Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

# 29 924 Toezichtsverslagen AIVD en MIVD

**Nr. 229**

## VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 16 mei 2022

De vaste commissie voor Defensie heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Defensie over de brief van 16 december over het Jaarplan MIVD 2022 (Kamerstuk 29 924, nr. 222) en over de brief van 30 april 2021 over het Openbaar jaarverslag over het jaar 2020 (Kamerstuk 29 924, nr. 212).

De vragen en opmerkingen zijn op 24 februari 2022 aan de Minister van Defensie voorgelegd. Bij brief van 22 april 2022 zijn de vragen beantwoord.

De voorzitter van de commissie,
De Roond

Adjunct-griffier van de commissie,
Mittendorff

kst-29924-229
ISSN 0921 - 7371
's-Gravenhage 2022

**Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersoon**

## VVD

1. **De leden van de VVD-fractie vragen de Minister met betrekking tot de urgente operationele knelpunten als gevolg van het wettelijk kader, die zich vooral manifesteren in het cyberdomein, aan te geven hoe het staat met de stappen om dit te mitigeren.**
   *Antwoord:* Naar aanleiding van de rapporten van de Evaluatiecommissie Wiv 2017 en de Algemene Rekenkamer is een wetswijziging gestart om de Wiv 2017 te herzien. Naar verwachting zal dit traject meerdere jaren in beslag nemen. De contouren van deze wetswijziging zullen middels een hoofdlijnennotitie aan de Tweede en Eerste Kamer worden aangeboden. De uitkomsten van de parlementaire gedachtewisseling worden vervolgens bij het daaropvolgende wetsvoorstel tot wijziging van de Wiv 2017 betrokken.
   Echter, door een toenemende en urgente dreiging in het cyberdomein is besloten tussentijds middels een tijdelijke wet een aantal knelpunten versneld te adresseren. Het kabinet werkt aan een voorstel voor een tijdelijke wet die de diensten in staat moet stellen bestaande bevoegdheden effectiever in te kunnen inzetten in onderzoeken gericht op landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen. Een sluitend systeem van toezicht dat past bij de dynamiek van cyberoperaties maakt deel uit van dit wetsvoorstel. De tijdelijke wet is van 1 tot 18 april 2022 in internetconsultatie geweest. Hiermee wordt tevens gevolg gegeven aan de aangenomen motie van het lid Van der Staaij c.s., waarbij de regering wordt verzocht om zo spoedig mogelijk met een voorstel te komen om de operationele knelpunten in het cyberdomein weg te nemen (Kamerstuk 36 045, nr. 16).
2. **Daarnaast hebben de leden van de VVD-fractie enkele vragen in relatie tot de ABDO-autorisaties.**
   a. **Zij vragen of de prioriteitsstelling in het aantal te autoriseren bedrijven ook betekent dat verzoeken tot autorisatie geweigerd worden, en hierdoor bedrijven een ABDO-status mislopen.**
      *Antwoord:* Nee. Ieder verzoek tot ABDO-autorisatie wordt door Bureau Industrieveiligheid (BIV) van de MIVD in behandeling genomen.
   b. **Deze leden vragen de Minister hierbij tevens aan te geven wat dit in het bijzonder betekent voor MKB-bedrijven en hoe dit strookt met de Nederlandse inspanningen om het Europees Defensiefonds ook toegankelijk te maken voor MKB-bedrijven. De leden van de VVD-fractie vragen of er gevallen zijn van bedrijven die aan EDF-projecten mee willen doen, maar dat nu niet kunnen omdat ze van Defensie geen ABDO-autorisatie krijgen of voortijdig afhaken.**
      *Antwoord:* Er zijn binnen de rijksoverheid structuren ingericht om het bedrijfsleven zo goed mogelijk te ondersteunen met betrekking tot een goede startpositie binnen het Europees Defensie Fonds (EDF), inclusief de mogelijkheden van cofinanciering en advisering. De rijksoverheid heeft de Rijksdienst voor Ondernemend Nederland (RVO) aangesteld om het bedrijfsleven hierover te informeren. Er is een brede Interdepartementale Coördinatie Groep (ICG) ten behoeve van Europese Defensiesamenwerking, deze geeft richting aan de Nederlandse inzet ten aan zien van de Europese defensiesamenwerking en legt

verantwoording af aan de Minister van Defensie en de Minister van Economische Zaken. Het hoofdonderwerp van deze ICG is het Europees Defensiefonds. Bureau Industrieveiligheid (BIV) is niet de primair verantwoordelijke voor EDF. Dit is een interdepartementale verantwoordelijkheid waarbij BIV ondersteunend is. Er zijn geen casussen bekend van bedrijven die niet aan EDF-projecten konden meedoen door het ontbreken van een ABDO-autorisatie. Er wordt door het Bureau Industrieveiligheid geen onderscheid gemaakt in de omvang van bedrijven.

c. **Deze leden vragen of de Minister daarnaast kan aangeven in hoeverre het Bureau Industrieveiligheid kampt het capaciteitstekorten, en wat er wordt gedaan om deze in te lopen dan wel de afdeling te laten groeien om aan de vraag om autorisaties door de verwervende instanties van Defensie te voldoen. Zij vragen in hoeverre de prioriteitsstelling ervoor zorgt dat verwervingstrajecten van Defensie vertraging oplopen, of niet ten volle gebruik kunnen maken van het potentieel van de Nederlandse industrie.**
*Antwoord:* Zie hiervoor het antwoord op vraag 2A. Omdat de dienst de toename in aanvragen had voorzien, is vooruitlopend hierop geïnvesteerd in het BIV.

3. **Daarnaast hebben de leden van de VVD-fractie enkele vragen over de ICT-achterstanden. Met betrekking tot de mededeling dat deze de komende jaren moeten worden ingehaald vragen deze leden welke concrete plannen hiervoor zij en wat het tijdpad is.**
*Antwoord:* Defensie heeft het wegwerken van de IT-achterstanden bij de MIVD als belangrijke prioriteit onderkend en daar sinds de Defensienota 2018 middelen voor beschikbaar gesteld. Vanwege de technische complexiteit, het fundament goed neerzetten, grote veranderambities en IT-inzet voor operationele belangen is het wegwerken van de achterstanden een meerjarige inspanning.
De MIVD heeft hiervoor een strategie opgesteld waarbij elk jaar een uitwerking plaatsvindt van de strategie naar plannen, rekening houdend met de beschikbare personele en financiële middelen. In het wegwerken van de achterstanden en het realiseren van haar veranderambities werkt de MIVD nauw samen met de AIVD en met Defensie.

4. **Daarnaast vragen de leden van de VVD-fractie hoe het zit met de capaciteit voor screening van medewerkers van de MIVD. Tenslotte vragen deze leden hoe het kabinet ervoor zorgt dat de benodigde capaciteit niet in gevaar komt.**
*Antwoord:* Gemiddeld handelen AIVD en MIVD momenteel 94% van de veiligheidsonderzoeken binnen de wettelijke termijn van acht weken af. Bij de uitvoering van veiligheidsonderzoeken naar medewerkers van de AIVD en MIVD is dit percentage gemiddeld 56%. Dit percentage ligt lager, omdat het gaat om intensievere veiligheidsonderzoeken. Als MIVD en/of Defensie uitbreiden dan zal rekening gehouden worden met extra capaciteit voor de Unit Veiligheidsonderzoeken.

## D66

**De leden van de D66-fractie hebben met interesse kennisgenomen van het jaarplan van de MIVD voor 2022 en het jaarverslag van de MIVD over 2020. Deze leden hebben nog enkele vragen.**

1. **De leden van de D66-fractie zijn bezorgd over de verhoogde veiligheidsrisico's die uitgaan van statelijke actoren als Rusland. Deze leden zijn geschrokken van de diverse**

**cyberaanvallen die vanuit Rusland hebben plaatsgevonden in Nederland.**

a. **Zij vragen hoe kwetsbaar de Minister momenteel de Nederlandse veiligheidsstructuur rondom cyber in de verschillende publieke en non-publieke domeinen acht en hoe deze kwetsbaarheid verminderd kan worden.**
*Antwoord:* Cybercriminaliteit, (digitale) spionage, ongewenste buitenlandse overnames en investeringen, inmenging en zelfs sabotage bedreigen het ongestoord functioneren van onze economie en onze samenleving. Deze problematiek komt daarom ook terug in het Cybersecuritybeeld Nederland (CSBN) van de NCTV, in de MIVD en AIVD-jaarverslagen en in het Dreigingsbeeld Statelijke Actoren. Niets doen kan tot grote economische schade leiden doordat het onze concurrentiepositie verzwakt, ons groeipotentieel verlaagt en de democratische rechtsstaat aantast. Het kabinet kiest er daarom in het coalitieakkoord voor om – in een oplopende reeks tot 2027 – structureel 300 miljoen te investeren in de AIVD, MIVD en NCTV. Deze complexe opgave vraagt om een integrale benadering van wat er daadwerkelijk nodig is om Nederland weerbaar te maken. Om hieraan invulling te geven voor het onderwerp cybersecurity werkt het kabinet aan een nieuwe Nederlandse Cybersecuritystrategie (NLCS), gecoördineerd door de Minister van Justitie en Veiligheid. Hierin worden de ambities voor de komende jaren verder uitgewerkt. Het kabinet zal de Kamer hierover medio 2022 informeren.

