De Wet op de inlichtingen- en veiligheidsdiensten 2017

De Wet op de inlichtingen- en veiligheidsdiensten 2017 regelt de taken, bevoegdheden en het toezicht op de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst. Deze wet trad in 2018 in werking en onderging in 2022 een herziening om aan te sluiten bij technologische ontwikkelingen en privacyvraagstukken. De politieke verantwoordelijkheid voor de diensten ligt bij de minister van Binnenlandse Zaken en Koninkrijksrelaties voor de Algemene Inlichtingen- en Veiligheidsdienst en bij de minister van Defensie voor de Militaire Inlichtingen- en Veiligheidsdienst. Beide bewindspersonen rapporteren aan de Tweede Kamer over het beleid, de prioriteiten en de incidenten binnen de diensten.

Het stelsel van toezicht en klachtbehandeling is een kernonderdeel van de wetgeving. Burgers kunnen een klacht indienen bij de Afdeling klachtbehandeling van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten over het optreden van de diensten, waaronder de rechtmatigheid van ongerichte bulkinterceptie van internet- en telefoonverkeer.

Volgens de rechtspraak van het Europees Hof voor de Rechten van de Mens moet de behandeling van klachten over dergelijke ingrijpende bevoegdheden kunnen leiden tot een juridisch bindend oordeel, waardoor een minister verplicht kan worden om de interceptie te staken en verzamelde gegevens te vernietigen. Bij klachten over onbehoorlijk handelen in het directe contact met een individu, zoals de overschrijding van termijnen, is het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden doorgaans niet van toepassing, omdat er geen sprake is van een beperking van de door dit verdrag beschermde grondrechten.

Met het oog op een definitieve herziening van de wet hebben de ministers de Afdeling advisering van de Raad van State om voorlichting gevraagd over de inrichting van de klachtbehandeling en de mogelijke samenvoeging van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten en de Toetsingscommissie Inzet Bevoegdheden.

Uit de op 7 juli 2025 gepubliceerde voorlichting blijkt dat de rechtspraak van het Europees Hof voor de Rechten van de Mens de combinatie van verschillende toezichtstaken binnen één instantie als kwetsbaar beschouwt vanwege mogelijke twijfels over de onafhankelijkheid.
Een beroepsmogelijkheid bij een onafhankelijke rechter biedt een solide waarborg om deze kwetsbaarheid te compenseren, terwijl organisatorische scheidingen zoals interne muren volgens de rechtspraak onvoldoende aanknopingspunten bieden. De Raad van State concludeerde tevens dat de Grondwet geen ruimte biedt om de Nationale ombudsman een juridisch bindende oordeelsbevoegdheid te geven, aangezien het ambt historisch is ingericht op een bemiddelende en laagdrempelige aanpak. Wel staat de Grondwet een niet-bindende, adviserende rol toe voor de Nationale ombudsman bij klachten over onbehoorlijk handelen, wat aansluit bij de positie van de ombudsman als externe klachtbehandelaar voor de gehele overheid.

Sinds 1 juli 2024 is de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen van kracht.
Deze tijdelijke wetgeving is gericht op het vergroten van de operationele snelheid en effectiviteit tegen statelijke actoren zoals China, Rusland en Iran.

De wet heeft geleid tot een accentverschuiving waarbij het bindende toezicht door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten op bepaalde vlakken is geïntensiveerd.

Vanwege de benodigde capaciteit voor dit intensievere toezicht is gekozen voor een gefaseerde uitvoering, waarbij de inzet voor 2026 inhoudt dat de Algemene Inlichtingen- en Veiligheidsdienst instemmingsverzoeken met verplicht bindend toezicht breder onder deze tijdelijke wet indient.

Het parlementaire traject voor de definitieve herziening van de Wet op de inlichtingen- en veiligheidsdiensten 2017 start naar verwachting eind 2026 of begin 2027 in de Tweede Kamer, waarbij het streven is om het wetsvoorstel in 2026 in consultatie te laten gaan.

Bij de vormgeving van deze herziening ligt de nadruk op het waarborgen van de operationele slagkracht, het verminderen van de administratieve lasten en de uitvoerbaarheid van de wet. De herziene wet moet uiterlijk op 1 juli 2028 in werking treden, omdat de huidige Tijdelijke wet op die datum van rechtswege vervalt.

Bij de Amerikaanse overheid wordt Europa omschreven als broedplaats voor terrorisme, aangewakkerd door massamigratie. “Het is voor iedereen duidelijk dat goed georganiseerde vijandige groeperingen misbruik maken van open grenzen en daarmee samenhangende globalistische idealen.

“Hoe groter deze groeperingen worden en hoe langer het huidige Europese beleid voortduurt, hoe onvermijdelijker terrorisme wordt“, dat staat in een document, dat werd ondertekend door de Amerikaansepresident Donald Trump.
“*Als bakermat van de westerse cultuur en waarden moet Europa nu handelen en een halt toeroepen aan zijn verval“,* zo staat in het nieuwe beleid, dat onder leiding van contraterrorisme coördinator Sebastian Gorka werd opgesteld.

De AIVD en MIVD delen sinds de benoeming van Donald Trump minder informatie met de Amerikaanse veiligheidsdiensten. Volgens Erik Akerboom (AIVD) en Peter Reesink (MIVD) wordt per geval beoordeeld welke informatie nog wel kan worden gedeeld.

De samenwerking met de CIA en NSA blijft volgens hen goed, maar beide diensten zijn voorzichtiger geworden vanwege zorgen over politisering en mensenrechtenschendingen in de Verenigde Staten. Akerboom benadrukt dat er nog steeds gegevens met de VS worden gedeeld (Palantir).

Het is de eerste keer dat de AIVD en MIVD erkennen dat de ontwikkelingen onder president Donald Trump invloed hebben op de inlichtingenrelatie.
Nederland richt zich intussen meer op samenwerking met Europese partners, waaronder het Verenigd Koninkrijk, Duitsland, Scandinavië, Frankrijk en Polen.
Deze landen wisselen intensiever inlichtingen uit, mede door de oorlog in Oekraïne en de Russische dreiging.

Volgens Akerboom en Reesink voert Rusland jaarlijks tientallen succesvolle hackaanvallen uit op Nederlandse bedrijven en overheden, met merkbare gevolgen.
De kans op een terroristische aanslag in Nederland is reëel, daarom blijft het dreigingsniveau op 4 (substantieel)

Sinds 2020 zijn terroristische aanslagen in Europa vrijwel uitsluitend gepleegd door daders die alleen handelden. Het zijn daders met een nieuw persoonlijk gecreëerd wereldbeeld, vaak met een mix van religieuze en politieke overtuigingen, samenzweringstheorieën en haat in combinatie met persoonlijke omstandigheden. Aanslagplegers kunnen ook handelen uit een pure fascinatie voor geweld."

Centraal geleide terroristische organisaties vormen nog steeds een grote dreiging voor de veiligheid in Europa. Tegelijkertijd vindt radicalisering steeds vaker plaats op bijvoorbeeld sociale media, gamingplatformen en in chatgroepen die niet direct door deze organisaties worden aangestuurd.

Door het gebruik van fluïde online netwerken verspreiden (aanhangers van) terroristische organisaties propaganda, kennis en ideeën om individuele personen te stimuleren terroristisch geweld te gebruiken.

Plannen van de Overheid uit het regeerakkoord

Het eerste Dreigingsbeeld Ondermijning Nederland (DON) rapport is opgesteld door het Strategisch Kenniscentrum

Ondermijnende Criminaliteit, onderdeel van het ministerie van Justitie en Veiligheid stelt dat ondermijning de fundamenten van onze samenleving aantast, sluimerend en vaak onzichtbaar is

DON concludeert dat de ondermijnende effecten op de Nederlandse samenleving de nationale veiligheid bedreigen en schetst dat in 5 dreigingen:

1.Sociaal vangnet door georganiseerde criminaliteit
Criminele netwerken bieden alternatieven voor maatschappelijke voorzieningen die onvoldoende beschikbaar zijn, zoals huisvesting of fysieke bescherming, zorg of leningen.
2.Olievlekwerking in samenleving van betrokkenheid bij georganiseerde criminaliteit
Mensen en organisaties met waardevolle posities zijn aantrekkelijk voor criminele netwerken. Bijvoorbeeld jongeren die op school worden geronseld voor criminele klusjes, gemeenteambtenaren of ondernemers.
3.Beïnvloeding van besluitvorming en taakuitoefening door structurele manipulatie van criminele netwerken
Wanneer grote belangen van georganiseerde criminelen onder druk komen te staan, zullen ze (lokale) besturen proberen naar hun hand te zetten en te manipuleren. De besluitvorming en uitvoering kan dan bewust of onbewust rekening gaan houden met criminelen, bijvoorbeeld om geweld of andere problemen uit de weg te gaan.
4.Illegale opbrengsten vinden weg in de samenleving
Complexe financiële constructies voor het verplaatsen van geld en witwassen worden maximaal benut.

5.Cumulatieve schade door verwevenheid met statelijke of ideologische actoren
Staten en ideologische actoren maken gebruik van de capaciteiten van criminele netwerken.
Het dreigingsbeeld laat ook zien dat de huidige integrale aanpak van ondermijning al op de juiste punten ingrijpt. Maar als de huidige aanpak niet met kracht wordt doorgezet en op punten wordt geïntensiveerd, zullen deze dreigingen op termijn werkelijkheid worden en kunnen deze leiden tot maatschappelijke ontwrichting.

