Ministerie van Defensie

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

Onze referentie
MINDEF20260046454

Bij beantwoording, datum, onze referentie en onderwerp vermelden.

> Retouradres Postbus 20701 2500 ES Den Haag

de Voorzitter van de Tweede Kamer
der Staten-Generaal
Bezuidenhoutseweg 67
2594 AC Den Haag

Datum	29 juni 2026
Betreft	Beantwoording Schriftelijk Overleg over de Militaire Inlichtingen- en Veiligheidsdienst

Geachte voorzitter,

Hierbij ontvangt u de antwoorden op de inbreng van de vaste commissie voor Defensie voor het schriftelijk overleg over de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Deze vragen werden ingezonden op 19 juni 2026 met kenmerk 2026Z08580. Waar dat dienstig is zijn gelijkluidende vragen van de leden van de diverse fracties in samengenomen vorm beantwoord.

Hoogachtend,

DE MINISTER VAN DEFENSIE

Dilan Yeşilgöz-Zegerius

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de D66-fractie
De leden van de D66-fractie hebben met belangstelling kennisgenomen van de agenda en de onderliggende stukken voor het schriftelijk overleg over de MIVD. Deze leden onderstrepen het belang van een sterke, wendbare en toekomstbestendige MIVD in een gespannen internationale veiligheidssituatie. Tegelijkertijd benadrukken deze leden dat operationele slagkracht altijd hand in hand moet gaan met rechtsstatelijke waarborgen, onafhankelijke toetsing en toezicht, zorgvuldige parlementaire controle en een veilige werkomgeving voor medewerkers en agenten. Deze leden hebben hierover de volgende vragen.

De leden van de D66-fractie constateren dat de CTIVD het monitoringstraject inzake de zorgplicht voor het mentale welzijn van agenten heeft beëindigd, omdat de MIVD voldoet aan de door de CTIVD opgestelde toetsingscriteria. Tegelijkertijd constateren deze leden dat de minister in de geannoteerde brief schrijft dat enkele verbetermaatregelen nog moesten worden afgerond, waaronder interne opleidingen, trainingen en beleidsdocumenten.

Kan de minister aangeven welke verbetermaatregelen inmiddels volledig zijn afgerond, welke maatregelen nog lopen en wanneer de minister verwacht dat eventuele openstaande verbetermaatregelen worden voltooid? Hoe wordt de structurele borging van deze verbeteringen binnen de MIVD gecontroleerd, ook nu het CTIVD-monitoringstraject is beëindigd? Welke rol speelt het Compliance & Risk Office daarbij, en beschikt deze over voldoende mandaat en onafhankelijkheid om kritisch te rapporteren?

De CTIVD heeft onderzoek gedaan naar de invulling van de zorgplicht door de AIVD en de MIVD voor het mentaal welzijn van hun agenten. Dit onderzoek is gedaan in de vorm van een monitoringstraject. Het doel daarvan was inzicht te krijgen hoe de diensten invulling geven aan hun zorgplicht voor het mentaal welzijn van agenten.

De inzet van agenten is een onmisbaar middel voor de MIVD, maar kan ook risico’s met zich meebrengen op het gebied van fysieke veiligheid en mentaal welzijn van agenten. Om dergelijke risico’s te minimaliseren heeft de MIVD ten aanzien van agenten een zorgplicht. Deze zorgplicht ziet niet alleen op de fysieke veiligheid van de agenten, maar ook op de psychische belasting die verbonden kan zijn aan de inzet van een agent. Om deze reden bereidt de MIVD elke inzet van een agent zeer zorgvuldig en professioneel voor.

De CTIVD heeft geconcludeerd dat de MIVD voldoet aan de toetsingscriteria die de CTIVD gedurende het monitoringstraject heeft opgesteld. Het Compliance & Risk Office is onafhankelijk gepositioneerd binnen de MIVD met een directe lijn naar de dienstleiding en ziet toe op de opvolging van alle aanbevelingen van de CTIVD en de bijbehorende (structurele) implementatie van de maatregelen. De beleidsdocumenten zijn inmiddels opgesteld en er wordt nader invulling gegeven aan de maatregelen voor interne opleidingen en trainingen.

De leden van de D66-fractie onderstrepen het belang van een weerbare defensieorganisatie. Polarisatie en radicalisering kunnen immers ook risico's opleveren voor de veiligheid en integriteit van de krijgsmacht. Welke trends ziet de minister ten aanzien van rechtsextremisme, jihadistisch extremisme en anti-institutioneel extremisme binnen of gericht tegen Defensie? In hoeverre spelen online gemeenschappen en sociale media daarbij een rol?
Welke maatregelen worden genomen om de weerbaarheid binnen Defensie te versterken en is daarbij voldoende aandacht voor preventie, bewustwording en een veilige meldcultuur?

De MIVD verricht onderzoek naar dreigingen van extremisme en terrorisme in relatie tot de Nederlandse krijgsmacht en dit onderzoek richt zich vooral op rechts-extremisme en anti-institutioneel extremisme. De MIVD onderkent rechts-extremistische (aspirant-)defensiemedewerkers die bij Defensie (wilden) werken. De MIVD constateert dat het beeld al enkele jaren gelijk blijft. De MIVD heeft in 2025 ook onderkend dat meerdere defensiemedewerkers het anti-institutioneel gedachtegoed aanhangen en daarnaar handelen. Ook dit beeld is al enkele jaren gelijk. Ook links-extremisme en jihadistisch extremisme zijn aandachtsgebieden van de MIVD.

De onderzoeken van de MIVD naar rechts-extremisme en anti-institutioneel extremisme spelen zich voor een belangrijk deel af in het online domein. Aanhangers van het rechts-extremistisch of anti-institutioneel extremistisch gedachtegoed staan online in contact met gelijkgestemden en consumeren en delen online extremistische content. Dit gebeurt zowel op openbare sociale media als binnen gesloten online gemeenschappen, bijvoorbeeld via versleutelde communicatieplatformen.

Binnen de Defensieorganisatie is geen plek voor extremisme. Om te voorkomen dat personen met extremistische sympathieën bij de krijgsmacht in dienst komen, of hun dienst voortzetten, heeft Defensie zowel het aannamebeleid als het integriteitsbeleid ingericht op het tegengaan van alle vormen van ongewenste gedragingen, waaronder extremisme. Zo worden selectiepsychologen bij Defensie gericht getraind om affiniteit met rechts-extremisme en andere vormen te herkennen tijdens de sollicitatieprocedure. Ook wordt ingezet op het tijdig signaleren van potentieel extremistisch gedrag, het bevorderen van het melden van dit gedrag en het inzetten op een multidisciplinaire aanpak van dit gedrag, door ter zake kundig personeel samen te brengen. Wanneer extremistische gedragingen bij defensiemedewerkers worden vastgesteld, volgen passende maatregelen, variërend van een waarschuwing tot in het uiterste geval ontslag.

De leden van de D66-fractie constateren dat de CTIVD in dit geval gebruik heeft gemaakt van een monitoringstraject en een toezichtbrief, terwijl de Wiv 2017 formeel vooral het toezichtsrapport kent. Deze leden begrijpen de behoefte aan flexibelere toezichtvormen, maar benadrukken dat dit niet mag leiden tot minder transparantie of minder parlementaire controle. Welke lessen trekt de minister uit dit monitoringstraject voor de herziening van de Wiv 2017? Welke nieuwe of aanvullende toezichtproducten zou de CTIVD volgens de minister moeten kunnen gebruiken? Hoe wordt daarbij geborgd dat de Kamer voldoende openbaar of vertrouwelijk wordt geïnformeerd over afgeronde toezichttrajecten? Kan de

minister daarnaast toelichten hoe bij de Wiv-herziening de balans wordt bewaakt tussen operationele wendbaarheid, proportionaliteit, subsidiariteit, onafhankelijke toetsing en effectieve rechtsbescherming?

De afdeling toezicht van de CTIVD heeft sinds 21 mei 2026 een geactualiseerd toezichtprotocol waarin zij beschrijft hoe zij toezicht houdt op de AIVD en de MIVD. Hierin staan ook andere vormen dan het toezichtsrapport dat is genoemd in artikel 113 van de Wiv 2017. De CTIVD noemt bijvoorbeeld een brief of factsheet. Wij onderschrijven het belang van flexibiliteit rondom toezichtvormen, maar vinden het met de D66-fractie belangrijk dat dit niet ten koste gaat van transparantie richting uw Kamer, de parlementaire controle door uw Kamer, en voorzienbaarheid voor de diensten. Om deze reden wordt met de herziening van de Wiv 2017 bezien of en in welke mate een wijziging van de wettelijke grondslag voor de manier van rapporteren door de CTIVD nodig is. Uitgangspunt hierbij is en blijft dat de betrokken minister uw Kamer informeert over de bevindingen van de toezichthouder en de opvolging van eventuele aanbevelingen, zowel openbaar als vertrouwelijk als dat vanwege het staatsgeheime karakter van de bevindingen noodzakelijk is.

De vraag over de balans tussen de operationele wendbaarheid, proportionaliteit, subsidiariteit, onafhankelijke toetsing en effectieve rechtsbescherming wordt op pagina 5 van deze brief beantwoord.

Verder vragen de leden van de D66-fractie hoe de herziene Wiv invulling geeft aan de politieke opdracht om een dreigingsgerichte wet te creëren in overeenstemming met het coalitieakkoord. Op welke punten verschilt de nieuwe dreigingsgerichte Wiv wezenlijk van de huidige Wiv 2017 en hoe wordt de balans tussen slagkracht en toezicht geborgd?

De huidige geopolitieke situatie in de wereld verandert in rap tempo en maakt dat sprake is van een sterk verslechterde veiligheidssituatie. Dit geldt ook voor de dreigingen tegen Nederland. Anno 2026 is het dreigingslandschap fundamenteel anders dan tijdens het opstellen van de huidige Wiv uit 2017. De dreigingen waar we mee worden geconfronteerd hebben een veel diffuser en complexer karakter gekregen. We hebben te maken met sterk toegenomen militaire en hybride dreigingen vanuit Rusland, en ook met bijvoorbeeld stelselmatige spionage, sabotage en ongewenste beïnvloedingsoperaties vanuit China.

Vanwege deze hedendaagse dreigingen vanuit onder andere Rusland en China, en om beter toegespitst te zijn op hun ‘whole-of-government’ en ‘whole-of-society’ benadering, wordt voorgesteld het wettelijk kader voor de nieuwe wet conceptueel anders op te bouwen. Conform het coalitieakkoord 2026-2030 vormt de ontwikkeling van een dreigingsgericht stelsel het uitgangspunt in de nieuwe Wiv, waardoor de diensten tijdig, effectief, en gesterkt door de noodzakelijke waarborgen, kunnen optreden in de huidige hybride en militaire dreigingscontext.

De inlichtingen- en veiligheidsdiensten hebben namelijk een belangrijke taak om ons land tegen dreigingen voor de nationale veiligheid te beschermen. De huidige wet die gericht is op inlichtingenmiddelen biedt de diensten niet langer het kader dat nodig is om effectief en wendbaar

onderzoek te kunnen doen naar de hedendaagse dreigingen. Om diezelfde reden is, in aanvulling op de Wiv 2017, de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen (hierna: Tijdelijke wet) sinds 2024 van kracht waarmee de diensten hun bestaande bevoegdheden onder de Wiv 2017 sneller en effectiever kunnen inzetten. De Tijdelijke wet vervalt van rechtswege op 1 juli 2028. De Wiv 2017 wordt mede daarom herzien.

Dit beogen we onder meer door in de nieuwe Wiv mogelijkheden tot differentiatie te bieden bij het verwerven van gegevens van personen en organisaties die een bijdrage leveren aan doelen en activiteiten die evident strijdig zijn met de Nederlandse (veiligheids)belangen. Dit geldt eveneens voor de wijze waarop de toetsing en het toezicht wordt georganiseerd. Met deze voorstellen willen we de koers voortzetten die met de Tijdelijke wet is ingezet, waarbij effectiever en sneller onderzoeken kunnen worden ingezet naar landen met een offensief cyberprogramma. Ook hiervoor gelden passende waarborgen, maar aangezien deze landen zich regelmatig manifesteren als opponenten van Nederland wordt de lat van noodzaak en proportionaliteit bij de inzet van bevoegdheden eerder gehaald.

