voor lokale milities en burgerarresten konden anderen bewogen worden tot het daadwerkelijk overgaan tot bewapening en fysiek geweld. Een deel van de groep werd daarnaast veroordeeld voor verboden wapenbezit. Het OM is in beroep gegaan tegen een deel van de uitspraak, omdat het OM het niet eens was met het oordeel van de rechtbank dat drie van de verdachten geen criminele of terroristische organisatie vormden.

In het kader van anti-institutioneel extremisme bracht de AIVD in 2025 over 14 personen een ambtsbericht uit. Bij 13 personen was dit in het kader van anti-institutioneel terrorisme.

Anti-institutioneel extremisten geloven dat een kwaadaardige elite mensen wil onderdrukken, tot slaaf maken of vermoorden. De coronapandemie en de toen getroffen maatregelen blijven belangrijke onderwerpen binnen deze beweging. En net als in 2024, was migratie in 2025 een belangrijk thema. Door massamigratie toe te staan of te stimuleren zou de elite de bevolking nog verder kunnen onderdrukken. Dit brede kwaadaardige-elite-narratief vindt weerklank binnen alle lagen van de bevolking. Van een zeer klein deel van de aanhangers gaat een gewelddadige dreiging uit. Zij richten zich op mensen die deze elite zouden vertegenwoordigen.

Regelmatig ontvangen onder andere bewindspersonen, deurwaarders, journalisten, rechters en lokale bestuurders bedreigingen uit anti-institutioneel extremistische hoek. Enkelen geven aan daarom te willen stoppen met de functie.

Gewelddadige uitingsvormen

Bovengenoemde twee rechtszaken laten zien dat deze nieuwe vorm van extremisme ook een gewelddadige vorm kan aannemen. Verschillende Europese veiligheidsdiensten constateren hetzelfde, in relatie tot vergelijkbare groeperingen in het eigen land. Het gaat hierbij echter om een zeer kleine minderheid van de anti-institutioneel extremisten.

Anti-institutioneel terrorisme vormt een ander type dreiging dan bijvoorbeeld jihadistisch terrorisme of rechts-terrorisme. Zo zijn geweldsbereide anti-institutioneel extremisten ouder dan geweldsbereide aanhangers van andere extremistische stromingen: zij zijn veelal 45+ en radicaliseren op latere leeftijd. Ook is het ontbreken van radicaliserende tieners een opmerkelijk verschil met de recente ontwikkelingen binnen andere vormen van extremisme.

Een ander belangrijk verschil is dat deze geweldsbereide extremisten relatief vaak kennis hebben over én vaardig zijn in het gebruik van geweldsmiddelen. Veel van hen hebben een fascinatie voor wapens en oefenen zich in het gebruik van deze wapens. Een kleine groep probeert illegale vuurwapens te kopen, maar de meesten beschikken over legale wapens, zoals kruisbogen en messen, of over zware persluchtwapens (een krachtigere variant van het bekendere luchtdrukwapen). Door diverse innovaties is de vuurkracht van deze persluchtwapens de afgelopen jaren sterk toegenomen. Hierdoor hebben veel van de zwaardere persluchtwapens een grotere vuurkracht dan een standaard vuurwapen.

Maatschappelijke opgave

De AIVD benadrukt dat anti-institutioneel extremisme vooral een breder, maatschappelijk vraagstuk is en niet alleen een veiligheidsprobleem. De voedingsbodem voor dit type extremisme is onder andere een toenemende onvrede over en wantrouwen tegen instituties, zoals de overheid. Hierin hebben niet alleen de wetenschap en de overheid, maar ook de politiek een rol. Alleen door een bredere aanpak van de oorzaken kan de dreiging van anti-institutioneel extremisme eventueel op termijn afnemen.

De grotere anti-institutioneel extremistische beweging

Tijdens en kort na de coronapandemie groeide de anti-institutionele beweging. Op dit moment is de beweging zeker niet kleiner geworden. Binnen deze beweging zijn er tientallen aanjagers die het narratief actief uitdragen.

De aanhoudingen in 2024 en 2025 lijken geen afschrikkende werking te hebben op de groep anti-institutioneel extremisten en de actieve aanjagers daarvan. Een deel van hen ziet de aanhoudingen als bevestiging van het eigen gedachtegoed, of als nieuw complot daarbinnen. De gedetineerden zouden ‘politieke gevangenen’ zijn, die ‘te dicht bij de waarheid kwamen’ en toen ‘door de kwaadaardige elite werden gearresteerd’. Deze gedetineerden krijgen steun van andere anti-institutioneel extremisten. Voor sommigen worden inzamelingsacties gehouden. Vele duizenden mensen blijken bereid te doneren.

Hoewel een deel van de aanjagers en overige aanhangers zich beschouwt als onderdeel van een beweging, is er geen sprake van een georganiseerd landschap. Zo is er geen consensus over wat men moet doen tegen de vermeende kwaadaardige elite.

Verspreiding van het gedachtegoed

De aanjagers organiseren met enige regelmaat fysieke bijeenkomsten, zoals lezingen en symposia. Ook verspreiden zij het narratief op sociale media, in podcasts en op alternatieve mediaplatforms. Op veel van deze platforms wordt het kwaadaardige-elite-narratief afgewisseld met overheidskritiek. Ook zijn er soms geluiden te horen die het narratief juist afzwakken of tegenspreken.

Pro-Russische desinformatie op deel alternatieve media

De alternatieve media zijn voor veel aanjagers en aanhangers een belangrijke bron van nieuwsgaring geworden. Deze online kanalen hebben vaak een groot bereik en zien er soms zeer professioneel uit. Een deel van deze media verspreidt pro-Russische desinformatie. De bezoekers van deze kanalen zijn mogelijk vatbaar voor dergelijke ondemocratische boodschappen: deze passen vaak naadloos in het eigen gedachtegoed.

> **Lees meer op aivd.nl/extremisme**

2.1.3 Rechts-extremisme

> **De AIVD bracht in 2025 over 8 personen ambtsberichten uit om een geweldsdreiging met een rechts-extremistische grondslag weg te nemen.**

> **Niet alle rechts-extremisten willen geweld gebruiken om hun doelen te bereiken. Een bredere, niet-geweld-dadige beweging maakt opportunistisch gebruik van politiek-maatschappelijke gebeurtenissen en ontwikkelingen.**

> **De AIVD ziet een nieuwe vorm van extremisme: het nihilistisch gewelddadig extremisme.**

De dreiging vanuit het rechts-extremisme is tweeledig. Enerzijds bestaat de dreiging uit de verspreiding van rechts-extremistisch gedachtegoed in de samenleving. Anderzijds is deze verspreiding voor sommigen een legitimatie voor het gebruik van geweld. De AIVD ziet grofweg dan ook twee groepen binnen het rechts-extremistische landschap: een bredere, niet-gewelddadige beweging en een smallere, gewelddadige beweging.

Beide groepen delen grotendeels dezelfde uitgangspunten en doelen. Er is dan ook geen sprake van een strakke scheiding. Rechts-extremisten uit beide groepen passen vijanddenken toe. Zij zien minderheidsgroepen of andersdenkenden als bedreiging. Bij beide groepen staat de bedreiging van ‘het blanke ras’ centraal en beide streven naar ‘een blanke etno-staat’.

Wel zijn er verschillende subideologieën. Ook ziet de AIVD dat subgroepen en individuen verschillende prioriteiten stellen. Hoewel sommige individuen uitgesproken voor of juist tegen het gebruik van geweld zijn, is deze scheids-lijn niet altijd even strak te trekken.

Rechts-extremistisch geweld

In 2025 heeft de AIVD een aantal ambtsberichten uitgebracht over personen die betrokken zijn bij (online) groepen die geweldloze methoden uitdragen, maar die ook wapens en munitie verzamelden en vervaardigden. Zij wilden deze wapens zeer waarschijnlijk inzetten.

Daarnaast is er al enkele jaren sprake van jongeren, veelal jongens, die radicaliseren in online chatgroepen. In deze online omgevingen worden geweld en aanslagplegers verheerlijkt, en ideologieën verspreid. Deze ideologieën zijn niet altijd eenduidig. Zo is er in veel gevallen sprake van grieven, occulte ideeën of een fascinatie voor dood, pijn en geweld. Bij personen die vanuit deze gedachtestroom doorradicaliseren naar geweld is het daarom niet altijd duidelijk hoe concreet hun doelen en onderbouwing zijn. En of ze, ook gezien hun jonge leeftijd, daadwerkelijk zullen overgaan tot het plegen van geweld. Verschillende voorbeelden uit het buitenland laten echter zien dat dit zeker niet uit te sluiten is.

Nihilistisch gewelddadig extremisme

Langlopend onderzoek naar de rechts-terroristische beweging wijst op een nieuw extremistisch fenomeen, dat is ontstaan in de afgelopen jaren: het nihilistisch gewelddadig extremisme. Dit extremistische fenomeen speelt zich grotendeels af in een bredere online omgeving van criminaliteit, waarbij sommige personen doelbewust maatschappij-ontwrichtende schade willen aanrichten. In deze specifieke gevallen raakt dit fenomeen ook het taakveld van de AIVD.

In 2025 zijn op basis van politieonderzoek verschillende personen aangehouden die vanuit deze nihilistische ideologie zijn overgegaan tot (het aanzetten tot) geweld. Deze gearresteerde individuen zijn geradicaliseerd in een online omgeving met heftige en gewelddadige beelden, kinder- en dierenmishandeling en kinderporno. Individuen binnen dit online netwerk zetten elkaar en anderen aan tot geweld, zoals zelfbeschadiging, suïcide of dodelijk geweld. Sommige groepen of personen willen ook aanzetten tot terrorisme. Geweldspleging en het online delen hiervan werken statusverhogend.

Normaliseren van het gedachtegoed

Binnen de rechts-extremistische beweging zijn veel personen en subgroepen die het rechts-extremistische geluid willen normaliseren en dit breed geaccepteerd proberen te krijgen. Ook in 2025 bleef normalisering een van de belangrijkste strategieën van de beweging. Daarbij presenteren ze hun gedachtegoed veelal in een mildere vorm om zo acceptabeler over te komen, terwijl ze achter de schermen het rechts-extremistische doel van een 'blanke etnostaat' nastreven. Een goed voorbeeld is het veelvuldige gebruik van de term 'remigratie', die op zichzelf neutraal is, maar in het narratief van rechts-extremisten staat voor het massale vertrek van mensen met een migratieachtergrond uit Europa. Nederlandse rechts-extremisten werken hierin samen met geestverwanten in andere Europese landen, voor wie normalisering ook een belangrijke strategie is. Zo organiseerden Europese rechts-extremisten in mei 2025 een goedbezocht congres over 'remigratie' in Italië, waaraan ook Nederlanders deelnamen. Op de conferentie was er een mix van Europese rechts-extremisten en leden van radicaal-rechtse partijen aanwezig. Rechts-extremisten zoeken op dergelijke bijeenkomsten toenadering tot zulke partijen.

De rechts-extremistische beweging maakt opportunistisch gebruik van politiek-maatschappelijke gebeurtenissen en ontwikkelingen. Om het draagvlak voor de beweging te vergroten wordt ingespeeld op angsten en onzekerheden die leven bij delen van de bevolking. Zo waren er meerdere rechts-extremistische groeperingen aanwezig bij de asieldemonstratie op het Malieveld, in september 2025 ('Elsfest'). Een deel van hen vertoonde nazistische uitingen, ging over tot geweld tegen de politie, trok de binnenstad in en probeerde brand te stichten bij het partijkantoor van D66.

Daarnaast zag de AIVD in 2025 dat er in de rechts-extremistische beweging een blijvende interesse is voor 'intredepolitiek'. Dit is het proces waarbij extremisten proberen invloed uit te oefenen door invloedrijke politiek-bestuurlijke functies te bekleden, om vanuit daar te werken aan hun extremistische beleidsdoelen. Deze interesse in het politieke speelveld vanuit rechts-extremisten is niet nieuw te noemen. Wel lijkt de aanpak doelmatiger te zijn dan voorheen. Daarbij speelt mee dat rechts-extremisten zich gesterkt voelen vanwege soortgelijke bewegingen in andere landen.

> **Lees meer op aivd.nl/extremisme**

> **Net als in 2024 was de oorlog in Gaza een van de belangrijkste onderwerpen voor de links-extremistische beweging.**

> **De dreiging vanuit deze beweging was gering. Veel van het linkse protest was activistisch van aard. Hoewel acties hinderlijk konden zijn, bedreigden deze de democratische rechtsorde veelal niet.**

2.1.4 Links-extremisme

Traditioneel gezien vormen met name anarchisten en in mindere mate marxisten-leninisten de links-extremistische beweging in Nederland. Zowel binnen de anarchistische beweging als bij diverse marxistisch-leninistische organisaties was er sprake van een sterk pro-Palestijns sentiment. Men keerde zich tegen Israël en tegen de steun die Israël kreeg vanuit onder meer Europa en de Verenigde Staten.