b. **Deze leden vragen hoe de Minister verder oordeelt over de mogelijke cyberaanvallen die vanuit Nederland op derde landen hebben plaatsgevonden zoals de recente cyberaanval op Oekraïne die deels via Nederland liep en welke maatregelen momenteel tegen dit soort praktijken worden genomen (zie ook recente Kamervragen van het lid Hammelburg).**
*Antwoord:* Misbruik van Nederlandse infrastructuur bij het uitvoeren van digitale aanvallen komt vaker voor. Dergelijke digitale aanvallen worden uitgevoerd vanuit zogenaamde command en control servers. Deze staan wereldwijd in datacenters, waaronder ook in Nederland. Voor datacenters is het vrijwel onmogelijk om te controleren welke servers in Nederland worden ingezet voor dergelijke malafide doeleinden en richting welke landen.
Deze vorm van misbruik kan het internationale imago van Nederland schaden en slecht zijn voor bondgenootschappelijke belangen en de integriteit van de Nederlandse infrastructuur. Ook kunnen Nederlandse organisaties geraakt worden door eventuele tegenacties, zoals het uit de lucht halen van misbruikte infrastructuur door landen die door een digitale aanval getroffen zijn. Verder kunnen bedrijven waarvan de IT-apparatuur onbewust deel uitmaakt van een DDoS-aanval daar een beschikbaarheidsprobleem ervaren. Er kunnen verbindingsproblemen optreden en ook kan een internetprovider de verbinding afsluiten.
Om aanvallen te stoppen, kan zodra duidelijk is om welke partij het gaat, een vordering of bevel worden uitgevaardigd naar de hoster om de server van de betreffende malafide afnemer offline te brengen. In de praktijk is de snellere route gebruikelijk, dan wordt een «notice and take down» (NTD) melding naar de betreffende hoster gestuurd, met de mededeling dat erbinnen zijn netwerk sprake is van onrechtmatige handelingen van afnemers.

Binnen de Cyber Info/Intel Cel (CIIC) brengen NCSC, MIVD, AIVD, Politie en OM dreigingsinformatie bijeen. Hierdoor kan sneller een beeld worden gevormd van nieuwe dreigingen en kunnen belanghebbende organisaties meer en sneller van handelingsperspectief worden voorzien.

2. **De leden van de D66-fractie zien het belang in van de geïntensiveerde samenwerking tussen de MIVD en het Nationaal Cyber Security Center (NCSC). Uit het jaarverslag blijkt dat digitale beveiligingsproducten zoals VPN-servers van Citrix, Fortinet en Pulse Secure alsmede Microsoft Webmail Exchange gewilde doelwitten vanuit Rusland zijn geweest.**

   a. **Deze leden vragen hoe de Minister de huidige veiligheidssituatie rondom deze systemen beoordeelt. Gezien de geïntensiveerde samenwerking tussen bovengenoemde organisaties vragen deze leden hoe vatbaar Nederland is voor Russische cyberaanvallen.**
   *Antwoord:* De capaciteit, kennis en expertise van Rusland, maar ook China, is dermate groot, dat wanneer deze actoren ergens digitaal binnen willen dringen, de slagingskans groot is. Ook kent Nederland een hoge mate van digitalisering. En hoewel er de laatste jaren belangrijke stappen inzake digitale weerbaarheid zijn gezet, is in het Cyber Security Beeld Nederland 2021 nogmaals onderkend dat in algemene zin de weerbaarheid op gebied van cybersecurity nog niet voldoende is. Dit heeft continu de aandacht.

   b. **Welke andere maatregelen volgen er uit deze geïntensiveerde samenwerking om digitale kwetsbaarheden in de Nederlandse samenleving te mitigeren?**
   *Antwoord:* Binnen de Cyber Info/Intel Cel (CIIC) brengen NCSC, MIVD, AIVD, Politie en OM dreigingsinformatie bijeen. Hierdoor kan snel een beeld worden gevormd van nieuwe dreigingen en kunnen belanghebbende organisaties meer en sneller van handelingsperspectief worden voorzien.
   Momenteel werken het NCSC en het Digital Trust Center (DTC) samen met de hosting sector in de Anti-Abuse Network coalitie aan het inrichten van faciliteiten voor het delen van informatie over kwetsbaarheden, in anticipatie op het wetvoorstel Wet beveiliging netwerk- en informatiesystemen (Wbni), dat het delen van deze informatie tussen overheid en brede bedrijfsleven mogelijk moet maken. Daarnaast wordt er gewerkt aan initiatieven[1], waarbij *hosters* wordt gevraagd zich in te spannen om hun netwerken schoon te houden van onrechtmatigheden door zich op private informatiebronnen zoals die van het Nationale Beheersorganisatie Internet Providers (NBIP), aan te sluiten.
   Met betrekking tot DDoS-aanvallen zetten het Ministerie van EZK en het DTC voornamelijk in op preventieve maatregelen die bijdragen aan het voorkomen dat IT-apparatuur, vaak onbewust, kan deelnemen aan een DDoS aanval. Het tijdig installeren van beveiligingsupdates is hierbij cruciaal. Het DTC heeft het belang van updaten opgenomen in de vijf Basisprincipes van veilig digitaal ondernemen en informeert de doelgroep wanneer belangrijke updates beschikbaar zijn voor ernstige beveiligingsproblemen. Ook IoT-apparaten (Internet of Things) worden ingezet om deel uit te maken van een DDoS aanval.
   Door de toename van IoT-apparatuur zet het Ministerie van EZK in op updaten middels de «doe je update» campagne. Deze

[1] Zoals onder andere de *herziening NIB-richtlijn* en *Digital Services Act.*

campagne is met name gericht op consumenten opdat zij zich ook bewust zijn van de risico's en de noodzaak om (IoT) apparaten zoals routers, camera's en printers up-to-date te houden.

c. **Hoe kijkt de Minister naar de bijdrage van niet-vitale sectoren op het veiligheidsrisico van onze samenleving als geheel en het belang van bredere deling van dreigingsinformatie en -trends? Zo vragen de leden van de D66-fractie.**
*Antwoord:* Ook niet-vitale sectoren kunnen uiteraard te maken krijgen met digitale kwetsbaarheden en cyberaanvallen. Daar waar de risico's voor maatschappelijke ontwrichting en schending van nationale belangen het grootst zijn, zijn sectoren geïdentificeerd welke onder de expertise en operatie van het NCSC vallen. In dat geval zijn er gevolgen van nationaal belang, voor onze samenleving als geheel. Ook dreigingen of incidenten bij niet-vitale sectoren kunnen veiligheidsrisico's opleveren. Het DTC versterkt daartoe de weerbaarheid van deze sectoren tegen toenemende cyberdreigingen. Zoals genoemd in de beantwoording bij vraag 2b, wordt gewerkt aan wet/regelgeving om het delen van informatie tussen overheid en het bedrijfsleven verbeteren.

3. **De leden van de D66-fractie zijn bezorgd over de structurele beïnvloedingsoperaties die Rusland uitvoert door middel van sociale media en digitale nieuwsplatforms. Zij vragen op welke manier de geïntensiveerde samenwerking tussen de MIVD en het NCSC geresulteerd heeft in de bestrijding van deze beïnvloedingsoperaties. Welke risico's vinden er momenteel nog hierbij plaats? Wat is de precieze rol van rechts-extremisme in deze beïnvloedingsoperaties? In welke mate is de Nederlandse politiek hierbij betrokken? Wat gebeurt er momenteel om dit te voorkomen? Zo vragen de leden van de D66-fractie.**
*Antwoord:* Hoewel beïnvloedingsoperaties zeker vaak een digitaal element hebben, richt de geïntensiveerde samenwerking tussen onder andere MIVD en NCSC zich primair op cybersecurity vraagstukken. Het gaat hier dus om informatie over cyberdreigingen en -incidenten, niet op beïnvloeding met digitale middelen. Over vragen over operationele aspecten zoals de rol van het rechts-extremisme doet de dienst geen openbare uitspraken. Het kabinetsbeleid voor het tegengaan van desinformatie bestaat uit drie actielijnen: preventie, informatiepositie verstevigen en (zo nodig) reactie. Onder preventie valt een aantal interdepartementale maatregelen zoals weerbaarheid burgers versterken, weerbaarheid politieke ambtsdragers vergroten, transparantie vergroten, pluriform medialandschap behouden. Zie de beleidsbrief van het Ministerie van BZK van 18 oktober 2019, beleidsinzet bescherming democratie tegen desinformatie[2].
Het kabinet zet zich daarbij al langer in om online platformen meer verantwoordelijkheid te laten nemen om de verspreiding van online desinformatie op hun diensten aan te pakken (o.a. Kamerstuk 30 821, nr. 91). De herziening van de Europese gedragscode tegen desinformatie (*Code of Practice against Disinformation*) en het voorstel voor de Digital Services Act zijn hiervoor momenteel de belangrijkste (co-)regulerende voorstellen (zie o.a. Kamerstuk 22 112 nrs. 3050 en 3159). Zoals eerder toegezegd zal uw kamer geïnformeerd worden over het kabinetsstandpunt op de vernieuwde gedragscode desinformatie zodra deze gepubliceerd is. Deze zal naar verwachting voor de