Op korte termijn wordt een aantal thema's en activiteiten door de Overheid opgepakt, zoals het verhogen van de weerbaarheid van jongeren tegen de roep om snel geld verdienen, de rol van ondernemers verstevigen om zelf malafide ondernemers te weren en de herziening van de wet bijzondere maatregelen grootstedelijke problematiek.
• Om het demonstratierecht te waarborgen gaat de Overheid de Wet Openbare Manifestaties aanpassen. Burgemeesters krijgen bevoegdheden tot bestuursrechtelijke handhaving of verplaatsing. Ook worden de strafbepalingen van de wet herzien, waardoor de strafrechter strafbare feiten gepleegd tijdens demonstraties zwaarder weegt.
• De benoeming van leden van de Raad voor de Rechtspraak worden onafhankelijk van de minister. De rechtspraak krijgt een aparte begroting.
• Om de rechtsbescherming te versterken gaat de Overheid constitutionele toetsing aan de klassieke grondrechten in onze Grondwet mogelijk maken. Hiervoor wordt artikel 120 van de Grondwet gewijzigd.

• Er komen meer wijkagenten en cyber- en zedenrechercheurs worden opgeleid en ingezet op meer politieposten.
Daarnaast investeert de Overheid in uitbreiding van gewelds- en verdedigingsmiddelen van de ME. Boa's en politieagenten die dat nodig hebben voor de uitvoering van hun taak krijgen een bodycam.
• Het vrijwilligerskorps wordt op termijn uitgebreid tot een programma waarin jongeren gedurende een jaar lang kennis kunnen maken met het werk bij de politie naar voorbeeld van het dienjaar bij defensie.
• De aanbevelingen van de parlementaire verkenning verward/onbegrepen gedrag en veiligheid worden geïmplementeerd, waaronder meer mogelijkheden voor burgemeesters om door middel van bemoeizorg in te grijpen en meer crisisplekken te realiseren.
• Voetbalfans én hooliganisme krijgen maatregelen, waaronder een boetesysteem voor clubs wanneer politie-inzet zelfs binnen het stadion nodig is.
• De mogelijkheden voor afdoening door de politie worden uitgebreid in de vorm van een politietransactie en/of een politiestrafbeschikking.
• De gegevensdeling ten behoeve van de justitieketen worden verbetert.
• De strafmaat voor zware cyberdelicten wordt verhoogd.
• Er gaat gewerkt worden aan een voorstel voor het beter beschermen van advocaten tegen druk van criminelen, met name bij verdachten in zwaardere regimes. de kroongetuigenregeling wordt uitgebreid en de handhaving op contrabande, zoals het binnensmokkelen van telefoons verscherpt.
• De celcapaciteit wordt uitgebreid en verbeterd door versobering, de instelling van aparte regimes voor beperkt risico gedetineerden en aanvullende maatregelen.

• Zedenzaken met minderjarige slachtoffers worden sneller achter gesloten deuren gehouden. Hun namen worden in grote zedenzaken vaker gecodeerd.
• Veroordeelden gaan voor hun zorg een eigen bijdrage betalen.
• Er komt normering en standaardbedragen voor schadevergoeding slachtoffers met meer ruimte voor collectieve vorderingen en een aparte, laagdrempelige procedure naast het strafproces.
• De griffierechten worden verlaagd en er komen investeringen in sociale advocatuur.
• Voor softdrugs geldt een strak gereguleerd gedoogbeleid. Het gebruik van harddrugs wordt denormaliseerd en handel en verkoop worden aangepakt.
• Het experiment gesloten cannabisketen wordt voortgezet en geëvalueerd en op basis daarvan komen er vervolgstappen.
• Grote festivals worden verplicht een drugspreventieplan te maken. Wie veroordeeld wordt voor overtreding van de Opiumwet krijgt vaker een educatieve maatregel opgelegd als onderdeel van een straf.
• In drie jaar tijd wordt de minimumleeftijd voor sexwerk van 18 jaar verhoogd naar 21 jaar. Uitstapprogramma's worden voortgezet. Er komt een zogeheten pooierverbod, betere toegang tot verzekeringen, zakelijke bankrekeningen en andere financiële dienstverlening. Het programma 'Samen tegen mensenhandel' wordt voortgezet
• Illegale goksites worden harder aangepakt en voor online gokken komt een volledig reclameverbod in met beperking van het aantal vergunningen voor online goksites.
• Professionals die een rol hebben in de aanpak van geweld tegen vrouwen krijgen adequate training over huiselijk geweld, intieme terreur en de rode vlaggen voorafgaand aan femicide. Er wordt vaker ingezet op combizittingen in het straf- en familierecht.

• Wetgeving rondom huiselijk geweld wordt aangescherpt en er wordt een aparte strafbaarstelling voor psychisch geweld geïntroduceerd. Er komt een wettelijke adviesplicht bij signalen van huiselijk geweld en andere schadelijke praktijken voor onderwijs- en zorgprofessionals.
• Versterken van de weerbaarheid tegen hybride (sabotage)acties door (non)statelijke actoren.
• Bestrijden van de dreiging vanuit jihadistische en extremistische netwerken in Nederland, met specifieke aandacht voor online radicalisering.
• Tegengaan van dreigingen tegen de democratische rechtsstaat door de georganiseerde en ondermijnende misdaad.
• Uitbouwen van technologische (inlichtingen)capaciteiten, zodat de diensten technologisch voorop lopen.
• Versterken van eigenstandige, unieke inlichtingenposities en minder afhankelijkheid van andere landen.
• De samenwerking op het gebied van inlichtingen- en veiligheidsdiensten op Europees niveau wordt geïntensiveerd met een Europese equivalent van Five Eyes, om zo met een kopgroep van Europese landen samen te werken op inlichtingengebied. Er wordt een nieuwe en versterkte Wet op de inlichtingen- en veiligheidsdiensten opgesteld.
• De operationele capaciteit voor inlichtingenonderzoek van de Militaire en Algemene Inlichtingen en Veiligheidsdienst (MIVD en AIVD) wordt vergroot, waarbij de diensten ook de eigenstandige inlichtingenpositie ontwikkelen en daarmee bijdragen aan Europese strategische autonomie
• De diensten worden in staat gesteld om nieuwe technologie maximaal te benutten en opponenten te doorzien, door te beschikken over het beste technisch talent en met voldoende technologische capaciteiten en door meer samenwerking met (innovatieve) techbedrijven;

• Defensieve en offensieve cybercapaciteiten tegen dreigingen vanuit het buitenland worden uitgebreid, onder andere door het ontwikkelen van actieve cyberverdedigingsmaatregelen;
• Cybercriminelen met duidelijke banden met het Russische regime worden op de Europese Sanctielijst geplaatst en er komt gedifferentieerd toezicht voor operaties tegen buitenlandse dreigingen en voor het onderscheppen van militaire communicatie enerzijds en inlichtingenwerk waarbij Nederlandse burgers rechtstreeks worden onderzocht anderzijds;
• De mogelijkheden om desinformatie te verwijderen in Europees verband worden uitgebreid. De taak voor het monitoren van de herkomst en verspreiding van desinformatie ligt bij de NCTV en de Minister van Binnenlandse Zaken en Koninkrijksrelaties;
• Samen met lokale overheden en veiligheidsregio's worden buurtcrisisteams opgezet met burgers die bij rampen en crises kunnen worden ingezet en zorgen dat de locaties waar mensen bij crisissituaties terecht kunnen in buurten en dorpen, zoals buurthuizen en brandweerkazernes, hiervoor beschikbaar zijn;
• De lokale aanpak van contraterrorisme wordt versterkt en en er wordt ingezet op een gecoördineerde aanpak van radicaliserende jongeren. Daarbij wordt (online) radicalisering tegengegaan door middel van preventie en vroegsignalering en door het vergroten van kennis en vaardigheden van professionals;
• Terroristische content dient altijd binnen één uur na het bevel van de toezichthouder offline te zijn gehaald;
• Wie zich aansluit bij een terroristische organisatie verliest het Nederlanderschap als er sprake is van een dubbele nationaliteit. Daarom wordt de Wet Permanentmaking intrekking Nederlanderschap in het belang van de nationale veiligheid doorgezet;
• Er komen meer juridische mogelijkheden voor uitbreiding van het toezicht op vrijgekomen terrorismeveroordeelden waarvan het Nederlanderschap is ingetrokken, maar die nog niet uitgezet kunnen worden en anders buiten beeld dreigen te raken.

De Raad van State heeft 12 mei 2026 negatief geadviseerd over het wetsvoorstel intrekken Nederlanderschap van personen aangesloten bij terroristische organisatie
Het wetsvoorstel heeft tot doel de sinds 2017 bestaande bevoegdheid tot intrekking van het Nederlanderschap te continueren.

Die bevoegdheid stelt de minister van Justitie en Veiligheid in staat het Nederlanderschap af te nemen van meerderjarige Nederlanders die zich buiten het Koninkrijk hebben aangesloten bij een terroristische organisatie. De maatregel is destijds als tijdelijk instrument ingevoerd om uitreizigers te weren en risico's voor de nationale veiligheid te beperken.

Omdat de wettelijke grondslag op 1 maart 2027 afloopt, wordt nu voorgesteld deze bevoegdheid permanent te maken.
De Afdeling advisering van de Raad van State is kritisch over dit voornemen.
Zij benadrukt dat het verlies van het Nederlanderschap een ingrijpende maatregel is, met langdurige en in de praktijk vaak onomkeerbare gevolgen voor de betrokkene. Juist daarom vergt een blijvende bevoegdheid tot intrekking een zwaarwegende en overtuigende rechtvaardiging. Volgens de Afdeling schiet de toelichting bij het wetsvoorstel daarin tekort. Niet wordt duidelijk gemaakt waarom bestaande middelen, met name binnen het strafrecht, onvoldoende zijn om de nationale veiligheid te beschermen.

Het blijft onbesproken welke specifieke noodzaak of meerwaarde de maatregel heeft voor Aruba, Curaçao en Sint Maarten, terwijl hij ook daar toepassing zou vinden.

Voor het geval een deugdelijke onderbouwing niet kan worden geleverd, wijst de Afdeling op een alternatief: verlenging van de bestaande regeling voor een beperkte periode van vijf jaar. In die verlengingsfase zou gericht onderzoek kunnen worden gedaan naar de effectiviteit en proportionaliteit van de intrekkingsbevoegdheid.