Bij de pro-Palestina- en anti-Israëlprotesten was er veelal sprake van een heel diverse samenstelling van groepen en individuen. Zij voerden samen actie, vanuit diverse ideologische motieven, maar ook vanuit persoonlijke verbondenheid en gedeelde emoties. Zo vonden vertegenwoordigers vanuit zowel de Palestijnse als de islamitische gemeenschap, klimaatactivisten, anti-imperialisten en studenten elkaar. De demonstraties verliepen, net zoals in 2024, over het algemeen activistisch. Een enkele keer kwam het hierbij tot verstoringen van de openbare orde.

Bekladdingen en vernielingen

De links-extremistische beweging voerde geen acties uit die expliciet waren gericht op Joodse instellingen of personen. Wel was er sprake van een opvallend groot aantal bekladdingen en vernielingen bij gebouwen van bedrijven die betrokken (zouden) zijn bij wapenleveranties aan de Israëlische strijdkrachten of bij de activiteiten van Joodse kolonisten op de Westelijke Jordaanoever. Ook overheidslocaties, zoals een kazerneterrein, het ministerie van Buitenlandse Zaken, en universiteiten waren doelwit van dergelijke acties. Zo werd er voor de ingang van gebouwen geprotesteerd, of werden panden 's nachts bezocht en met brandblussers bespoten met verf. Ook werden veelvuldig ruiten vernield van dergelijke panden. Vaak werden deze acties vervolgens online geclaimd, waarbij de reden(en) voor de acties ook werden genoemd.

Samidoun Nederland

Een van de organisaties die actief betrokken is bij de pro-Palestina- en anti-Israëlprotesten is de Nederlandse tak van de internationaal gevestigde, marxistisch-leninistische organisatie Samidoun. Samidoun Nederland toont zich in daad activistisch. De organisatie roept niet op tot geweld, maar verheerlijkt geweld tegen Israëliërs en de Israëlische staat wel, bijvoorbeeld door acties van terroristische organisaties te legitimeren. Hoewel de aanhang van Samidoun in Nederland klein is, resoneert deze extremistische boodschap breder. Dit komt mede door de huidige aandacht voor de kwestie en de kruisbestuiving die de organisatie heeft met andere (veelal linkse) organisaties van pro-Palestina- en anti-Israëlprotesten.
De dreiging van Samidoun tegen de nationale veiligheid is beperkt. Wel kan de boodschap die de organisatie uitdraagt als bedreigend worden ervaren en mogelijk bijdragen aan radicalisering en toenemende polarisatie.

Antimilitarisme

In 2025 leefde het antimilitarisme op, vanwege de acties gericht tegen bedrijven die wapenonderdelen (zouden) leveren aan Israël en de in Nederland gehouden NAVO-top. Antimilitaristische acties bleven beperkt tot de hiervoor vermelde vernielingen aan gebouwen en activistische uitingen zoals demonstraties.

Tijdens de NAVO-top was er sprake van activistisch protest. Er was hierbij geen sprake van extremisme. Mogelijk dat eventuele extremistische plannen niet haalbaar bleken, door de grootschalige beveiligingsmaatregelen. Ook vanuit het buitenland bleef de toevloed van actievoerders beperkt tot hooguit enige honderden activisten.

Antifascisme

Bij antifascistische acties, veelal afkomstig uit de anarchistische beweging, zijn de actiemethoden al jaren dezelfde: het aanrichten van vernielingen, het verstoren van bijeenkomsten, het intimideren van personen en het in kaart brengen en online publiceren van persoonlijke gegevens (doxing). De AIVD acht dergelijke acties extremistisch omdat ze het functioneren van de democratische rechtsorde ondermijnen.

In 2023, een jaar met Tweede Kamerverkiezingen, zag de AIVD nog een duidelijk verhoogde activiteit van antifascistische acties. Deze acties waren destijds gericht op politieke partijen, op individuele politici, maar ook op andere als fascistisch aangeduide groepen en personen. In 2025 was het, op enkele kleinschalige acties na, juist opmerkelijk rustig rond de Tweede Kamerverkiezingen. Wel waren er enkele dreigementen uit de hoek van dierenrechtenextremisten tegen politici, die ook aandacht kregen in de media. De AIVD schat in dat onderwerpen die eerder sterk polariserend werkten tussen links en rechts, minder een rol speelden in de verkiezingscampagne van 2025.

> **Lees meer op aivd.nl/extremisme**

2.2

Criminele ondermijning van de nationale veiligheid

- **Ook in 2025 heeft de AIVD onderzoek gedaan naar criminele netwerken die een geweldsdreiging vormen tegen belangendragers van de democratische rechtsorde.**
- **Eind 2024 heeft de AIVD een ambtsbericht uitgebracht over de heimelijke communicatie vanuit de Extra Beveiligde Inrichting (EBI) met een crimineel netwerk. Dit heeft ertoe geleid dat in 2025 een advocaat werd aangehouden door de politie.**
- **Nieuw in 2025 is het onderzoek door de AIVD naar de verwevenheid tussen criminele netwerken en statelijke actoren.**

Verwevenheid statelijke actoren en criminele netwerken

Criminele netwerken zijn over de gehele wereld actief. Zij zijn gespecialiseerd in het opereren buiten het zicht van opsporing- en veiligheidsdiensten. Daarmee zijn ze voor veel statelijke actoren een aantrekkelijke samenwerkingspartner voor onder meer spionage, inmenging en geweld tegen politieke opposanten. In 2025 heeft de AIVD onderzoek gedaan naar het gebruik van dodelijk geweld door criminele netwerken in opdracht van statelijke actoren. Uit dit onderzoek komt onder meer naar voren dat sommige criminele netwerken structureel actief zijn voor statelijke actoren in het uitvoeren van geweld. De reden ligt onder meer in de mogelijkheden die de statelijke actor heeft om in ruil voor verleende diensten de criminele netwerken bescherming te bieden.

Deze bescherming is ook de reden dat (Nederlandse) criminele netwerken zich in het buitenland vestigen. Vaak doen zij dit in landen waar zij minder risico lopen om te worden vervolgd of uitgeleverd, bijvoorbeeld omdat zij geen prioriteit vormen voor de lokale autoriteiten of omdat zij via corrupte contacten bescherming kunnen kopen. Sommige van deze netwerken vormen een dreiging voor de nationale veiligheid. De bescherming door de statelijke actor vergroot dan de dreiging tegen de nationale veiligheid omdat het netwerk buiten bereik van de opsporing blijft. Onderzoek door de AIVD laat zien dat dergelijke netwerken door de verwevenheid met statelijke actoren in 2025 een sterke positie hebben kunnen opbouwen.

Internationale samenwerking is van groot belang voor het beschermen van de nationale veiligheid. Dit is zeker ook het geval wanneer criminele netwerken verweven raken met statelijke actoren. Door middel van inlichtingenberichten heeft de AIVD in 2025 zowel nationale partners als Europese partners over deze verwevenheid geïnformeerd en hen in staat gesteld hierop te handelen.

Heimelijke communicatie vanuit EBI met crimineel netwerk verstoord

Uit onderzoek door de AIVD is naar voren gekomen dat vanuit detentie in de Extra Beveiligde Inrichting (EBI) heimelijke communicatie plaatsvond met een crimineel netwerk. De AIVD heeft vervolgens een ambtsbericht uitgebracht aan het Openbaar Ministerie, zodat het een strafrechtelijk onderzoek kon starten. Dit onderzoek heeft ertoe geleid dat in 2025 een advocaat werd aangehouden door de politie.

De taak van de AIVD op het thema criminele ondermijning

Het beschermen van de nationale veiligheid is de wettelijke kerntaak van de AIVD. Als het ernstige vermoeden bestaat dat een crimineel netwerk de nationale veiligheid schaadt, of nog kan en wil schaden, kan de AIVD hier onderzoek naar doen. De AIVD heeft daarbij een eigen, scherp afgebakende taak. Het opsporen (en vervolgen) van strafbare feiten is de taak van het Openbaar Ministerie en de politie. Doordat de politie, het OM en de AIVD elk vanuit hun eigen taakstelling onderzoek doen naar criminele netwerken ontstaat een vollediger beeld van hoe Nederland weerbaarder kan worden tegen criminele ondermijning.

> **Lees meer op aivd.nl/ondermijning**

2.3

Statelijke inmenging in Nederland

- **Sinds 2025 zijn meer vormen van spionage strafbaar in Nederland, zoals digitale spionage en diasporaspionage.**
- **Verschillende landen verzamelen inlichtingen over personen uit de diaspora-gemeenschap die kritiek hebben op het regime in het land van (familie)herkomst.**
- **In 2025 onderkenden de AIVD en MIVD dat landen ook cyberaanvallen inzetten tegen critici die in het Westen verblijven.**

Statelijke inmenging is een verzamelnaam voor allerlei manieren waarop buitenlandse overheden zich proberen te bemoeien met of te mengen in de gang van zaken in Nederland. Onder statelijke inmenging valt elke activiteit die de democratische rechtsorde ondermijnt en die wordt ondernomen door of in opdracht van een buitenlandse overheid. Dit kan in de vorm zijn van bijvoorbeeld heimelijke politieke beïnvloeding of sabotage. Ook kan de statelijke actor de diaspora controleren en onder druk zetten. Dit kan diep ingrijpen op de persoonlijke levenssfeer en het gevoel van veiligheid van mensen in deze diasporagemeenschappen, en vormt een inbreuk op de Nederlandse soevereiniteit en op de grondrechten van deze mensen.

Via spionage proberen andere landen op heimelijke wijze verschillende soorten informatie te verkrijgen in Nederland en Europa. De meeste spionageactiviteiten, zoals het schenden van staats-, ambts- of bedrijfs-geheimen, zijn al lange tijd strafbaar in Nederland. Vanaf 15 mei 2025 zijn er meer vormen strafbaar, zoals digitale spionage en diasporaspionage. De uitbreiding van de wet zorgt voor meer mogelijkheden voor het Openbaar Ministerie om op te treden tegen spionageactiviteiten.

Uitbreiding strafbaarheid spionageactiviteiten
Als een persoon gevoelige informatie lekt en/of prijsgeeft die niet staatsgeheim is, of als iemand handelingen uitvoert voor een buitenlandse overheid, is dat nu strafbaar als dit de Nederlandse belangen ernstig kan schaden. De AIVD ziet dat er een grote aanhoudende spionagedreiging uitgaat van de inlichtingen- en veiligheidsdiensten uit landen als Rusland, China en Iran, maar ook van de diensten uit landen met een grote diasporagemeenschap in Nederland, zoals Marokko.

Diaspora als bronnennetwerk

Onder meer de Turkse en de Marokkaanse inlichtingen- en veiligheidsdiensten verzamelen inlichtingen over personen uit de diasporagemeenschap die kritiek hebben op het regime in het land van (familie) herkomst. Deze diensten maken vaak gebruik van een bronnennetwerk, met personen uit diezelfde diasporagemeenschap als bron. Personen uit deze gemeenschappen zijn dan ook extra kwetsbaar om hiervoor benaderd te worden. Vaak zijn zij nog verbonden met het land van herkomst, bijvoorbeeld via familie of onroerend goed. Deze buitenlandse inlichtingen- en veiligheidsdiensten kunnen deze verbondenheid misbruiken, bijvoorbeeld door consulaire gunsten te verlenen in het land van herkomst, in ruil voor medewerking.

Uit onderzoek van de AIVD blijkt dat de Marokkaanse diensten interesse hebben in personen die werkzaam zijn op posities met toegang tot informatie die belangrijk is voor Marokko. De AIVD gaat met de betrokken werkgevers in gesprek om een groter veiligheidsbewustzijn te creëren en de weerbaarheid te vergroten. Hiermee hoopt de AIVD ook de meldingsbereidheid te verhogen.

> **Lees meer op aivd.nl/inmenging**

In samenwerking met de NCTV bracht de AIVD in het najaar van 2024 de fenomeenanalyse *Over de grens. Statelijke inmenging in diasporagemeenschappen in Nederland* uit.

> **Lees meer op aivd.nl/overdegrens**

Geweld en cyberaanvallen tegen politieke tegenstanders

In uiterste gevallen kunnen andere landen overgaan tot het gebruik van geweld tegen politieke tegenstanders. Landen die overgaan tot deze vormen van statelijke inmenging proberen hun betrokkenheid bij deze gewelddadige activiteiten te verhullen. Zij maken hiervoor bijvoorbeeld gebruik van criminele netwerken.

In 2025 onderkenden de AIVD en MIVD in een gezamenlijk cyberonderzoek dat landen ook cyberaanvallen inzetten richting critici die in het Westen verblijven.