[2] Beleidsbrief van het Ministerie van BZK van, Beleidsinzet bescherming democratie tegen desinformatie, 18 oktober 2019 Kamerstuk 30 821, nr. 91.

zomer gepubliceerd worden. Daarnaast heeft het kabinet onlangs tijdens de informele Telecomraad van 8-9 maart 2022 in Parijs en Nevers gepleit voor proportionele maatregelen om desinformatie te adresseren en te voorkomen in de context van de oorlog in Oekraïne. Daarbij heeft Nederland het belang van betrouwbare informatie over de oorlog in Oekraïne, ook voor Russische burgers, benadrukt. Nederland sprak steun uit voor de oproep van diverse lidstaten richting de grote platforms om meer te doen om desinformatie te adresseren en te voorkomen. In de bijeenkomst werd vastgesteld dat er brede steun was voor de verklaring waarin een oproep werd gedaan aan de grote online platformen om de fundamentele waarden te respecteren en zich aan te sluiten bij de Code of Practice[3].

4. **Ook zijn de leden van de D66-fractie bezorgd over de veiligheidsrisico's die vanuit China komen.**
   a. **Deze leden vragen wat het huidige dreigingsbeeld rondom de Nederlandse hoogwaardige (defensie-) industrie en Chinese spionage is. Gezien het gestelde in het jaarverslag over 2020 dat is gebleken dat vitale infrastructuur, hoogwaardige technologie en militaire systemen een voornaam doelwit vormen van Chinese cyberoperaties, vragen deze leden welke maatregelen de Minister neemt om deze cyberoperaties het hoofd te bieden.**
   *Antwoord:* Zoals ook in het MIVD-jaarverslag over 2020 aangegeven, gaat er van China een ernstige spionagedreiging uit richting de Nederlandse (defensie)industrie. Deze dreiging heeft niet alleen betrekking op wapensystemen in enge zin, maar ook op technologie met een dubbele civiele en militaire toepassing. Deze dreiging is ook in 2022 actueel. Om deze dreiging het hoofd te bieden voert de MIVD doorlopend onderzoek uit.
   b. **Zij vragen welke samenwerkingsverbanden er hierbij plaats vinden zowel op Europees als multilateraal verband en welke verdere politieke stappen er hierbij kunnen worden gezet.**
   *Antwoord:* Veiligheidsrisico's van buitenlandse cyberactoren worden zowel in de EU als in de NAVO besproken. Nederland spant zich hierbij in voor het vergroten van het gedeeld bewustzijn mede met het oog op diplomatieke respons. Zo hebben zowel de EU als de NAVO in juli 2021 middels verklaringen de kwaadwillende cyberactiviteiten afkomstig vanuit Chinees grondgebied veroordeeld en gewezen op het belang van verantwoordelijk statelijk gedrag in lijn met de VN-cybernormen.
5. **De leden van de D66-fractie zijn benieuwd naar het gezamenlijke onderzoek van de AIVD en de MIVD naar landen zoals Iran, die ervan worden verdacht dat zij, in strijd met die internationale verdragen, werken aan het ontwikkelen van massavernietigingswapens en hun overbrengingsmiddelen of daar al over beschikken.**
   a. **Deze leden vragen wat de verwachtingen rondom dit onderzoek zijn. Zij vragen hoe de Minister het huidige risico rondom de nucleaire proliferatie van Iran op de veiligheid in het Midden-Oosten en de veiligheid van Europa beoordeelt.**
   *Antwoord:* De MIVD en de AIVD doen gezamenlijk onderzoek naar de schendingen door Iran van het *Joint Comprehensive Plan of Action (JCPOA)*. Het JCPOA is in het leven geroepen als

[3] Gezamenlijke verklaring over desinformatie en hybride oorlogsvoering: https://presse.economie.gouv.fr/download?id=91749&pn=3020%20-%20Joint%20appeal%20by%20EU%20ministers%20responsible%20for%20digital%20and%20electronic%20

nucleaire deal tussen Iran en de vijf kernwapenstaten[4] plus Duitsland samen met de Europese Unie. Het JCPOA beperkt de Iraanse voorraad van verrijkt uranium en tevens de verrijkingscapaciteit, zodat Iran niet snel een kernwapen kan maken. Sinds de terugtrekking van de VS uit het verdrag in 2018, zien de AIVD en MIVD het aantal technische schendingen door Iran toenemen.

6. **De leden van de D66-fractie hechten grote waarde aan de maatregelen om de economische veiligheid binnen Nederland te verbeteren.**
   a. **Deze leden vragen hoe de Minister specifiek denkt bij te dragen aan de inzet van de MIVD bij het voorkomen van strategische afhankelijkheden in verschillende sectoren.**
   *Antwoord:* Onderzoek van de MIVD naar ongewenste strategische afhankelijkheden betreft met name de nationale veiligheidsaspecten hiervan. Zo doet de MIVD onderzoek naar de betrokkenheid van statelijke actoren bij overnames en investeringen waar een dreiging van uitgaat tegen de nationale veiligheid, of die de inzet van de krijgsmacht kan beperken. Dit kan ook onderzoek omvatten naar leveranciers waar de krijgsmacht van afhankelijk is of naar leveranciers voor vitale infrastructuur waarvan de krijgsmacht afhankelijk is en onderzoek naar ongewenste kennis- en technologieoverdracht. Hierbij werkt de MIVD samen met de strategische partners binnen de rijksoverheid zoals onder andere BZ, BZK, EZK, I&W, OCW en NCTV.
   b. **Wat kan er nog meer gedaan worden?**
   *Antwoord:* Er zijn recent extra middelen toegekend vanuit het coalitieakkoord ten behoeve van maatregelen ter bevordering van economische veiligheid. Daarnaast zijn de afgelopen jaren al enkele maatregelen ingevoerd. Denk hierbij aan het onlangs opgerichte Bureau Toetsing en Investeringen (BTI) van het Ministerie van EZK dat beoordeelt of meldingen van investeringen, overnames en fusies een risico vormen voor de nationale veiligheid. Een wetsvoorstel op dit gebied (Wet veiligheidstoets investeringen, fusies en overnames (Vifo), Kamerstuk 35 880) is op 30 juni 2021 ingediend bij de Kamer. Met de brief van 9 juli 2021(Kamerstuk 31 125, nr. 120) is de Kamer geïnformeerd over de voortgang van het wetgevingstraject voor een sectorale investeringstoets op het gebied van de defensie-industrie. Een ander voorbeeld is het Loket Kennisveiligheid van Ministerie van OCW en de nieuwe Leidraad Kennisveiligheid waarmee de rijksoverheid kennisinstellingen wil ondersteunen bij ongewenste buitenlandse inmenging met gevolgen voor de economische veiligheid op lange termijn.
   c. **In hoeverre kan multilaterale samenwerking hierbij een rol spelen? Zo vragen de leden van de D66-fractie.**
   *Antwoord:* Internationale en multilaterale samenwerking en afstemming is bij dit soort trajecten van groot belang. Nederland zet o.a. in EU-verband in op de bescherming van kritische infrastructuur, bijvoorbeeld middels de EU-cybersecuritystrategie. In het EU Strategisch Kompas is ook aandacht voor economische veiligheid en worden voorstellen gedaan voor het verbeteren van de weerbaarheid van de EU tegen dreigingen op dit gebied.
7. **De leden van de D66-fractie begrijpen de waarde van het doel van de MIVD om een gezaghebbende inlichtingenpositie te hebben.**

[4] China, Frankrijk, Rusland, Verenigd Koninkrijk en de Verenigde Staten

a. **Deze leden vragen wat de huidige situatie omtrent deze gezaghebbende positie is en hoe deze positie verbeterd kan worden. Zij vragen wat hierbij de belemmeringen zijn.**
*Antwoord:* Naar aanleiding van de rapporten van de Evaluatiecommissie Wiv 2017 en de Algemene Rekenkamer is een wetswijziging gestart om de Wiv 2017 te herzien. Naar verwachting zal dit traject meerdere jaren in beslag nemen. De contouren van deze wetswijziging zullen middels een hoofdlijnennotitie aan de Tweede en Eerste Kamer worden aangeboden. De uitkomsten van de parlementaire gedachtewisseling worden vervolgens bij het daaropvolgende wetsvoorstel tot wijziging van de Wiv 2017 betrokken.
Echter, door een toenemende en urgente dreiging in het cyberdomein is besloten tussentijds middels een tijdelijke wet een aantal knelpunten versneld te adresseren. Het kabinet werkt aan een voorstel voor een tijdelijke wet die de diensten in staat moet stellen bestaande bevoegdheden effectiever in te kunnen inzetten in onderzoeken gericht op landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen. Een sluitend systeem van toezicht dat past bij de dynamiek van cyberoperaties maakt deel uit van dit wetsvoorstel. De tijdelijke wet is van 1 tot 18 april 2022 in internetconsultatie geweest. Hiermee wordt tevens gevolg gegeven aan de aangenomen motie van het lid Van der Staaij c.s., waarbij de regering wordt verzocht om zo spoedig mogelijk met een voorstel te komen om de operationele knelpunten in het cyberdomein weg te nemen.