Tegen de achtergrond van de diffusere en complexere dreigingen voor de nationale veiligheid wordt ook gekeken naar het actualiseren van benodigde grondslagen voor samenwerking met partners, medeoverheden, kennisinstellingen en bedrijven. Daarnaast zal, gezien de huidige geopolitieke ontwikkelingen en dreigingen waar Nederland en zijn bondgenoten mee worden geconfronteerd, in de wetsherziening uitdrukkelijk aandacht worden besteed aan het effectiever kunnen ondersteunen van de krijgsmacht door de diensten en de MIVD in het bijzonder.

Hoe voorziet de nieuwe Wiv in een juiste balans tussen de inzet van bijzondere bevoegdheden, enerzijds, en toetsing/toezicht, anderzijds? Daarnaast lezen de leden van de CDA-fractie dat wordt ingezet op een werkbare wet die operationele slagkracht en wendbaarheid biedt zonder afbreuk te doen aan fundamentele waarborgen, waarbij geldt: hoe groter de inbreuk, hoe zwaarder de waarborgen. Deze leden onderschrijven dit uitgangspunt. Zij vragen de minister wel hoe deze balans, gezien de toegenomen en snel veranderende dreiging vanuit Rusland, zo wordt vormgegeven dat de diensten ook bij de meest ingrijpende bevoegdheden tijdig en slagvaardig kunnen blijven optreden.

Een doelstelling van de nieuwe Wiv is een wet die beter aansluit bij de opgaven waar de MIVD en de AIVD voor staan. De herziene Wiv heeft ten doel de diensten in staat te stellen om tijdig, effectief, en met de noodzakelijke waarborgen, op te treden in de huidige hybride en militaire dreigingscontext (zie tevens de beantwoording op de voorgaande vraag voor een nadere uiteenzetting van deze dreigingscontext). Hiervoor zijn slagvaardige en wendbare diensten nodig die tijdig en effectief hun rol kunnen vervullen. Om tijdig te kunnen inspelen op dreigingen voor de nationale veiligheid wordt met de nieuwe Wiv gestreefd naar waarborgen bij het verwerven van gegevens die passen bij de aard van de dreiging en de actor. Daarnaast wordt gestreefd naar een eenduidiger kader voor het verwerken van de verworven gegevens, meer mogelijkheden voor samenwerking en betere aansluiting op de krijgsmacht. Een robuust stelsel van toetsing en toezicht is hierbij noodzakelijk, waarbij stevigere waarborgen gelden bij een

grotere inbreuk van de persoonlijke levenssfeer. In de herziening wordt het hele systeem van toetsing en toezicht opnieuw bezien.

Uit de evaluatie van de Wiv 2017 door de Evaluatiecommissie Wiv 2017 (ECW), een rapport van de Algemene Rekenkamer en de ervaringen van zowel de diensten als de toezichthouder in de uitvoeringspraktijk is ten aanzien van het stelsel van toetsing en toezicht een aantal knelpunten naar voren gekomen. Zo was er onduidelijkheid over de taakomschrijving en –afbakening van de toezichthouders, schuurde de dynamische operationele praktijk met statische toetsing vooraf en bleek de omvang van de TIB en CTIVD kwetsbaarheden voor de continuïteit met zich te brengen. Om die reden is het voorstel dat de TIB en de CTIVD opgaan in het College van Toetsing en Toezicht Inlichtingen- en Veiligheidsdiensten (CTT), waardoor geïntegreerd toezicht kan plaatsvinden met voldoende (rechtsstatelijke) waarborgen. Dit voornemen is ook neergelegd in het coalitieakkoord 2026-2030. Hierdoor ontstaat één organisatie, waarbij daarnaast wijzigingen worden voorgesteld om de onafhankelijkheid van deze toezichthouder sterker wettelijk te verankeren.

Wij onderstrepen daarnaast het belang van intern toezicht. In het wetstraject is daarom ook aandacht voor het creëren van een expliciete grondslag voor een interne compliance- en auditfunctie bij de diensten. Dit onderstreept het belang van intern toezicht. Met een wettelijk neergelegde interne compliance- en auditfunctie wordt uiting gegeven aan het toenemende belang van stevig ingebed, effectief en onafhankelijk intern toezicht. Dit past binnen de professionaliseringsslag die de afgelopen jaren reeds door de MIVD en de AIVD is ingezet op dit terrein, zoals ook is geconstateerd door de ECW.

De introductie van een meer dreigingsgerichte wet, zoals bij de beantwoording van de vorige vraag reeds is toegelicht, leidt ook tot fundamentele wijzigingen binnen het stelsel van toetsing en toezicht. Ten aanzien van actoren waarvan een verhoogde en persistente dreiging richting Nederland en Nederlandse belangen uitgaat, bijvoorbeeld China en Rusland, wordt een separaat regime ingericht met een gedifferentieerd en passend waarborgenstelsel. Daarnaast blijft een regime bestaan met haar eigen, passende waarborgen ten aanzien van de overige onderzoeken van de diensten.

De afdeling toezicht van het nieuw te vormen College van Toetsing en Toezicht zal, net als de CTIVD nu, tot taak hebben om toezicht te houden op de rechtmatigheid van alle activiteiten die de diensten uitvoeren ten behoeve van hun wettelijke taakuitvoering. Toezichtsbevindingen worden via de minister aan het parlement aangeboden (zowel openbaar als ter vertrouwelijke kennisneming). De minister legt hierover verantwoording af aan het parlement.

Onderdeel van het voorstel is dat, in voortzetting van de Tijdelijke wet, de afdeling toezicht van het CTT in een beperkt aantal situaties een bindend oordeel kan verbinden aan een toezichtsoordeel. Bindend toezicht wordt op die plaatsen voorgesteld waar een grote inbreuk op grondrechten kan worden gemaakt op het niveau van een individuele burger en/of groepen burgers, zonder dat dit vooraf effectief kan worden getoetst door de afdeling toetsing van het CTT. Deze bindende bevoegdheid geldt als uitzondering en ultimum remedium.

Om balans te brengen in het stelsel van toetsing en toezicht wordt daarom tot slot een beroepsmogelijkheid voorgesteld bij de Afdeling bestuursrechtspraak van de Raad van State (ABRvS) tegen bindende oordelen van het CTT.

En voorziet de nieuwe Wiv in de wettelijke kaders die nodig zijn in geval van een grootschalig conflict?

Vanwege de fundamenteel verslechterde veiligheidssituatie is sprake van een hernieuwde focus van Defensie op hoofdtaak 1; de verdediging van het eigen grondgebied en dat van onze bondgenoten. Naast inlichtingenondersteuning ten behoeve van de militaire besluitvorming op het strategisch niveau, bestaat een groeiende en een noodzakelijke vraag naar meer inlichtingen op het operationeel en tactisch niveau. Dit betekent dat Defensie ook bij het uitvoeren van een militaire operatie onverminderd op de MIVD moet kunnen vertrouwen voor een tijdige en accurate inlichtingenondersteuning. Zo laat de oorlog in Oekraïne zien dat ontwikkelingen zich in razendsnel tempo opvolgen en de MIVD de krijgsmacht iedere minuut van de dag van een update moet kunnen voorzien wanneer daar aanleiding toe is.

Met de voorgenomen dreigingsgerichte wet, waarbij tevens sprake zal zijn van gedifferentieerd toezicht voor actoren waarvan een verhoogde en persistente dreiging richting Nederland en Nederlandse belangen uitgaat wordt voorzien in het voornemen om de nieuwe wet in de basis al zo crisisbestendig mogelijk te maken.

Dat betekent in de eerste plaats dat de mogelijkheden voor inlichtingenondersteuning aan de Nederlandse krijgsmacht worden versterkt. Hierbij kan gedacht worden aan het doeltreffender verstrekken van gegevens, onder meer door de mogelijkheid te creëren om ook onbewerkte gegevens (in de huidige wet ongeëvalueerde gegevens genoemd) aan de krijgsmacht te verstrekken. Juist in (de aanloop naar) een (potentiële) conflictsituatie verlangt het militaire besluitvormingsproces om tijdige en accurate inlichtingenondersteuning. Het verstrekken van onbewerkte gegevens, en in zwaarwegende omstandigheden mogelijk zelfs in bulk, kan vanwege het tijd-kritische karakter of het onderkennen van een directe dreiging gericht tegen de krijgsmacht noodzakelijk zijn. Dit kan onder meer noodzakelijk zijn om de krijgsmacht in de gelegenheid te stellen de betreffende (bron)gegevens te correleren met haar eigen inlichtingenpositie. De veiligheid van het personeel van de krijgsmacht staat daarbij voorop.

Ook kan gedacht worden aan de mogelijkheid om met de krijgsmacht over en weer technische of andere vormen van ondersteuning te bieden. Zowel de MIVD als de krijgsmacht beschikken over technische (inlichtingen)apparatuur en gespecialiseerd personeel. Het efficiënt inzetten van capaciteiten is daarbij, met name in een conflictsituatie, van belang. Daarbij wordt de uit te wisselen capaciteit ingezet onder het juridisch mandaat van de verzoekende partij. Ingeval de MIVD bij haar goede taakuitvoering verzoekt om ondersteuning van de krijgsmacht, wordt de capaciteit van de krijgsmacht (tijdelijk) onder de Wiv gebracht en gelden de van toepassing zijnde waarborgen van toestemming en toezicht. Verder wordt een grondslag gecreëerd om samen te werken met buitenlandse militaire entiteiten.

Ook zet de nieuwe Wiv in op een forse verbreding van het aantal in de wet opgenomen nationale overheidsinstanties dat met de MIVD samenwerkt. Deze samenwerking is, onder andere, noodzakelijk om de veiligheid en paraatheid van de krijsmacht te garanderen. Zo laat onder andere de OPCW-casus uit

2018 zien dat militaire (cyber)dreiging zich ook op Nederlands grondgebied kan manifesteren.[1] Voor het doen van onderzoek en het kunnen treffen van weerbaarheidsbevorderende maatregelen is daarnaast ook samenwerking met private partners van groot belang. Hierbij kan gedacht worden aan samenwerking in het kader van troepen- of materieelverplaatsing over het spoor, water, lucht of de weg. In de nieuwe wet wordt daarom ook een grondslag voor publiek-private samenwerking voorgesteld, waarbij zal worden aangesloten bij de reeds bestaande waarborgenmethodiek, inclusief intern en extern toezicht die de huidige wet voor internationale samenwerking kent.

Inzet in of een aanloop naar een conflictsituatie vraagt veel van de inlichtingenondersteuning door de MIVD. De MIVD zal in zeer hoog tempo gegevens moeten verwerven, verwerken en – veelal in de vorm van een inlichtingenbericht – moeten uitbrengen over het verloop van de situatie, specifiek aan de krijgsmacht ten behoeve van de militaire besluitvorming op het strategisch, operationeel én tactisch niveau. Dit maakt dat voor deze uitzonderlijke gevallen (buitengewone omstandigheden) in dit wetsvoorstel ook enkele bepalingen van staatsnoodrecht voorgesteld worden.

De voorgenomen bepalingen van staatsnoodrecht beogen de MIVD en ook de AIVD in staat te stellen hun taken ingeval van grootschalig conflict of andere buitengewone omstandigheden voort te zetten. Deze bepalingen kunnen enkel in werking worden gesteld als sprake is van een situatie die zodanig ernstig is dat andere opties geen begaanbare weg meer zijn. Het voornemen is te voorzien om de specifieke bepalingen van staatsnoodrecht die in buitengewone omstandigheden noodzakelijk zijn ook separaat in werking te stellen. Aangesloten wordt bij het stelsel van staatsnoodrecht zoals dat onder meer met de Coördinatiewet uitzonderingstoestanden is beoogd. De ministers leggen over de inwerkingtreding en de toepassing van het staatsnoodrecht verantwoording af aan het parlement en de beide Kamers der Staten-Generaal komt zeggenschap toe over de voortduring hiervan.