2.4

Cyberdreigingen

- **De AIVD zag in 2025 dat dreiging door landen met een offensief cyberprogramma groter is dan voorheen. Spraakmakende cyber-incidenten en aanvals-campagnes in binnen- en buitenland onderstreepten opnieuw de omvang en impact van digitale dreigingen op de (inter)nationale veiligheid.**
- **Technologische ontwikkelingen geven aanvallers de mogelijk-heid om steeds geavanceerdere aanvalstechnieken te ontwik-kelen en te gebruiken.**

In 2024 signaleerde de AIVD al dat het aantal landen met een offensief cyberprogramma toeneemt. In 2025 zag de AIVD dat de dreiging die uitgaat van deze cyberprogramma's nog groter is dan voorheen werd ingeschat. De dreiging van offensieve cyberprogramma's uit China en Rusland bleef ook in 2025 onverminderd hoog.

De NAVO-top in Den Haag

De AIVD heeft bijgedragen aan de NAVO-top op 24 en 25 juni 2025. Achter de schermen is door velen een bijdrage geleverd om dit grootschalige evenement veilig te laten verlopen. In de lijn der verwachting vonden enkele cyberincidenten plaats. De impact hiervan bleef beperkt. Dit komt mede door maatregelen van organisaties die verantwoordelijk waren voor de beveiliging van het evenement.

Cyber: ongelijke strijd tegen een steeds grotere dreiging

De strijd in het cyberdomein is een ongelijke strijd. Het is voor 'verdedigers', zoals Nederlandse organisaties, vaak een ingewikkelde taak om zich blijvend te weren tegen statelijke actoren die binnen andere wettelijke kaders opereren.

Steeds meer aanvallers maken gebruik van automatisering om met succes cyberaanvallen uit te voeren. Zo is het in toenemende mate mogelijk om bijvoorbeeld systematisch te zoeken naar kwetsbaarheden in systemen of om meerdere doelen tegelijk aan te vallen. De mogelijkheden van kunst-matige intelligentie zorgen bovendien voor een flinke versnelling in de ontwikkeling van nieuwe aanvalsmiddelen en -manieren. Om hier effectief tegenwicht aan te bieden, is innovatie en samenwerking onontbeerlijk.

Cybersecurityaanpak: de basis op orde

In het Cybersecuritybeeld Nederland (CSBN) 2025 van de NCTV, waar de AIVD een bijdrage aan levert, staat: 'De conclusie dat dreigingen onvoor-spelbaarder en complexer worden, betekent niet per definitie dat het verdedigen daartegen dat ook wordt. Veel digitale incidenten vinden namelijk hun oorzaak in het niet op orde hebben van "digitale basishygiëne". (...) Voor een gemiddelde organisatie geldt dan ook: fixeer je niet op het complexe dreigingslandschap, maar weer je daar in eerste instantie tegen met de basisprincipes.'

Aantal incidenten met onbekende kwetsbaarheid neemt toe

Het aantal incidenten waarbij aanvallers een onbekende kwetsbaarheid (een *zero day*) misbruiken neemt toe. Dit is een kwetsbaarheid waarvan bij softwareleveranciers nog niet bekend is dat deze bestaat. Hiervoor zijn dus ook nog geen beveiligingsmaatregelen beschikbaar. Dit maakt dit type kwetsbaarheid interessant voor kwaadwillenden. Aanvallers slagen er bovendien in om deze kwetsbaarheden steeds sneller uit te buiten en daarmee in een kort tijdsbestek veel slachtoffers te maken.

In 2025 zijn in Nederland verschillende incidenten geweest waarbij aanvallers gebruikmaakten van onbekende kwetsbaarheden en kwetsbaarheden die nog maar kort daarvoor bekend waren geworden. Zo werd in de zomer van 2025 misbruik gemaakt van onbekende kwetsbaarheden in *Citrix NetScaler*, dat organisaties onder andere gebruiken om thuiswerken te faciliteren. De aanvallers vielen onder meer het Openbaar Ministerie aan. Deze aanval verstoorde het dagelijkse functioneren van een organisatie die een essentiële rol vervult in de samenleving.

Aanvallers gebruiken niet alleen onbekende kwetsbaarheden. Net als voorgaande jaren blijven ook software en hardware die oudere en reeds bekende kwetsbaarheden bevatten bij hen geliefd.

Statelijke actoren hanteren brede doelwitselectie: van (westerse) politici tot dissidenten

Statelijke actoren hebben ook interesse in politici en ambtenaren en in critici uit de diasporagemeenschap. Statelijke actoren proberen onder andere gegevens over hen te verkrijgen via cyberaanvallen. In 2025 hebben statelijke actoren communicatie buitgemaakt van deze personen. Dit lukte onder meer door telecomproviders buiten Nederland te compromitteren. Met deze data kunnen statelijke actoren inzicht krijgen in bijvoorbeeld Europese besluitvorming. In ernstigere gevallen kan dit hen ook helpen om actuele verblijfslocaties van personen te verkrijgen in bijvoorbeeld oorlogsgebied.

Meer digitale aanvallen tegen mobiele apparaten

De AIVD en MIVD zagen in 2025 een toename van digitale aanvallen tegen mobiele apparaten zoals telefoons. Dit zijn kwetsbare communicatiemiddelen, onder andere vanwege de berichten-applicaties die veelvuldig worden gebruikt hierop. Ook monitoren werkgevers deze mobiele apparaten doorgaans minder intensief dan computers en servers. Daarnaast zijn mensen zich minder bewust van de risico's bij telefoongebruik.

Voor aanvallen op deze mobiele apparaten en andere apparatuur zetten statelijke actoren bijvoorbeeld commercieel verkrijgbare spyware in. Ook ontwikkelen zij zelf malware hiervoor. Daarnaast proberen ze bijvoorbeeld berichten-apps over te nemen, door middel van *social engineering*.

Via *social engineering* toegang tot berichten-apps

De AIVD en MIVD stellen vast dat meerdere statelijke actoren proberen om persoonlijke gegevens van hun doelwitten in handen te krijgen via *social engineering*. Dit zijn technieken die (cyber)criminelen inzetten om personen te verleiden om gevoelige informatie te delen en/of hen aan te zetten tot handelen. Zo is het in 2025 meerdere keren voorgekomen dat statelijke actoren zich voordeden als medewerker of chatbot van een berichten-app zoals WhatsApp of Signal. De zogenaamde medewerker of chatbot geeft aan dat het slachtoffer opnieuw moet inloggen en laat het slachtoffer vervolgens een bepaalde code invullen. Hierdoor krijgt de actor toegang tot het account van het slachtoffer.

Een andere manier waarop statelijke actoren slachtoffers maakten was via *voice phishing*. Hierbij bouwt een actor contact op met een slachtoffer om uiteindelijk met deze persoon te bellen. Het opbouwen van dit contact duurt soms zelfs maanden. Tijdens of na het telefoongesprek wordt vervolgens een link gestuurd waarmee de actor het account kan overnemen.

Landen met een offensief cyberprogramma

De AIVD en MIVD doen onderzoek naar verschillende landen met een offensief cyberprogramma. In de volgende paragrafen wordt de cyberdreiging vanuit Iran en Noord-Korea uitgelicht. De cyberdreiging uit China en Rusland wordt beschreven in de paragrafen die hierop volgen.

Cyberdreiging vanuit Iran

De AIVD en MIVD schatten in dat het Iraanse regime onverminderd inzet op zijn offensieve cyberprogramma. Iraanse cyberactoren ondernemen onder andere beïnvloedingsoperaties, digitale sabotage en digitale spionage. Zij richten zich op regionale tegenstanders, zoals Israël, maar ook op landen daarbuiten, zoals in West-Europa en Noord-Amerika.

Ook individuen zijn doelwit. In 2025 bleek dat Iran cyberspionage-campagnes voortzet richting in het Westen verblijvende critici van het Iraanse regime, onder wie dissidenten en journalisten. Iraanse actoren zetten hierbij onder andere geavanceerde malware in. Ze proberen op deze wijze toegang te verkrijgen tot de persoonlijke apparatuur en accounts (e-mail, sociale media) van deze personen. Deze dreiging is dan ook jegens hen persoonlijk. Het feit dat deze critici in sommige gevallen ook staats-burger zijn van westerse landen, weerhoudt Iran niet.

De diensten constateren ook dat de Iraanse cyberdreiging continueert richting experts die zich met het Midden-Oosten bezighouden. Daarnaast toonde Iran in 2025 ook interesse in westers overheidspersoneel.

Cyberdreiging vanuit Noord-Korea

Noord-Korea blijft een belangrijke dreiging voor de Nederlandse veiligheidsbelangen via zijn (nucleaire) wapenprogramma, offensieve cyberprogramma en de ondersteuning van Rusland in de oorlog tegen Oekraïne. Noord-Korea zet een offensief cyberprogramma in om het huidige regime in stand te houden.

Een van de belangrijkste doelen van Noord-Koreaanse cyberprogramma is financieel gewin. Het offensieve cyberprogramma draagt zeer waarschijnlijk bij aan de financiering van het Noord-Koreaanse (nucleaire) wapen-programma. Een ander doel is cyberspionage: het regime wil hoogwaardige (militaire) technologie verkrijgen, net als (geo)politieke en wetenschappe-lijke informatie.

De diensten hebben in 2025 verschillende cyberaanvallen waargenomen tegen Nederlandse bedrijven en personen, die werden uitgevoerd door of met behulp van Noord-Koreaanse IT'ers. Deze aanvallen waren vooral gericht op het ontvreemden van cryptovaluta, ten gunste van het Noord-Koreaanse regime. De aanvallers gaan hierbij opportunistisch te werk. Als zij ook gevoelige data kunnen verkrijgen, laten zij deze mogelijkheid niet onbenut.

> **Lees meer op aivd.nl/cyberdreiging**

2.5

Rusland

- **Ook in 2025 stelde Rusland zich steeds aanvallender op tegen Europese landen. De AIVD en MIVD doen gezamenlijk onderzoek naar welke dreiging Rusland vormt voor Nederland.**
- **Om deze dreiging beter te begrijpen, is het essentieel om het Russische perspectief te kennen. Ook als de oorlog in Oekraïne eindigt, zal de confrontatie, die voor Rusland breder en existentieel is, voortduren.**
- **De AIVD en MIVD traden in 2025 naar buiten over een voorheen publiek onbekende Russische cyberactor genaamd LAUNDRY BEAR. Deze actor was verantwoordelijk voor een aanval waarbij werk-gerelateerde contactgegevens van Nederlandse politie-medewerkers zijn buitgemaakt.**

Net als in 2024 stelde Rusland zich in 2025 steeds agressiever, brutaler en provocerender op tegen Europese landen. Vanwege de westerse politieke en militaire steun aan Oekraïne karakteriseert het Russische regime Europa, en vooral de Europese Unie, als een opponent. Het beschouwt deze opponent bovendien als steeds vijandiger.

Het Russische perspectief

De AIVD en MIVD zien dat Rusland zich verwikkeld ziet in een breder en existentieel conflict met het Westen. De oorlog in Oekraïne – het grootste en meest dodelijke conflict in Europa sinds de Tweede Wereldoorlog – is daar voor het Russische regime slechts een onderdeel van.

Het narratief van het Russische regime is dat het Westen agressief is, en dat het Rusland wil destabiliseren en een nederlaag wil laten lijden. Er zou hierbij maar één partij kunnen winnen (een *zero-sum game*). De instand-houding van dit vijandbeeld draagt eraan bij dat het volk zich achter de president blijft scharen en helpt het regime aan de macht te blijven. Rusland bereidt zich voor op een langdurige confrontatie met het Westen. Als gevolg hiervan is een militair conflict tussen Rusland en het Westen niet langer ondenkbaar. Ook als de strijd in Oekraïne ten einde komt, zal deze bredere en in de ogen van het Russische regime existentiële confrontatie voortduren.

Putins regime bleef in 2025 stabiel, al dwingt het dat af met steeds meer repressie en een groeiende controle op met name het digitale informatie-domein. Deze initiatieven zijn er in zekere zin op gericht om Rusland verder te isoleren van westerse invloeden, die een bedreiging kunnen vormen voor de stabiliteit van het regime. De economische problemen die gepaard gaan met de oorlog bleken hanteerbaar voor Rusland. Van enige binnenlandse oppositie is na de dood van Aleksey Navalny in 2024 geen sprake meer.

Het afgelopen jaar is de Russische houding ten aanzien van de oorlog in Oekraïne verder verhard en onverzettelijker geworden, ondanks enkele Russisch-Oekraïense onderhandelingsrondes en meerdere inhoudelijke besprekingen met het Witte Huis. Duidelijker dan eerder blijkt dat Rusland niet bereid is tot een compromis in Oekraïne. Rusland zet de strijd op het Oekraïense slagveld onverminderd voort.