b. **De leden van de D66-fractie lezen dat het streven naar informatiegestuurd optreden (IGO) hierbij centraal staat. Zij vragen welke lessen de MIVD heeft getrokken uit de incidenten die bij het Land Information Manoeuvre Centre hebben plaatsvonden.**
*Antwoord*: De MIVD werkt onder de Wiv 2017. In de Wiv 2017 zijn de bevoegdheden en bijbehorende waarborgen van de MIVD geregeld. Effectieve waarborgen zorgen zowel voor de bescherming van de persoonlijke levenssfeer van burgers als voor de doeltreffende uitvoering van de taken van de diensten ter bescherming van diezelfde burgers.

8. **De leden van de D66-fractie hechten veel waarde aan de beschermende werking van de Wiv 2017.**
a. **Deze leden vragen op welke termijn de herziening van de Wiv kan worden verwacht. Zij vragen hoe de toezichthouders betrokken worden bij het verbeterproces van de Wiv.**
*Antwoord:* Er wordt gewerkt aan een interdepartementale analyse van de aanbevelingen van de evaluatiecommissie Jones-Bos. Bij deze analyse wordt ook het rapport van de Algemene Rekenkamer naar de slagkracht van beide diensten betrokken alsook de uitkomsten van de recente debatten met uw Kamer en de Eerste Kamer en de zienswijzen van de CTIVD en de TIB. Het is de bedoeling om deze brede analyse te laten neerslaan in een hoofdlijnennotitie, waarover wij vervolgens graag met uw Kamer nader van gedachten wisselen. We hechten er grote waarde aan dat na het uitbrengen van de hoofdlijnennotitie en de bespreking daarvan met uw Kamer, de werkzaamheden aan de voorbereiding van een voorstel tot wijziging van de Wiv 2017 voortvarend ter hand worden genomen.

9. **De leden van de D66-fractie zijn enorm bezorgd over de recente polarisering en radicalisering in de Nederlandse maatschappij en in de krijgsmacht.**

a. **Wat gebeurt er naast onderzoek momenteel nog meer om deze risicofactoren te mitigeren?**
*Antwoord:* Onderzoek van de AIVD en MIVD is er primair op gericht dreigingen te onderkennen en anderen in staat te stellen maatregelen te nemen. Dit doen de AIVD en MIVD door ambtsberichten te sturen aan het Openbaar Ministerie of bijvoorbeeld aan de commandant van een defensiemedewerker. De MIVD kan zelf een veiligheidsonderzoek uitvoeren. Dit kan leiden tot het weigeren of intrekken van de Verklaring van Geen Bezwaar die vereist is voor een baan bij Defensie. De AIVD voert eveneens veiligheidsonderzoeken uit. Dit kan leiden tot het weigeren of intrekken van de Verklaring van Geen Bezwaar die vereist is voor een baan buiten Defensie, die als vertrouwensfunctie is aangemerkt.
Commandanten die kennisnemen van tekenen van polariserend of radicaliserend gedrag binnen de krijgsmacht – die ook strafrechtelijke gevolgen zouden kunnen hebben – dienen dit te melden aan de KMar. De krijgsmacht kent voor personeel, naast de KMar en de eigen commandant, meerdere meldpunten waar dergelijk (rechts-)extremistisch gedrag gemeld kan worden. Indien er aanleiding toe is zal de KMar een strafrechtelijk onderzoek starten. Op basis van het «Kader veiligheid in opleidingen» is sociale veiligheid een vast onderdeel van de initiële- en loopbaanopleidingen geworden. Inclusiviteit is een belangrijk deel van sociale veiligheid. Aandacht voor verschillen in opvatting en attitude en hoe dat bespreekbaar te maken is de kern. Polarisatie en radicalisering worden regelmatig besproken in samenhang met de gedragscode Defensie.

b. **Welke politieke elementen kunnen hierbij een rol spelen?**
*Antwoord:* Radicalisering en extremisme op grond van bijvoorbeeld een extreemrechts gedachtegoed kennen een voedingsbodem in, en dragen ook bij aan een toenemende polarisatie in Nederland. Naast de directe impact op de nationale veiligheid betreft het ook een breder maatschappelijk probleem. Het raakt namelijk aan de kern van het functioneren van onze democratische rechtsorde en ondermijnt sociale stabiliteit. Het voorkomen en tegengaan van polarisatie en radicalisering vraagt dan ook een brede inzet van het kabinet.

c. **Hoe gaan andere landen hiermee om?**
*Antwoord:* Zoals reeds vermeld in het openbaar jaarverslag 2020 van de MIVD is de opkomst van rechts-extremisme een wereldwijd fenomeen. Ook in de ons omringende landen is geconstateerd dat deze dreiging complex en veranderlijk is en noopt tot blijvende alertheid. Een effectieve aanpak vereist informatiedeling en een nauwe samenwerking met (inter)nationale en lokale partners. Dit onderwerp heeft dan ook de volle aandacht in bi- en multilaterale overleggen met partners. Het fenomeen is een belangrijk aandachtspunt en zal dat naar verwachting de komende jaren ook blijven.

10. **Tot slot benadrukken de leden van de D66-fractie het belang van expertise binnen de MIVD en het binnenhalen van deze expertise. Deze leden vragen wat de huidige situatie is omtrent het aantrekken van talent in deze sector en wat hierbij de knelpunten zijn. Zij vragen welke maatregelen hieraan bij kunnen dragen.**
*Antwoord:* De dienst zet de komende jaren in op de versterking van de HR-functies met als doel om o.a. werving, loopbaansporen en samenwerking met andere organisaties te versterken op het terrein van strategische personeelsplanning. Denk dan aan gezamenlijke werving inspanningen met het Defensie Cyber Commando, waardoor

er een bredere pool ontstaat van specialisten binnen Defensie op kritieke functies (bijv. hackers).

## CDA

**De leden van de CDA-fractie hebben kennisgenomen van het jaarplan MIVD 2022 en het openbaar jaarverslag van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) over het jaar 2020. Zij hebben nog enkele vragen en opmerkingen.**

1. **De leden van de CDA-fractie lezen in de brief van 16 december 2021 over de hoofdlijnen van het MIVD Jaarplan 2022 dat wordt ingegaan op de middelen die in de Augustusbrief 2021 aan de diensten zijn toegekend en dat in de begroting van 2022 voor het versterken van de MIVD vanaf 2022 structureel 15 miljoen euro beschikbaar is gemaakt. Deze leden merken op dat daar bovenop inmiddels in het coalitieakkoord is vastgelegd dat er de komende jaren meer middelen gaan naar de inlichtingendiensten.**
   a. **De leden van de CDA-fractie vragen hoe de additionele financiële middelen de komende jaren worden besteed.**
   *Antwoord:* Het kabinet wil dat inlichtingen- en veiligheidsdiensten beter in staat zijn om hun slagkracht te benutten en hun capaciteit uitbreiden om nieuwe en toenemende digitale dreigingen en aanvallen van met name statelijke actoren te onderkennen, onderzoeken en te mitigeren, met waarborgen voor goed en effectief toezicht en digitale burgerrechten. Om aan de uiteenlopende complexe uitdagingen te voldoen heeft het kabinet in het coalitieakkoord een oplopende reeks tot 300 miljoen euro structureel in 2027 ter beschikking gesteld aan de AIVD, MIVD en de NCTV.
   b. **Deze leden vragen welke taken en opdrachten extra aandacht krijgen, naast de investeringen die in de brief worden genoemd om de dienst toekomstbestendig te maken.**
   *Antwoord:* De additionele investeringen in de MIVD hebben als primair oogmerk om de dienst over de gehele breedte van de taken en opdrachten te versterken
   c. **Deze leden vragen met betrekking tot de versterking van de slagkracht van de diensten hoe deze groei ten goede komt aan de digitale weerbaarheid van Nederland (en die van de partners).**
   *Antwoord:* De Algemene Rekenkamer heeft geconcludeerd dat de inlichtingen- en veiligheidsdiensten destijds onvoldoende voorbereid en toegerust waren om de Wiv 2017 te implementeren. De additionele middelen stellen de diensten daarom in staat meer capaciteit in te zetten ten behoeve van onderzoek naar de intenties, capaciteiten en modus operandi van statelijke actoren in het cyberdomein, die zich richten tegen de nationale veiligheid. Dit is voorwaardelijk voor het verhogen van de cyber weerbaarheid. Daarnaast is het voorwaardelijk voor het kunnen bepalen van een eventuele respons. De middelen in de Augustusbrief en de investeringen in het coalitieakkoord stellen de MIVD en de AIVD in staat meer capaciteit in te zetten ten behoeve van het primaire proces.
   d. **Deze leden vragen hoe de informatie effectief wordt gedeeld met het Nationaal Cyber Security Centrum, zodat de rijksoverheid (en overige overheidsinstellingen) en de aanbieders van vitale diensten tijdig en compleet, in ieder geval afdoende, worden geïnformeerd en geadviseerd.**

*Antwoord:* De samenwerking met het NCSC loopt over meerdere vlakken. Binnen de Cyber Info/Intel Cel (CIIC) brengen NCSC, AIVD, MIVD, Politie en OM dreigingsinformatie bijeen. Hierdoor kan sneller een beeld worden gevormd van nieuwe dreigingen en kunnen belanghebbende organisaties meer en sneller van handelingsperspectief worden voorzien. In geval van incidenten wordt deze structuur ook gebruikt voor coördinatie. Binnen het Nationaal Detectie Netwerk (NDN) wordt samengewerkt op het vlak van detectie en monitoring.