Ook vragen deze leden zich af of in de nieuwe Wiv wordt voorzien in andersoortige samenwerking met (inter)nationale instanties gezien de hedendaagse dreigingen. Welke waarborgen zijn daarvoor passend?

Samenwerking met nationale en internationale partners is voor de diensten van cruciaal belang voor een goede taakuitvoering. In het huidige tijdsgewricht neemt de noodzaak tot samenwerking verder toe. Dat is gelegen in de exponentiële groei van informatie door verdergaande digitalisering en het in toenemende mate grensoverschrijdende karakter van dreigingen.

Met de Wiv 2017 is een professionaliseringsslag gemaakt voor de samenwerking met internationale partners, onder andere door de introductie van de wegingsnotities. Aan de hand van wettelijke criteria kunnen de diensten bezien of met een beoogde partner een samenwerkingsrelatie kan worden aangegaan en zo ja, wat de aard en intensiteit van de samenwerkingsrelatie kan zijn. Deze methodiek wordt in de nieuwe wet uitgebreid zodat deze beter aansluit bij de operationele praktijk. Hierdoor zijn de waarborgen nu ook van toepassing op militaire evenknieën van de MIVD die in andere landen die bij een krijgsmachtonderdeel zijn ondergebracht.

[1] Tweede Kamer, vergaderjaar 2018–2019, 33 694, nr. 21

Waar op basis van de huidige wet alleen bilaterale samenwerkingsrelaties worden gewogen, geldt deze waarborg in de nieuwe wet ook voor multilaterale samenwerking. Hiermee wordt gehoor gegeven aan de aanbeveling van de ECW.

De leden van de D66-fractie lezen dat de MIVD te maken heeft met een breed en ernstig dreigingsbeeld, waaronder Rusland, China, cyberdreigingen, economische veiligheid, extremisme, contraproliferatie en instabiliteit in verschillende regio's. Ook weegt de focus op Hoofdtaak 1 zwaar mee in de prioriteiten van de dienst. Deze leden begrijpen dat scherpe keuzes nodig zijn, maar vragen hoe de minister voorkomt dat de taakdruk sneller groeit dan de beschikbare capaciteit, juridische kaders en toezichtstructuren.

In de Geïntegreerde Aanwijzing Inlichtingen- en Veiligheidsdiensten (GA I&V) wordt vastgelegd op welke landen en thema's de AIVD en MIVD hun onderzoek moeten richten. De GA I&V komt tot stand in overleg tussen de behoeftestellende departementen en de diensten. In dat overleg moeten vanwege capaciteits- en inzetoverwegingen keuzes worden gemaakt. De diensten dienen na vaststelling uitvoering te geven aan de GA I&V.

Als de taakdruk volgend uit de GA I&V te hoog wordt, dan kan de GA I&V worden aangepast met scherpere prioritering of kan de capaciteit worden verhoogd. In de Defensienota 2026 wordt beschreven hoe Defensie in alle breedte investeert in een sterkere informatiepositie. Inlichtingen zijn cruciaal om een dominante informatiepositie ten opzichte van een tegenstander op te bouwen. Defensie investeert daarom ook in inlichtingentechniek, opleidingen en contra-inlichtingen.

Kan de minister toelichten op basis van welke criteria de MIVD prioriteiten stelt wanneer de vraag naar inlichtingen groter is dan de beschikbare capaciteit? Welke taken of onderzoeksdoelstellingen komen onder druk te staan door de intensivering van het onderzoek naar Rusland en de focus op Hoofdtaak 1? Hoe wordt bij nauwere samenwerking tussen de MIVD, het Netherlands Joint Forces Command en defensieonderdelen geborgd dat rollen, mandaten en verantwoordelijkheden helder blijven, met name bij optreden in het informatiedomein? Kan de minister daarnaast aangeven waar de grootste personele knelpunten bij de MIVD liggen en in welke mate de dienst in 2026 afhankelijk is van externe inhuur?
De leden van de D66-fractie constateren dat de MIVD in toenemende mate moet inspelen op acute crises en een breed scala aan dreigingen. Tegelijkertijd achten deze leden het van belang dat voldoende ruimte blijft bestaan voor strategische analyses en vroegtijdige waarschuwingen, juist om verrassingen te voorkomen en tijdig te kunnen anticiperen op toekomstige ontwikkelingen.

Ook de leden van de SGP-fractie hebben met betrekking tot het jaarplan vragen hoe de behoefte aan nieuw en gekwalificeerd personeel zich verhoudt tot de brede defensieorganisatie, in termen van tekorten op korte en lange termijn.

De MIVD kan in het openbaar niet aangeven waar wel of niet onderzoek naar gedaan wordt. Bij het opstellen van de eerder beschreven GA I&V worden keuzes gemaakt. De keuzes worden gemaakt op basis van de dreigingen die de diensten waarnemen en beleidsprioriteiten van de afnemende departementen.

Het mandaat van de MIVD is vastgelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017). Het Netherlands Joint Forces Command en defensieonderdelen vallen niet onder deze wet. Wel is het mogelijk dat medewerkers van het Netherlands Joint Forces Command en defensieonderdelen op basis van een tijdelijke tewerkstelling worden geplaatst bij de MIVD. Deze medewerkers vallen daarmee vervolgens onder de verantwoordelijkheid van de MIVD en dienen zich aan de Wiv 2017 te houden, waardoor het mandaat van de dienst geborgd blijft.

Het Inlichtingen en Veiligheidsdomein (I&V-domein) van Defensie is de afgelopen jaren fors uitgebreid en de verwachting is dat het I&V-domein ook de komende jaren blijft groeien vanwege de hernieuwde focus van de Krijgsmacht op Hoofdtaak 1. De uitdagingen in deze voorziene groei zitten, zowel bij de MIVD als bij de krijgsmachtonderdelen, in het werven en behouden van voldoende militair I&V-personeel. Defensie investeert daarom bijvoorbeeld in het vormgeven van defensiebrede strategische personeelsplanning voor militair inlichtingen- en veiligheidspersoneel. Hiermee zorgen we dat we in de hele I&V-keten van Defensie voldoende personeel met de juiste kwaliteiten krijgen en behouden.

Externe inhuur bij de MIVD is vooral gericht op ondersteunende onderdelen, denk aan IT, beveiliging, recruitment en opleidingen. Als personeel wordt ingehuurd bij de MIVD dan gelden dezelfde veiligheidseisen als bij vast personeel. Ik kan in het openbaar niet ingaan op de precieze verhouding tussen inhuur en vast personeel bij de MIVD, maar het percentage inhuur is een klein onderdeel van het personeelsbestand van de MIVD.

Hoe wordt gewaarborgd dat de capaciteit voor strategische early warning en langetermijnanalyse voldoende behouden blijft wanneer de druk van actuele crises en operationele ondersteuning verder toeneemt? Is de minister van oordeel dat de huidige balans tussen acute inzet en strategisch inlichtingenonderzoek toereikend is?

We onderschrijven het belang van voldoende capaciteit voor het uitvoeren van strategische analyses en anticipatie op toekomstige ontwikkelingen. In de eerder beschreven GA I&V worden in overleg tussen behoeftestellers en de diensten de onderzoeksdoelstellingen met de gewenste diepgang vastgelegd. Deze onderzoeken zijn goed te plannen. De acute crises of een (potentiele) missie leggen druk op de geplande onderzoeken omdat deze altijd leiden tot een tijdelijke en intensieve extra inlichtingenvraag. Dat betekent dus ook tijdelijke verschuiving van capaciteiten. Zolang dit tijdelijk is zal het effect op de geplande onderzoeken op de langere termijn beperkt zijn. Mocht een crisis of een (potentiele) missie en de daarmee gepaard gaande extra inlichtingenvraag langer voortduren dan is herprioritering in de GA I&V aan de orde.

De leden van de D66-fractie steunen de inzet om cyberdreigingen en technische werkwijzen vaker openbaar te maken wanneer dit bijdraagt aan bewustwording en weerbaarheid. Tegelijkertijd is openbaarmaking alleen effectief als organisaties waarschuwingen ook daadwerkelijk opvolgen. De brief over NCSC-adviezen vermeldt dat essentiële en belangrijke entiteiten onder het concept-Cyberbeveiligingsbesluit schriftelijk moeten vastleggen wat zij doen met attenderingen op kwetsbaarheden of cyberdreigingen.

Kan de minister toelichten hoe in de praktijk wordt gecontroleerd of organisaties voldoende opvolging geven aan adviezen of waarschuwingen van het NCSC, een CSIRT, de MIVD, de AIVD of andere overheidsinstanties? Welke toezichthouder beoordeelt dit, en welke interventies zijn mogelijk wanneer opvolging onvoldoende is? Hoe wordt voorkomen dat de vastleggingsplicht vooral een administratieve verplichting wordt, zonder aantoonbare risicoreductie? Wordt informatie over onvoldoende opvolging gebruikt om toekomstige cyberadviezen concreter en beter uitvoerbaar te maken?

In artikel 17 van het Cyberbeveiligingsbesluit wordt geregeld dat essentiële entiteiten en belangrijke entiteiten, indien zij gerichte attenderingen, adviezen of dreigingsinformatie ontvangen over voor de beveiliging van hun netwerk- en informatiesystemen relevante kwetsbaarheden of cyberdreigingen, moeten beoordelen of op basis daarvan aanpassingen nodig zijn van de maatregelen die zij in het kader van de zorgplicht in de Cyberbeveiligingswet nemen én de uitkomsten daarvan vastleggen. Deze attenderingen, adviezen en dreigingsinformatie kunnen onder andere afkomstig zijn van een CSIRT, de bevoegde autoriteit of een andere betrokken overheidsinstantie. Het zal hierbij in de praktijk veelal gaan om attenderingen, beveiligingsadviezen en dreigingsinformatie die gericht zijn aan de ICT-contactpersoon van de entiteit. Deze attenderingen, adviezen en informatie moeten door de betrokken entiteit niet automatisch worden opgevolgd. Wel moet de betrokken entiteit naar aanleiding hiervan dus beoordelen of er aanvullende of andere maatregelen ter beveiliging van hun netwerk- en informatiesystemen noodzakelijk zijn én de uitkomsten daarvan schriftelijk vastleggen. Op de naleving van deze verplichting wordt, net als bij andere verplichtingen in de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit, toezicht gehouden. Krachtens artikel 15 van de Cyberbeveiligingswet is deze toezichtstaak toegekend aan de ministers die voor de betrokken sectoren verantwoordelijk zijn. Deze ministers zullen op grond van artikel 68 van deze wet de ambtenaren c.q. ambtelijke diensten aanwijzen die in de praktijk met het toezicht zijn belast. Deze sectorale toezichthouders kennen de sector en de entiteiten die zich daarin bevinden. Zij hebben de benodigde expertise om adequaat toezicht te houden. De instrumenten die deze sectorale toezichthouders tot hun beschikking hebben variëren van soft controls tot het toepassen van handhavingsmaatregelen. Voor toezicht en handhaving voorzien de Cyberbeveiligingswet en de Algemene wet bestuursrecht in verschillende wettelijke instrumenten, waaronder de bevoegdheid tot het vorderen van inlichtingen, de bevoegdheid om een bindende aanwijzing te geven en de bevoegdheid om een bestuurlijke boete op te leggen.

Daarnaast onderstrepen de leden van de D66-fractie het belang van economische veiligheid en de bescherming van strategische kennis. Hoe werkt de MIVD samen met kennisinstellingen, bedrijven en Europese partners om ongewenste kennisoverdracht tegen te gaan?

De MIVD en de AIVD informeren waar mogelijk instellingen en bedrijven over de risico's en dreigingen vanuit statelijke actoren waar de diensten aandacht voor hebben. Zo kunnen de diensten hen wijzen op de onderwerpen of technologieën waar actoren interesse in hebben of kunnen de diensten de wijze van ongewenste kennisoverdracht delen. Dit is altijd gericht op het verhogen van de weerbaarheid van de betreffende instelling of het betreffende bedrijf. Daarnaast zoekt de MIVD, waar nodig, samenwerking met internationale partners op om ongewenste kennisoverdracht bij Nederlandse en Europese bedrijven tegen te gaan.