Die optie verdient volgens de Afdeling nadrukkelijk een plaats in de afweging over het voortbestaan van de regeling.
Alles bij elkaar bezien adviseert de Afdeling om het wetsvoorstel in deze vorm niet in te dienen tenzij het voorstel inhoudelijk wordt aangepast en beter wordt gemotiveerd.

De Wet bestuurlijke maatregelen terrorismebestrijding wordt permanent, met een tijdelijke toezicht maatregel nationale veiligheid naar analogie van het Verenigd Koninkrijk en Duitsland en de mogelijkheid van elektronische monitoring in combinatie met een gebiedsgebod wordt gecreëerd.

De tijdelijke toezicht maatregel wordt periodiek getoetst en levert geen aanspraak op op voorzieningen. De Overheid blijft tegelijkertijd inzetten op vertrek.

Er wordt geïnvesteerd in het stelsel van bewaken en beveiligen, om tegenwicht te bieden aan de toegenomen dreiging tegen bijvoorbeeld politici, journalisten en advocaten.
Aanbevelingen uit het rapport van de Onderzoeksraad voor Veiligheid naar aanleiding van de moord op Peter R. de Vries, worden onverkort uitgevoerd.

De dreiging tegen belangendragers komt deels vanuit criminele netwerken die de democratische rechtsorde willen ondermijnen.

Naast het werk van de Nationale Politie en het OM, die hiertegen optreden, zal de AIVD binnen het huidige mandaat een versterkte bijdrage leveren aan het duiden van dreigingen en het samenbrengen van relevante inlichtingen.

Het Kabinet Jetten heeft een dekking gevonden voor een nieuw modern luchtalarm, dat landelijk bediend moet gaan worden. De maandelijkse test op de eerste maandag van de maand zou stoppen in 2028. In 2024, toen er ook al gesproken werd over het stoppen van de testen, riep een meerderheid van de Kamer het kabinet al op om de toekomst van het sirenenetwerk veilig te stellen.
Het onderhoudscontract met de leveranciers werd daarop verlengd tot 1 januari 2028. Staatssecretaris Van Weel liet weten dat "uitfasering conform eerder besluit vanaf dan uitgevoerd moest gaan worden". Al eerder constateerde het kabinet dat het systeem met 4200 alarmpalen verspreid over Nederland sterk verouderd is en lang niet iedereen bereikt. NL-Alert, waarbij burgers gewaarschuwd worden via hun mobiele telefoon, is veel effectiever, vond Van Weel.
Het kent al jaren een stabiel bereik van zo'n 92 procent van de inwoners. Er zijn echter nog zat mensen zonder mobiel of kunnen fysiek geen communicatie aan.
Ook als het mobiele netwerk om wat voor reden dan ook uitvalt, is er geen alternatieve methode om alarm te kunnen slaan. Daarom is nu gekozen om de financiering te halen uit het beschikbare ruime defensiebudget.

INLICHTING- EN VEILIGHEIDSDIENSTEN

ACA
*O(*Ambtelijke Commissie Aanpak Ondermijning)

De ACAO) is de interdepartementale ambtelijke werkgroep die de Ministeriële Commissie Aanpak Ondermijning (MCAO) ondersteunt bij de bestrijding van georganiseerde en ondermijnende criminaliteit. De commissie speelt een cruciale rol in de coördinatie tussen verschillende ministeries, overheidsinstanties en veiligheidspartners. Bewindspersonen kunnen ingewikkelde of technische onderwerpen voorbespreken in een onderraad. Pas daarna komt het onderwerp op de agenda van de ministerraad. Naast onderraden zijn er ministeriële overleggen. Deze zijn tijdelijk, in principe voor de duur van de kabinetsperiode. De minister-president is voorzitter van alle onderraden en ministeriële overleggen.

AIVD
(Algemene Inlichtingen en Veiligheidsdienst)

De nationale veiligheid staat van veel verschillende kanten “langdurig onder druk”, stelt AIVD-directeur Simone Smit 23 april 2026 op basis van het jaarverslag van afgelopen jaar. Er is sprake van “een veelvoud aan dreigingen die met elkaar samenhangen”. De AIVD signaleerde in 2025 onder meer dreigingen binnen het islamitisch extremisme, anti-institutioneel extremisme, links-extremisme en rechts-extremisme.

De belangrijkste terroristische dreiging komt voort uit het jihadisme en in Nederland komt die “vrijwel geheel vanuit ISIS”. De beweging stuurt aanslagplegers aan. De AIVD ziet een toename van het aantal aanhangers onder jongeren tot 24 jaar.

De rechts-extremistische dreiging is tweeledig: er is een brede, niet-gewelddadige beweging, terwijl sommige rechts-extremisten daarin “een legitimatie voor het gebruik van geweld” zien.

De AIVD greep in bij personen die wapens en munitie maakten en verzamelden om die “zeer waarschijnlijk” in te zetten.
De oorlog in Gaza blijkt, net als in 2024, één van de belangrijkste onderwerpen voor de links-extremistische beweging. Veel van het linkse protest was activistisch: dreiging vanuit die beweging was “gering”.
In 2024 signaleerde de AIVD al een toename van het aantal landen met “een offensief cyberprogramma” en in 2025 bleek dat de dreiging die uitgaat van zulke programma’s groter is dan eerst werd ingeschat en de bestrijding daarvan is ingewikkeld. “De strijd in het cyberdomein is een ongelijke strijd”, stelt de dienst. In 2025 vonden verschillende cyberaanvallen plaats, bijvoorbeeld op het Openbaar Ministerie.

De nationale veiligheid wordt onder meer bedreigd door samenwerkingen tussen criminele netwerken en buitenlandse overheden.
Bepaalde overheden beschermen criminele netwerken in ruil voor hun diensten, waaronder het gebruik van dodelijk geweld, spionage en inmenging. Zulke netwerken hebben in 2025 “een sterke positie kunnen opbouwen”.
Via spionage proberen buitenlandse overheden informatie te krijgen in Nederland en Europa.

De AIVD ziet “een grote aanhoudende spionagedreiging” uitgaan van onder meer Rusland, China, Iran en Marokko

AFRIPOL
(Afrikaanse Politie)

AFRIPOL is het officiële mechanisme van de Afrikaanse Unie (AU) voor politiecoöperatie, opgericht in 2014 met het hoofdkantoor in Algiers, Algerije.
Het doel is het versterken van de samenwerking tussen politie-instanties van AU-lidstaten om transnationale georganiseerde misdaad, terrorisme, cybercriminaliteit en andere grensoverschrijdende veiligheidsdreigingen te bestrijden. De organisatie biedt capaciteitsopbouw via trainingen, technische ondersteuning en het delen van best practices.

Een belangrijk instrument is het Afrikaanse Veilige Communicatiesysteem (AFSECOM), dat veilige communicatie en gegevensuitwisseling tussen lidstaten mogelijk maakt. AFRIPOL werkt samen met internationale partners zoals INTERPOL, de Europese Unie en de Verenigde Naties om gezamenlijke operaties en strategische initiatieven te ondersteunen.

De structuur van AFRIPOL omvat een Algemene Vergadering van politiechefs, een Sturingscomité en een Secretariaat. Het programma INTERPOL Support Programme for the African Union in relation to AFRIPOL (ISPA) ondersteunt AFRIPOL bij het ontwikkelen van zijn functies over het continent.

AFRIPOL speelt een cruciale rol in het bevorderen van politiecoöperatie op strategisch, tactisch en operationeel niveau tussen AU-lidstaten.

AVIM
(Afdeling Vreemdelingen Politie en Mensenhandel)

Migratiecriminaliteit en Mensenhandel (AVIM) weer gaan naar de politietaken in het vreemdelingendomein zoals het binnenlands toezicht op de naleving en de handhaving van de vreemdelingenwetgeving.

Het identificeren en registreren van vreemdelingen die asiel aanvragen is in 2025 geen taak meer voor de politie. Dit wordt uitgevoerd door de Dienst Identificatie en Screening Asielzoekers (DISA).
AVIm is een gespecialiseerde afdeling binnen de Nederlandse Nationale Politie die toezicht houdt op de naleving van de Vreemdelingenwet en onderzoek doet naar migratiecriminaliteit. De kerntaken van de AVIM omvatten:

- Identificatie en verblijf: Het onderzoeken van de identiteit en de verblijfsrechtelijke status van vreemdelingen in Nederland.
- Bestrijding van criminaliteit: Het opsporen van zware en georganiseerde misdrijven zoals mensensmokkel, mensenhandel en identiteitsfraude.

- Toezicht en handhaving: Het controleren of vreemdelingen zich aan de regels houden, zoals de wekelijkse 'AVIM-meldplicht' voor asielzoekers die in een COA-opvang verblijven maar geen geldige verblijfsvergunning hebben.

De focus van de AVIM ligt op de aanpak van overlastgevend en crimineel gedrag onder een relatief kleine groep vreemdelingen, ongeacht hun verblijfsstatus; van toerist tot arbeidsmigrant, van EU-burger tot asielzoeker.

CBRN Centrum
((Chemisch, Biologisch, Radiologiesch, Nucliair Centrum)

Het Defensie CBRN Centrum (DCBRNC) in Vught is de plek waar alle kennis, opleidingen, trainingen en inzet op het gebied van chemische, biologische, radiologische en nucleaire middelen samenkomen.
Er werken ongeveer 110 medewerkers (militairen en burgers). Het centrum is gevestigd in Vught. En maakt deel uit van het Opleidings- en Trainingscentrum Genie (OTC Genie) van de landmacht.
Het Defensie CBRN Centrum ondersteunt Nederlandse civiele hulpdiensten bij chemische, biologische, radiologische en nucleaire (CBRN-) dreigingen en incidenten.
Het beschermt tegen inademen van vervuilde lucht en tegen sproei- en aerosolaanvallen.
Het acroniem verwijst naar gevaarlijke stoffen en situaties die een risico vormen voor de volksgezondheid en het milieu, variërend van ongelukken met industrieel materiaal tot moedwillige aanslagen.
Onderverdeling van CBRN:C - Chemisch: Giftige industriële chemicaliën, pesticiden of chemische strijdmiddelen (bijv. zenuwgas).B - Biologisch: Ziekteverwekkers zoals bacteriën, virussen of toxines (bijv. miltvuur of ebola).R - Radiologisch: Radioactief materiaal dat bijvoorbeeld per ongeluk vrijkomt of door een 'vuile bom' wordt verspreid.N - Nucleair: De inzet van kernwapens of incidenten met kernreactoren en splijtstoffen.
Omdat CBRN-incidenten vaak onzichtbaar zijn en een grote impact kunnen hebben, zijn er gespecialiseerde eenheden en instituten opgericht voor bescherming, detectie en decontaminatie (ontsmetting). Bij incidenten kunnen gespecialiseerde teams, zoals het CBRN-Team Ambulancezorg, levensreddende zorg verlenen in risicovolle omstandigheden.