2. **Daarnaast vragen de leden van de CDA-fractie wat de stand van zaken is omtrent de herziening van de Geïntegreerde Aanwijzing Inlichtingen en Veiligheid (GA I&V), die dit jaar gepland staat. Deze leden vragen wanneer deze wordt afgerond.**
   *Antwoord:* In 2022 zal de Geïntegreerde Aanwijzing Inlichtingen en Veiligheid (GA I&V), conform reguliere planning, volledig worden herzien voor de periode 2023–2026. Naar verwachting wordt de definitieve GA I&V 2023–2026 in november 2022 vastgesteld en zal uw Kamer hierover via de geëigende kanalen worden geïnformeerd.
3. **De leden van de CDA-fractie lezen in de hoofdlijnen van het MIVD Jaarplan 2022 dat de nationale inlichtingendiensten hun samenwerking intensiveren en uitbreiden. Deze leden juichen dit toe.**
   a. **Tegelijkertijd lezen zij weinig over samenwerking met buitenlandse partners. In het jaarverslag 2020 wordt hier wel aandacht aan besteed. Deze leden vragen in hoeverre de Minister mogelijkheden ziet om de samenwerking van de MIVD met buitenlandse partners te versterken. Zij stellen dat onderzoeken naar landen en missiegebieden, economische veiligheid, ontwikkelingen van militaire technologie en wapensystemen, spionage en cyber wellicht zijn gebaat bij de informatie van inlichtingendiensten van partnerlanden. De uitwisseling van informatie versterkt volgens deze leden de inlichtingenpositie van de samenwerkende diensten.**
      *Antwoord:* Voor alle onderzoeken van de MIVD geldt dat samenwerking met internationale partners cruciaal is. Zij vormen een belangrijke bijdrage aan een effectieve taakuitvoering. Omdat internationale samenwerking en relatiemanagement van strategisch belang is -zet de MIVD momenteel in op het intensiveren van deze samenwerking.
   b. **De leden van de CDA-fractie vragen welke initiatieven om de samenwerking tussen inlichtingendiensten te versterken er op dit moment lopen in NAVO en EU verband.**
      *Antwoord:* Multilaterale samenwerking op inlichtingengebied is van cruciaal belang in een globaliserende wereld met toenemende complexe dreigingen. De MIVD onderschrijft het belang van intensieve samenwerking met deze multilaterale organisaties. Zeker de NAVO is voor de MIVD van essentieel belang. De dienst heeft in 2021 capaciteit vrijgemaakt om de relatie met de NAVO te versterken en zal dit ook in 2022 continueren. In het licht van de toenemende samenwerking tussen de EU en de NAVO, bijvoorbeeld op het gebied van hybride dreigingen, zal de MIVD de komende jaren ook investeren in de relatie met de EU. Daarnaast wordt in EU-verband momenteel gesproken over uitwerking van het Strategisch Kompas dat tijdens de RBZ van 21 maart aangenomen is. In de doelstellingen met betrekking tot het vergroten van de weerbaarheid van de EU tegen dreigingen speelt EU-inlichtingensamenwerking een rol. Het gaat hier met

name om het versterken van de *Single Intellingence Analysis Capacity* (SIAC) van de EU.

## PVDA

**De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het jaarplan van de MIVD voor 2022. Zij hebben daarbij enige vragen en opmerkingen.**

1. **De leden van de PvdA-fractie zien een focus op statelijke actoren door het gehele jaarplan heen en erkennen dat statelijke actoren van groot belang zijn voor de (inter-) nationale veiligheid en de hoofdmoot van de taken betreffen. Deze leden merken op dat er echter weinig niet-statelijke actoren zijn opgenomen in het plan en vragen zich af of de genoemde onderzoeken hier ook specifiek naar kijken. Zij vragen de Minister dit toe te lichten en, als de focus vooral op statelijke actoren ligt en niet op niet-statelijke actoren, uit te leggen waarom hiervoor is gekozen.**
   *Antwoord*: Bij diverse aandachtsgebieden van de MIVD is het van groot belang om, in het licht van een landenonderzoek, ook onderzoek te doen naar niet-statelijke groeperingen om ontwikkelingen in de veiligheidssituatie goed te kunnen duiden. Dit betreft bijvoorbeeld de landenonderzoeken gericht op het Midden-Oosten, de Sahel-regio en Afghanistan. Onderzoek naar niet-statelijke actoren kan dus onderdeel uitmaken van een landenonderzoek.
2. **Met betrekking tot (Inter-)Nationale veiligheid en de rol van de MIVD lezen de leden van de PvdA-fractie dat erop wordt gewezen dat het van belang is dat de «Wiv 2017 voldoende aansluit op de technologisch complexe en dynamische inlichtingenpraktijk» en dat het huidige wettelijk kader daarvoor op dit moment te kort schiet. Ook lezen deze leden dat daarbij wordt gesteld dat dit in de praktijk voor de diensten «tot urgente operationele knelpunten, die zich vooral manifesteren in het cyberdomein» leidt. Deze leden vragen de Minister daar nader op in te gaan. Zij vragen waar die knelpunten in de praktijk toe leiden. De leden van de PvdA-fractie hebben bij de totstandkoming van de Wiv 2017 al gepleit voor strenge regels ten aanzien van kabelinterceptie. Zij waren toen al van mening dat vanwege een mogelijk zware inbreuk op de privacy van burgers een onafhankelijke Toetsingscommissie Inzet Bevoegdheden (TIB) die vooraf toestemming moet geven voor een verzoek tot kabelinterceptie of andere bijzondere bevoegdheden door de AIVD en de MIVD nodig was. Deze leden vragen de Minister daar nader op in te gaan. Zij vragen waar die knelpunten in de praktijk toe leiden. De leden van de PvdA-fractie hebben bij de totstandkoming van de Wiv 2017 al gepleit voor strenge regels ten aanzien van kabelinterceptie. Zij waren toen al van mening dat vanwege een mogelijk zware inbreuk op de privacy van burgers een onafhankelijke Toetsingscommissie Inzet Bevoegdheden (TIB) die vooraf toestemming moet geven voor een verzoek tot kabelinterceptie of andere bijzondere bevoegdheden door de AIVD en de MIVD nodig was. De leden van de PvdA-fractie zijn er niet van overtuigd dat dergelijk toezicht niet meer nodig zou zijn enkel omdat dat voor de diensten belemmerend zou werken. De rol van de TIB is volgens deze leden juist bedoeld ter voorkoming van ongebreidelde informatievergaring door de diensten. Deze leden vragen de Minister hierop nader in te gaan.**

*Antwoord:* Naar aanleiding van de rapporten van de Evaluatiecommissie Wiv 2017 en de Algemene Rekenkamer is een wetswijziging gestart om de Wiv 2017 te herzien. Naar verwachting zal dit traject meerdere jaren in beslag nemen. De contouren van deze wetswijziging zullen middels een hoofdlijnennotitie aan de Tweede en Eerste Kamer worden aangeboden. De uitkomsten van de parlementaire gedachtewisseling worden vervolgens bij het daaropvolgende wetsvoorstel tot wijziging van de Wiv 2017 betrokken.
Echter, door een toenemende en urgente dreiging in het cyberdomein is besloten tussentijds middels een tijdelijke wet een aantal knelpunten versneld te adresseren. Het kabinet werkt aan een voorstel voor een tijdelijke wet die de diensten in staat moet stellen bestaande bevoegdheden effectiever in te kunnen inzetten in onderzoeken gericht op landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen. Een sluitend systeem van toezicht dat past bij de dynamiek van cyberoperaties maakt deel uit van dit wetsvoorstel. De tijdelijke wet is van 1 tot 18 april 2022 in internetconsultatie geweest. Hiermee wordt tevens gevolg gegeven aan de aangenomen motie van het lid Van der Staaij c.s., waarbij de regering wordt verzocht om zo spoedig mogelijk met een voorstel te komen om de operationele knelpunten in het cyberdomein weg te nemen.