Om dit proces te stroomlijnen en nog effectiever op te kunnen treden tegen ongewenste kennisoverdracht is op 24 maart 2025 het Nationaal Bureau Industrieveiligheid (NBIV) opgericht. Dit is een samenvoeging van twee reeds bestaande industrieveiligheidsentiteiten van de MIVD en AIVD. NBIV staat met het bedrijfsleven in contact om maatregelen ten aanzien van de beveiliging van gegevens en materiaal bij bedrijven te bevorderen die opdrachten voor de Rijksoverheid uitvoeren.

De leden van de D66-fractie constateren dat Rusland zich in toenemende mate bedient van hybride middelen en cyberoperaties, bijvoorbeeld Signal en WhatsApp. Deze leden onderschrijven het belang van een sterke informatiepositie en digitale weerbaarheid. Kan de minister aangeven welke concrete maatregelen binnen de Rijksoverheid en Defensie zijn genomen om accountovername via verificatiecodes, gekoppelde apparaten en impersonatie van supportkanalen tegen te gaan? Bestaat er een Rijksbreed protocol voor het melden, onderzoeken en beperken van schade wanneer een account van een overheidsmedewerker vermoedelijk is gecompromitteerd? Is de minister van oordeel dat de MIVD en de betrokken ketenpartners over voldoende capaciteit beschikken om Nederland weerbaar te houden tegen de snel toenemende cyberdreiging vanuit statelijke actoren?

Cyberspionagecampagnes zoals die van de Russische Federatie gericht op de accounts van Signal en Whatsapp zijn een goed voorbeeld van de cyberdreiging die uitgaat van actoren met een offensief cyberprogramma gericht tegen de Nederlandse belangen. Om de dreiging het hoofd te bieden is het van belang dat de MIVD en ketenpartners hiervoor voldoende geëquipeerd zijn. Het kabinet zet daarom in op het versterken van eigenstandige, unieke inlichtingenposities en samenwerking met andere inlichtingen- en veiligheidsdiensten die snel, doortastend en proactief kunnen handelen. Daarnaast is het beveiligen en veilig houden van de eigen systemen en informatievoorziening een van de primaire taken van Defensie in het cyberdomein, zoals verwoord in de Defensienota 2024 en de Defensie Cyberstrategie 2025.

Om accountovername via verificatiecodes tegen te gaan geldt in algemene zin dat er binnen de Rijksoverheid verschillende kennisproducten zijn waarin staat uitgelegd hoe men dient om te gaan met de digitale werkomgeving. Zoals toegelicht in de beantwoording van het informatieverzoek van het lid Kathmann (PRO)[2], heeft de Rijksoverheid voor medewerkers de gedragsregeling voor de digitale werkomgeving opgesteld en geactualiseerd in oktober 2025. Dit kennisproduct geeft ambtenaren een kader voor het gebruik van berichtenapps, die enkel voor informeel gebruik zijn. Het advies luidt: app met beleid, maar niet over beleid. Dit advies is ook overgenomen en herhaald in het cyberadvies van de AIVD en MIVD *'Phishing via chatapps Signal en WhatsApp'*. Deze lijn is ook onderdeel van de

[2] Kamerstukken II, 2025/2026, 26643, 1508.

basisopleiding digitale weerbaarheid die verplicht is voor alle rijksambtenaren. De gedragsregeling, in combinatie met de basisopleiding, draagt bij aan zorgvuldige omgang met communicatiemiddelen en heeft een risicoreducerend effect op het gebruik daarvan.

Voor Defensie geldt dat er vanwege veiligheid en vertrouwelijkheid geen uitspraken gedaan worden over specifieke dreigingen, operationele werkwijzen van aanvallers of de concrete technische inrichting van eigen beveiligingsmaatregelen. In algemene zin geldt voor Defensie dat een risicogebaseerde benadering wordt gehanteerd voor de bescherming van accounts, identiteiten en communicatiemiddelen. Daarbij worden organisatorische, technische en bewustwordingsmaatregelen toegepast die zijn gericht op het voorkomen, detecteren en beperken van accountovername, misbruik van verificatiemechanismen en social-engineeringaanvallen, waaronder pogingen tot misleiding via digitale communicatiekanalen. Dit omvat in algemene zin maatregelen gericht op het veilig gebruik van verificatiemechanismen, het beheer van gekoppelde apparaten en het vergroten van de weerbaarheid tegen vormen van digitale impersonatie en social engineering.

De leden van de D66-fractie constateren dat kunstmatige intelligentie het inlichtingenwerk ingrijpend verandert en dat ook tegenstanders steeds vaker gebruikmaken van nieuwe technologieën. Deze leden achten het van belang dat de MIVD technologisch voorop blijft lopen, zonder dat dit ten koste gaat van de kwaliteit van analyses en menselijke oordeelsvorming.
Hoe bereidt de MIVD zich voor op de gevolgen van kunstmatige intelligentie voor het inlichtingenwerk? Worden AI-toepassingen reeds ingezet en hoe wordt daarbij menselijke controle geborgd? Beschikt de MIVD over voldoende specialistische kennis om gelijke tred te houden met deze ontwikkelingen? De leden van de D66-fractie zien de beantwoording met belangstelling tegemoet.

Om voorbereid te zijn op de gevolgen van kunstmatige intelligentie moet de MIVD AI kunnen inzetten om AI-gedreven dreigingen van tegenstanders te herkennen, te mitigeren en waar nodig te belemmeren. De MIVD zet AI bijvoorbeeld in bij patroonherkenning, triage, vertaling, documentverwerking en het sneller doorzoeken van grote hoeveelheden data. De inzet van AI is altijd een hulpmiddel, nooit een vervanging van een menselijk oordeel. Het is algemeen bekend dat bij de praktische toepassing AI uitdagingen ondervindt zoals modelveroudering, interpretatie bias en de behoefte aan continue training van personeel. Om risico’s te mitigeren en omdat we onderkennen dat menselijke expertise onmisbaar blijft, investeert de MIVD in het voortdurend observeren en evalueren van modellen om ervoor te zorgen dat ze naar behoren functioneren en dat de kennis van medewerkers actueel is. De MIVD werkt daarnaast nauw samen met Defensie en internationale partners om kennis en ervaringen te delen.

Vragen en opmerkingen van de leden van de PVV-fractie

De leden van de PVV-fractie hebben kennisgenomen van het Openbaar Jaarverslag MIVD 2025 en het Jaarplan MIVD 2026. Naar aanleiding hiervan hebben zij nog enkele vragen.

Interne weerbaarheid
De MIVD waarschuwt terecht voor dreigingen van buitenaf, zoals Rusland, China, cyberaanvallen en sabotage. Tegelijkertijd geven de politieke en militaire leiders van onze belangrijkste NAVO-bondgenoot een opvallende waarschuwing af. Tijdens de Munich Security Conference stelde vicepresident J.D. Vance dat de grootste bedreiging voor Europa niet Rusland, China of een andere externe actor is, maar een dreiging van binnenuit. Ook de Amerikaanse minister van Oorlog Pete Hegseth waarschuwde tijdens de D-Day-herdenking voor een vorm van "invasie" van Europa via massamigratie en open grenzen. Volgens hem wordt Europa niet alleen geconfronteerd met externe tegenstanders, maar ook met ideologieën die zich verzetten tegen de westerse waarden van vrijheid, gelijkwaardigheid, democratie en nationale soevereiniteit.

De leden van de PVV-fractie constateren dat deze waarschuwingen afkomstig zijn van de vicepresident en de minister van Oorlog van de Verenigde Staten, één van onze belangrijkste bondgenoten binnen de NAVO. Hoe beoordeelt de minister deze waarschuwingen in het kader van hybride oorlogsvoering en nationale weerbaarheid?

De veiligheid van Nederland, onze welvaart en onze manier van leven staan onverminderd onder druk. Nederland heeft onder meer te maken met hybride dreigingen. Opponenten proberen verdeeldheid binnen Westerse democratieën en het NAVO bondgenootschap uit te vergroten en te voeden. Zo zien de diensten onder andere dat Rusland en China het liberaal democratisch waardesysteem van de Europese Unie proberen te ondermijnen door middel van desinformatiecampagnes. De diensten doen onderzoek naar beïnvloedingscampagnes van dergelijke vijandelijke actoren. Het detecteren van dreigingen tegen de democratische rechtstaat is een wettelijke taak van de diensten. De diensten doen geen uitspraken over specifieke onderzoeken.

Welke betekenis kent de minister toe aan deze analyse van de Amerikaanse politieke en militaire leiding? Hoe beoordeelt zij de door minister Hegseth gebruikte kwalificatie van een vorm van "invasie"? Ziet zij hierin aspecten die relevant zijn voor de taakuitoefening van de MIVD, mede gelet op het feit dat hybride oorlogsvoering zich niet uitsluitend richt op militaire doelen, maar ook op het verzwakken van de weerbaarheid, cohesie en stabiliteit van samenlevingen? Welke maatregelen neemt Nederland momenteel om zich te beschermen tegen dergelijke vormen van hybride oorlogsvoering en welke rol vervullen de MIVD en Defensie daarbij?

Wij delen de opvatting dat de hybride dreigingen gericht op Nederland en onze bondgenoten toeneemt. De diensten hebben de taak om de dreigingen tegen Nederland en onze bondgenoten tijdig te ontdekken, tegen te gaan en bij te dragen aan de weerbaarheid. De diensten verrichten daartoe onderzoek, leveren relevante inlichtingen en treden daar waar nodig op, binnen de mogelijkheden die de Wet op de inlichtingen- en veiligheidsdiensten 2017 hiervoor biedt. In het geval van hybride dreigingen doen de

diensten onderzoek naar de spionage- en sabotageactiviteiten en beïnvloeding door statelijke actoren in het fysieke en digitale domein. Daarnaast verrichten de diensten onderzoek naar vormen van ongewenste inmenging in Nederland door statelijke actoren en de mate waarin dit een dreiging vormt voor de nationale veiligheid. Ook zetten de diensten in op structureel onderzoek naar economische veiligheid. In het kader van de brede weerbaarheid van de Nederlandse staat tegen hybride en militaire dreigingen is er in 2025 een rijksbreed traject gestart waarin deze weerbaarheid van de Nederlandse staat wordt versterkt.[3]

Rusland
De MIVD concludeert dat de Russische krijgsmacht ondanks de enorme verliezen in Oekraïne groter en effectiever is geworden dan voor de oorlog. Tegelijkertijd heeft Rusland na jaren oorlog zijn oorspronkelijke doelstellingen in Oekraïne nog altijd niet bereikt en volgens de MIVD circa 1,2 miljoen permanente verliezen geleden, waaronder meer dan een half miljoen doden.

Tegen deze achtergrond schrijft de MIVD dat Rusland onder gunstige omstandigheden binnen één jaar na beëindiging van de gevechtshandelingen in Oekraïne voldoende gevechtskracht kan opbouwen om een regionaal conflict met de NAVO te initiëren. Hoe verhouden deze factoren zich volgens de minister tot de inschatting dat Rusland ondanks de omvangrijke verliezen binnen relatief korte tijd opnieuw voldoende gevechtskracht kan opbouwen voor een regionaal conflict met de NAVO? In hoeverre spelen factoren als het verlies van ervaren militairen, de mogelijkheden om nieuwe militairen te werven, demografische ontwikkelingen en het maatschappelijke en politieke draagvlak voor verdere oorlogsvoering daarbij een rol? Hoe weegt de minister deze factoren af bij de inschatting dat Rusland ondanks de omvangrijke verliezen binnen relatief korte tijd opnieuw voldoende gevechtskracht kan opbouwen voor een regionaal conflict met de NAVO, zo vragen de leden van de PVV-fractie.