Commissie Stiekem

De commissie heet zo omdat zij in tegenstelling tot de meeste andere Kamercommissies achter gesloten deuren vergaderen en haar documenten en besprekingen strikt vertrouwelijk zijn.
Dit is noodzakelijk om de werkwijze, bronnen en methoden van de geheime diensten te beschermenSophia Theodora Monique (Sophie) Hermans (Nijmegen, 1 mei 1981) (VVD) is sinds 2 juli 2024 minister van Klimaat en Groene Groei en vicepremier en sinds 23 augustus 2025. Zij is belast met de portefeuille Onderwijs, Cultuur en Wetenschap. Van 3 juni tot 19 juni 2025 was zij waarnemend minister van Infrastructuur en Waterstaat. Voor haar ministerschap was zij vanaf 23 maart 2017 Tweede Kamerlid. Van 11 januari 2022 tot 6 december 2023 was zij fractievoorzitter van de VVD.
Vanaf 16 september 2021 tot 6 december 2023 was zij tevens voorzitter van de Commissie voor de Inlichtingen- en Veiligheidsdiensten. Commissie Stiekem, is een commissie van de Tweede Kamer die belast is met de parlementaire controle op de Nederlandse geheime diensten.
De commissie bestaat uit minimaal vijf en maximaal zeven fractievoorzitters en vergadert onder strikte geheimhouding, maar brengt over haar werkzaamheden wel verslag uit aan de Tweede Kamer. De Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD), ook wel de “Commissie Stiekem” genoemd, bestaat uit fractieleiders van de grootste partijen in de Tweede Kamer. Deze commissie krijgt vertrouwelijke briefings over gevoelige operaties en houdt toezicht op strategische keuzes.
Geert Wilders (PVV), voorzitter
Dilan Yeşilgöz-Zegerius (VVD)
Rob Jetten (D66)
Henri Bontenbal (CDA)

CTIVD/
(Commissie Toezicht Inlichtingen- en Veiligheids Diensten)

De Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten (CTIVD) is in 2002 opgericht. Sinds de inwerkingtreding van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) op 1 mei 2018 bestaat de CTIVD uit 2 afdelingen: de afdeling toezicht en de afdeling klachtbehandeling.

De afdeling toezicht heeft tot taak:

- onderzoek doen en verslag uitbrengen in openbare toezicht rapporten;
- betrokken ministers gevraagd en ongevraagd adviseren over haar conclusie.

De afdeling klachtbehandeling heeft tot taak:
- het onderzoeken van en oordelen over klachten;
- het onderzoeken van en oordelen over een melding van een vermoeden van een misstand.

Het gaat hierbij om klachten over het handelen en meldingen van een vermoeden van een misstand bij de AIVD en de MIVD.
De CTIVD stelt na onderzoek vast of de betreffende afdeling tekort heeft geschoten in het delen van geheime informatie met andere diensten.
Burgers of organisaties kunnen klachten indienen bij de CTIVD of, in sommige gevallen, bij de rechter (bijv. de Raad van State) als ze menen dat hun rechten zijn geschonden. Dit systeem is ontworpen om te voorkomen dat veiligheidsdiensten autonoom opereren. Het combineert politieke verantwoordelijkheid (regering), onafhankelijk toezicht (CTIVD, TIB) en parlementaire controle.

De Eerste Kamer heeft 12 maart 2024 ingestemd met de Tijdelijke wet cyberoperaties.
Met deze nieuwe bevoegdheid kan de CTIVD een operatie per direct stopzetten en besluiten dat de gegevens die hierbij verworven zijn moeten worden vernietigd. Ook is een beroepsmogelijkheid geïntroduceerd bij de Raad van State. Hiermee wordt een weeffout in het stelsel van toetsing en toezicht hersteld en ligt de definitieve uitleg van de wetgeving waar hij thuishoort, bij de rechter.

De CTIVD bestaat uit drietoto zes leden, die voor een termijn van zes jaar worden benoemd bij Koninklijk Besluit op voordracht van een aanbevelingscommissie, bestaande uit de vice-president van de Raad van State, de president van de Hoge Raad der Nederlanden, de Nationale ombudsman.
De CTIVD heeft twee afdelingen: de afdeling toezicht (drie leden, inclusief de voorzitter) en de afdeling klachtbehandeling (drie leden, inclusief een voorzitter uit de CTIVD).
De leden van de CTIVD zijn primair betrokken bij het toezicht, terwijl de klachtbehandeling een aparte rol heeft.

Door de Tijdelijke wet die op 1 juli 2024 van kracht werd, is de manier waarop de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) toezicht houdt op de AIVD en MIVD veranderd. Waar de CTIVD voorheen preventief controleerde, wordt het toezicht nu dynamischer. De commissie controleert nu terwijl de inlichtingenoperaties al gaande zijn.

Deze nieuwe aanpak richt zich op operaties die te maken hebben met landen met een vijandig cyberprogramma, zoals Rusland en China.
Volgens secretaris-directeur Kristel Koese is dit een goede ontwikkeling, omdat het beter aansluit bij de snelle en wendbare werkwijze van de inlichtingendiensten.

De AIVD stelt dat de wet nodig is om de nationale veiligheid te waarborgen en hun slagkracht te vergroten.

Tegelijkertijd heeft de CTIVD meer bevoegdheden gekregen. Zo kan de commissie een operatie per direct stopzetten en de vernietiging van de verzamelde gegevens eisen. Ook is er een beroepsmogelijkheid bij de Raad van State geïntroduceerd.

Ondanks de nieuwe bevoegdheden kampt de CTIVD met praktische problemen. De commissie moet meer specialisten aannemen, maar had daarvoor geen ruimte. De zoektocht naar een nieuwe, permanent beveiligde locatie is complex, omdat de eisen even hoog zijn als die voor de inlichtingendiensten zelf. Er is een tijdelijke oplossing gevonden in Den Haag, wat een belangrijke stap is, maar het probleem van een definitieve locatie blijft bestaan.
Hoewel er per 6 januari 2025 een nieuwe voorzitter en een nieuw lid zijn aangetreden, blijft ook het werven van andere specialisten een uitdaging.
Het mee naar huis kunnen nemen van geheime stukken door een verdachte baart de commissie ernstige zorgen. Vooral de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) was volgens de toezichthouder eerder onzorgvuldig. Er was onvoldoende toezicht op de informatie die de AIVD deelde met de antiterrorismecoördinator. Ook bleek er geen goed beleid voor het delen van informatie binnen de diensten tye bestaan. Zo is niet altijd duidelijk waarom informatie überhaupt gedeeld moest worden.
Welke informatie wel en niet gedeeld wordt, is vaak afhankelijk van het team dat het verzoek kreeg. De AIVD moet dan ook beter beoordelen wie toegang nodig heeft tot staatsgeheime informatie, stelt de toezichthouder. Daarbij moet de dienst ook kijken naar mogelijke politieke banden met een ander land.

Naast de AIVD moet de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) beter beoordelen wie toegang heeft tot staatsgeheime informatie. Bovendien moet de dienst beter in de gaten houden wat er met die informatie gebeurt.
Als de gegevensbeveiliging bij de ontvanger niet op orde is na het delen van de informatie, moet de dienst daar iets aan doen.
Ondanks de onzorgvuldigheid hadden beide diensten het lek volgens de CTIVD niet kunnen voorkomen.

De diensten zijn beide afhankelijk van elkaar, van andere instanties en van de betrouwbaarheid van medewerkers.
De CTIVD is nog volop bezig met de implementatie van de nieuwe taken, waaronder de jaarlijkse beoordeling van bulkdatasets.

Hoewel er vooruitgang is geboekt met de tijdelijke huisvesting en de aanstelling van nieuwe leiding, zijn de oorspronkelijke uitdagingen, zoals het vinden van een permanente locatie en het aannemen van alle benodigde specialisten, nog steeds actueel.

De CTIVD rapporteert aan de regering en publiceert openbare verslagen (met uitzondering van geclassificeerde details).
Ze onderzoekt bijvoorbeeld of afluisterpraktijken of dataverzameling voldoen aan de wet.
De Toetsingscommissie Inzet Bevoegdheden (TIB), opgericht in 2018, toetst vooraf of verzoeken voor zware middelen (zoals afluisteren of hacken) rechtmatig zijn. Dit gebeurt voordat de minister goedkeuring geeft

Twee medewerkers van de NCTV werden veroordeeld vanwege het delen van staatsgeheime informatie met de Marokkaanse veiligheidsdiensten. Een medewerker werd in oktober 2023 op Schiphol aangehouden toen hij met een tas vol gegevensdragers naar Marokko wilde reizen. Er werden in zijn bagage honderden staatsgeheime documenten aangetroffen, onder meer van de AIVD en MIVD. Hij zou ruim 900 staatsgeheime documenten van onder meer inlichtingendiensten AIVD en MIVD in bezit hebben gehad.
“Op het nachtkastje naast zijn bed zijn stukken uit 2022 en 2023 aangetroffen. Bij de printer in de slaapkamer van een van de kinderen; heel veel stukken hoofdzakelijk uit 2022-2023. (..) op zolder op de werkkamer nog meer staatsgeheime hardcopy stukken. Stukken opgemaakt in de jaren 1993 t/m 2023 in gestapelde dozen of tussen de boeken en in boeken van de boekenkasten. Een totaal van 973 fysieke stukken werd bij verdachte aangetroffen die daar simpel niet hadden mogen liggen vanwege hun inhoud. Ruim 800 daarvan bleken staatsgeheim gerubriceerd.”
Bij huiszoeking bi de Rotterdamse senior wetenschappelijk medewerker, analist en tolk van de NCTV werd 46 terabyte aan vertrouwelijke data aangetroffen en in beslag genomen. oftewel 11,5 miljard A4’tjes.
Er werden talloze gegevensdragers, vooral usb-sticks, in beslag genomen zijn met informatie van en over de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en politie.
Hierbij zaten honderden Staatsgeheime documenten die hij deels uitprintte en 30 jaar lang (10 x per jaar) geregeld mee nam op zijn door de geheime dienst van Marokko betaalde vakanties naar zijn land van herkomst. De man werkte op de afdeling Academie voor een salaris van 7.834,47 euro bruto. Met daarbovenop een potje voor eigen ontwikkeling van 16 procent van zijn salaris.