3. **Met betrekking tot contraproliferatie en proliferatie van militaire technologie lezen de leden van de PvdA-fractie dat de MIVD-onderzoek doet naar de ontwikkelingen van militaire technologie en wapensystemen in andere landen en de proliferatie van (hoogwaardige) militaire technologie en wapensystemen naar crisisgebieden om Nederland zo goed mogelijk voor te bereiden op bestaande en toekomstige dreigingen. Deze leden vragen of hier alleen naar massavernietigingswapens wordt gekeken. Zo nee, dan vragen deze leden naar wat voor wapens er verder wordt gekeken en of hierbij ook wordt gekeken naar bijvoorbeeld de verkoop van offensieve algoritmen en geavanceerde technologieën voor autonome wapensystemen. Zij vragen waarom wel, dan wel niet.**
   *Antwoord:* De MIVD en de AIVD beschikken over een gezamenlijk unit contraproliferatie die onderzoek doet naar de verwerving van kennis en goederen voor massavernietigingswapens door landen van zorg. In aanvulling hierop doet de MIVD-onderzoek naar conventionele en *dual-use* militaire technologie. In het kader van missieondersteuning is onderzoek naar wapensystemen een aspect dat relevant is als «threat to the force», de directe dreiging tegen Nederlandse militairen en de coalitiepartners in een inzetgebied.
4. **Met betrekking tot radicalisme, terrorisme en extremisme lezen de leden van de PvdA-fractie dat de MIVD eerder het onderzoek naar de rechts-extremistische dreiging heeft geïntensiveerd en dat ook voor het jaar 2022 zal blijven doen. Deze leden zijn van mening dat extremistisch gedachtengoed van welke aard dan ook niet in de krijgsmacht thuishoort.**
   a. **Zij vragen de Minister aan te geven waarom de krijgsmacht dan toch «deel uitmaakt van het rechts-extremistische narratief». Voorts vragen deze leden waarin de aantrekkingskracht van de krijgsmacht voor rechts-extremistische jongeren zit en hoe die aantrekkingskracht kan worden verminderd.**
      *Antwoord:* Rechts-extremisten voelen zich mogelijk aangetrokken tot Defensie omdat zij Defensie kunnen zien al een subcultuur van militarisme en een narratief aanhangen waarbinnen militaire vaardigheden als middel worden gezien in de voorbe-

reiding op een zogenaamde toekomstige rassenoorlog. Voor sommige rechts-extremisten is een baan bij Defensie een manier om militaire vaardigheden op te doen. Vooropgesteld staat dat voor rechts-extremisme geen plaats is in de krijgsmacht. Onderzoek van de MIVD is erop gericht dreigingen aan het licht te brengen en anderen in staat te stellen maatregelen te nemen. Dit doet de MIVD door ambtsberichten te sturen aan het Openbaar Ministerie of bijvoorbeeld aan de commandant van een defensiemedewerker. De MIVD kan zelf een veiligheidsonderzoek uitvoeren. Dit kan leiden tot het weigeren of intrekken van de Verklaring van Geen Bezwaar die vereist is voor een baan bij Defensie.

b. **Deze leden vragen in hoeverre veiligheidsonderzoeken bijdragen aan het voorkomen dat (rechts)extremistische jongeren de krijgsmacht binnendringen.**
*Antwoord:* Veiligheidsonderzoeken zijn daarvoor een instrument, maar kunnen niet geheel voorkomen dat (rechts)extremistische jongeren de krijgsmacht binnen komen. Momenteel wordt bij aanstelling een veiligheidsonderzoek uitgevoerd en vervolgens, afhankelijk van het niveau van de screening, om de vijf of tien jaar herhaald. Dit kan eveneens bij een wijziging van omstandigheden. Op basis van een veiligheidsonderzoek kan de MIVD, mits daartoe voldoende gronden zijn, overgaan tot intrekken of weigeren van afgifte van de Verklaring van Geen Bezwaar (VGB).

5. **Met betrekking tot de Wiv 2017 begrijpen de leden van de PvdA-fractie dat de MIVD in samenwerking met de AIVD en de departementen werkt aan aanpassingen op de huidige Wiv 2017 of nieuwe wetsartikelen. De diensten krijgen de kans om op basis van conceptteksten een uitvoeringstoets uit te voeren. Deze leden vragen of in deze fase van wetgeving ook toezichthouders zoals het TIB of de CTIVD al de gelegenheid krijgen om hun mening te geven over deze aanpassingen, zodat niet alleen vanuit het oogpunt van de diensten naar de aanpassingen wordt gekeken. Zo ja, dan vragen deze leden hoe dat proces wordt ingericht. Zo nee, dan vragen zij waarom niet. Worden de uitkomsten van de uitvoeringstoetsen openbaar gemaakt en eventuele opmerkingen van de toezichthouders ook? Zo ja, op welke wijze? Zo nee, waarom niet? Zo vragen de leden van de PvdA-fractie.**
*Antwoord:* In lijn met de door uw Kamer aangenomen motie om de CTIVD en de TIB bij de wijziging van de Wiv 2017 te betrekken, zal na overleg met de CTIVD en de TIB gekomen worden tot een hoofdlijnennotitie waarin onder andere een voorstel voor een duurzame inrichting van het stelsel van toetsing en toezicht wordt opgenomen. Nadat er met uw Kamer is gesproken over deze hoofdlijnennotitie zal er verder gewerkt worden aan een voorstel tot wijziging van de Wiv 2017, daarover zal vanzelfsprekend ook overleg met de TIB en de CTIVD plaatsvinden. Daarnaast zullen de TIB en de CTIVD, zoals gebruikelijk, een belangrijk onderdeel uitmaken van de formele consultatie van het wetswijzigingsvoorstel. De uitkomsten van de uitvoeringstoets zullen met uw Kamer worden gedeeld, voor zover deze uit operationeel oogpunt ook (volledig) openbaar kunnen worden gedeeld.

**GroenLinks**

**De leden van de GroenLinks-fractie hebben met interesse kennisgenomen van het jaarverslag en de jaarplanbrief. Deze leden hebben nog enkele vragen die zij aan het kabinet willen voorleggen.**

1. **De leden van de GroenLinks-fractie lezen in de stukken geen stand van zaken over de verplaatsing van de satellietinstallatie in het Friese Burum naar een ander land. Eerder hebben deze leden hun zorgen geuit over de juridische grondslag voor een eventuele verhuizing naar een ander land en over het feit dat voor de Kamer nog onvoldoende duidelijk was onder welke jurisdictie de verkregen informatie in zo'n geval zou moeten worden verwerkt. Deze leden vragen de Minister aan te geven wat op dit moment de stand van zaken is met betrekking tot de mogelijke verplaatsing van deze satellietinstallatie.**
   *Antwoord;* Ten aanzien van de stand van zaken van de internationale oplossing wordt uw Kamer geïnformeerd via de geëigende kanalen.
2. **Een andere vraag die de leden van de GroenLinks-fractie hebben betreft de internationale samenwerking en de eigenstandige informatiepositie die de MIVD heeft. Zij vragen de Minister aan te geven of Nederland bij bijvoorbeeld de evacuatie uit Afghanistan en de thans dreigende situatie in Oekraïne naar het oordeel van de regering over een adequate eigenstandige informatievoorziening beschikt om zelfstandig (en in overleg met bondgenoten) in te spelen op actuele veiligheidssituaties voor Nederlanders en andere personen die de bescherming van Nederland nodig hebben in conflictgebieden.**
   *Antwoord:* De MIVD kan in het openbaar niet ingaan op de mate van eigenstandigheid van informatieposities op specifieke dossiers. Zoals ook al gesteld in het antwoord op vraag 3a en b van CDA: voor alle onderzoeken van de MIVD geldt dat samenwerking met internationale partners cruciaal is voor een effectieve taakuitvoering. In het algemeen is het streven om op elk onderzoek in staat te zijn om eigenstandig oordelen te kunnen vellen over bijvoorbeeld de veiligheidssituatie.
3. **Tot slot hebben de leden van de GroenLinks-fractie nog een vraag over de gegevensverwerking conform de Wiv 2017. Zij lezen dat de MIVD nog steeds met IT-achterstanden kampt en dat hierdoor van een Wiv-conforme geavanceerde informatievoorziening, IT en dataverwerking nog geen sprake is en dat hieraan wordt gewerkt. Deze leden vragen de Minister dit nader toe te lichten. Zij vragen wat de MIVD concreet gaat doen om zo snel mogelijk aan de Wiv te voldoen en wat het tijdpad is dat de regering voor zich ziet.**
   *Antwoord:* Het op orde brengen van de IT heeft hoge prioriteit. Er moet een achterstand worden ingehaald. Dat kost tijd en vraagt om investeringen. De afgelopen jaren is er, zoals ook opgenomen in de Defensienota 2018, geïnvesteerd in de IT bij de MIVD. Deze investeringen waren een belangrijke eerste stap om de IT van de MIVD op orde te krijgen. Wiv-conforme geavanceerde informatievoorziening, moderne IT en dataverwerking heeft continu de aandacht.