Moskou kan in de huidige situatie voor 2030 klaar zijn voor een grootschalig gewapend conflict met de NAVO. Mochten grootschalige militaire operaties in Oekraïne eindigen, dan kan de Russische krijgsmacht – onder de meest gunstige omstandigheden voor Rusland – in tenminste een jaar voldoende militair vermogen opbouwen voor een geografisch beperkte oorlog met de NAVO. Deze oorlog is niet gericht op het militair verslaan van de NAVO, maar op het (verder) uiteenspelen van het bondgenootschap. Zolang Rusland in Oekraïne vecht is een grootschalige oorlog tegen de NAVO vrijwel uitgesloten, omdat de lopende oorlog te veel militair vermogen van de Russen vergt. Zorgwekkend blijft wel de opgedane gevechtservaring in Oekraïne en een aantal kwalitatieve verbeteringen in het militair optreden. Die zorgen ondanks de slijtage voor een toegenomen militaire dreiging voor de NAVO.

Ondanks de enorme verliezen, beschikt de Russische Federatie nog steeds over grote personele en materiele reserves. De Russische krijgsmacht beschikt kwantitatief over meer capaciteit dan in 2021. De op dit moment nog ontbrekende randvoorwaarden voor het kunnen voeren van een beperkte oorlog tegen de NAVO is enerzijds munitievoorraden, die Rusland steeds sneller opbouwt door verhoogde productie. Anderzijds is de huidige Russische krijgsmacht getraind voor een statische oorlog in Oekraïne en niet voor een hoog mobiele oorlog in Oost-Europa. De MIVD beoordeelt dat Rusland deze randvoorwaarden binnen een jaar na het beëindigen van grootschalige gevechtsoperaties kan invullen.

[3] Kamerstukken II, 2024/2025, 30821, nr. 249 en 2025/2026, 30821, nr. 326.

Dit betekent dat Oekraïne momenteel niet alleen een eigen oorlog met Rusland uitvecht, maar ook een dreiging van Rusland richting de NAVO afhoudt. Militaire steun aan Oekraïne is daarmee óók een belangrijke investering in onze eigen veiligheid. Tegelijkertijd is Rusland momenteel in staat veel sneller zijn krijgsmacht op te bouwen dan de NAVO. Naar verwachting zal Rusland een direct militair conflict vooralsnog vermijden en activiteiten blijven uitvoeren in de 'grey zone' – wat zowel voor de AIVD als de MIVD de komende jaren grote capaciteit zal vragen. Met de toename van Russisch militair vermogen, zeker na het beëindigen van gevechtsoperaties in Oekraïne, is een conflict een reële mogelijkheid. Gezien de extreem grote impact van een direct conflict tussen Rusland en de NAVO is het van belang ons hierop voor te bereiden. Belangrijk om hierbij te vermelden is dat we thans geen concrete intentie zien vanuit Rusland op dit moment om een militair conflict met de NAVO aan te gaan. De economische situatie in Rusland is tevens ongunstig waardoor onduidelijk is hoe lang Rusland deze oorlog in Oekraïne kan volhouden. Daarbij dient te worden aangetekend dat het absorptievermogen van economische malaise door de Russische maatschappij aanzienlijk hoger ligt dan in het Westen wel eens wordt ingeschat.

Welke gevolgen verbindt de minister aan deze analyse voor de Nederlandse defensieplanning en voor de omvang, gereedheid en uitrusting van de Nederlandse krijgsmacht? Kan de minister toelichten welke aannames aan deze analyse ten grondslag liggen? Waarom acht de MIVD juist een termijn van één jaar realistisch en wat verstaat zij precies onder de in het jaarverslag genoemde "gunstige omstandigheden"?

De analyse benadrukt het belang van het versneld gereedstellen van de Nederlandse krijgsmacht. In het openbaar kan ik niet ingaan op de precieze aannames die ten grondslag liggen aan deze analyse. Bij het naar buiten brengen van dit soort informatie kijkt de MIVD steeds nauwlettend naar het doel - het vergroten van het maatschappelijk bewustzijn en daarmee het versterken van de weerbaarheid van de Nederlandse samenleving - en tegelijkertijd het niet naar buiten brengen van inlichtingen die de nationale veiligheid weer in gevaar kunnen brengen. Door dieper in te gaan op de onderliggende bronnen en informatie die ten grondslag hebben gelegen aan deze analyse, zouden de diensten de nationale veiligheid en daarmee ook de weerbaarheid van onze samenleving schade berokkenen. Zie het antwoord hierboven ten aanzien van de vragen over een termijn van één jaar en de in het jaarverslag genoemde "gunstige omstandigheden"..

China

De leden van de PVV-fractie lezen dat de MIVD waarschuwt voor Chinese spionage, kennisverwerving en beïnvloeding. China probeert hoogwaardige technologie en kennis in handen te krijgen en richt zich daarbij ook op kennisinstellingen en bedrijven in Nederland. Hoe groot acht de minister deze dreiging? Zijn universiteiten, onderzoeksinstellingen en defensiegerelateerde bedrijven voldoende beschermd? Hoeveel onderzoeken lopen er momenteel naar Chinese beïnvloedings- en spionageactiviteiten? Zijn er aanwijzingen dat Chinese actoren proberen toegang te verkrijgen tot Nederlandse defensieprojecten, militaire technologie of defensietoeleveranciers? Zo ja, hoe wordt hiertegen opgetreden?

De Chinese dreiging ten aanzien van de Nederlandse technologie en kennisveiligheid is onverminderd hoog. Het verkrijgen van hoogwaardige en unieke kennis en technologie in Nederland is voor China van groot belang voor hun geopolitieke en strategische doelen. Hiervoor zet China een breed scala aan instrumenten in, waaronder klassieke spionage en hoogtechnologische cyberspionage. Ook zijn alle Chinese staatsburgers bij Chinese wet verplicht bij te dragen aan inlichtingenactiviteiten.

De MIVD draagt bij aan de bescherming van universiteiten, onderzoeksinstellingen en defensiegerelateerde bedrijven door waar nodig en mogelijk hen te informeren over de aard, oorsprong of modus operandi van de dreiging van onder meer China, al dan niet met tussenkomst van het ministerie van Onderwijs, Cultuur en Wetenschap, Economische Zaken en Klimaat of Defensie. Hiertoe wordt doorlopend onderzoek verricht.

De mate waarin organisaties voldoende beschermd zijn, hangt daarbij grotendeels af van de opvolging die organisaties zelf geven aan het mitigeren van de risico’s die de MIVD met hen deelt. In deze gezamenlijke verantwoordelijkheid blijft de MIVD de urgentie van de onverminderd hoge dreiging en het belang van mitigerende maatregelen benadrukken.

In het openbaar kan ik niet ingaan op de hoeveelheid onderzoeken die er op dit moment lopen naar Chinese beïnvloedings- en spionageactiviteiten. Zoals gedeeld in het jaarverslag neemt de MIVD structurele Chinese cyberspionage waar die gericht is tegen de westerse defensie-industrie. In algemene zin kan ik delen dat de MIVD, wanneer zij een poging om toegang te verkrijgen onderkennen, de wettelijke basis hebben om een poging te verstoren. Dit kan door het doelwit van de toegangspoging op de hoogte te stellen, zodat zij zelf weerbaarheidsverhogende maatregelen kunnen treffen. Ook kan de MIVD ervoor kiezen zelf toegangspogingen te verstoren.

Welke risico's ziet de minister voor de Nederlandse defensie-industrie als doelwit van spionage, sabotage of cyberaanvallen door statelijke actoren? Zijn er sectoren of bedrijven die volgens de MIVD bijzondere aandacht verdienen? Hoe beoordeelt de minister bestuurlijke samenwerkingsverbanden tussen Nederlandse overheden en Chinese overheden in het licht van de waarschuwingen van de MIVD over Chinese beïnvloeding en spionage?

De Nederlandse defensie-industrie kan doelwit zijn van statelijke actoren omwille van de (hoog)technologische innovatie. De risico’s die hiermee gepaard gaan betreffen onder andere ongewenste kennis- en technologieoverdracht. Via samenwerkingen, spionage of cyberaanvallen bestaat het risico dat ongewenste kennis- en technologieoverdracht plaatsvindt via illegale wijze. De MIVD acht het van belang om te benadrukken dat deze ongewenste kennis- en technologieoverdracht zich ook via legale wijze kan voordoen, bijvoorbeeld door samenwerkingen tussen Nederlandse en Chinese partijen. Ook daar zijn we alert op.

De diensten wijzen al langer op het risico van beïnvloeding of ongewenste kennis- en technologieoverdracht door of via samenwerking met Chinese partijen. De diensten wijzen op de risico’s,

zodat partijen deze kunnen meenemen in hun bredere belangenafweging over het al dan niet aangaan van een samenwerking.

Zoals de diensten reeds in openbare berichtgeving hebben gedeeld, is Nederland een klein, maar hoogontwikkeld land met een uitgebreide kenniseconomie. Verschillende statelijke actoren zijn geïnteresseerd in kennis en expertise op bijvoorbeeld op gebied van halfgeleiders en quantumtechnologie. Zij ontplooien concrete inlichtingenactiviteiten om deze technologie te verkrijgen. De MIVD en de AIVD trachten dit tegen te gaan.

De leden van de PVV-fractie wijzen erop dat de provincie Noord-Brabant recent de banden met haar Chinese zusterprovincie Jiangsu verder heeft aangehaald en een nieuwe vriendschapsverklaring heeft ondertekend. Ziet de minister risico's dat dergelijke contacten kunnen worden gebruikt voor politieke beïnvloeding, kennisverwerving of het creëren van strategische afhankelijkheden? Heeft de MIVD zicht op dergelijke risico's en worden decentrale overheden hierover actief geïnformeerd?

De MIVD signaleert al langer in haar jaarverslagen dat contact met China risico's kent. Dat komt onder andere naar voren in samenwerkingsovereenkomsten, waarbij de kennisuitwisseling veelal niet wederkerig is. De combinatie van China's wettelijke structuren, economische strategie en cybercapaciteiten zorgen ervoor dat kennis en technologie die bedoeld is voor samenwerking, vaak onbedoeld resulteert in een verlies van concurrentie-, wetenschappelijk- en strategisch vermogen voor de Nederlandse partij.

Daarom werkt de MIVD, samen met de AIVD, de afgelopen jaren hard aan bewustzijnsverhogende maatregelen en het informeren van betrokken partijen. Hiermee wordt de weerbaarheid van de Nederlandse kennissector vergroot en draagt de MIVD bij aan de gezamenlijke verantwoordelijkheid om ongewenste kennis- en technologieoverdracht alsmede de creatie van risicovolle strategische afhankelijkheden te voorkomen.

De MIVD is bevoegd met iedere relevante persoon of organisatie informatie te delen ten behoeve van de nationale veiligheid, daartoe behoren ook decentrale overheden. Mocht het voorkomen dat uit inlichtingen de noodzaak verrijst een gesprek aan te gaan met het lokale bestuur, dan gaat de MIVD hiertoe over.

Islamitisch extremisme

De leden van de PVV-fractie lezen dat de MIVD jihadistisch terrorisme expliciet noemt als een van de grootste dreigingen voor de nationale veiligheid. Tegelijkertijd bevat het openbare jaarverslag relatief weinig informatie over de aard en omvang van deze dreiging. Kan de minister nader toelichten waarom jihadistisch terrorisme door de MIVD nog steeds wordt aangemerkt als een van de grootste dreigingen voor de nationale veiligheid? Op welke wijze manifesteert deze dreiging zich momenteel richting Defensie en Nederlandse militaire belangen?

De MIVD verricht onderzoek naar extremisme en (jihadistisch) terrorisme in relatie tot de Nederlandse krijgsmacht, met als doel de verspreiding van extremistisch gedachtegoed en gedrag vroegtijdig te signaleren. Kan de minister aangeven hoe groot de dreiging van islam op dit moment is voor Defensie? Is er sprake van een toe- of afname van signalen van jihadistisch gedachtegoed of jihadistisch extremisme binnen de defensieorganisatie? Hoeveel onderzoeken lopen er momenteel en welke ontwikkelingen ziet de MIVD op dit terrein?

Welke jihadistische organisaties vormen momenteel volgens de minister en de MIVD de grootste dreiging voor Nederland, de Nederlandse krijgsmacht en Nederlandse belangen in het buitenland? Zijn er aanwijzingen dat statelijke actoren direct of indirect steun verlenen aan dergelijke organisaties? Zo ja, om welke landen gaat het en in hoeverre wordt deze steun beschouwd als onderdeel van hybride dreigingen gericht tegen westerse belangen, zo vragen de leden van de PVV-fractie.