Russische cyberactoren actief

Net als voorgaande jaren zijn Russische cyberactoren actief op het gebied van offensieve cyberoperaties tegen Europa. Het gaat hierbij zowel om actoren die direct gelieerd zijn aan de Russische inlichtingen- en veiligheidsdiensten, als om pro-Russische aanvallers die verder afstaan van de Russische overheid maar wel worden gesteund door de staat. Operaties variëren van relatief eenvoudig *spearphishing* tot geavanceerde inbraken in systemen van overheden, bedrijven en instanties.

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

De AIVD en MIVD signaleren dat de Russische capaciteiten om cyberaanvallen uit te voeren groeien. Ook kunnen deze actoren hun cyberaanvallen in een hoog tempo uitvoeren. Dit komt mede doordat zij hun aanvallen deels kunnen automatiseren, ook door middel van AI.

Publieke attributie LAUNDRY BEAR

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

Chataccounts Nederlandse overheids-medewerkers doelwit

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

Cyber op het slagveld

Een fors deel van het Russische offensieve cyberprogramma richt zich op de oostflank van Europa. Net als in voorgaande jaren vervult digitale spionage hierin een hoofdrol. Daarnaast zien de AIVD en MIVD dat de Russische staat op nieuwe manieren buitgemaakte informatie gebruikt. Zo zet het Russische leger tijdens militaire operaties informatie in die afkomstig is van cyberoperaties, zoals informatie over troepenbewegingen of locatiegegevens van Oekraïense militairen.

Prioritering bij sabotageactiviteiten

Ook in het geval van sabotageactiviteiten in het cyberdomein geldt Oekraïne nog altijd als de hoogste prioriteit van Russische cyberactoren. Daar waren vooral de Oekraïense energie- en logistieke sector doelwit. Deze prioritering kan veranderen bij een einde van de oorlog. Zo is het mogelijk dat Russische cyberactoren hun capaciteiten dan breder gaan inzetten op Nederland, en op andere NAVO-bondgenoten en EU-lidstaten.

Voor zowel digitale als fysieke sabotageactiviteiten geldt dat Nederland een potentieel targetland blijft voor Russische sabotageactiviteiten. Dat komt omdat Nederland nog steeds aanzienlijke steun levert aan Oekraïne, en omdat Nederland een transport- en informatieknooppunt is in Europa.

Rusland voerde in 2025 diverse digitale sabotageaanvallen en pogingen daartoe uit in Europese lidstaten. De AIVD en MIVD onderkenden geen acute succesvolle Russische cybersabotageaanvallen in Nederland in 2025.

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

Russische escalatie en de-escalatie

Met de fysieke sabotageactiviteiten lijkt Rusland naar eigen inzicht te escaleren en te de-escaleren. De omvang van deze activiteiten varieert door de tijd heen. Sabotageactiviteiten die aan de Russische inlichtingen- en veiligheidsdiensten kunnen worden toegeschreven, kenden in Europa een (voorlopig) hoogtepunt in de zomer van 2024. Hierna zagen de diensten minder Russische sabotageactiviteiten in Europa. Vooralsnog is onduidelijk waarom deze activiteiten destijds zijn afgeschaald. Wel is sinds de zomer van 2025 weer een voorzichtige toename zichtbaar van sabotage-activiteiten of voorbereidingen daartoe. Deze activiteiten zijn nog steeds veelal gericht tegen militaire en logistieke doelen, en tegen organisaties die betrokken zijn bij de oorlog in Oekraïne.

In het kader van de Russische hybride dreiging is er in de media veel gespeculeerd over drones. De AIVD en MIVD hebben in 2025 inderdaad een toenemend aantal meldingen ontvangen over waarnemingen van drones in de buurt van vitale infrastructuur, luchthavens en bijvoorbeeld militaire faciliteiten. Bij dit soort meldingen geldt dat het vaststellen van vermeende Russische betrokkenheid gecompliceerd is en veelal kan deze voorstelbare Russische betrokkenheid niet worden bevestigd. Ook is een gesignaleerde drone niet altijd een dreiging.

Nieuwe modus operandi: inzet van gelaagde netwerken

Het is voor de Russische inlichtingen- en veiligheidsdiensten moeilijker geworden om activiteiten te ontplooien in Europa. Dit komt mede door de grootschalige uitzetting van Russische inlichtingenofficieren onder diplomatiek dekmantel in een groot aantal Europese landen, die volgde op de Russische invasie in Oekraïne in 2022, en door de striktere visumregels binnen het Schengengebied. Om sabotageactiviteiten uit te voeren maken de Russische inlichtingen- en veiligheidsdiensten daarom ook gebruik van een nieuwe werkwijze: de inzet van gelaagde netwerken.

Gelaagde netwerken bestaan uit coördinatoren, facilitators en zogeheten *low-level* agenten die de sabotageacties uitvoeren. Een eenduidig profiel van dit type agent is niet te geven. Wel geldt dat het in veel gevallen personen betreft die sabotageactiviteiten als een manier zien om snel en gemakkelijk geld te verdienen. Deze, soms minderjarige, *low-level* agenten lijken zich veelal niet bewust dat ze activiteiten uitvoeren in opdracht van Rusland. In tegenstelling tot inlichtingenofficieren zijn zij niet of maar deels getraind.

Deze gelaagde constructies maken het voor Rusland relatief gemakkelijk om de eigen betrokkenheid bij sabotageoperaties te verhullen.

De AIVD en de MIVD achten het onwaarschijnlijk dat een toename van deze sabotageactiviteiten en deze nieuwe werkwijze de al bestaande modus operandi van de Russische diensten zullen vervangen. Deze bestaande werkwijzen, zoals de meer klassieke vormen van spionage en statelijke inmenging, hebben zich immers al bewezen in het verleden.

Russische inmenging

Een kerntaak van de Russische inlichtingen- en veiligheidsdiensten blijft spionage, een vorm van statelijke inmenging. Niet alleen via technische, maar ook via menselijke bronnen proberen de Russische diensten de hand te leggen op strategische geheimen, kennis en technologie om een politiek of militair voordeel te verkrijgen. Russische inlichtingenofficieren maken gebruik van diverse dekmantels, zoals wetenschapper of journalist, om toegang te verkrijgen tot deze informatie. Daarnaast blijven zij actief onder diplomatiek dekmantel, in Nederland en de rest van Europa.

De Russische inlichtingen- en veiligheidsdiensten zijn actief in onder meer de landen aan de oostgrens van het NAVO-bondgenootschap. Hier willen zij informatie verzamelen over de militaire capaciteiten van de NAVO en proberen zij de oorlog in Oekraïne te beïnvloeden in het voordeel van Rusland.

Ook spelen de Russische diensten een belangrijke rol bij het verwerven van technologie en *dual-use*-goederen voor de Russische defensie-industrie. Deze werkwijze stelt Rusland in staat om het westerse sanctiebeleid deels te omzeilen.

Russische benaderingen van Europese parlementariërs

De Russische diensten zoeken toenadering tot parlementariërs in Europese lidstaten. Dit doen zij zowel heimelijk als in de openheid. Openlijk nodigt Moskou parlementariërs uit om bijvoorbeeld deel te nemen aan evenementen in en buiten Rusland. Ook stelt het gezamenlijke initiatieven voor om samenwerkingen te hervatten. Tegelijkertijd lijken deze open toenaderingspogingen minder effect te hebben dan Rusland ambieert. Dit komt mede door terughoudendheid van Europese politici voor al te grote publieke affiliatie met Rusland. Dit noopt Rusland op zijn beurt weer tot meer discretie bij toenaderingspogingen richting deze politici.

Vergroten veiligheidsbewustzijn: AIVD brieft parlementariërs
De AIVD heeft briefings gegeven aan Tweede Kamerleden en Nederlandse Europarlementariërs over de dreiging die uitgaat van Russische heimelijke beïnvloeding.

Verspreiding van Rusland welgevallige boodschappen

Ondanks verschillende westerse tegenmaatregelen blijft Rusland onverminderd digitale desinformatiecampagnes uitvoeren ten aanzien van verschillende Europese landen. Het toenemende gebruik van kunstmatige intelligentie kan Rusland helpen om de kwaliteit en omvang van desinformatiecampagnes te verbeteren.

Rusland gebruikt gebeurtenissen in onder andere Nederland voor het uitdragen van Rusland welgevallige boodschappen. Deze boodschappen zijn vaak bedoeld voor de Russische bevolking. Dit krijgt vooral gestalte via demonstraties met boodschappen die Moskou goed uitkomen. In berichtgeving van Russische staatsmedia en op sociale media wordt het belang en de omvang van deze demonstraties zodanig uitvergroot dat bij een (pro-) Russisch publiek het beeld kan ontstaan dat in het Westen een substantieel kritisch geluid wordt geuit ten aanzien van militaire steun aan Oekraïne of ten aanzien van de NAVO.

In februari 2026 hebben de AIVD en MIVD de publicatie *Tussen vrede en oorlog: De oorlog in Oekraïne en de Russische dreiging in Europa* uitgebracht. Hierin is meer te lezen over onder andere het Russische perspectief en hybride activiteiten.

> Lees meer op aivd.nl/tussen-vrede-en-oorlog

2.6

China

- **De Chinese dreiging verbreedt en verdiept. De AIVD en MIVD doen gezamenlijk onderzoek naar de dreiging van China voor Nederland.**
- **China bouwt verder aan een internationale orde die de belangen van China bevordert.**
- **China verwerft hoogwaardige technologische kennis, zowel op legale als heimelijke wijze.**
- **De AIVD en de MIVD dragen bij aan bewustwording over en het tegengaan van Chinese cyberdreiging.**

China bouwt aan een nieuwe wereldorde

3 september 2025: in Beijing vindt een grote militaire parade plaats ter viering van het einde van de Tweede Wereldoorlog, tachtig jaar geleden. De parade laat een zelfverzekerde Chinese leider zien, en ook de contouren van een wereldorde die hij voor zich ziet: een wereld waarin China het krachtige middelpunt is. Een middelpunt waarnaar andere wereldleiders zich richten.

Enkele dagen voor deze parade had de Chinese leider Xi een nieuw mondiaal initiatief aangekondigd: het *Global Governance Initiative* (GGI). En nog eerder in 2025 vond in Hongkong de oprichting plaats van de door China geïnitieerde *International Organization for Mediation* (IOMed). Beide initiatieven zijn voorbeelden van hoe China nieuwe internationale structuren opzet waarmee het de eigen belangen beter kan behartigen dan via bestaande internationale organisaties. Ook stellen ze China in staat om de eigen invloed verder te vergroten, in het bijzonder in landen in Latijns-Amerika, Afrika en Azië. De wereldorde die China op deze manier tot stand wil brengen is erop gericht de westerse invloed in de wereld – vooral van de Verenigde Staten, maar ook van Europa – te verminderen.

Uitbuiten van economische afhankelijkheden

In de onderzoeken die de AIVD gezamenlijk met de MIVD doet, wordt de concurrentie tussen China en het Westen onder meer zichtbaar op het gebied van de economie. Toen de Verenigde Staten handelstarieven afkondigde, beantwoordde China deze met handelstarieven voor Amerikaanse producten en later met restricties op de uitvoer van zeldzame aardmetalen. China laat hiermee zien hoe afhankelijk andere landen zijn van China voor het maken van producten die zowel een civiel als militair doel kunnen hebben. Het heeft deze afhankelijkheid ook in 2025 tegen de VS en Europa ingezet. Deze afhankelijkheid kan risicovol zijn en ook de Europese en Nederlandse economie en het vermogen om autonoom strategische keuzes te maken, bedreigen.

Het bemachtigen van gevoelige kennis en technologie

Voor China's voortgaande technologische en economische ontwikkeling is China echter ook voor een deel afhankelijk van westerse landen. Veel kennis ontwikkelt China zelf door hoogwaardig onderzoek. De AIVD en de MIVD constateren dat China hiervoor ook westerse onderzoekers aantrekt, en dat het Chinese studenten en onderzoekers naar het Westen stuurt om kennis op te doen die zij later in China kunnen toepassen of verder ontwikkelen. Op deze wijze krijgt China geavanceerde en soms zeer gevoelige kennis en technologieën in handen. Deze zaken kan China toepassen in zijn eigen verdere technologische en economische ontwikkeling en de modernisering van zijn krijgsmacht. Dat China op sommige terreinen, zoals het maken van zeer geavanceerde chips, een achterstand heeft op het Westen, sluit niet uit dat het in staat is tot opmerkelijke prestaties. Zo werd de wereld verrast door het AI-programma DeepSeek, dat zich met de meest geavanceerde westerse programma's op dit terrein bleek te kunnen meten, ondanks dat er werd gewerkt met minder geavanceerde chips.