De medewerker werkte al sinds 1990 voor de overheid, in verschillende functies, had een lange staat van dienst bij de politie en justitie en werkte behalve voor de NCTV ook nog voor de Landelijke Eenheid van de Nationale Politie in tal van gevoelige onderzoeken.
De overheid mocht hem van de rechter ontslaan en hoefde hem geen 200.000 euro vertrekvergoedingen te betalen.
Tegen de spion rezen al in 2021 vermoedens dat hij informatie doorspeelde aan zijn moederland. Hij werd samen met een 35-jarige collega uit Gouda aangehouden.
De vrouw werkte sinds kort voor de politie, maar was daarvoor ook werkzaam bij de NCTV. Volgens het OM bestond het contact tussen de medewerker en de Marokkaanse inlichtingendienst mogelijk al sinds 1995.
De man zat een tijd in beperkende voorlopige hechtenis en de vrouw werd in afwachting van behandeling begin december 2023 vrijgelaten. De AIVD hing een camera op bij de NCTV en zag hoe hij staatsgeheime stukken uitprintte met het pasje van de collega.
Zij zou ook haar inlog hebben uitgeleend, toen M. vanwege een nieuwe functie niet meer bij staatsgeheime stukken kon.
Zij heeft verklaard dat ze geen idee had van de spionageactiviteiten en werd door de rechter vrijgesproken.
De rechtbank Rotterdam wilde demissionair premier Dick Schoof horen, omdat hij ten tijde van deze grote spionagezaak hoofd was van de NCTV. Ook het huidige hoofd, Pieter-Jaap Aalbersberg, zou getuigen in de zaak.
Beiden hebben echter niet hoeven te verklaren verklaren over de geoorloofde toegang van de verdachte tot en het mee naar huis nemen van staatsgeheime en vertrouwelijke stukken.
Omdat het onderzoek in de strafzaak nog langer ging duren, kwam de medewerker voorlopig vrij. Zelf heeft hij de beschuldigingen, ondanks alle bewijzen altijd ontkend. '*Ik heb op geen enkele wijze staatsgeheime informatie overhandigd, aan wie dan ook*', zei hij tijdens een eerdere zitting.

De rechtbank wilde ook een vertrouweling van de Marokkaanse Koning Mohammed VI Mohamed Yassine Mansouri horen. Mansouri is het hoofd van de Marokkaanse inlichtingendienst (DGED). Dit wijst op de mogelijke internationale implicaties van de zaak. De zitting in de strafzaak werd in februari 2026 voortgezet.
De nu 66-jarige medewerker stond bekend als een expert op het gebied van salafisme en jihadisme. Voor de NCTV schreef hij daar rapportages over. Het vertrouwen dat M. daardoor genoot, zou hij hebben benut om grote hoeveelheden staatsgeheimen te vergaren. Het ging daarbij om een groot aantal analyses van de AIVD en de MIVD, zoals een rapport over Marokkaanse inlichtingenactiviteiten in Nederland. Ook zou hij een lijst hebben doorgespeeld met telefoonnummers van Marokkaanse IS-strijders.
Dat hij daadwerkelijk informatie verstrekte aan de Marokkaanse inlichtingendienst, blijkt volgens het OM uit berichtenverkeer met meerdere medewerkers van die dienst. In die berichten vroeg hij. of hij “het medicijn” of “een klein dingetje” kon overhandigen. Als tegenprestatie werd hij getrakteerd op gratis vakanties naar Marokko.
Uit het politieonderzoek bleek dat de medewerker tot wel tien keer per jaar met zijn hele gezin op en neer vloog, waarvan meerdere trips betaald werden door de Marokkaanse inlichtingendienst. “Het is weer voortreffelijk geweest”, schreef M. in een bedankje aan een van zijn contacten.
De AIVD was te makkelijk met het delen van informatie en de NCTV had de eigen beveiliging niet op orde. De zaak diende 4 februari 2026 en OM eiste 12 jaar cel..
Marokko wordt al jaren verdacht van inmenging in de Nederlands-Marokkaanse diaspora (activisten, imams, journalisten). De AIVD waarschuwt hier expliciet voor in jaarverslagen.

DCC
(Defensie Cyber Commando

(DCC) voert militaire cyberoperaties uit en draagt bij aan de algehele slagkracht van de krijgsmacht. Militaire cyberoperaties kunnen zowel defensief, offensief of voorwaardenscheppend van aard zijn.Onderdeel van het DCC is het expertisecentrum op het gebied van cyber voor heel Defensie: het Cyber Warfare and Training Centre (CWTC).
Daarnaast speelt cyber bij militaire operaties in de andere vier operationele domeinen ook een essentiële rol, bijvoorbeeld in de vorm van informatieoperaties, het vergaren van gevechtsinlichtingen en het ondersteunen dan wel bewerkstelligen van militaire effecten op strategisch, operationeel en tactisch niveau.

DCC levert digitale slagkracht voor Nederland en de krijgsmacht. Het voert militaire operaties uit in en via de digitale wereld, de cyberspace. Dit doet het DCC zelfstandig of samen met militaire en civiele partners.

Het DCC bedenkt digitale middelen om acties uit te voeren. Ook ondersteunt het de krijgsmacht om digitale technieken goed te gebruiken. Zij zijn specialisten in militaire digitale operaties. Hierbij werkt het DCC volgens 3 vaste waarden:

- slagvaardig (doelgericht en wendbaar)
- deskundig (specialistische kennis)
- verbonden (sterk in samenwerken)

De belangrijkste taak van het DCC is het plannen en uitvoeren van cyberoperaties voor de krijgsmacht. Dat gebeurt door mensen die slim vooruitdenken, samenwerken en durven te handelen in de veranderlijke digitale wereld.

Het DCC werkt in opdracht van de Commandant der Strijdkrachten.

DCSC
(Defensie Cyber Security Centrum)

Het DCSC moet ervoor zorgen dat militaire operaties geen hinder ondervinden van digitale dreigingen en dat de informatiesystemen van Defensie betrouwbaar blijven.

Hiervoor moet DCSC:

- cyberdreigingen op tijd zien;
- onderzoeken van kwetsbaarheden binnen Defensiesystemen;
- onderzoeken hoe groot de dreiging is;
- zorgen dat de dreiging vermindert of verdwijnt.

Daarnaast kan DCSC ook civiele autoriteiten ondersteunen bij het verhelpen van cyberincidenten.

Bij het uitvoeren van haar werkzaamheden werkt het DCSC nauw samen met andere teams, zoals:

- het Nationaal Cyber Security Centrum (NCSC);
- het Nationaal Response Netwerk (NRN);
- het NATO Computer Incident Response Capability (NCIRC);
- het Forum of Incident Response and Security Teams (FIRST).

De cyberveiligheid van Defensie is primair ondergebracht bij het Defensie Cyber Security Centrum (DCSC). Het DCSC monitort samen met de Security Operating Centers (SOCs) van de Defensieonderdelen dagelijks netwerken van Defensie op cyberaanvallen. Bij het tegengaan van cyberincidenten heeft het DCSC onder meer de beschikking over Cyber Rapid Response Teams (CRRT) en voorziet het DCSC in het uitwisselen van relevante informatie tussen verschillende defensieonderdelen.
De DCS geeft focus aan de taken van Defensie in het cyberdomein. Defensie is namelijk dagelijks doelwit van cyberaanvallen. Er worden daarom proactief maatregelen genomen om cyberrisico's te beheersen. En om tijdig te kunnen optreden bij eventuele cyberincidenten.
De tweede taak is het uitvoeren van militaire cyberoperaties. De krijgsmacht moet in staat zijn om vanuit het cyberdomein zelfstandig effecten te bereiken die militaire doelen kunnen dienen. Militaire cyberoperaties kunnen bijvoorbeeld ondersteunend zijn aan informatie-operaties die weer integraal onderdeel uitmaken van een militaire campagne. Tot slot draagt Defensie bij aan de algehele cyberweerbaarheid van het Koninkrijk der Nederlanden en zijn bondgenoten. Hoewel dit in eerste instantie een civiele aangelegenheid is, speelt Defensie wel een significante rol vanuit bijvoorbeeld de inlichtingen- en veiligheidstaak en eventuele militaire steunverlening. Defensie voert daarom militaire cyberoperaties uit om Nederland te beschermen en bondgenoten te steunen.
Verder blijft de krijgsmacht investeren in de samenwerking met andere departementen, private partijen, kennisinstellingen en bondgenoten. Naast gekwalificeerd cyberpersoneel is ook het innovatieve vermogen van Defensie noodzakelijk om de cybertaken te kunnen uitvoeren. Hierbij is het belangrijk om nauw samen te werken met private partijen om hun kennis en expertise aan te boren. Bijvoorbeeld op het gebied van quantum-cryptografie en kunstmatige intelligentie.