Het openbaar jaarverslag van de MIVD rapporteert dat Afrika momenteel het wereldwijde zwaartepunt is van jihadistisch terrorisme. Op verschillende locaties op het Afrikaanse continent zijn meerdere aan al-Qaida en ISIS gelieerde terroristische groeperingen actief. Dit is vooral waarneembaar in Mali, Burkina Faso, Niger, Nigeria en Somalië, maar ook in landen aan de Golf van Guinee, in de Democratische Republiek Congo en in Mozambique.

Het onderzoek van de MIVD naar Afrika richt zich op het tijdig onderkennen en signaleren van strategische en veiligheidsrelevante ontwikkelingen die een (potentiële) dreiging vormen ten aanzien van Nederland, de NAVO en/of (potentiële) missies van de EU. Ik kan hierover in het openbaar geen uitspraken doen. Indien daartoe aanleiding is, worden de geëigende kanalen daarover geïnformeerd.

De MIVD verricht onderzoek naar dreigingen van extremisme en terrorisme in relatie tot de Nederlandse krijgsmacht en dit onderzoek richt zich vooral op rechts-extremisme en anti-institutioneel extremisme. De MIVD ziet op dit moment geen aanleiding om te stellen dat de krijgsmacht enige specifieke aantrekkingskracht heeft ten aanzien van personen met jihadistisch extremistisch gedachtegoed.

In algemene zin geldt zonder meer dat binnen de Defensieorganisatie geen plek is voor extremisme. Om te voorkomen dat personen met extremistische sympathieën bij de krijgsmacht in dienst komen, of hun dienst voortzetten, heeft Defensie zowel het aannamebeleid als het integriteitsbeleid ingericht op het tegengaan van alle vormen van ongewenste gedragingen, waaronder extremisme.

Sabotage en hybride dreigingen

Deze leden lezen dat de MIVD waarschuwt voor sabotage en hybride dreigingen. Welke delen van de Nederlandse vitale en militaire infrastructuur lopen volgens de minister momenteel het grootste risico op sabotage en hybride activiteiten van statelijke actoren? Zijn havens, energievoorzieningen, datakabels en militaire objecten voldoende beschermd? Kan de minister aangeven of militaire complexen, kazernes, munitieopslagplaatsen en andere defensielocaties voldoende zijn beveiligd tegen sabotage, spionage en andere hybride dreigingen?

De MIVD noemt daarnaast een toenemend aantal meldingen van drones boven vitale infrastructuur en militaire locaties. Hoe vaak komt dit voor? Welke landen worden hierbij als mogelijke dreiging gezien? Beschikken commandanten over voldoende bevoegdheden en middelen om hiertegen op te treden?

De inlichtingendiensten werken samen met overheidspartijen en bedrijven in Nederland om de weerbaarheid van kritieke en militaire infrastructuur te verhogen. Over de exacte aard en risico van de dreiging, alsmede de zichtbare en niet zichtbare maatregelen die genomen worden om de dreiging te mitigeren doen we vanuit het oogpunt van operationele veiligheid geen mededelingen. In oktober en november 2025 was er inderdaad een toenemend aantal meldingen van waarnemingen van drones rond kritieke infrastructuur, zoals luchthavens en militaire faciliteiten. De meldingen van oktober en november 2025 hebben zich niet doorgezet in 2026. Attributie is lastig. In algemene zin geldt dat dit soort incidenten passen in het beeld van de hybride dreiging vanuit Rusland. Het vaststellen van Russische betrokkenheid is echter gecompliceerd en kon veelal niet worden bevestigd. Een melding van een drone lopen we uit en we kijken aan wie deze te linken valt. Zelden lukt het een drone in handen te krijgen, wat onderzoek lastig maakt.

Commandanten beschikken over een tijdelijk beleidskader in geval van een gedetecteerde drone. Bovendien beschikken ze over detectiemiddelen. Met de Rijkswet ’Geweldgebruik bewakers militaire objecten’ heeft defensiepersoneel in de uitoefening van de bewakings- en beveiligingstaak een grondslag op te treden tegen drones die een bedreiging kunnen vormen voor te bewaken vaste of mobiele objecten. Het tijdelijk beleidskader voor de bestrijding van drones zal worden verlengd tot 1 juli 2027 en geeft alle uitvoerders (zowel van politie, KMar als Defensie) die mogen optreden tegen drones handvatten voor de beoordeling welke maatregelen tegen drones wanneer proportioneel zijn.

De Noordzee wordt steeds belangrijker voor de Nederlandse energievoorziening, datacommunicatie, economie en nationale veiligheid. Tegelijkertijd waarschuwen de MIVD en bondgenoten voor toenemende dreigingen tegen vitale infrastructuur op zee, waaronder onderzeese datakabels, pijpleidingen, windparken en havenfaciliteiten. Hoe beoordeelt de minister de huidige dreiging voor de Nederlandse belangen op de Noordzee? Beschikt Nederland over voldoende maritieme, militaire en inlichtingenmiddelen om vitale infrastructuur op de Noordzee te bewaken en te beschermen? Welke rol vervullen de MIVD, de Koninklijke Marine en internationale partners hierbij? Heeft Nederland voldoende zicht op activiteiten van Russische schepen en de Russische schaduwvloot in de Noordzee? Kan de minister daarnaast aangeven in hoeverre de snelle uitbreiding van windparken op de Noordzee gevolgen heeft voor toezicht, detectiecapaciteit en militaire operaties op zee? Zijn aanvullende maatregelen noodzakelijk om sabotage, spionage en andere vormen van hybride oorlogsvoering op de Noordzee tegen te gaan?

De leden van de CDA-fractie wijzen in hun inbreng ook op de kwetsbaarheid van vitale onderzeese infrastructuur, zoals internet- en stroomkabels, die steeds vaker doelwit kan zijn van sabotage. Beschikt de MIVD over voldoende capaciteit en middelen om dreigingen tegen deze infrastructuur tijdig te signaleren, en hoe wordt daarbij samengewerkt met de krijgsmacht en internationale partners, zo vragen de leden van de CDA-fractie?

De Noordzee bevat kritieke maritieme infrastructuur en het is de verwachting dat de dichtheid van deze infrastructuur de komende decennia verder toeneemt. Dat betekent een toename van mogelijke doelwitten van spionage en/of sabotage. De MIVD probeert deze dreigingen tijdig te onderkennen en de MIVD werkt daarvoor nauw samen met bijvoorbeeld de Koninklijke Marine en de Kustwacht. Naast het onderzoeken van dreigingen, ondersteunt de MIVD bij het verhogen van de weerbaarheid van overheidsorganisaties, kennisinstellingen en bedrijven van vitale sectoren. De MIVD en de AIVD helpen deze instellingen bij het vergroten van kennis over de gevaren van spionage, sabotage en kennisdiefstal. Dit gebeurt aan de hand van onder meer (technische) publicaties over dreigingen en het delen van concrete handelingsperspectieven. Het fysiek en digitaal beschermen van de vitale infrastructuur op de Noordzee vraagt een civiel-militaire aanpak. Naast militaire inzet vraagt de bescherming ook om het verhogen van weerbaarheid van de infrastructuur, publiek-private informatiedeling en crisisbeheersing. Departementen bundelen daarom hun krachten in een gecoördineerde aanpak. Dit doet het Kabinet in de huidige interdepartementale aanpak, waarbinnen het ministerie van Infrastructuur en Waterstaat een belangrijke coördinerende rol heeft.

De schaduwvloot is in de afgelopen jaren enorm in omvang toegenomen. Sinds de invasie van Rusland in Oekraïne is de schaduwvloot steeds belangrijker geworden voor de Russische oorlogsinspanningen. De regering werkt aan een nationale strategie voor de aanpak van de schaduwvloot. In de Kamerbrief over de stand van zaken van de aanpak schaduwvloot heeft de regering de verschillende sporen geschetst waarlangs de aanpak van de schaduwvloot wordt vormgegeven.[4] Een van de onderdelen is het robuuster maken van nationale wetgeving. Een voorstel daartoe wordt na het zomerreces aan uw Kamer aangeboden.

Cyberdreigingen

De leden van de PVV-fractie constateren dat de MIVD en AIVD recent hebben gewaarschuwd voor Russische pogingen om Signal- en WhatsApp-accounts van militairen, ambtenaren en hoogwaardigheidsbeklеders over te nemen. Hoeveel Nederlandse overheidsmedewerkers zijn hiervan daadwerkelijk slachtoffer geworden? Is daarbij gevoelige informatie buitgemaakt?
Hoe groot acht de minister de dreiging van geavanceerde spyware, zoals Pegasus en vergelijkbare systemen, voor Nederlandse militairen, commandanten en defensiemedewerkers? Kan de minister bevestigen dat de MIVD actief onderzoek doet naar de mogelijke inzet van dergelijke software tegen Nederlandse militairen en defensiebelangen? Welke maatregelen worden genomen om te voorkomen dat operationele informatie, locatiegegevens, communicatie of persoonsgegevens van militairen via dergelijke systemen in handen komen van buitenlandse statelijke actoren?

De MIVD en de AIVD hebben recent gewaarschuwd voor Russische pogingen om Signal- en Whatsapp-accounts van militairen, ambtenaren en hoogwaardigheidsbeklеders over te nemen.
Vanwege operationele redenen kan er niet worden ingegaan op specifieke cijfers met betrekking tot het aantal slachtoffers. De cybercampagne van Rusland is tot op heden nog voortdurend.

[4] Kamerstukken II, 2025-2026, 36124, nr. 57.

Voor de MIVD en de AIVD is het van belang bewustzijn te creëren over deze cybercampagne. Ook wordt er een concreet technisch handelingsperspectief geboden om de weerbaarheid van dit soort campagnes te verhogen.

Voor de dreiging van geavanceerde Spyware geldt dat Defensie vanwege veiligheid en vertrouwelijkheid geen uitspraken doet over specifieke dreigingen, operationele werkwijzen van aanvallers of de concrete technische inrichting van de eigen beveiligingsmaatregelen.

In lijn met het nationale beleid, zet het IT-beleid van Defensie al langer in op wendbare en weerbare communicatie- en informatiesystemen (CIS), en sensor- wapen- en commandosystemen (SEWACO). Ook worden complexe Defensiesystemen gelaagd ingericht voor extra bescherming

Personele veiligheid
Ziet de minister een toename van pogingen van buitenlandse actoren om defensiepersoneel te benaderen, te beïnvloeden of onder druk te zetten? Beschikt de MIVD over voldoende mogelijkheden om dergelijke risico's tijdig te signaleren en tegen te gaan, zo vragen de leden van de PVV-fractie.

Ik kan in het openbaar geen uitspraken doen of er sprake is van een toename van pogingen van buitenlandse actoren om defensiepersoneel te benaderen, te beïnvloeden of onder druk te zetten. Indien daartoe aanleiding is, worden dergelijke pogingen door de diensten gemonitord en onderzocht en worden passende maatregelen getroffen. De geëigende kanalen worden daarover geïnformeerd, indien daartoe aanleiding is. Defensiemedewerkers hebben diverse mogelijkheden om ongewenste benaderingen te melden. Er is een formeel meldingssysteem dat beschikbaar is voor iedere Defensiemedewerker. Bij meldingen van ongewenst benaderingen is het in de praktijk lastig vast te stellen of hier een statelijke actor achter zit. Het onderwerp krijgt in zijn algemeenheid bij herhaling aandacht bij de beveiligings-awarenesscampagnes en wordt er met regelmaat aandacht besteed aan de risico’s van onder andere sociale media.

Ruimtedomein
De MIVD noemt het ruimtedomein als een steeds belangrijker operationeel domein. Hoe beoordeelt de minister de kwetsbaarheid van Nederlandse en bondgenootschappelijke satellietcapaciteiten voor verstoring, sabotage, spionage of andere vijandelijke activiteiten? Beschikt Nederland over voldoende kennis, middelen en internationale samenwerking om dergelijke dreigingen het hoofd te bieden? Welke rol vervullen de MIVD en Defensie hierbij?