**VOLT**

**De Volt-fractie heeft kennisgenomen van het Jaarplan voor de MIVD 2022 en het openbaar jaarverslag van de Militaire Inlichtingen- en Veiligheidsdiensten over het jaar 2020. Daarover heeft de Volt-fractie een aantal vragen.**

1. **Met betrekking tot (Inter-)Nationale veiligheid en de rol van de MIVD leest de Volt-fractie dat de Minister aangeeft intensief samen te werken binnen de krijgsmacht met de AIVD en de NCTV.**

a. **Deze leden vragen hoe de samenwerking met de NCTV wordt vormgegeven en hoe de twee onderdelen zich tot elkaar verhouden.**
*Antwoord: De* MIVD werkt, binnen de bestaande wettelijke kaders, nauw samen met NCTV op het gebied van contraterrorisme en het tegengaan van statelijke dreigingen. Een concreet voorbeeld van samenwerking tussen de MIVD, AIVD en NTCV is het uitbrengen van het «Dreigingsbeeld Statelijke Actoren» in 2021. Daarbij moet vermeld worden dat de MIVD werkt onder de Wiv 2017. De NCTV valt niet onder deze wet.

b. **Zij vragen welke (soorten) gegevens/informatie de MIVD van de NCTV ontvangt.**
*Antwoord:* De NCTV ontvangt inlichtingenproducten van de MIVD. De MIVD ontvangt geen gegevens of informatie van de NCTV, met uitzondering van beleidsstukken en fenomeen analyses die gebaseerd zijn op de inlichtingenproducten van de diensten en informatie uit openbare bronnen.

c. **De leden van de Volt-fractie vragen wanneer de Minister het onderzoek ten aanzien van de operationele knelpunten voor opsporing in het digitale domein verwacht af te ronden en welke onderzoeksvragen daarin worden beantwoord.** *Antwoord:* Naar aanleiding van de rapporten van de Evaluatiecommissie Wiv 2017 en de Algemene Rekenkamer is een wetswijziging gestart om de Wiv 2017 te herzien. Naar verwachting zal dit traject meerdere jaren in beslag nemen. De contouren van deze wetswijziging zullen middels een hoofdlijnennotitie aan de Tweede en Eerste Kamer worden aangeboden. De uitkomsten van de parlementaire gedachtewisseling worden vervolgens bij het daaropvolgende wetsvoorstel tot wijziging van de Wiv 2017 betrokken.
Echter, door een toenemende en urgente dreiging in het cyberdomein is besloten tussentijds middels een tijdelijke wet een aantal knepunten versneld te adresseren. Het kabinet werkt aan een voorstel voor een tijdelijke wet die de diensten in staat moet stellen bestaande bevoegdheden effectiever in te kunnen inzetten in onderzoeken gericht op landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen. Een sluitend systeem van toezicht dat past bij de dynamiek van cyberoperaties maakt deel uit van dit wetsvoorstel. De tijdelijke wet is van 1 tot 18 april 2022 in internetconsultatie geweest. Hiermee wordt tevens gevolg gegeven aan de aangenomen motie van het lid Van der Staaij c.s., waarbij de regering wordt verzocht om zo spoedig mogelijk met een voorstel te komen om de operationele knelpunten in het cyberdomein weg te nemen.

d. **Deze leden vragen of de MIVD over voldoende middelen, mogelijkheden en connecties beschikt om tijdig inlichtingen te verzamelen die essentieel zijn voor het beschermen van Nederlandse belangen en de belangen van haar burgers en militairen of dat Nederland hierin afhankelijk is van andere landen.**
*Antwoord:* Over specifieke werkwijzen van de MIVD worden, vanwege de vertrouwelijkheid, in het openbaar geen uitspraken gedaan. In het algemeen kan worden gesteld dat internationale samenwerking met partners daarbij van groot belang is.

2. **Voorts vragen deze leden of de Minister voorstander is van een gezamenlijke Europese inlichtingendienst. Zo ja, hoe zou deze samenwerking volgens de Minister moeten worden vormgegeven, zo vragen deze leden. Zo nee, dan vragen zij of de Minister van mening is dat de samenwerking op het gebied van inlichtingen binnen de EU en tussen de**

**EU-lidstaten voor verbetering vatbaar is en welke ruimte voor verbetering de Minister ziet.**
*Antwoord:* Nee, Nederland is geen voorstander van een gezamenlijke Europese inlichtingendienst. De bescherming van de nationale veiligheid is de uitsluitende verantwoordelijkheid van elke lidstaat. In algemene zin geldt dat tussen de Europese inlichtingen- en veiligheidsdiensten intensieve samenwerking plaatsvindt. Deze bi- en multilaterale samenwerking vindt plaats buiten het kader van de EU. Nederland is voorstander van het verder versterken van de *Single Intelligence Analysis Capacity* (SIAC). Het SIAC vertolkt een centrale rol in de verwerkende en verspreidende inlichtingencapaciteit van de EU. Het beschikt over de expertise om de militaire inlichtingen verkregen vanuit het EUMS-inlichtingen directoraat (EUMS INT), en civiele inlichtingen vanuit het *EU Intelligence and Situation Centre* (EU INTCEN) samen te brengen om inlichtingenproducten te produceren. In het Strategisch Kompas worden enkele voorstellen gedaan om het SIAC te versterken zodat het omgevingsbewustzijn en de strategische vooruitblik van de EU als geheel verbeterd kunnen worden. Nederland steunt deze doelstelling.

3. **Met betrekking tot prioriteiten en accenten vragen de leden van de Volt-fractie op welke manier polarisering en radicalisering in de Nederlandse maatschappij een negatieve invloed op de Nederlandse defensiebelangen vormen. Deze leden vragen of de Minister kan delen of er sprake is van rechtsextremistische geluiden binnen de Nederlandse krijgsmacht of werknemers bij de Nederlandse krijgsmacht en of het bestrijden van dergelijk gedachtegoed onderdeel is van de opleidingen van de krijgsmacht.**
*Antwoord:* Zoals reeds benoemd in het jaarverslag van 2020 is de opkomst van rechts-extremisme een wereldwijd fenomeen. In lijn met deze opkomst heeft de MIVD een toegenomen interesse in Defensie binnen Nederlands rechts-extremistische netwerken gesignaleerd.
Op basis van het «Kader veiligheid in opleidingen» is sociale veiligheid een vast onderdeel van de initiële- en loopbaanopleidingen geworden. Inclusiviteit is een belangrijk deel van sociale veiligheid. Aandacht voor verschillen in opvatting en attitude en hoe dat bespreekbaar te maken is de kern. Polarisatie en radicalisering worden regelmatig besproken in samenhang met de gedragscode Defensie.
4. **Zij vragen hoe de gegevensuitwisseling binnen de samenwerking in «intelligence based cybersecurity» plaatsvindt tussen de AIVD en MIVD enerzijds, en ketenpartners als de NCSC anderzijds en of hier belemmeringen in zitten.**
*Antwoord:* In 2020 is de Cyber Info/Intel Cel (CIIC) ingesteld, waarbinnen AIVD, MIVD, NCSC, OM en politie dreigingsinformatie bijeenbrengen en medewerkers van deze organisaties deze informatie op één fysieke locatie bij het NCSC structureel gezamenlijk beoordelen. Hierdoor kan sneller een beeld worden gevormd van nieuwe dreigingen en kunnen belanghebbende organisaties meer en sneller van handelingsperspectief worden voorzien. De ervaringen zijn tot nu toe positief. Tegelijkertijd is het bij dit soort nieuwe vormen van samenwerking van belang om te blijven ontwikkelen. Daarom wordt er vooruitlopend op de aankomende Nederlandse Cyber Security Strategie gekeken naar verdere verbetering van deze samenwerking.
5. **Met betrekking tot overige taken en doelstellingen 2022 vragen de leden van de Volt-fractie of de MIVD naast investeringen in risico- en compliance management, andere investeringen zal doen om beter te voldoen aan de eisen uit de Wiv**

**2017. Deze leden vragen waarom het tot nu toe niet is gelukt om aan die eisen te voldoen en waarom dat nu wel gaat lukken. Deze leden vragen welke maatregelen de MIVD treft om de schaarste expertise binnen de dienst binnen te halen.**
*Antwoord:* De MIVD zet de komende jaren in op het op orde brengen van de IT. Deze investeringen vormen niet alleen een meerwaarde voor de performance van de dienst, ook de compliance wordt hierdoor verbeterd. In de IT-systemen zal veel meer sprake zijn van compliance by design. De vereisten uit wet- en regelgeving worden direct bij de ontwikkeling meegenomen. Hierdoor is de MIVD beter in staat om te voldoen aan de eisen uit de Wiv 2017.
De samenwerking met de AIVD heeft op het gebied van compliance een grote vlucht genomen. De diensten werken immers onder dezelfde wet en onder dezelfde toezichthouders. Daarom is eind 2021 besloten om op het gebied van compliance toe te werken naar een geïntegreerd gezamenlijk compliance managementsysteem. Door deze samenwerking kan expertise worden gebundeld en wordt voorkomen dat werkzaamheden dubbelop worden uitgevoerd.