DISA
(Dienst Identificatie Screening Asielzoekers)

DISA verzamelt en controleert biometrische gegevens zoals vingerafdrukken en gezichtsherkenning in nationale en Europese databases. Deze gegevens gebruikt de DISA om een asielaanvraag te registreren. Zo krijgen partners informatie op het gebied van veiligheid, opvang, procedure en terugkeer. Het doel van het identificatie- en registratieproces is om snel duidelijk te krijgen wie de aanvrager is, zodat niemand zonder registratie in Nederland kan verblijven.

DISA is een nieuwe organisatie van het ministerie van Asiel en Migratie, die het identificeren en registreren van asielzoekers op zich neemt. Daar waar nodig levert de politie kennis en expertise.

Tegelijkertijd start met het loslaten van deze taak een reorganisatie voor de politie en voor de betrokken politiemedewerkers in Noord-Nederland en Oost-Brabant. Het identificeren en registreren van vreemdelingen die asiel aanvragen is in 2025 geen taak meer voor de politie.

ECTC
(Europees Counter Terrorism Center)

ECTC van Interpol werd als maatregel tegen het internationale terrorisme in januari 2016 opgericht. Het ECTC richt zich op het aanpakken van buitenlandse terroristen, illegale wapenhandel, het verspreiden van online terroristische propaganda en extremisme en de internationale terrorismebestrijding in het algemeen. De voornaamste taak van het ECTC is operationele steun verlenen aan de lidstaten bij onderzoeken, zoals die na de aanslagen van Parijs, Nice en Brussel hebben plaats gevonden.

De ECTC kan voortbouwen op de door Europol opgerichte terrorismebestrijdingsnetwerken die al een belangrijke rol hebben gespeeld bij onder andere de aanslagen in Parijs. De ECTC teams van analisten en experts verzamelen operationele informatie van de wetshandhaving uit alle lidstaten, alsmede van derden en werkt nauw samen met andere operationele centra bij Europol, zoals het Europees Cybercrime Centrum (EC3) en het Europees Mensensmokkel Centre (EMSC).
Europol heeft behalve terroristen ook de gevaarlijkste criminele netwerken in Europa in kaart gebracht.
Het gaat in totaal om 821 organisaties waarbij in totaal minstens 25.000 criminelen zijn betrokken. De 821 organisaties die in heel Europa actief zijn, zitten voornamelijk in de cocaïnehandel. Het andere deel maakt zich onder andere schuldig aan fraude, migrantenhandel, mensenhandel of vermogenscriminaliteit. De resultaten kwamen uit een onderzoek onder alle EU-lidstaten en de zeventien landen die Europol-partner zijn.

EMPACT
(European Multidisciplinary Platform Against Criminal Threats)

EMPACT is een coördinatiekader (platform) binnen de EU voor georganiseerde en ernstige criminaliteit, zonder hiërarchische macht. Het bepaalt strategische prioriteiten op basis van Europol's SOCTA en organiseert lidstaten rond gezamenlijke acties, waarbij één of meerdere landen als drijvende kracht optreden. Lidstaten voeren vervolgens de operaties uit. EU-agentschappen leveren steun, Europol levert inlichtingen en coördinatie, OLAF de technische ondersteuning en expertise in financiële fraude, Frontex ondersteunt grensbeheer en grensoperaties,
Eurojust coördineert justitiële samenwerking en Interpol kan extern worden betrokken bij internationale onderzoeken die EMPACT prioriteert.

EMPACT ontstond in 2010 toen de Raad van de Europese Unie besloot tot de invoering van een beleidscyclus voor de bestrijding van zware criminaliteit. Dit besluit werd genomen naar aanleiding van de behoefte aan een gestructureerde en langdurige aanpak van dreigingen die de interne veiligheid van de Unie ondermijnen.
De doelstelling van EMPACT is het bestrijden van mensenhandel, migrantensmokkel, de productie en handel in drugs, cybercriminaliteit, de illegale handel in vuurwapens, financiële en economische criminaliteit waaronder valsemunterij, en milieucriminaliteit. Door deze brede opzet kan de Unie meerdere sectoren van georganiseerde criminaliteit gelijktijdig aanpakken binnen één gecoördineerd raamwerk.

EMPACT werkt in vierjarige cycli. Elke cyclus begint met een uitgebreide dreigingsbeoordeling door de Serious and Organised Crime Threat Assessment (SOCTA), opgesteld door Europol. Op basis van deze analyse bepalen de lidstaten en de Raad van de Europese Unie welke vormen van criminaliteit de hoogste prioriteit krijgen. Voor elke vastgestelde prioriteit wordt een meerjarig strategisch plan opgesteld. Dat plan wordt vervolgens vertaald naar jaarlijkse operationele actieplannen die de concrete maatregelen en operaties vastleggen.

De uitvoering berust bij de lidstaten en hun opsporingsdiensten. Een of meerdere landen nemen de rol van drijvende kracht of medeorganisator op zich en dragen verantwoordelijkheid voor het aansturen van de acties binnen hun toegewezen prioriteit. Europol levert analytische en operationele steun en fungeert als centrale spil voor de uitwisseling van informatie. De Europese Commissie, de Raad en agentschappen zoals Frontex, OLAF en ondersteunen beleidsmatig en dragen bij met expertise en middelen.
De reikwijdte van EMPACT gaat verder dan de lidstaten alleen. Naast alle EU-landen nemen ook derde landen zoals Noorwegen, Zwitserland en de Verenigde Staten deel aan onderzoeken.

Bovendien werken internationale organisaties als Interpol en de Wereld Douaneorganisatie mee. Door deze samenwerking worden politie, douane, grenswachten, fiscale autoriteiten en inlichtingenstructuren gebundeld in gezamenlijke acties tegen grensoverschrijdende criminaliteit.

Sinds de oprichting in 2010 heeft EMPACT geleid tot duizenden inbeslagnames, arrestaties en de ontmanteling van talloze criminele netwerken. Het model heeft zich ontwikkeld tot een permanent instrument binnen de EU-beleidscyclus voor georganiseerde en zware criminaliteit. Daarmee vormt EMPACT de vaste structuur waarbinnen de gezamenlijke inzet van politie, douane en justitie wordt gecoördineerd, met Europol als spil en de lidstaten als uitvoerende trekkers.

Europol verleende van oktober 2024 tot maart 2025 operationele en analytische steun aan IMPECT bij een gecoördineerde internationale rechtshandhavingsactie die de distributie van vals geld via postdiensten verstoorde. In totaal werden 990.000 namaakproducten onderschept, waaronder vervalste bankbiljetten en munten met een gezamenlijke nominale waarde van meer dan 66 miljoen euro. De in beslag genomen valuta bestonden uit meer dan 280.000 euro, 679.000 Amerikaanse dollars en 12.000 Britse ponden.
De operatie vond plaats vanuit Oostenrijk, Portugal en Spanje. Achttien landen leverden een directe bijdrage aan de uiteindelijke start van start van 102 nieuwe onderzoeken naar criminele netwerken die zich toeleggen op productie en distributie van vervalste valuta. De meeste geïdentificeerde netwerken opereerden buiten de Europese Unie, met hoofdactiviteiten gelokaliseerd in Azië, alsook in bepaalde delen van Noord- en Zuid-Amerika en het Midden-Oosten. Een concreet resultaat in Roemenië leidde tot een inbeslagname van 600.000 vervalste Amerikaanse dollars.

EUROJUST
(Europese Justitie)

Eurojust is het Europees College van Procureurs en Officieren van Justitie, een agentschap van de Europese Unie dat de samenwerking tussen nationale justitiële autoriteiten in strafzaken coördineert. Het werd opgericht in 2002 en heeft zijn hoofdzetel in Den Haag. Eurojust ondersteunt lidstaten bij complexe grensoverschrijdende strafzaken, vooral op het gebied van georganiseerde en ernstige internationale criminaliteit, waaronder terrorisme, mensenhandel, drugshandel, witwassen en fraude.

De kerntaken van Eurojust zijn het faciliteren van samenwerking, het coördineren van onderzoeken en vervolgingen, en het oplossen van conflicten tussen nationale jurisdicties. Het agentschap kan voorstellen doen voor gezamenlijke onderzoeks- en vervolgingsteams, informatie-uitwisseling coördineren en juridische obstakels zoals verschillen in nationale wetgeving helpen overbruggen.
Eurojust treedt op als een platform waar nationale aanklagers en officieren van justitie samenkomen om strategieën en acties af te stemmen en zorgt voor de efficiënte uitvoering van Europese opsporingsbevelen en andere gerechtelijke instrumenten.
Eurojust heeft geen eigen opsporings- of arrestatiebevoegdheden, maar fungeert als coördinerend en ondersteunend orgaan. Het kan echter operationele aanbevelingen geven, gezamenlijke vergaderingen van nationale teams organiseren en directe ondersteuning bieden bij het opzetten van complexe internationale onderzoeken. Het agentschap werkt nauw samen met Europol, OLAF en nationale autoriteiten en is actief betrokken bij projecten die grensoverschrijdende criminaliteit aanpakken, zoals grootschalige operaties tegen valsemunterij, drugshandel en mensenhandel.

Europol
(Europese Politie)

Het Europese politiebureau dat als centrale coördinator fungeert voor de bestrijding van ernstige en georganiseerde internationale criminaliteit binnen de Europese Unie.
Het werd opgericht in 1999 en heeft zijn hoofdzetel in Den Haag.
Europol ondersteunt de lidstaten met inlichtingen, analyses en coördinatie van grensoverschrijdende opsporing en opsporingsonderzoeken.

De kerntaken omvatten het verzamelen en analyseren van informatie over criminele netwerken, het verstrekken van operationele ondersteuning bij onderzoeken, het faciliteren van de uitwisseling van gegevens tussen lidstaten en het ontwikkelen van risicoprofielen en dreigingsanalyses.
Europol voert zelf geen arrestaties uit; alle handhaving wordt door de nationale autoriteiten gedaan.