Zoals de MIVD in haar jaarverslag benadrukt, wordt Nederlandse en bondgenootschappelijke satellietcapaciteit bedreigd door een breed scala aan antisatellietwapens van landen van zorg. Verstoring van GPS-signalen is aan de orde van de dag. Hiermee wordt niet alleen de krijgsmacht geconfronteerd, maar civiele partijen zoals luchtvaartmaatschappijen hebben hier ook dagelijks last van. In toenemende mate voeren satellieten van landen van zorg tevens nabijheidsoperaties uit waardoor inlichtingen kunnen

worden vergaard of satellieten gesaboteerd kunnen worden. Ook de in open bronnen gerapporteerde ontwikkeling van een nucleair antisatellietwapen door de Russische Federatie is een dreiging waar doorlopend onderzoek op is gericht.

De MIVD bouwt voort op jarenlange ervaring in het onderzoeken van dergelijke dreigingen, en wordt hier in toenemende mate op bevraagd. Nationaal en internationaal neemt het bewustzijn inzake de dreiging in het ruimtedomein toe. Dit is van belang vanwege de afhankelijkheid van de krijgsmacht van satellietcapaciteit voor operaties in alle domeinen. De MIVD investeert de komende jaren in het vergroten van eigenstandige satellietcapaciteit om inzicht in en door middel van het ruimtedomein te vergroten. In nauwe samenwerking met het Commando Lucht- en Ruimtestrijdkrachten worden investeringen in kennis en middelen internationaal afgestemd om de meeste meerwaarde te realiseren ten behoeve van de krijgsmacht.

Capaciteit MIVD
Uit de stukken blijkt dat de MIVD steeds meer taken krijgt. Rusland, China, terrorisme, extremisme, cyberdreigingen, sabotage, proliferatie en het ruimtedomein vragen allemaal aandacht. Beschikt de MIVD over voldoende mensen, middelen en bevoegdheden om al deze dreigingen het hoofd te bieden? Welke onderzoeken of taken blijven momenteel liggen vanwege capaciteitsgebrek? Welke maatregelen neemt de minister om ervoor te zorgen dat de MIVD ook de komende jaren effectief kan blijven opereren, zo vragen de leden van de PVV-fractie.

Zoals eerder beschreven wordt in de GA I&V vastgelegd op welke onderzoeksdoelstellingen en –thema's de AIVD en MIVD zich moeten richten. De GA I&V komt tot stand in overleg tussen de behoeftestellende departementen en de diensten. In dat overleg moeten vanwege capaciteits- en inzetoverwegingen keuzes worden gemaakt. De diensten dienen uitvoering te geven aan de GA I&V. Over welke keuzes worden gemaakt en waar de MIVD wel of geen onderzoek naar doet, worden in het openbaar geen uitspraken gedaan.

Vragen en opmerkingen van de leden van de CDA-fractie
De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het MIVD Jaarplan 2026 en het openbaar jaarverslag 2025 van de MIVD. Deze leden hebben nog enkele vragen en opmerkingen over het dreigingsbeeld vanuit Rusland, de knelpunten en kansen in de uitvoering van het werk van de MIVD, internationale samenwerking, het Caribisch deel van het Koninkrijk en cyberweerbaarheid.

Dreiging Rusland
De leden van de CDA-fractie lezen dat de MIVD beoordeelt dat Rusland onder gunstige omstandigheden binnen een jaar na beëindiging van de gevechtshandelingen in Oekraïne voldoende gevechtskracht kan genereren voor een regionaal conflict tegen de NAVO. De MIVD heeft als doelstelling voor 2024–2030 "gereed voor een grootschalig gewapend conflict". Waar staat de MIVD ten opzichte van haar eigen doelstelling? Is de MIVD inmiddels "gereed voor een grootschalig gewapend conflict"? Zo niet, wat heeft de MIVD hier nog voor nodig?

De MIVD is altijd gereed om bij te dragen aan de veiligheid en verdediging van het Koninkrijk der Nederlanden en de bondgenootschappelijk belangen, onder meer door de ondersteuning van de Nederlandse krijgsmacht, de NAVO en de Nederlandse overheid met tijdige en hoogwaardige inlichtingen. De MIVD werkt hiervoor nauw samen met de AIVD, niet alleen in voorbereiding op een eventuele verdere escalatie naar oorlog, maar ook in het hier en nu, in de zogenoemde *grey zone*. De MIVD stelt zich gereed voor een mogelijk grootschalig conflict terwijl de MIVD de reguliere wettelijke taken blijft uitvoeren en de rol van de MIVD in de *grey zone* steeds belangrijker wordt. Dat vraagt veel van de MIVD.

Het kabinet investeert daarom fors in Defensie, en daarmee ook in de MIVD, onder andere om ervoor te zorgen dat Defensie gereed is voor eventuele inzet in het kader van hoofdtaak 1. Defensie investeert in een sterke informatiepositie, waarin sensoren, inlichtingen en informatiegestuurd optreden nauw met elkaar zijn verbonden. Door te investeren in sensoren, onder meer in het ruimte- en cyberdomein, wordt het vroegtijdig begrip van de veiligheidsomgeving vergroot. Door deze investeringen kan Defensie dreiging zelfstandiger waarnemen en, waar nodig, daar proactief tegen optreden ter afschrikking of verdediging.

De leden van de CDA-fractie lezen ook dat Rusland zijn hybride dreiging steeds vaker vormgeeft via gelaagde netwerken van lokaal gerekruteerde agenten. Tegelijkertijd neemt het aantal dronemeldingen boven vitale en militaire objecten toe, terwijl de herkomst van deze drones vaak niet kan worden herleid. Acht de minister de bevoegdheden van de MIVD toereikend om deze dreiging te onderkennen en tegen te gaan, ook in crisis- of oorlogstijd, en hoe wordt dit in de herziening van de Wiv 2017 geborgd? Is daarnaast het handelingsmandaat toereikend om bij dronewaarnemingen daadwerkelijk te kunnen optreden?

In oktober en november 2025 was er inderdaad een toenemend aantal meldingen van waarnemingen van drones rond kritieke infrastructuur, zoals luchthavens en militaire faciliteiten. Bij dit soort meldingen geldt dat het vaststellen van vermeende Russische betrokkenheid gecompliceerd is en veelal niet kan worden bevestigd, zoals de MIVD ook in het jaarverslag schrijft.

Indien er – om deze of andere redenen – opgeschaald dient te worden, worden op basis van de opgedragen algemene beveiligingsmaatregelen passende aanvullende maatregelen genomen. Bij de herziening van de Wiv wordt bezien op welke wijze effectiever invulling gegeven kan worden aan de wettelijke taak van de MIVD om de krijgsmacht te voorzien in een tijdige en gedegen inlichtingenondersteuning. Een schaalbare en hoogwaardige inlichtingencapaciteit is daarvoor essentieel. De diensten zijn continu bezig de nodige voorbereidingen te treffen op voorspellingen voortkomend uit inlichtingen en de dreigingsanalyse. Dit vereist een doorlopend (en met regelmaat te herzien) proces van prioritering van de inzet van onze mensen en middelen. Zie ook de eerdere antwoorden over de herziening van de Wiv en bevoegdheden van de diensten.

Knelpunten en kansen uitvoering

De leden van de CDA-fractie steunen de groei van de MIVD en de intensivering van de samenwerking met het bedrijfsleven en kennisinstellingen. Deze leden constateren dat de voorgenomen groei van Defensie en de samenwerking met de defensie-industrie leiden tot een sterk toenemende vraag naar veiligheidsonderzoeken. Verwacht de minister knelpunten in de capaciteit van de Unit Veiligheidsonderzoeken (UVO), en blijven de doorlooptijden (in 2025 nog 92,6% binnen acht weken) bij deze groei houdbaar? Volstaat de gewijzigde Wet veiligheidsonderzoeken, die gefaseerd in 2026 in werking treedt, ook wanneer de veiligheidssituatie in Europa verandert?

De Unit Veiligheidsonderzoeken (UVO) heeft structurele maatregelen getroffen om minimaal 90% van de uitgevoerde veiligheidsonderzoeken binnen de wettelijke termijn van acht weken te kunnen blijven afronden. In 2025 heeft de UVO extra gelden gekregen vanuit Defensie om extra personeel voor de UVO te werven om te kunnen voldoen aan de toenemende vraag in 2025 en 2026. Dit personeel zal starten in 2026 om de hogere instroom van veiligheidsonderzoeken, die nu al plaatsvindt, aan te kunnen en te verwerken. De effectiviteit van het nieuwe personeel wordt door instroom- en inwerkperiode pas verwacht eind 2026, begin 2027. Daarnaast heeft de UVO afspraken met behoeftestellers om meer grip te krijgen op vraag en aanbod en zet de UVO in op automatisering en verdere uniformering van de processen waar mogelijk. Daarbij blijven maatwerk en zorgvuldigheid gewaarborgd.

De gewijzigde Wet veiligheidsonderzoeken (Wvo) is primair aangepast om flexibiliteit te bieden aan sectoren waar medewerkers die een vertrouwensfunctie bekleden veelvuldig van werkgever wisselen, en waarbij de werkzaamheden en de locatie nagenoeg hetzelfde blijven. Dat speelt vooral in de burgerluchtvaart. De aangepaste wet introduceert hiertoe de locatiegebonden verklaring van geen bezwaar (vgb). Deze vgb blijft geldig bij een overstap naar een nieuwe vertrouwensfunctie op dezelfde aangewezen locatie. Dit scheelt de UVO in het uitvoeren van veiligheidsonderzoeken doordat er geen nieuw veiligheidsonderzoek uitgevoerd moet worden en leidt tot snellere plaatsing van medewerkers op de functies. In dat opzicht draagt de wet in positieve zin bij aan het beheersen van de doorlooptijden. Voor zover de laatste vraag moet worden opgevat of de Wvo in een veranderende veiligheidssituatie in Europa voldoende ruimte kent voor het betrekken van nieuwe dreigingen, geldt dat de Wvo voldoende beoordelingsruimte biedt om hierop in te kunnen spelen.

De leden van de CDA-fractie lezen dat het streven is om de brede herziening van de Wiv 2017 in de eerste helft van 2026 in consultatie te brengen. Ligt dit traject op schema?

Het streven is na de zomer van 2026 een conceptwetsvoorstel in consultatie te brengen. Beoogd is om het wetsvoorstel uiterlijk 1 juli 2028 in werking te laten treden, aangezien de Tijdelijke wet dan van rechtswege komt te vervallen.

De MIVD streeft samen met de AIVD naar technologisch koploperschap, onder meer op het gebied van kwantumtechnologie en kunstmatige intelligentie. De leden van de CDA-fractie vragen hoe de minister de voortgang hiervan beoordeelt, en hoe wordt voorkomen dat de toenemende samenwerking met bedrijven

en kennisinstellingen zelf een kwetsbaarheid wordt voor de kennisveiligheid. Daarnaast vragen deze leden zich af welke kansen de MIVD ziet in de oprichting van de Defensie Innovatie- en Opschalingsautoriteit.

De MIVD zoekt wanneer opportuun samenwerking met kennisinstellingen en marktpartijen, wat steeds beter verloopt. Het borgen van de kennisveiligheid is een elementaire randvoorwaarde. Om de veiligheid en integriteit te waarborgen zijn bedrijven en instellingen verplicht zich te houden aan beveiligingseisen zoals vastgelegd in de ABRO (voorheen ABDO) indien zij opdrachten uitvoeren voor de Rijksoverheid.

Op 2 juni 2026 bent u geïnformeerd over de stand van zaken rondom de Defensie Innovatie Opschaling Autoriteit.[5] Hoewel de precieze uitwerking nog volgt, sluiten de strategische doelstellingen van de Defensie Innovatie en Opschalingsautoriteit aan bij de opgave van de MIVD. De autoriteit vormt daarmee een waardevol instrument om technologisch koploperschap te verwerven en te behouden.

Internationale samenwerking
Het is voor de leden van de CDA-fractie vanzelfsprekend dat Europa nadrukkelijker zelf verantwoordelijkheid moet nemen voor de eigen veiligheid. Zij vragen welke stappen de MIVD zet om de samenwerking met Europese inlichtingenpartners te verdiepen, binnen zowel EU- als NAVO-verband, en welke rol initiatieven als het Intelligence College Europe daarin vervullen.