Dat China de eigen inspanningen op veel hoogwaardig technologische terreinen wil versterken en uitbouwen in de komende jaren, wordt ook duidelijk in de eerste contouren van het Vijftiende Vijfjarenplan, dat ingaat in 2026. Deze Chinese inspanningen vormen een bedreiging voor het innovatie- en verdienvermogen van westerse kennisinstituten en bedrijven. Dit komt enerzijds doordat Chinese onderzoekers met wie zij samenwerken onder druk gezet (kunnen) worden om opgedane technologische kennis te delen. Anderzijds kan China op heimelijke wijze kennis vergaren. Zowel deze voortdurende aandacht voor hoogwaardige kennis en technologie als het uitbuiten van economische afhankelijkheden, zorgen voor een verbreding van de dreiging die van China uitgaat.

Chinese cyberdreiging blijkt telkens groter dan gedacht

Voor het verwerven van kennis, die bedoeld is voor China's economische ontwikkeling, maakt China ook gebruik van cyberaanvallen. Economische doelen zijn echter niet de enige doelen waarop Chinese cyberactiviteiten zich richten. China heeft een voortdurende en omvangrijke behoefte aan informatie die van belang kan zijn voor diverse onderdelen van de Chinese staat, Chinese besluitvormers, bedrijven en krijgsmacht. Om aan deze informatie te komen worden vele Chinese digitale aanvalsgroepen (APT's) ingezet. De Chinese cyberdreiging blijkt telkens groter dan gedacht.

De Chinese president Xi Jinping (midden), de Russische president Putin (links) en de Noord Koreaanse leider Kim Jong-un (rechts) herdachten in september gezamenlijk het einde van de Tweede Wereldoorlog (toen tachtig jaar geleden). China, Rusland, Noord-Korea en Iran trekken steeds meer samen op om hun invloed in de wereld te vergroten. Foto: Korean News Service via AP.

Niet altijd is direct aan te tonen dat de Chinese staat achter cyberoperaties zit. Toch constateert de AIVD samen met de MIVD dat er een groot ecosysteem van Chinese cyberactoren, bedrijven en statelijke entiteiten bestaat dat een rol speelt in het initiëren, faciliteren en uitvoeren van cyberaanvallen. Enkele Chinese cyberactoren richten zich hierbij structureel op Europa, de NAVO en ook op Nederland. Daarnaast speelt opportunisme soms een rol bij cyberaanvallen, bijvoorbeeld wanneer massaal en wereldwijd een nieuw ontdekte kwetsbaarheid wordt uitgebuit. Daarbij kunnen ook slachtoffers in Nederland worden gemaakt.

Chinese aanvalsgroepen zijn wereldwijd actief en treffen met succes bedrijven, overheden en organisaties in vrijwel elk land. De telecomsector is daarbij een belangrijk doelwit. Naast dat dit China veel waardevolle informatie kan opleveren, kunnen de aanvallen op verschillende manieren bijdragen aan de opbouw van (sabotage)capaciteiten van China in het geval van een conflict. Het Chinese cyberprogramma is zo omvangrijk en geavanceerd dat waarschijnlijk slechts een klein deel van de cyberaanvallen op Nederland en bondgenoten tijdig wordt onderkend en afgeweerd. Dit laat zien dat de dreiging van China zich niet alleen verbreedt, maar ook verdiept.

Publieke waarschuwing SALT TYPHOON

De cyberdreiging die van China uitgaat en het relatief geringe vermogen om zicht op die dreiging te krijgen en deze af te weren, zijn zorgwekkend. De AIVD en de MIVD doen daarom niet alleen onderzoek naar de Chinese cyberdreiging, maar treden ook actief naar buiten met informatie over deze dreiging en hoe die kan worden tegengegaan. Zo brachten de AIVD en de MIVD in de zomer van 2025 – samen met inlichtingen-, veiligheids- en cybersecuritydiensten uit veel andere landen – een gezamenlijk cyberadvies uit over de Chinese cyberactor SALT TYPHOON. Deze groep had het voorzien op telecombedrijven in de Verenigde Staten, maar ook in Nederland. De groep heeft bijna twee jaar ongemerkt zijn gang kunnen gaan. In deze twee jaar kon de groep op grote schaal informatie buitmaken uit kritieke en vitale onderdelen van telecomnetwerken. Door met deze informatie publiekelijk naar buiten te treden, kunnen de AIVD en MIVD waarschuwen voor Chinese cyberaanvallen en weerbaarheidsmaatregelen delen met bedrijven en organisaties die anders niet worden bereikt.

De AIVD wil het bredere publiek ook bereiken met openbare cyber-adviezen, zoals met het cyberadvies *Risico op malwarebesmetting tijdens reizen naar China*. Dit advies volgde nadat de AIVD FlowCloud-malware had aangetroffen op mobiele apparatuur van personen die beroepsmatig naar China reisden. Deze malware diende zeer waarschijnlijk een spionage-motief: de slachtoffers zijn werkzaam binnen publieke en private organisaties op onderwerpen en dossiers die relevant zijn voor China. Ook geven de diensten presentaties over deze en andere thema's, bijvoorbeeld tijdens cybersecurityconferenties.

> **Lees meer op aivd.nl/cyberadvies**

Chinese spionage en inmenging

Chinese inlichtingen- en veiligheidsdiensten voeren actief inlichtingen-activiteiten uit in Nederland. Dit bleek ook in 2025 weer. Deze diensten benaderen individuen die voor China relevant zijn en bouwen hier inlichtingennetwerken op. Ook vergaren zij kennis en technologie die China in zijn voordeel kan gebruiken. Mensen kunnen hier bewust of onbewust aan meewerken. Zoals ook in het hoofdstuk over statelijke inmenging staat, kunnen inlichtingenactiviteiten in Nederland sinds 2025 strafrechtelijk vervolgd worden.

China werkt volgens een *whole of society-approach*. Dit houdt onder andere in dat alle onderdelen van de samenleving, van individuen tot bedrijven en organisaties, door de Chinese overheid ingezet kunnen worden voor bijvoorbeeld inlichtingenactiviteiten. Zij zijn wettelijk verplicht om hieraan mee werken. Omdat deze wetgeving een extraterritoriale werking heeft, kan hiermee ook de Chinese diaspora onder druk gezet worden.

Chinese diensten oefenen controle en druk uit op de Chinese diaspora die in veel landen aanwezig is. Deze diensten willen dissidente geluiden onderdrukken en hier woonachtige Chinese staatsburgers mobiliseren om dergelijke geluiden tegen te gaan. De Chinese Communistische Partij (CCP) beschouwt afwijkend gedachtegoed namelijk als een bedreiging voor haar voortbestaan.

Daarnaast probeert China op heimelijke wijze politieke invloed uit te oefenen in het buitenland. Dit werd in 2025 in verschillende westerse landen zichtbaar. Zo wees het Verenigd Koninkrijk een Chinese zakenman uit omdat hij ervan werd verdacht zich te hebben beziggehouden met politieke beïnvloeding tot in de hoogste maatschappelijke kringen. Ook voor het uitoefenen van politieke invloed buiten eigen grenzen gebruikt China onder meer de Chinese diaspora in Nederland, al dan niet onder dwang.

2.7

Politieke inlichtingen

> **De ontwikkelingen in Venezuela en de oplopende spanningen tussen de Verenigde Staten en Venezuela leidden in 2025 tot zorgen in en over het Caribische deel van het Koninkrijk.**

> **De Gaza-oorlog had op meerdere manieren effect op de nationale veiligheid.**

Gebeurtenissen en ontwikkelingen in het buitenland kunnen sterk van invloed zijn op de veiligheid van Europees Nederland of het Caribische deel van het Koninkrijk. De AIVD doet daarom – in een aantal onderzoeken in nauwe samenwerking met de MIVD – onderzoek naar de dreiging hiervan. De diensten zorgen zo voor politieke inlichtingen. Eigen politieke inlichtingen zijn belangrijk voor de Nederlandse regering. Op basis hiervan kan zij het Nederlandse standpunt bepalen voor bijvoorbeeld internationale onderhandelingen, of afgewogen keuzes maken voor het Nederlandse buitenlandbeleid. Twee van deze onderzoeksgebieden worden hieronder uitgelicht.

Venezuela

De ontwikkelingen in Venezuela in 2025, en de oplopende spanningen tussen de Verenigde Staten en Venezuela, leiden tot zorgen in en over het Caribische deel van het Koninkrijk. De AIVD en MIVD doen gezamenlijk onderzoek naar de politieke en militaire ontwikkelingen in Venezuela en de mogelijke uitstralingseffecten richting het Koninkrijk der Nederlanden, en houden de situatie daarom nauwgezet in de gaten.

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

Het Venezolaanse regime leek eind 2025 de Venezolaanse oppositie effectief buitenspel te hebben gezet.

Op 3 januari 2026 voeren de Verenigde Staten een militaire operatie uit in Venezuela, waarbij Maduro en zijn vrouw, Cilia Flores, werden gearresteerd en naar de VS zijn overgebracht. Voormalig vicepresident Delcy Rodriguez heeft op interim-basis de leiding in Venezuela overgenomen. Dit heeft de spanningen tussen de VS en Venezuela voorlopig doen afnemen. Ondanks dat blijft de situatie onvoorspelbaar. Dit heeft ook effect op het Caribische deel van het Koninkrijk.

Gevolgen voor het Caribische deel van het Koninkrijk

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

Midden-Oosten

Eind 2025 kwam het tot een staakt-het-vuren tussen Israël en Hamas. De AIVD schat in dat een stabiel Gazaans bestuur echter nog ver weg is. Ook in 2025 was een tweestatenoplossing niet in zicht.

De humanitaire en logistieke uitdagingen met betrekking tot de wederopbouw van de Gazastrook zijn groot. De Palestijnse soevereiniteit staat onder zware druk – niet alleen in de Gazastrook, maar ook op de Westelijke Jordaanoever. De AIVD houdt er rekening mee dat een eventuele annexatie van de Westelijke Jordaanoever meer instabiliteit kan geven in de regio.

De situatie in de Palestijnse Gebieden heeft effect op de Nederlandse nationale veiligheid. Ten eerste vormen gevechtshandelingen van de verschillende partijen een mogelijke fysieke dreiging tegen Nederlandse personen en objecten aldaar. Tevens heeft de oorlog consequenties voor de Nederlandse sociale stabiliteit. Ook heeft de oorlog mogelijk een katalyserend effect op sommige individuele jihadisten en op de links-extremistische beweging. Bovendien is de geweldsdreiging toegenomen tegen Joodse en Israëlische doelwitten in Nederland. Tot slot vraagt de situatie om extra inzet van veiligheidspartners, om het Internationaal Strafhof en het Internationaal Hof van Justitie, waarvoor Nederland gastland is, ongestoord te laten functioneren – ook op het Gazadossier.

De veranderende regionale machtsverhoudingen hadden in 2025 ook een grote impact op het bredere Midden-Oosten, waaronder op Syrië. In december 2024 werd het regime van Bashar al-Assad verdreven, aangevoerd door Hay'at Tahrir al-Sham. De leider van deze groep, Ahmed al-Sharaa, is sinds maart 2025 de nieuwe interim-president van het land. De politieke situatie in Syrië heeft zich in dit jaar ontwikkeld tot een gespannen status quo, waarin ontwikkelingen elkaar snel opvolgen. De huidige Syrische overgangsregering weet de macht vast te houden, maar moet daarbij wel het hoofd bieden aan een bescheiden opleving van ISIS. Van een stabiele eenheidsstaat is nog geen sprake. Ondanks de relatief toegenomen stabiliteit en veiligheid, lijkt het er vooralsnog niet op dat verschillende regionale en etnische groepen bereid zijn om hun agenda van autonomie los te laten: Koerdische groepen in het noordoosten, Druzen in het zuidwesten en Alawieten in het noordwesten. De wederopbouw van de economie en infrastructuur blijft een uitdaging, mede omdat diverse buitenlandse actoren hun invloed in het land laten gelden.

Instabiliteit in Syrië zet ook Nederlandse veiligheidsbelangen onder druk. Het biedt aan terroristische groeperingen de mogelijkheid om (verder) op te leven. Inmiddels zijn ook gevangengenomen ISIS-strijders in vrijheid gekomen.

2.8 Contraproliferatie

- **Samen met de Duitse inlichtingendienst BND hebben de AIVD en MIVD in 2025 naar buiten gebracht dat Rusland het gebruik van chemische wapens in Oekraïne heeft geïntensiveerd.**
- **In de Twaalfdaagse oorlog is aanzienlijke schade toegebracht aan het Iraanse nucleaire en raketprogramma.**
- **De AIVD en MIVD hebben een aantal ongewenste verwervingspogingen verstoord. Daarmee is voorkomen dat apparatuur terecht is gekomen bij programma's voor de ontwikkeling van massa-vernietigingswapens in enkele landen van zorg.**

De ontwikkeling, productie en verspreiding van massavernietigingswapens en overbrengingsmiddelen (meestal ballistische raketten) wordt wereldwijd beschouwd als een reëel gevaar voor de internationale veiligheid. De AIVD en de MIVD doen in gezamenlijkheid onderzoek naar landen die (mogelijk) massavernietigingswapens ontwikkelen. De diensten informeren de Nederlandse regering over relevante ontwikkelingen in deze zogeheten landen van zorg. De diensten hebben in 2025 onderzoek gedaan naar de activiteiten van onder meer Iran, Rusland en Noord-Korea. Ook spannen de AIVD en MIVD zich in om te voorkomen dat Nederlandse bedrijven (onbedoeld) bijdragen aan de proliferatie van massavernietigingswapens.