Europol werkt nauw samen met andere EU-agentschappen zoals Eurojust, OLAF en Frontex, en kan ook internationale partners zoals Interpol betrekken.
Het speelt een centrale rol in strategische initiatieven zoals EMPACT, waar het de SOCTA-dreigingsanalyse levert en helpt prioriteiten en gezamenlijke strategieën te bepalen.

Europol werkt samen met veel niet-EU-partnerstaten en internationale organisaties. Grootschalige criminele en terroristische netwerken vormen een aanzienlijke bedreiging voor de interne veiligheid van de EU en voor de veiligheid en het levensonderhoud van haar bevolking.

FAST NL
(Fugitive Actice Search Team)

FAST NL van de Eenheid Landelijke Opsporing en Interventies is aangesloten bij het European Network of Fugitive Active Search Teams (ENFAST) en is een samenwerkingsverband van opsporingsteams van politiediensten binnen de Europese Unie.
In Etten-Leur werd in januari 2025, dankzij FAstNL, de 30-jarige voortvluchtige Krystian K. uit Polen aangehouden die in Polen en Duitsland sinds 2020 werd gezocht voor meerdere drugs- en geweldsincidenten. Hij wordt onder meer verdacht van een gewelddadige beroving in 2021 in de Poolse stad Krakau, waarbij het slachtoffer om het leven kwam. Ook was K. eerder al in Polen veroordeeld tot 3,5 jaar cel voor drugsdelicten en tot nog een jaar cel voor een geweldsincident in 2019. Na de overval verdween hij. Later werd vastgesteld dat K. niet langer in Polen was, waarna er een internationaal opsporingsbevel werd uitgevaardigd.

FIT
(Flexibel Interventie Team)
De Eenheid Landelijke Expertise en Operaties (LX)

Het FIT controleert auto's op onze snelwegen en houdt bestuurders aan die met grote geldbedragen door ons land rijden. In 2024 heeft het FIT 8,2 miljoen euro contant geld in beslag genomen en in de afgelopen vijf jaar was dit in totaal 46,8 miljoen. Afgelopen jaren waren er auto's waarin een half miljoen of zelfs een miljoen zat verstopt. Soms in verborgen ruimtes, maar ook in een koffer in de achterbak.
Het transport van geld houdt voor een groot deel verband met de handel in verdovende middelen, maar kan ook onderdeel zijn van een systeem van ondergronds bankieren. Het FIT houdt verdachten aan en geld wordt in beslag genomen.

De straf hiervoor varieert van een taakstraf tot een gevangenisstraf van gemiddeld een jaar.
Door het geld te onderscheppen raken ze criminele organisaties in de basis.
De informatie en resultaten van het FIT worden ook gebruikt door andere teams binnen de politie, bijvoorbeeld in onderzoeken naar vormen van financiële criminaliteit of bij de aanpak van criminele samenwerkingsverbanden. Het FIT pakt problemen aan zoals witwassen en de handel in verdovende middelen en wapens.

Daarbij letten collega's bij controles ook op indicaties die kunnen wijzen op zorgfraude of bankhelpdeskfraude, bijvoorbeeld als iemand veel verschillende bankpassen bij zich heeft. In 2024 heeft het team 879 personen aangehouden en bijna 100 rijbewijzen ingevorderd.

Naast contant geld treft het FIT ook andere illegale spullen aan in auto's. Zo werden afgelopen jaar ruim 1400 kilo harddrugs, 860 kilo softdrugs en bijna 9000 xtc-pillen in beslag genomen.
Het team onderzoekt handel in medicijnen, buiten het legale circuit van apotheken en artsen om, en nam dit jaar ruim 22.000 illegale pillen in beslag.

Verder werden ook flinke hoeveelheden lachgas en een tiental vuurwapens en munitie aangetroffen.

Het FIT werkt dag en nacht op de snelwegen en hebben meestal te maken met heterdaad situaties, waarbij ze een verdacht voertuig zien rijden en overgaan tot controle.

FIU
(Financiel Intelligance Unit)

FIU-Nederland) is op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) het centrale meldpunt waar verschillende instellingen, die verplicht zijn tot melden, ongebruikelijke transacties moeten rapporteren.

FIU-Nederland werkt samen met publieke en private partners, zowel nationaal als internationaal, om witwassen, terrorismefinanciering en onderliggende delicten te voorkomen en te bestrijden. Dit helpt om de integriteit van het financiële stelsel te waarborgen.
FIU-Nederland draagt hieraan bij door effectieve financiële inlichtingen te verzamelen en door vroegtijdig nieuwe trends en fenomenen te signaleren, waarover ze hun partners informeren.

De Wwft benoemt verschillende groepen als meldingsplichtige instellingen die fungeren als “poortwachters” van het financiële stelsel. Dit kunnen onder andere kunsthandelaren, banken, notarissen, betaaldienstverleners en casino’s zijn. Deze instellingen moeten hun activiteiten controleren op transacties die mogelijk gerelateerd zijn aan witwassen, onderliggende delicten of terrorismefinanciering.

FIU-Nederland ontvangt deze meldingen van ongebruikelijke transacties. Zij analyseren deze, om te bepalen of de transacties verdacht zijn. Als dat het geval is delen we de verdachte transacties met opsporings-, inlichtingen- en veiligheidsdiensten. Op deze manier versterkt de hele Wwft-keten de integriteit van het financiële stelsel.

Formeel maakt de FIU-Nederland onderdeel uit van de rechtspersoon Staat der Nederlanden.
Beheersmatig is de FIU ondergebracht bij de Nationale Politie als een zelfstandige, operationeel onafhankelijke entiteit.
Door (onder)mandatering beschikt het hoofd FIU-Nederland over de vereiste bevoegdheden ten aanzien van personeel en middelen, waarmee de zelfstandigheid en operationele onafhankelijkheid van de organisatie zijn gewaarborgd.

De beleidslijn loopt rechtstreeks van de minister van Justitie en Veiligheid naar het hoofd van de FIU-Nederland. De beheersmatige lijn loopt via de korpschef van de Nationale Politie naar het hoofd FIUNederland.
De FIU voert analyses uit op ongebruikelijke transacties. Met een nieuwe bevoegdheid die per 1 juli 2026 ingaat kunnen zij, tijdens een analyse een transactie (tijdelijk) laten opschorten die mogelijk gelinkt is aan witwassen, onderliggende delicten of financieren van terrorisme.

FIU-Nederland kreeg deze opschortingsbevoegdheid op grond van de Wwft (artikel 17a). En per 10 juli 2027 staat de bevoegdheid in de nieuwe Implementatiewet ter voorkoming van witwassen en terrorismefinanciering (Iwt, artikel 3.6). In dit artikel focussen we ons op de Wwft-variant van de bevoegdheid.

Wanneer zij een opschortingsverzoek sturen, ben je als entiteit verplicht om hieraan onverwijld opvolging te geven. Dat wil zeggen: zo snel mogelijk en zonder onnodige vertraging. Je houdt de transactie dan maximaal vijf werkdagen tegen. FIU-Nederland kan dit verzoek ook bij jou doen namens een buitenlandse FIU. In dat geval geldt zelfs een termijn van maximaal 10 werkdagen.

In die periode analyseren zij de transactie verder om te beslissen of verdere maatregelen nodig zijn. Na afloop van de termijn beëindigt je dan de opschorting. Het kan ook zijn dat ze je verzoeken om de opschorting eerder te beëindigen dan de gestelde termijn.

Ze zetten deze bevoegdheid alléén in bij een verzoek van een buitenlandse FIU of als hune eigen analyse hiertoe aanleiding geeft. Er zijn dan sterke aanwijzingen van witwassen, onderliggende delicten of terrorismefinanciering. Een proportionele inzet is altijd het uitgangspunt.
Door het opschorten van een transactie voorkomen ze dat crimineel geld wordt weggesluisd en zorgen ze ervoor dat er tijdig passende maatregelen genomen kunnen worden. Bijvoorbeeld beslag door opsporingsdiensten.

Veel buitenlandse FIU's hebben deze bevoegdheid al. Nu dit ook voor Nederland gaat gelden, bevordert dat de internationale samenwerking. Zo kan een buitenlandse FIU vragen om een transactie op een Nederlandse bankrekening op te laten schorten. Andersom kunnen zij dit ook vragen aan een buitenlandse FIU. Dit versterkt de internationale aanpak van witwassen en terrorismefinanciering.
FIU-Nederland kan wettelijk elke meldingsplichtige entiteit vragen om een transactie op te schorten. In de praktijk gaat het vooral om banken, crypto- en betaaldienstverleners.

In het huidige betalingslandschap vinden veel transacties bijna realtime plaats (instant payments). Hierdoor kan het voorkomen dat de op te schorten transacties al (gedeeltelijk) zijn uitgevoerd. In zulke gevallen is opschorten niet mogelijk en dien je een tegoed ter grootte van de transactie(s) te blokkeren. Je blokkeert dan alleen het aanwezige saldo op het moment van het verzoek tot opschorting.

Wanneer er geen saldo beschikbaar is, is dit uiteraard niet mogelijk. Geld dat later op de rekening wordt gestort, valt niet onder het betreffende opschortingsverzoek.

Als de termijn van de opschorting is verlopen, moet het geblokkeerde tegoed worden vrijgegeven, tenzij de opsporing hierop beslag legt. Doet FIU-Nederland het opschortingsverzoek namens een buitenlandse FIU? Dan ligt het initiatief voor beslaglegging bij een buitenlandse opsporingsdienst, die via een rechtshulpverzoek beslag kan laten leggen.

Als meldingsplichtige entiteit kun je niet aansprakelijk worden gesteld voor eventuele economische schade die je cliënt lijdt als je zo'n een opschortingsverzoek opvolgt. Dit staat in artikel 20c Wwft

Naast de Nederlandse aanpak zijn er ook op Europees niveau nieuwe regels op komst: het 'AML-pakket' (Anti Money Laundering).