De MIVD en de AIVD werken intensief samen met inlichtingen- en veiligheidsdiensten uit andere landen om dreigingen voor de veiligheid van Nederland vroeg te kunnen signaleren. De samenwerking tussen Europese diensten is van oudsher hecht en effectief. De details omtrent de internationale en multilaterale samenwerkingsverbanden zijn geheim. Daarover worden in het openbaar geen mededelingen gedaan.

De Nederlandse diensten ondersteunen ook initiatieven als het Intelligence College Europe (ICE), dat tot doel heeft het versterken van een gezamenlijke Europese strategische inlichtingencultuur. Dit doet het ICE door het bevorderen van dialoog, voornamelijk in wetenschappelijke seminars en cursussen. Het is één van de weinige Europese fora waarin zowel civiele als militaire inlichtingen- en veiligheidsdiensten met academici en beleidsmakers samenkomen. ICE activiteiten leveren een bijdrage aan de verbetering en versterking van Europese zelfstandigheid op inlichtingengebied, maar het is geen operationeel platform voor het delen van inlichtingen.

Caribisch deel van het Koninkrijk / Venezuela
De leden van de CDA-fractie lezen dat de MIVD en de AIVD gezamenlijk onderzoek doen naar de ontwikkelingen in Venezuela en de mogelijke uitstralingseffecten richting het Koninkrijk. Deze leden constateren dat de situatie sinds de beschreven periode is veranderd. Zij vragen de minister om een actuele duiding van de dreiging tegen het Caribisch deel van het Koninkrijk, en hoe wordt geborgd dat de eilandbesturen en hun bevolking tijdig en adequaat over eventuele dreigingen worden geïnformeerd.

[5] Zie ook brief Stand van zaken Defensie Innovatie Opschaling Autoriteit, Kamerstuk 33 009 nr. 178

De MIVD beoordeelt dat er geen verhoogde dreiging bestaat voor het Caribisch deel van het Koninkrijk. Sinds de arrestatie van Maduro in januari groeit de samenwerking tussen Venezuela en de VS. Aanvankelijk richtte die samenwerking zich vooral op de Venezolaanse olie-industrie. Recente berichtgeving wijst echter ook op afstemming en samenwerking op veiligheidsgebied. Zo heeft de VS een militaire oefening in Caracas georganiseerd en meldt zij operaties tegen de criminele groepering *Tren de Aragua* op Venezolaans grondgebied. Zolang deze samenwerking voortduurt, blijft het risico op een nieuwe (militaire) escalatie – en daarmee de bijbehorende risico's voor het Caribisch deel van het Koninkrijk – zeer waarschijnlijk laag.

De Koninkrijksministeries van Defensie en van Buitenlandse Zaken houden de regeringen van Aruba, Sint Maarten en Curaçao geïnformeerd over geopolitieke ontwikkelingen. Ook houdt de commandant in het Caribisch deel van het Koninkrijk de autoriteiten voortdurend op de hoogte. Het is de verantwoordelijkheid van de landen binnen het Koninkrijk om hun parlementen te informeren via het zogenaamde Seniorenconvent. Dat past bij hun autonomie positie binnen het Koninkrijk.

Cyberweerbaarheid

De leden van de CDA-fractie lezen dat de MIVD zich in 2026 nadrukkelijk richt op het verstoren en openbaar maken van cyberoperaties van statelijke en niet-statelijke actoren, en op het in kennis stellen van slachtoffers en het treffen van weerbaarheidsverhogende maatregelen. Zij vragen hoe deze inzet zich verhoudt tot de constatering dat de cybersecuritymaatregelen bij veel organisaties binnen de Rijksoverheid ontoereikend zijn, en hoe wordt geborgd dat attributies en adviezen, van zowel de MIVD als het NCSC, daadwerkelijk leiden tot een hogere weerbaarheid bij getroffen organisaties. Welke structurele maatregelen worden daarnaast genomen naar aanleiding van de bekendmaking dat Russische actoren chataccounts van overheidsmedewerkers compromitteren en zelfs kunnen overnemen?

De MIVD richt zich in 2026 nadrukkelijk op het verstoren en openbaar maken van cyberoperaties van statelijke en niet-statelijke actoren, door het in kennis stellen van slachtoffers en het treffen van weerbaarheid verhogende maatregelen. Een voorbeeld hiervan is het recent uitgebrachte cyberadvies over Signal van 9 maart jl.[6] Dit advies is naar buiten gebracht om bewustzijn te creëren over de malicieuze phising campagne van de Russische Federatie. Tegelijkertijd biedt het advies concreet technisch handelingsperspectief wat kan worden overgenomen om de weerbaarheid tegen de cybercampagne te verhogen.

Het cyberadvies is, net als andere producten van de MIVD, complementair aan bijvoorbeeld algemene kennisproducten over 'social engineering', die het NCSC doorgaans publiceert. Zowel de cyberadviezen als de kennisproducten zijn onderdeel van de structurele maatregelen de worden genomen om o.a. accountcompromitatie van overheidsmedewerkers tegen te gaan of daar in ieder geval adequaat op te kunnen reageren.

[6] Cyberadvies. Phishing via chatapps Signal en WhatsApp | AIVD en MIVD

De leden van de CDA-fractie lezen dat actoren hun cyberaanvallen met behulp van kunstmatige intelligentie automatiseren en daarmee sneller en geavanceerder maken. Welke stappen zet de MIVD om zich ook in de toekomst te blijven wapenen tegen dergelijke, door kunstmatige intelligentie versnelde en steeds geavanceerdere, cyberaanvallen? Daarnaast vragen de leden welke impact deze toenemende cyberdreiging op de samenleving heeft, bijvoorbeeld voor de economische veiligheid, vitale diensten en het vertrouwen van burgers in de overheid.

Geavanceerde AI-modellen spelen in algemene zin op twee manieren een rol in het huidige dreigingsbeeld. Enerzijds kunnen AI-modellen worden ingezet door kwaadwillende om systemen aan te vallen. Zo kan AI worden ingezet om kwetsbaarheden op te sporen, code te ontwikkelen, phishing te personaliseren of grote hoeveelheden data te verwerken. Dit kan ervoor zorgen dat actoren sneller en op grotere schaal cyberaanvallen kunnen uitvoeren. Anderzijds kunnen AI-modellen worden ingezet ter verdediging. Zo kan AI worden ingezet voor detectie van afwijkend netwerkverkeer, het geautomatiseerd controleren van systemen of het reageren op incidenten. Ook hiervoor geldt dat dergelijke processen sneller en op grotere schaal kunnen worden uitgevoerd. Voor specifiekere beantwoording op de impact op de samenleving en economische veiligheid, verwijs ik u door naar de beantwoording van vragen van de leden El Boujdaini en Kathmann over het bericht “AI-model Mythos geprezen en gevreesd lijkt in handen gevallen van onbevoegden”. [7]

Binnen Defensie geldt dat de risico’s van AI op drie manieren wordt gemitigeerd. Er wordt actief ingezet op de eigen cyberveiligheid in alle omstandigheden, zoals beschreven in de Defensie Cyberstrategie. Daarnaast zet Defensie in op de capaciteit om eigen AI capaciteiten van tegenstanders te belemmeren (counter-AI), onder andere in samenwerking met kennispartners. Dit wordt als noodzakelijk geacht om verweer te kunnen geven aan vijandelijk gebruik van AI. Daarnaast wordt ingezet op het vergaren van inlichtingen omtrent de AI-capaciteiten van statelijke actoren met een cyberoffensief programma, zodat tijdig de juiste tegenmaatregelen kunnen worden getroffen.

Vragen en opmerkingen van de leden van de SGP-fractie

De leden van de SGP vernemen graag voor welk type inlichtingenbehoefte inhuur plaatsvindt, onder welke voorwaarden en wat de verhouding is van inhuur ten opzichte van het vaste personeelsbestand.

[7] Kamerstukken II, 2025/2026, 2026Z08988

De inhuur bij de MIVD is vooral gericht op ondersteunende onderdelen, denk aan IT, beveiliging, recruitment en opleidingen. Als personeel wordt ingehuurd bij de MIVD dan gelden dezelfde veiligheidseisen als bij vast personeel. Ik kan in het openbaar niet ingaan op de precieze verhouding tussen inhuur en vast personeel bij de MIVD, maar het percentage inhuur is een klein onderdeel van het personeelsbestand van de MIVD.

Daarnaast vragen zij zich af in hoeverre de Iraanse dreigingsperceptie sinds het opstellen van het jaarplan is toegenomen, gelet op de aanslagen in Amsterdam en Rotterdam die werden opgeëist door Harakat Ashab Al Yamin Al Islamiyyah, waarvan het logo sterke overeenkomsten vertoont met dat van Hezbollah en de IRGC en waarvan beelden werden verspreid via een pro-Iraans propagandakanaal.

Deze aanslagen volgden op oproepen vanuit het Iraanse regime om aanslagen te plegen in het Westen en tegen Joodse doelen. Kan de minister ten slotte aangeven of inmiddels meer duidelijkheid bestaat over een mogelijke relatie tussen de verijdelde aanslag op een synagoge in Heemstede en de eerdere aanslagen?

Zoals beschreven in de fenomeenanalyse ‘Over de grens’ van 2024 en de jaarverslagen van de inlichtingen- en veiligheidsdiensten, ontplooien statelijke actoren verschillende vormen van inmenging in Nederland, waarmee zij op onwenselijke wijze proberen de Nederlandse samenleving en politieke besluitvorming te beïnvloeden. Dat kan zijn in de vorm van zogenoemde transnationale repressie, activiteiten gericht op personen/organisaties die als dreiging of tegenstander worden gezien. Dat kan ook gaan om ondermijnende beïnvloeding, zoals openlijke en heimelijke activiteiten om diasporagemeenschappen of de Nederlandse politiek of publieke opinie te beïnvloeden.

Ik acht dergelijke vormen van statelijke inmenging volstrekt onacceptabel. Iran of door het land aangestuurde groeperingen worden wereldwijd, waaronder in Nederland, in verband gebracht met (pogingen tot) liquidaties op dissidenten, critici en opposanten van het regime. Daarnaast heeft Iran zich ook vaker op Joodse en Israëlische doelwitten in het buitenland gericht.

Uw vragen over in hoeverre de Iraanse dreiging is toegenomen en in hoeverre Harakat Ashab Al Yamin Al Islamiyyah daadwerkelijk betrokken is bij de in uw vraag omschreven aanslagen raakt aan de onderzoek van de AIVD. Daarover kan in het openbaar geen uitspraak worden gedaan. De minister van Binnenlandse Zaken en Koninkrijksrelaties rapporteert hierover via de geëigende kanalen, indien daartoe aanleiding is.

De leden van de SGP-fractie lezen in het jaarverslag dat Turkije een van de routes is die door Rusland en Iran benut worden om strategische goederen in Nederland te verwerven. Welke inspanningen levert Nederland in Europees, NAVO- en bilateraal verband om deze sanctieontwijking tegen te gaan? Erkent de Turkse regering dit probleem?

In algemene zin zet de MIVD zich in tegen sanctieomzeilingen door Rusland, Iran China, Pakistan, Syrië en Noord-Korea. Naast de Verenigde Arabische Emiraten, Kazachstan en China gebeurt dit inderdaad ook via Turkije. De Nederlandse diensten, en daarmee dus ook de MIVD, werken in verschillende internationale coalities samen om dit tegen te gaan. Zo doet de MIVD diepteonderzoek naar verwervende of aankopende actoren ende methoden waarop zij illegaal of ongewenst aan kennis of technologie komen. De opbrengsten van deze onderzoeken deelt de MIVD met partners die hier opvolging aan kunnen geven om weerbaarheidsverhogende maatregelen te treffen of verwerving te voorkomen.

Vragen en opmerkingen van de leden van de Groep Markuszower

De leden van de Groep Markuszower hebben met interesse kennisgenomen van de stukken en hebben geen verdere vragen of opmerkingen.