Iran

In juni 2025 voerden Israël en de Verenigde Staten aanvallen uit op de nucleaire en raketfaciliteiten van Iran, met als doel het Iraanse nucleaire programma te verzwakken. Die aanvallen zijn bekend geworden onder de naam 'de Twaalfdaagse oorlog'. Beide landen wilden Iran de capaciteiten ontnemen om een kernwapen te kunnen ontwikkelen.

Om een kernwapen te ontwikkelen, moet een land beschikken over voldoende hoogverrijkt uranium, evenals over de politieke wil en technische capaciteiten om hier daadwerkelijk een wapen van te maken. Ten tijde van de Twaalfdaagse oorlog kon Iran in zeer korte tijd beschikken over voldoende hoogverrijkt uranium om enkele kernwapens te maken. De AIVD en MIVD hadden geen aanwijzingen dat Iran ook die andere noodzakelijke stappen zette om een kernwapen te maken.

In de Twaalfdaagse oorlog werden belangrijke Iraanse kopstukken van zowel de nucleaire als raketprogramma's uitgeschakeld. Hoewel er verschillende claims circuleren over de precieze omvang van de schade, is het duidelijk dat deze aanzienlijk is. Iran reageerde met meerdere raketaanvallen op Israël, waarbij het honderden ballistische raketten lanceerde. Iran zal veel tijd en middelen moeten investeren voordat het nucleaire programma weer op het niveau van voor de aanvallen staat. Ook aan het ballistische raketprogramma is aanzienlijke schade toegebracht. Iran zet grote stappen om de toegebrachte schade te herstellen. Hiertoe probeert Iran materialen en apparatuur te verkrijgen uit andere landen. Zelf levert Iran ook materieel aan andere landen. In 2025 heeft Iran wederom korteafstandsraketten geleverd aan Rusland. De diensten vermoeden dat Rusland die raketten wil inzetten in Oekraïne.

De Verenigde Naties hebben Iran het recht op uraniumverrijking ontzegd, omdat Iran zich niet hield aan het nucleaire akkoord uit 2015. Iran blijft echter vasthouden aan zijn recht op een civiel nucleair programma en ziet uraniumverrijking als een onbetwistbaar onderdeel daarvan. Volgens een ander internationaal verdrag, het Non-proliferatieverdrag (NPV), is Iran verplicht om de uraniumvoorraden en verrijkingsinstallaties aan het Internationaal Atoomenergieagentschap (IAEA) te tonen. Dat is sinds de aanvallen in juni 2025 niet meer gebeurd. Binnen deze internationale verbanden wordt Iran gesteund door Rusland en China. De samenwerking tussen deze landen is de laatste jaren versterkt.

Rusland

De AIVD en MIVD hebben in juli 2025 samen met de Duitse inlichtingendienst BND naar buiten gebracht dat Rusland het gebruik van chemische wapens in Oekraïne heeft geïntensiveerd. Uit onderzoek van de diensten is gebleken dat Rusland in 2025 is doorgegaan met de inzet van chemische wapens in deze oorlog. De diensten beschouwen de inzet van chloorpicrine als bevestigd. Daarmee laat Rusland een escalatie zien in de bereidheid tot inzet van chemische wapens.

Chloorpicrine heeft een vergelijkbaar effect als traangas, maar dan sterker. Volgens het Verdrag Chemische Wapens, waar Rusland bij is aangesloten, mogen deze middelen nooit worden ingezet in een militair conflict. Daarnaast blijft Rusland investeren in chemische en biologische wapenprogramma's.

Noord-Korea

Noord-Korea heeft in 2025 verder ingezet op de uitbreiding van het nucleaire arsenaal. Nadat het land in 2024 foto's toonde van bekende uraniumverrijkingshallen, bouwde het in 2025 aan een nieuwe faciliteit die veel wegheeft van de bestaande hallen voor deze verrijking. Daarnaast ging Noord-Korea door met de ontwikkeling van nieuwe intercontinentale ballistische raketten, zoals de nieuwe Hwasong-20. Deze is door Noord-Korea gepresenteerd als het krachtigste nucleaire strategische wapensysteem ter wereld. Ook blijft het land werken aan de ontwikkeling van hypersonische glijvoertuigen: raketkoppen die bij terugkeer in de atmosfeer op zeer hoge snelheid manoeuvres kunnen uitvoeren.

Noord-Korea toonde zich in 2025 prominent aanwezig op het mondiale toneel. Zo liepen Noord-Koreaanse troepen mee in een militaire parade in Moskou. Kim Jong-un bezocht zelf Beijing om een parade bij te wonen. Op de achtergrond blijft Noord-Korea de samenwerking met Rusland intensiveren, om de eigen Noord-Koreaanse wapenindustrie te moderniseren. Ook blijft het korteafstandsraketten leveren die Rusland gebruikt om doelen aan te vallen in Oekraïne.

Ongewenste verwerving

Landen zoals Iran, Rusland en Noord-Korea zijn voor de (door)ontwikkeling en productie van hun massavernietigingswapens voor een deel afhankelijk van kennis en goederen uit het Westen. Daarom doen de AIVD en MIVD onderzoek naar verwerving van kennis en goederen uit bijvoorbeeld Nederland, die deze landen kunnen gebruiken voor hun programma's waarin ze massavernietigingswapens maken. Gezien de huidige geopolitieke situatie heeft het onderzoek naar Iraanse en Russische verwerving de prioriteit.

Ook in 2025 hebben Rusland en Iran hun activiteiten voortgezet om in Nederland en Europa strategische goederen te verwerven. Als gevolg van het opleggen en uitbreiden van internationale sancties tegen Rusland en Iran, zijn handelsnetwerken verschoven. Daardoor worden nu ook omleidingsroutes gebruikt, bijvoorbeeld via de Verenigde Arabische Emiraten, Turkije, Kazachstan en China. Daarnaast signaleren de AIVD en MIVD dat landen als Rusland, Iran, China en Noord-Korea steeds intensiever onderling samenwerken bij de verwerving van goederen en kennis die kunnen worden gebruikt bij de vervaardiging en verdere ontwikkeling van massavernietigingswapens.

Wanneer bedrijven gevoelige goederen, kennis of technologie leveren aan het buitenland, bestaat dus het risico dat zij direct of indirect bijdragen aan programma's die gericht zijn op de ontwikkeling van massavernietigingswapens en bijbehorende overbrengingsmiddelen. Voor de meeste bedrijven is dit risico vooral zichtbaar als zij een aanvraag krijgen uit een risicoland. Het risico is minder duidelijk als de gevraagde levering loopt via bijvoorbeeld een van bovengenoemde omleidingslanden.

De AIVD en de MIVD zien dat zowel grote als MKB-bedrijven worden benaderd door statelijke actoren die hun goederen, kennis en technologie willen gebruiken voor massavernietigingswapens en bijbehorende overbrengingsmiddelen. Ongewenste kennis- en technologieoverdracht heeft niet alleen gevolgen voor individuele ondernemingen, bijvoorbeeld in de vorm van negatieve publiciteit wanneer deze levering aan het licht komt. Het vormt bovenal een bedreiging voor de nationale en internationale veiligheid.

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

> Lees meer op aivd.nl/massavernietigingswapens

3. Verhogen van de Nederlandse weerbaarheid

Windmolens voor de kust van Nederland. Adviezen van de AIVD dragen bij aan de veiligheid van onder meer nieuwe windmolenparken en de maritieme sector. Foto: ANP

3.1

Hoe de AIVD bijdraagt aan een weerbaar Nederland

> **Een weerbare samenleving kan beter omgaan met dreigingen. Dit vereist dat de samenleving geïnformeerd wordt over die dreigingen.**

> **De AIVD draagt op verschillende manieren bij aan deze weerbaarheid. Dat gebeurt op basis van inlichtingen en de weerbaarheidsexpertise van de dienst. De dienst droeg bij aan een veilig en ononderbroken verloop van de NAVO-top in Den Haag.**

Op basis van de inlichtingen en weerbaarheidsexpertise van de dienst, is de AIVD een aanjager van een weerbaar Nederland. Een weerbare samenleving kan beter omgaan met de dreigingen uit voorgaande hoofdstukken.

Weerbaarheid ontstaat in effectieve samenwerking tussen onder meer overheidsinstellingen, bedrijven, kennisinstellingen en burgers. Alleen samen kunnen we voor een verhoging van de Nederlandse weerbaarheid zorgen. Dit hoofdstuk beschrijft hoe de AIVD hieraan een bijdrage levert.

In 2025 heeft de AIVD opnieuw gerichte adviezen uitgebracht met inzicht in de dreigingen en met uitleg over welke maatregelen hiertegen genomen kunnen worden. Deze adviezen en inschattingen zijn zowel technisch-inhoudelijk als beleidsmatig. Een deel hiervan gaat specifiek over digitale weerbaarheid. In 2025 hadden deze adviezen betrekking op onder andere de NAVO-top in Den Haag, de risico's van reizen naar het buitenland, soevereiniteit, windenergie op zee, omgaan met kwetsbaarheden in software, en berichten-apps.

Ook begeleidt de AIVD de ontwikkeling van informatiebeveiligingsproducten. Voordat deze producten gebruikt kunnen worden met vertrouwelijke informatie moet de AIVD deze goedkeuren. Daarnaast draagt de dienst bij aan de doorontwikkeling van publiek-private samenwerkingsverbanden. Deze samenwerking is cruciaal voor het verhogen van de weerbaarheid.

Een weerbare overheid

De AIVD heeft in 2025 veel aandacht gehad voor het verhogen van de weerbaarheid van de overheid zelf – bij met name de Rijksoverheid, de Nationale Politie, het Openbaar Ministerie, en de Eerste en Tweede Kamer. Met gerichte adviezen heeft de AIVD daar bijgedragen aan het vergroten van het dreigingsbewustzijn en het bevorderen van veiligheidsmaatregelen. Zo heeft de AIVD in 2025 voor het tweede opeenvolgende jaar de 'dreigingsanalyse Rijksoverheid' uitgebracht. Met deze analyse wees de dienst onder meer BVA's en CISO's van de ministeries op de meest relevante fysieke en digitale dreigingen, en op de werkwijzen van aanvallers. Deze analyse wordt jaarlijks geactualiseerd.

> Lees meer op aivd.nl/weerbaarheid

Bescherming van personen, objecten, diensten en evenementen tegen (terroristische) aanslagen

De AIVD draagt er ook aan bij dat de NCTV en het OM beveiligingsmaatregelen kunnen nemen of aanpassen voor personen, objecten, diensten en evenementen. Daarvoor informeert de dienst deze partners door zogeheten dreigingsproducten. In 2025 heeft de AIVD ruim de helft meer van deze producten uitgebracht dan in 2024.

Meer dreigingsproducten voor bewaken en beveiligen
Het taakveld bewaken en beveiligen heeft tot doel personen, objecten, diensten en evenementen te beschermen tegen (terroristische) aanslagen. Denk bijvoorbeeld aan politici, ambassades, leden van het Koninklijk Huis en internationale organisaties. De AIVD brengt ten behoeve van dit taakveld dreigingsproducten uit: dreigingsinschattingen, dreigingsanalyses, risicoanalyses en mededelingen. Op basis hiervan kunnen de NCTV en het OM beveiligingsmaatregelen nemen of aanpassen.

In 2025 heeft de AIVD 108 dreigingsproducten uitgebracht, ruim de helft meer dan in 2024. Deze toename is onder meer het gevolg van een toegenomen vraag vanuit de NCTV en het OM, van nieuwe casussen die zich in 2025 aandienden. Ook is geïnvesteerd in extra capaciteit voor het taakveld. Daarnaast waren er ontwikkelingen in de dreiging die tot meer dreigingsproducten leidden.

Zo is de dreiging van statelijke actoren tegen personen in Nederland de afgelopen jaren toegenomen. Dit betreft onder meer mensen die actief zijn (geweest) voor oppositie- of afscheidingsbewegingen en mensen die zich publiekelijk kritisch uitlaten over het regime in het land van herkomst (zoals activisten, journalisten en dissidenten). Ook de dreiging tegen politie, justitie en overige partijen die betrokken zijn bij de strafrechtspleging is de afgelopen jaren toegenomen.