Het doel is de antiwitwasregels in de hele EU te harmoniseren en toezicht beter te organiseren. Ook in dit pakket krijgen FIU's een opschortingsbevoegdheid, met een iets ruimere reikwijdte. Het Europese AML-pakket gaat medio 2027 in.

FRONTEX
(Frontières extérieures/buitengrenzen).

Frontex is het Europees Grens- en Kustwachtagentschap dat verantwoordelijk is voor de coördinatie van de externe grenzen van de Europese Unie. Het werd opgericht in 2004 en heeft zijn hoofdzetel in Warschau. Frontex ondersteunt de lidstaten bij grensbeheer, migratiecontrole en de bestrijding van grensoverschrijdende criminaliteit, zoals mensensmokkel en illegale migratie.

De kerntaken van Frontex omvatten het plannen en uitvoeren van gezamenlijke grensoperaties, het leveren van technische en operationele middelen aan lidstaten, en het trainen van grensbewakingspersoneel.
Het agentschap verzamelt en analyseert informatie over migratiebewegingen en veiligheidsdreigingen aan de EU-buitengrenzen en ontwikkelt risicobeoordelingen en operationele strategieën op basis van deze gegevens. Frontex kan eigen operationele teams inzetten of lidstaten ondersteunen met gespecialiseerd personeel, patrouilles, surveillanceapparatuur en snelle interventiemiddelen.

Het agentschap werkt nauw samen met nationale grensdiensten, Europol, Eurojust en andere EU-agentschappen om grensoverschrijdende criminaliteit te bestrijden en de veiligheid van de EU-buitengrenzen te waarborgen.
Het agentschap heeft geen wetgevende macht en kan geen strafrechtelijke beslissingen nemen; het functioneert als coördinerend, ondersteunend en analyserend orgaan.
Frontex speelt een centrale rol in gezamenlijke operaties en projecten die grensbeheer combineren met de opsporing van misdrijven zoals mensensmokkel, mensenhandel en de verspreiding van illegale goederen.

GrIT
(Grensverleggende IT)

Defensie heeft in de eerste helft van 2025 stappen gezet met het programma Grensverleggende IT (GrIT). De derde release van dit programma was vooral gericht op het ontwikkelen van IT-systemen die militairen nodig hebben om het eigen grondgebied en dat van bondgenoten te beschermen.
De voorbereidingen voor grootschalige productie zijn inmiddels afgerond. Ook zijn de eerste 9 prototypes van de verschillende varianten van de Modules Ontplooid in elkaar gezet. Daarmee komt de inzet van deze nieuwe technologie in het veld langzaam in zicht.

Verder is nu een deel beschikbaar van de diensten van het Private Cloud Platform. Dit biedt Defensie een veilige en flexibele cloudomgeving. De eerste proeven met het overzetten van applicaties naar dit systeem zijn gestart. Ook is het Protected Core Network uitgebreid, onder meer met een speciaal segment voor satellietgrondstations.

In de tweede helft van dit jaar staat de vierde release van het programma gepland. Daarbij wordt de productiecapaciteit verder opgevoerd. Ook worden dan meer clouddiensten opgeleverd en het netwerk verder uitgebreid. Daarnaast wordt de nieuwste versie van een communicatieplatform aan de modules gekoppeld. Het doel is dat 90 procent van de krijgsmacht binnen 2 jaar na de start van deze fase toegang heeft tot de nieuwe modules.
De nieuwe IT-voorzieningen zijn essentieel voor een moderne krijgsmacht. Ze zorgen ervoor dat militairen sneller en veiliger kunnen werken, zowel in Nederland als tijdens internationale missies. Het programma GrIT speelt daarmee een belangrijke rol in de digitale toekomst van Defensie.

HARC-NZKG

Het HARC-NZKG-team is een gespecialiseerd samenwerkingsverband van Nederlandse opsporings- en handhavingsdiensten, gericht op de bestrijding van drugssmokkel en aanverwante criminaliteit in het Noordzeekanaalgebied (NZKG). De naam staat voor Haven Aanpak Rotterdam Criminele (HARC), maar in deze context is het een gezamenlijke aanpak die is aangepast aan het NZKG, het gebied rond de havens van Amsterdam, IJmuiden en Velsen.

Het team opereert onder supervisie van het Openbaar Ministerie Amsterdam en richt zich op grootschalige import van verdovende middelen, zoals cocaïne, via logistieke knooppunten.De oprichting van HARC-NZKG werd op 12 juni 2025 officieel bekrachtigd met een samenwerkingsovereenkomst tussen de betrokken partijen, waaronder de Douane, de Fiscale Inlichtingen- en Opsporingsdienst (FIOD), de politie en andere handhavingsinstanties.

Dit structurele verbond, voor een minimale duur van vijf jaar, bouwt voort op de succesvolle HARC-model uit Rotterdam, dat sinds 2018 drugscriminaliteit in de Rotterdamse haven aanpakt. Het NZKG, met zijn strategische ligging en hoogwaardige infrastructuur, is kwetsbaar voor misbruik door criminele netwerken, die containers en scheepstransporten inzetten voor smokkelroutes uit Zuid-Amerika en West-Afrika.

Het team coördineert intensieve controles, intelligence-uitwisseling en gezamenlijke operaties om criminelen af te schrikken en hun logistieke methoden in kaart te brengen. Belangrijke pijlers zijn het versterken van de informatiepositie, het delen van data over verdachte zendingen en het ontmantelen van schijnconstructies, zoals dekmantelbedrijven voor drugstransporten

In 2025 leidde HARC-NZKG al tot meerdere recordvangsten, waaronder de onderschepping van bijna 4500 kilo cocaïne op 13 juni 2025 in een container met hout uit Ghana, arriveerde via de Amsterdamse haven.

Deze partij, met een straatwaarde van honderden miljoenen euro's, was bestemd voor een Duits bedrijf dat volgens het OM fungeerde als katvanger.

Het onderzoek in deze zaak, geleid door HARC-NZKG, resulteerde in de aanhouding van een 69-jarige man uit Amsterdam op 5 oktober 2025, die wordt verdacht van import van harddrugs, deelname aan een criminele organisatie en witwassen.

Eerdere arrestaties in het dossier omvatten een 72-jarige uit Chaam als nominale eigenaar van het dekmantelbedrijf en een 42-jarige uit Amsterdam.
Het team verwacht meer aanhoudingen, met focus op geldstromen en internationale verbindingen.HARC-NZKG draagt bij aan een bredere nationale strategie tegen haven-gerelateerde criminaliteit, in lijn met de Havenaanpak van het ministerie van Justitie en Veiligheid.

Door de gezamenlijke aanpak wordt de effectiviteit verhoogd, met nadruk op preventie en langetermijninformatie.

IARPA
(Intelligence Advanced Research Projects Activity)

IARPA investeert in hoogrisico, hoogrendement onderzoek om complexe uitdagingen binnen de Intelligence Community (IC) aan te pakken. IARPA wil de grenzen van de wetenschap verleggen en oplossingen ontwikkelen die het IC effectiever maken, zonder zelf operationele taken uit te voeren, en faciliteert de overdracht van onderzoeksresultaten naar IC-klanten.

Door nauwe samenwerking met IC-agentschappen stemt IARPA onderzoek af op toekomstige behoeften, pakt interagency-uitdagingen aan en coördineert transitiestrategieën. Belangrijke programma's omvatten kwantumtechnologie, biometrie, voorspellingsonderzoek en menselijke taaltechnologie, die wereldwijd toonaangevende doorbraken hebben opgeleverd, waaronder Nobelprijzen, patenten, duizenden publicaties en innovatieve toepassingen die de informatieverwerking en veiligheid binnen de IC hebben getransformeerd.

I&S
(Interceptie & Sensing)

Het expertisecentrum binnen de Nationale Politie dat "alle belangrijke datastromen samenbrengt": IP-taps, sensoren, camera's, etc.
Volgens een officieel besluit (via de overheid) verzorgt I&S "de interceptie voor de Nationale Politie, de Rijksrecherche, de bijzondere opsporingsdiensten en de Koninklijke Marechaussee." I&S valt formeel onder de Landelijke Eenheid van de politie. De politie mag alleen afluisteren/tappen met toestemming: er moet een machtiging komen van de rechter-commissaris, én vaak ook een bevel van de officier van justitie.

De afluisterperiode is wettelijk begrensd: de politie mag maximaal 4 weken tappen zonder verlenging.
Na afronding van de zaak moeten tapgegevens weer worden vernietigd binnen twee maanden (tenzij er uitzonderingen zijn). Er zijn technische problemen geweest met het tapsysteem van de politie. Het nieuw aangeschafte tapsysteem (van Elbit) werkt al jaren niet goed, waardoor de politie terugvalt op oudere systemen van Cognyte/Verint.
De Rijksoverheid (via de Rijksinspectie Digitale Infrastructuur, RDI) beschrijft dat telecomaanbieders wettelijke verplichtingen hebben om taps te faciliteren voor bevoegde diensten, en dat getapte data via I&S worden aangeleverd. Er zijn ook “data-interceptie”-bevoegdheden voor de politie waarmee met technische middelen communicatie of gegevens op geautomatiseerde systemen onderschept mogen worden.
Niet bekend is in hoeverre Palantir behalve voor analyse ook zal worden ingezet voor het tappen zelf nu AI uitstekende notulistenfuncties heeft.

INTERPOL
(International Criminal Police Organization)

Interpol is een wereldwijd samenwerkingsverband van nationale politieautoriteiten dat in 1923 werd opgericht om grensoverschrijdende criminaliteit aan te pakken. Het hoofdkantoor is gevestigd in Lyon, Frankrijk, en het netwerk omvat momenteel 195 lidstaten, waarmee het de grootste internationale politieorganisatie ter wereld is. Interpol faciliteert samenwerking tussen politiediensten van verschillende landen door informatie-uitwisseling, waarschuwingen over criminelen en verdachten, en coördinatie van gezamenlijke operaties. Het beheert centrale databanken met informatie over gestolen eigendommen, vermiste personen, verdachten, valse documenten en criminelen die internationaal actief zijn.