6. **Met betrekking tot het openbaar jaarverslag van de MIVD over 2020 lezen de leden van de Volt-fractie dat de Chinese inlichtingen- en veiligheidsdiensten en andere overheidsinstanties nauw samenwerken met Chinese informatiebeveiligingsbedrijven, hackersgroepen en universiteiten.**
   a. **Deze leden vragen hoe de Minister denkt over het optuigen van strategische en duurzame onderzoeksprogramma's met Nederlandse universiteiten om de strategische kennispositie van Nederland met betrekking tot inlichtingen en cyberdreigingen te versterken.**
   *Antwoord:* Defensie werkt met Nederlandse universiteiten en het NWO aan het versterken van de strategische kennispositie op deze gebieden. De strategische kennispartners TNO, NLR en MARIN houden bovendien de defensie-specifieke kennisbasis in stand, onder andere ten aanzien van «Cyber & Elektronische Oorlogsvoering». Op dit moment lopen er op dit gebied twee onderzoeksprogramma's. Daarnaast komen specifieke vormen van cyberdreiging aan de orde in nog twee andere onderzoeksprogramma's.
   De samenwerking met de strategische kennispartners is de basis maar sluit andere partijen niet uit. Zo is Defensie mede initiator van het Cybersecurity onderzoeksprogramma «Cybersecurity» dat onder de vlag van de Nationale Wetenschapsagenda heeft geleid tot een vijftal onderzoeksprojecten waaraan verschillende universiteiten deelnemen.
   b. **Zij vragen hoe de Minister denkt over meer samenwerking en uitwisseling tussen de Nederlandse diensten en private actoren die de informatie- en kennispositie van Nederland kunnen versterken.**
   *Antwoord:* De samenwerking tussen de Nederlandse inlichtingen- en veiligheidsdiensten en private Nederlandse partijen kan de informatie- en kennispositie van Nederland mogelijk versterken en daarom worden de mogelijkheden voor een dergelijke samenwerking nader onderzocht. In verband met de operationele veiligheid kan uw kamer over de uitkomsten van een dergelijk onderzoek alleen via de geëigende kanalen worden geïnformeerd.
   c. **De leden van de Volt-fractie stellen dat een aantal Europese landen uit nationale veiligheidsoverwegingen hebben besloten om Huawei uit het 5G-netwerk te weren, waarop China dreigde met negatieve gevolgen voor de bilaterale economische en handelsrelaties. Deze leden**

**vragen of de Minister in deze beoordeling ook meeneemt dat Ericsson en Nokia veel van de onderdelen van hun netwerken in China laten produceren, veelal in samenwerking met Chinese staatsbedrijven. Zij zien in dit kader dat in het jaarverslag ook staat dat waar de Chinese economische belangen eindigen en de politieke of militaire overwegingen beginnen onduidelijk is. De leden van de Volt-fractie stellen dat in een gelekte versie van de Amerikaanse National Security Council document staat dat, als China wijdverbreide 5G-dekking krijgt voor de VS, «China will win politically, economically, and militarily.» Deze leden vragen of de Minister de mening deelt dat in het kader van 5G de grens tussen economische belangen en politieke of militaire overwegingen niet alleen voor China onduidelijk is.**

*Antwoord:* Vooropgesteld moet worden dat er door de veiligheidsdiensten in het openbaar nooit gereageerd wordt op gelekte documenten van bondgenoten. De Taskforce Economische Veiligheid (TFEV) heeft in 2019 een risicoanalyse uitgevoerd naar de kwetsbaarheid van mobiele telecommunicatienetwerken voor misbruik via leveranciers van technologie. Deze risicoanalyse heeft ertoe geleid dat het kabinet in juli 2019 een stevig pakket aanvullende maatregelen heeft aangekondigd om de weerbaarheid van genoemde netwerken tegen deze dreiging te verhogen. Deze maatregelen zijn onder andere toegelicht in de Kamerbrief «*Stappen veiligheid en integriteit telecom»* [5].
Zoals gesteld in het Dreigingsbeeld Statelijke Actoren (Kamerstuk 30 821 nr.124) zorgt de verwevenheid tussen staat en economie in China ervoor dat er geen gelijk speelveld is voor Nederlandse bedrijven. China beschermt zijn eigen markt zowel offensief als defensief. Zo equipeert China zijn (staats)bedrijven met inlichtingen en voordelen als staatssteun en subsidies, maakt het gebruik van wetgeving die (buitenlandse) bedrijven dwingt om gegevens te delen en van de inzet van proxy-ondernemingen. Ook dwingt het buitenlandse bedrijven bij toegang tot de Chinese markt om samenwerkingen aan te gaan met Chinese partners. Dit alles kan leiden tot de ongewenste overdracht van kennis en technologie.

d. **Zij vragen of de Minister aandacht heeft voor de rol van de strijd tussen de VS en China om leiderschap van de vierde industriële revolutie in de discussie over 5G en economische sancties.**

*Antwoord:* Het Chinese economische beleid is primair gericht op transformatie van een productie-economie naar een kenniseconomie die grotendeels onafhankelijk is van buitenlandse technologie. Om deze economische modernisering en onafhankelijkheid te realiseren investeert China in strategische meerjarenplannen en beleidsinitiatieven zoals *Made in China 2025* (MIC2025), het *Belt and Road Initiative* (BRI), *Military-Civil Fusion* (MCF) en het geplande *China Standards 2035* (CST2035). Deze plannen en initiatieven zijn gericht op het overkoepelende doel om voor 2049 een «great modern socialist country» te zijn, oftewel een economische en militaire grootmacht. De plannen kunnen worden gezien als een boodschappen- of wensenlijst van het Chinese leiderschap. BRI-investeringen leiden, gezien het belang van de investering, tot een toename van digitale inlichtingenvergaring bij bevriende BRI-partners. Chinese beleidsplannen worden minutieus vertaald in omvangrijke en

[5] Kamerstuk 30 821, nr. 143

structurele spionagecampagnes. Die campagnes zijn gericht op het verkrijgen van hoogwaardige kennis en technologie ten behoeve van de eigen economische ontwikkeling en de ontwikkeling van de krijgsmacht. Hieruit volgt dat Nederlandse topsectoren, de Nederlandse defensie-industrie en Nederlandse kennisinstellingen een groot risico lopen op Chinese (digitale) spionage. Spionageactiviteiten tegen het Nederlands bedrijfsleven, geïnitieerd door statelijke actoren of aan statelijke actoren gelieerde partijen, tasten weliswaar in alle gevallen de nationale veiligheid aan, maar hoeven niet altijd een specifieke dreiging te zijn voor de economische veiligheid. Toch is het een zorgwekkende en onwenselijke situatie, omdat het de concurrentiekracht van het betrokken bedrijf ondergraaft.
Daarnaast investeert China in de ontwikkeling van hoogwaardige, nieuwe technologieën zoals *artificial intelligence*, quantum en 5G-communicatie. Conform het geplande beleidsplan CST2035 richt het zich op een positie als marktleider voor die technologieën. Een mogelijke technologische dominantie kan leiden tot een China dat de technologische producten, diensten en standaarden voor de toekomst bepaalt, waardoor er een strategische afhankelijkheid van één land ontstaat – in dit geval China. Die afhankelijkheid kan leiden tot dreigingen tegen de nationale veiligheid, met name daar waar ze raken aan de vitale processen en sensitieve technologie. Daarnaast kan deze afhankelijkheid het Nederlandse bedrijfsleven op termijn nog kwetsbaarder maken voor oneerlijke concurrentie, (digitale) spionage en mogelijk ook sabotage, en de Nederlandse overheid gevoeliger voor economische druk. Bovendien kan het beïnvloeden van het standaardiseringsproces China substantiële economische voordelen opleveren en zelfs van invloed zijn op burgerlijke vrijheden.
De kennis over de hierboven beschreven ontwikkelingen worden meegenomen in relevante beleidstrajecten.

7. **De leden van de Volt-fractie stellen dat spionage wordt genoemd als middel van de Chinese overheid om de noodzakelijke kennis en technologie uit het buitenland te halen. Deze leden vragen of de MIVD ook voldoende oog heeft voor juist de geavanceerde Chinese technologiebedrijven die op basis van eerlijke concurrentie de Europese markt veroveren met hun geavanceerde IoT-apparaten vol sensoren zoals industriële schoonmaakrobots en camera's en daarmee ongewild data kunnen verzamelen.**
*Antwoord:* De MIVD doet onderzoek naar dreigingen tegen de nationale veiligheid waaronder de spionagedreiging. Daaronder kunnen ook technologiebedrijven vallen.