Verder heeft de AIVD in 2025 dreigingsanalyses uitgebracht over de NAVO-top die in juni 2025 in Den Haag is gehouden, en over de dreiging tegen nationale politici en de verkiezingen voor de Tweede Kamer in oktober 2025.

De AIVD is de afgelopen jaren nauw betrokken geweest bij de vernieuwing van dit taakveld en bij de vorming van een nieuw stelsel beveiligen van personen. Deze vernieuwing zal grotendeels in 2026 worden geïmplementeerd. Dit draagt onder andere bij aan een ongestoord functioneren van een groot aantal functionarissen die een cruciale rol vervullen in onze democratische rechtsorde.

> Lees meer op aivd.nl/bewakenenbeveiligen

Weerbaarheid bij vitale sectoren

De AIVD onderhoudt nauwe relaties met bedrijven uit de vitale sectoren, en geeft daarbij prioriteit aan de sectoren energie, maritiem, digitale infrastructuur en burgerluchtvaart. Ook had de AIVD in 2025 contact met bedrijven uit andere sectoren, die een belangrijke rol spelen in de nationale veiligheid.

Ter illustratie: de energiesector en het maritieme domein

De energiesector is essentieel voor het goed functioneren van de Nederlandse samenleving. De Nederlandse zeehavens spelen een belangrijke rol in zowel de werkgelegenheid, energievoorziening, levensmiddelenhandel en de veiligheid van Nederland. Uitval of verstoring van de energiesector of (delen van) havens kunnen de logistieke ketens in de samenleving ernstig ontregelen. In tijden van internationale spanningen zijn deze sectoren doelwit van bijvoorbeeld (economische) spionage of verstoring van processen in de havens. Ook in het uiterste geval van een grootschalig conflict kunnen deze sectoren aantrekkelijke doelwitten zijn.

Weerbaarheid via kennis- en economische veiligheid

De AIVD draagt samen met de MIVD tevens bij aan de weerbaarheid tegen ongewenste kennis- en technologieoverdracht. Nederland is een klein, maar hoogontwikkeld land met een uitgebreide kenniseconomie, bijvoorbeeld op het gebied van halfgeleiders en quantumtechnologie. Verschillende statelijke actoren zijn geïnteresseerd in deze kennis en expertise, en ontplooien concrete inlichtingenactiviteiten om deze te verkrijgen.

In 2025 constateerde de AIVD dat de bewustwording van hightechbedrijven en vooraanstaande kennisinstellingen over de dreiging vaak op adequaat of goed niveau was. Daarmee is een stijgende lijn te zien ten opzichte van eerdere jaren. Awareness is de cruciale eerste stap.

De bedrijven en instellingen die zich bewust zijn van de dreiging willen het liefst risico-gestuurd maatregelen nemen. De AIVD ziet echter dat zij hierbij moeite hebben om te signaleren wat dan precies de risico's zijn voor de organisatie.

Om risico's te kunnen identificeren moet het antwoord op de volgende vragen helder zijn: 'wat is het belang?' en 'wat is de dreiging?'. Informatie over dreiging wordt door de AIVD, MIVD en andere veiligheidspartners gedeeld in staatsgeheime stukken en publicaties zoals dit jaarverslag. Maar het belang moet een bedrijf of organisatie zelf duiden: welke specifieke aspecten zijn zo belangrijk dat men beschermende maatregelen zou moeten treffen? De complexiteit van deze vraag zorgt soms voor brede en ongerichte maatregelen waarvan de haalbaarheid en kosten niet realistisch zijn. Het is de kunst om scherpe keuzes te maken over wat de te beschermen belangen zijn en waar vervolgens meer of minder risico's geaccepteerd kunnen worden.

Weerbaarheid via industrieveiligheid

Samen met de MIVD zet de AIVD zich eveneens in voor industrieveiligheid. Industrieveiligheid gaat over het toezicht op de veiligheidseisen waar bedrijven zich aan moeten houden als zij opdrachten uitvoeren voor de Rijksoverheid, Defensie en de Politie, die van invloed kunnen zijn op de nationale veiligheid. Eerder vond dit toezicht plaats vanuit twee separate afdelingen bij de AIVD en de MIVD. Deze afdelingen zijn in 2025 opgegaan in een nieuwe, gezamenlijke unit: het Nationaal Bureau Industrieveiligheid (NBIV), dat dit jaar verder is opgebouwd en versterkt.

Weerbaarheid via verdragsrechtelijke taken

Daarnaast vervult de AIVD in internationaal verband een aantal taken die verdragsrechtelijk zijn vastgelegd. Zo houdt de dienst als *National Security Authority* toezicht op de manier waarop de Nederlandse overheid omgaat met de bescherming van vertrouwelijke informatie van de EU, de NAVO en het Europese ruimtevaartprogramma ESA.

Ook is de AIVD verantwoordelijk voor het onderhandelen over *General Security Agreements* (GSA's) tussen Nederland en andere landen, om gerubriceerde informatie veilig onderling te kunnen delen. Deze onderhandelingen komen tot stand in samenwerking met de ministeries van Buitenlandse Zaken, Defensie en Economische Zaken. In 2025 zijn de GSA's met Letland, Noorwegen, Oekraïne, Portugal, Slowakije en Zweden geratificeerd en in werking getreden. Daarnaast nam de AIVD deel aan raadswerkgroepen binnen de EU en de NAVO om een bijdrage te leveren aan de totstandkoming van de regulering van informatiebeveiliging voor EU-entiteiten. De uitvoering van deze verdragsrechtelijke taken wordt alleen maar belangrijker in het licht van de dreigingen en ontwikkelingen uit dit jaarverslag.

Weerbaarheid via elektronische veiligheidsonderzoeken

De AIVD heeft in goede samenwerking en coördinatie met de MIVD en de politie 124 ruimtes 'gesweept' in 2025. *Sweepen* draagt eraan bij dat staatsgeheime informatie die wordt besproken in ruimtes veilig blijft: met unieke kennis en middelen wordt de betreffende ruimte onderzocht, op zoek naar afluisterapparatuur, verborgen camera's en andere sensoren. Dit deed de AIVD op verzoek van onder andere het ministerie van Algemene Zaken en tijdens de NAVO-top in Den Haag.

Tijdens de NAVO-top heeft de AIVD samen met de politie een succesvolle zoekactie gedaan naar een malafide netwerk. Deze actie werd opgestart toen daar een wifinetwerk zichtbaar was met dezelfde naam als het legitieme NAVO-*guest*-netwerk.

De AIVD draagt op verschillende manieren bij aan de weerbaarheid van de samenleving. Ook de veiligheidsonderzoeken uit het volgende hoofdstuk zijn hier een concreet voorbeeld van. Tegelijkertijd vormt het werk van de AIVD een schakel in de collectieve inspanning die nodig is voor de weerbaarheid: het veelvoud aan dreigingen vraagt om kennis en samenwerking binnen de gehele samenleving.

3.2 Veiligheidsonderzoeken

> **De dreigingen uit voorgaande hoofdstukken zijn van invloed op veiligheidsonderzoeken die de dienst uitvoert. De Unit Veiligheidsonderzoeken (UVO) zag hierdoor in 2025 een verschuiving in het type veiligheidsonderzoek dat werd aangevraagd: de UVO deed zeventien procent meer A- en B-onderzoeken dan in 2024.**

> **Veiligheidsonderzoeken dragen bij aan de Nederlandse weerbaarheid.**

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

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

In totaal heeft de UVO 85.637 besluiten genomen in 2025. Dit is een lichte stijging ten opzichte van 2024. Van dit totaal zijn voor de burgerluchtvaart 32.862 besluiten genomen door de mandaathouder, de Koninklijke Marechaussee. Ondanks de niet afnemende vraag naar veiligheids-onderzoeken, heeft de UVO 92,6% van de veiligheidsonderzoeken binnen acht weken afgerond.

Meer A- en B-onderzoeken

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

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

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

Voldoen aan de groeiende vraag

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

Met de publicatie in het Staatsblad op 30 oktober 2025 is de laatste stap gezet voor de inwerkingtreding van de herziene Wet Veiligheidsonderzoeken (Wvo). De herziene wet treedt in 2026 in werking.

> **Lees meer op aivd.nl/veiligheidsonderzoek**

Tabel 1

Kengetallen veiligheidsonderzoeken (inclusief mandaathouder)

Onderzoeken	Positieve besluiten	Negatieve besluiten	Totaal aantal besluiten
A-niveau door UVO	7.136	46	7.182
B-niveau door UVO	27.485	269	27.754
C-niveau door UVO	6.627	55	6.682
BL-niveau door UVO overgenomen van KMar	7.279	1.570	8.849
NAVO-top 2025, Den Haag	516	10	526
E-BL-niveau[2]	1.774	8	1.782
Totaal door UVO	50.817	1.958	52.775
BL-niveau door de KMar	32.862	0[3]	32.862
Totaal aantal onderzoeken	**83.679**	**1.958**	**85.637**

Tabel 2

Veiligheidsonderzoeken: afhandeling van bezwaar- en (hoger) beroepsprocedures

Status	Bezwaar	Beroep	Hoger beroep	Voorlopige voorziening
Ingediend (in 2025)	206	11	64	2
Afgedaan (in 2025)	167	11	3	2
Ongegrond	121	9	0	0
Gegrond	16	2	0	1
Niet-ontvankelijk	7	1	0	0
Ingetrokken	24	0	0	0
Afgewezen	0	0	0	0

Toelichting bij afhandeling van bezwaar- en (hoger)beroepsprocedures

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

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

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

4. Organisatie en kerncijfers

Het gebouw van de AIVD in Zoetermeer. De dienst groeide afgelopen jaar verder, omdat het aantal onderzoeken toeneemt. Foto: AIVD

4.1

Het wettelijk kader van de AIVD

> **In 2025 kon de AIVD steeds meer gebruikmaken van de bevoegdheden uit de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkgegevens en overige specifieke voorzieningen.**

> **De AIVD is verder gegaan met de voorbereidingen voor de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv). Het betreft een brede herziening van de Wiv 2017 en is noodzakelijk om de taken van de dienst effectief en wendbaar te blijven uitvoeren in de toekomst.**

> **In september 2025 heeft de Eerste Kamer het wetsvoorstel verbetering uitvoering Wet veiligheidsonderzoeken aangenomen.**

> **Lees meer op aivd.nl/wiv**

Om onze taken in het kader van de nationale veiligheid effectief uit te voeren, moet de AIVD soms inbreuk maken op grondrechten van burgers. Wat de AIVD mag en welke kaders daarvoor gelden, is geregeld in de Nederlandse wet. Hieraan moet de AIVD zich altijd houden.

Op dit moment zijn er drie wetten die samen het wettelijk kader vormen: de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017), de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyber-programma, bulkdatasets en overige specifieke voorzieningen (Tijdelijke wet) en de Wet veiligheidsonderzoeken (Wvo). De Tijdelijke wet is op 1 juli 2024 in werking getreden. In 2025 hebben de diensten steeds meer bevoegdheden uit de Tijdelijke wet kunnen toepassen.

Voor de uitoefening van onze taken, is het belangrijk dat de diensten ook in de toekomst effectief en wendbaar kunnen optreden als de dreiging daarom vraagt, met voldoende passende waarborgen. Daarom loopt nu een wetstraject voor een nieuwe Wiv, waarmee de Wiv 2017 wordt herzien. Dit hoofdstuk gaat daarom niet alleen in op de Tijdelijke wet, maar ook op de nieuwe Wiv. Daarnaast staat het stil bij de aanpassing van de Wet veiligheidsonderzoeken.

Toepassing Tijdelijke wet

Landen met een offensief cyberprogramma voeren steeds vaker digitale aanvallen uit op Nederland en zijn bondgenoten. Om met grotere snelheid en meer wendbaarheid inlichtingenonderzoek te doen naar de verschillende dreigingen vanuit deze landen, was het noodzakelijk om het wettelijk kader voor de diensten versneld aan te passen. Deze veranderingen zijn vastgelegd in de Tijdelijke wet en gelden naast, of als aanvulling op, de Wiv 2017.

De CTIVD heeft laten weten sinds 1 oktober 2025 klaar te zijn voor een zo goed als volledige toepassing van de Tijdelijke wet. Sindsdien kunnen de AIVD en de MIVD deze wet stapsgewijs in gebruik nemen. Vanwege de beperkte mate waarin de Tijdelijke wet tot die tijd invulling heeft gekregen, is op dit moment nog geen compleet beeld van de uitvoeringsconsequenties.

Resultaten invoeringstoets Tijdelijke wet
In 2025 vond een invoeringstoets plaats van de Tijdelijke wet. Voor de onderdelen waarvan de diensten gebruik konden maken, geldt dat deze een positieve bijdrage hebben geleverd aan de snelheid en wendbaarheid van de diensten – en daarmee aan de bescherming van de nationale veiligheid. De diensten beoordelen de inzetmogelijkheden van kabelinterceptie en de regeling rondom bulkdatasets als positief.

De in de Tijdelijke wet opgenomen mogelijkheid van beroep bij de Afdeling Bestuursrechtspraak van de Raad van State beoordelen de diensten eveneens als positief. Een geschil kan zo snel worden voorgelegd aan de hoogste bestuursrechter. Door de diensten is in 2025 een keer gebruikgemaakt van de beroepsmogelijkheid die de Tijdelijke wet biedt. Op 9 mei 2025 heeft de Afdeling Bestuurs-rechtspraak van de Raad van State uitspraak gedaan in een beroepszaak. De Afdeling Bestuursrechtspraak heeft het beroep gegrond verklaard en het oordeel van de TIB vernietigd.

Uit de invoeringstoets is verder gebleken dat er geen consequenties zijn onderkend voor de bedrijfsvoering van de AIVD en MIVD. Wel is geconcludeerd dat de uitoefening van kabelinterceptie onder de combinatie van de Tijdelijke wet en de Wiv 2017 onuitvoerbaar is. Vanwege operationele noodzaak is daarom het voorstel gedaan om de uitvoeringspraktijk op dat punt te gaan passen naar één regime, zoals dat is geregeld voor onderzoeken die vallen onder de Tijdelijke wet.

Ook na deze invoeringstoets blijven de diensten de Tijdelijke wet evalueren en monitoren. Als de resultaten van de monitoring daar aanleiding toe geven, wordt daar in de verschillende stadia van het wetstraject voor de nieuwe Wiv rekening mee gehouden.

Nieuwe Wiv

Momenteel wordt gewerkt aan een nieuwe Wiv. In 2025 heeft de AIVD met veel partners en andere experts bijgedragen aan de voorbereiding van het conceptwetsvoorstel. Zij hebben hierbij de ervaringen met de Tijdelijke wet meegenomen. Momenteel wordt het conceptwetsvoorstel door de diensten getoetst op de uitvoerbaarheid van de voorgenomen wijzigingen. Het streven is dat de wet in de eerste helft van 2026 in consultatie gaat.

> Lees meer op aivd.nl/nieuwewiv

Bij de nieuwe Wiv ligt een sterke focus op een techniekneutrale en meer dreigingsgerichte wet, en daarmee een goede uitvoerbaarheid, toekomstbestendigheid en een eenduidiger regime voor gegevensverwerking. Ook voor de nieuwe Wiv geldt: met voldoende passende waarborgen. Zo blijft solide toetsing en toezicht cruciaal. Daarnaast is een goede samenwerking met partners, medeoverheden, bedrijven en kennisinstellingen een prioriteit.

Wet verbetering uitvoering Wet veiligheidsonderzoeken

De Eerste Kamer heeft eind september 2025 het voorstel aangenomen voor verbetering van de uitvoering van de Wet veiligheidsonderzoeken (Wvo). Deze aanpassing zorgt voor minder administratieve lasten rondom veiligheidsonderzoeken. Deze wet treedt in 2026 stapsgewijs in werking.

De belangrijkste verandering ten opzichte van de huidige Wvo is de invoering van een locatiegebonden verklaring van geen bezwaar (vgb). Deze vgb blijft geldig als iemand overstapt naar een nieuwe functie op dezelfde locatie met hetzelfde veiligheidsniveau – bijvoorbeeld bij een persoon die werkt in de luchtvaartsector en van werkgever wisselt. Ook komt er een register met personen die een vertrouwensfunctie vervullen.

4.2

Toetsing en toezicht op het werk van de AIVD

- **In de democratische rechtsorde past stevige toetsing en toezicht op de AIVD. De AIVD, de TIB en de CTIVD hebben in 2025 constructief contact gehad over het AIVD-onderzoek naar de dreiging tegen de nationale veiligheid vanuit criminele netwerken.**
- **Vooruitlopend op de nieuwe Wiv zijn beleidsregels in de maak voor publiek-private samenwerking. Dit type samenwerking wordt alleen maar belangrijker – zeker in het cyberdomein.**
- **De interne toezichtfuncties worden verankerd in de herziening van de Wiv 2017.**

Ons werk wordt stevig gecontroleerd. Het waarborgenstelsel van de Wiv 2017 en de aanpassingen uit de Tijdelijke wet zorgen voor een effectief toezichtstelsel op de werkpraktijk van de AIVD en de MIVD.

Intern gebeuren deze controles door de compliance- en auditfunctionarissen van de AIVD. Extern door het parlement. Zo nodig kan dit ook vertrouwelijk. Daarnaast is er de Toetsingscommissie inzet bevoegdheden (TIB) en de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). De TIB is een onafhankelijke commissie die vooraf toetst of de inzet van de meest ingrijpende bijzondere bevoegdheden door de AIVD rechtmatig is. Het oordeel van de TIB is bindend. De CTIVD doet onderzoek tijdens en na onderzoeken en beoordeelt of de AIVD zich aan de wet houdt. Ook kunnen burgers en organisaties die menen in hun belangen te zijn geschaad, een klacht indienen bij de afdeling Klachtbehandeling van de CTIVD.

Criminele ondermijning van de nationale veiligheid

In maart 2025 zorgde een kritische brief van de CTIVD en de TIB aan de Tweede Kamer over het AIVD-onderzoek naar de dreiging tegen de nationale veiligheid vanuit criminele netwerken voor aandacht in de media en de politiek. Na deze brief heeft de AIVD een technische briefing verzorgd aan de Tweede Kamer over dit onderzoek. Naar aanleiding van de parlementaire behandeling zijn er meerdere constructieve gesprekken geweest met de TIB en de CTIVD over het onderzoek naar de dreiging tegen de nationale veiligheid vanuit criminele netwerken. Met de CTIVD zijn goede afspraken gemaakt.

Publiek-private samenwerking en openbare beleidsregels

De samenwerking met private partijen is van groot belang voor de AIVD en de MIVD, met name in het cyberdomein. Deze publiek-private samenwerking wordt in de toekomst alleen maar belangrijker. Door bijvoorbeeld analyses van malwarebestanden en domeinnamen uit te wisselen, waarvan bekend is dat deze van een statelijke actor afkomstig zijn, kunnen de diensten een beter beeld krijgen van digitale dreigingen en bedrijven zich beter weren hiertegen.

In februari 2025 heeft de CTIVD een brief gestuurd aan de Tweede Kamer over dit type samenwerking van de diensten. De CTIVD heeft zorgen over het ontbreken van een wettelijke grondslag en heeft opgeroepen om een juridisch kader op te stellen, om zo de voorzienbaarheid te vergroten. Op basis hiervan komen er openbare beleidsregels voor publiek-private samenwerking. Deze beleidsregels worden begin 2026 gepubliceerd. Ook worden in de lopende herziening van de WIV 2017 de juridische kaders nader uitgewerkt voor dit type samenwerking.

Intern toezicht

Naast extern toezicht heeft de AIVD ook een intern toezichtstelsel. De afdeling Compliance is een van de afdelingen die deel uitmaakt van dit (onafhankelijk) intern toezichtstelsel. De hoofdtaak van deze afdeling is om op een permanente en systematische wijze ervoor te zorgen dat de werkzaamheden van de AIVD binnen de kaders van de relevante wet- en regelgeving, interne (beleids)regels en ethische normen blijven. Dit doet de afdeling onder andere door periodieke controles uit te voeren, te adviseren op compliance-vraagstukken en door actief te monitoren hoe de organisatie de CTIVD-aanbevelingen opvolgt.

De afdeling Compliance heeft in 2025 een digitaal dashboard ontwikkeld, waarmee de organisatie nog beter zicht heeft op deze opvolging en daarop kan sturen. Daarnaast heeft de afdeling zich de afgelopen jaren ingezet voor het verbeteren van het intern toezichtstelsel. De interne toezichtfuncties worden verankerd in de nieuwe Wiv.

4.3

Mensen en organisatie

> **Met meer dan 2800 medewerkers zet de AIVD zich in voor de bescherming van de nationale veiligheid en de democratische rechtsorde.**

> **Op het vlak van bedrijfsvoering was in 2025 extra aandacht voor onder andere bedrijfscontinuïteit en aantrekkelijk werkgeverschap.**

Bij de AIVD zetten meer dan 2800 medewerkers zich elke dag in voor de bescherming van de nationale veiligheid en de democratische rechtsorde. Altijd met het algemeen belang voor ogen. Onze mensen begrijpen dat veiligheid niet vanzelfsprekend is en werken vanuit verschillende functies hard om Nederland zo veilig mogelijk te houden.

Vanwege de dreigingen zoals in dit jaarverslag staan beschreven, werken we aan het vergroten van de weerbaarheid en robuustheid van onze bedrijfsvoering. We versterken de bedrijfscontinuïteit door uitwijklocaties te realiseren. Met een stevige en toekomstbestendige basis zijn we als organisatie beter voorbereid op veranderingen en risico's. Daarnaast hebben we aandacht voor duurzaamheid in de bedrijfsvoering. Dit sluit aan bij onze bredere ambitie om niet alleen onze rol in de veiligheidsketen te vervullen, maar dit ook op een verantwoorde, toekomstbestendige en rechtvaardige manier te doen.

Het jaar stond opnieuw in het teken van groei van de organisatie. Om die groei mogelijk te maken, hebben we geïnvesteerd in de uitbreiding van het aantal werkplekken.

Wij hebben aandacht en zorg voor onze medewerkers. In 2025 hebben we een inwerkprogramma opgezet voor nieuwe medewerkers, met vernieuwde digitale leerprogramma's. Zo maken we nieuwe medewerkers snel bekend en vertrouwd met het werk van de AIVD.

Ook zorgden we voor mogelijkheden voor actuele kennisontwikkeling voor alle medewerkers en waren er sociale activiteiten, bijvoorbeeld in het kader van het tachtigjarig jubileum van de AIVD.

Afgelopen jaar stonden wij nog nadrukkelijker stil bij diversiteit en inclusie. Er is een coördinator diversiteit, gelijkwaardigheid en inclusie aangesteld. Leidinggevenden en HR-medewerkers zijn getraind in 'inclusief werven'. Voor het werken met mensen met een afstand tot de arbeidsmarkt wordt de training Werkplekbegeleiding aan leidinggevenden aangeboden. Verschillende perspectieven en achtergronden versterken onze organisatie en helpen ons om wendbaar en toekomstgericht te blijven werken aan een veilig Nederland.

Simone Smit is sinds 1 maart 2026 directeur-generaal van de AIVD.
Foto: AIVD

Kerncijfers

87
uitgebrachte notificatiebrieven

93
uitgebrachte ambtsberichten, waarvan 30 samen met de MIVD

96
uitgebrachte schriftelijke dreigingsproducten

363
uitgebrachte inlichtingenrapporten

101010
010101
101010

1.434
taps ingezet op basis van art. 47 lid 1 Wiv 2017

Tabel 3

Verzoeken tot kennisneming van informatie aanwezig bij de AIVD (inzageverzoeken) per soort

Verzoek	Ingediend	Afgehandeld	Inzagedossier verstuurd	Nog in behandeling
Gegevens over eigen persoon	234	292	140	68
Gegevens over overleden familielid	48	58	23	4
Gegevens over bestuurlijke aangelegenheden	82	80	49	43
Gegevens over derden	-	6	-	1
Totaal	**364**	**436**	**212**	**116**

Tabel 4

De afhandeling van bezwaar- en (hoger)beroepsprocedures met betrekking tot inzageverzoeken

Status	Bezwaar	Beroep	Hoger beroep
Afgehandeld	**34**	**3**	**0**
Ongegrond	29	2	0
(Gedeeltelijk) gegrond	4	1	-
Niet-ontvankelijk	1	-	-
Ingetrokken	-	-	-

Tabel 5

Klachten over de AIVD bij de minister van Binnenlandse Zaken en Koninkrijksrelaties

Nog in behandeling op 1 januari 2025	19
Ingediend in 2025	15
Geheel ongegrond verklaard	2
Deels gegrond verklaard	3
Geheel gegrond verklaard	6
Informeel afgedaan	11
Niet in behandeling genomen	0
Ingetrokken	0
Doorverwezen	6
Nog in behandeling op 31 december 2025	6

Tabel 6
Klachten over de AIVD bij de CTIVD

Nog in behandeling op 1 januari 2025	7
Ingediend in 2025	28
Geheel ongegrond verklaard	0
Deels gegrond verklaard	3
Geheel gegrond verklaard	0
Informeel afgedaan	5
Niet in behandeling genomen	22
Ingetrokken	0
Doorverwezen	0
Nog in behandeling op 31 december 2025	5

Colofon

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Algemene Inlichtingen- en Veiligheidsdienst
aivd.nl

Postbus 20010
2500 EA Den Haag

April 2026