Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

29 924 Toezichtsverslagen AIVD en MIVD

Nr. 207

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 26 maart 2021

De vaste commissie voor Defensie heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Defensie over de brief van 30 april 2020 over het openbaar jaarverslag van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) over het jaar 2019 (Kamerstuk 29 924, nr. 201), over de brief van 12 december 2019 over de hoofdlijnen van het MIVD jaarplan 2020 (Kamerstuk 29 924, nr. 196) en over de brief van 15 december 2020 over de Jaarplanbrief MIVD 2021 (Kamerstuk 29 924, nr. 206).

De vragen en opmerkingen zijn op 4 februari 2021 aan de Minister van Defensie voorgelegd. Bij brief van 22 maart 2021 zijn de vragen beantwoord.

De voorzitter van de commissie,
Aukje de Vries

De adjunct-griffier van de commissie,
Mittendorff

kst-29924-207
ISSN 0921 - 7371
's-Gravenhage 2021

Vragen en opmerkingen vanuit de fractie en reactie van de bewindspersoon

VVD

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de stukken betreffende de MIVD en hebben hier geen verdere vragen over.

D66

De leden van de D66-fractie hebben met interesse kennisgenomen van het openbaar jaarverslag 2019 van het MIVD, de hoofdlijnen van het MIVD-jaarplan 2020 en de jaarplanbrief MIVD **2**021. Deze leden hebben daar nog enkele vragen over.
De leden van de D66-fractie lezen dat vanuit landenperspectief de grootste dreigingen nog steeds vanuit Rusland en China komen. Daarbij lopen deze landen, met name China, al jaren hard in op Nederland en haar bondgenoten als het gaat om technologische ontwikkelingen. Ook Rusland is hard op weg met bijvoorbeeld hypersonische wapens.
De leden van de D66-fractie vragen in hoeverre deze dreiging al reëel is? Is de NAVO toegerust op een dreiging van hypersonische wapens? Is er al sprake van een early warning met betrekking tot dit nieuwe wapensysteem? Zijn er bondgenoten in de NAVO die ook bezig zijn met de ontwikkeling van hypersonische wapens?

1. Antwoord
De dreiging van hypersone wapens is reëel. Van in ieder geval twee soorten hypersone wapens is bekend dat deze deels operationeel zijn of op korte termijn die status bereiken. Zowel in Rusland als China lopen verschillende ontwikkelingstrajecten voor toekomstige nieuwe hypersone wapens. De hoge snelheid van hypersone wapensystemen zorgt voor een beperkte reactietijd, zelfs in het geval van een succesvolle detectie door *early warning* systemen.

In reactie op deze en andere ontwikkelingen in de veiligheidssituatie in de afgelopen jaren, is de NAVO onder meer overgegaan tot herziening van het NAVO Integrated Air- and Missile Defense (IAMD) Standing Defence Plan. De herziening van dit plan voorziet in een toekomstgerichte geïntegreerde 360-graden lucht- en raketverdediging voor het bondgenootschap, waarbij rekening wordt gehouden met politieke, militaire en technologische ontwikkelingen. Als het gaat om *early warning* is de NAVO zich dus terdege bewust van de dreiging die van de ontwikkeling van deze wapensystemen uitgaat.
Voor zover bekend houdt binnen de NAVO uitsluitend de VS zich bezig met de ontwikkeling van hypersone wapensystemen.

De leden van de D66-fractie maken zich zorgen over de berichten over China en spionage. De leden van de D66-fractie vragen of er signalen dat er gespioneerd wordt in het Nederlandse onderwijs zijn, bijvoorbeeld via Confucius Instituten? Ook het bedrijfsleven, via overnames of investeringen is een doelwit. Moet hier voornamelijk worden gedacht aan Nederlandse bedrijven die ook een afdeling hebben in China?

2. Antwoord
Zoals het *Dreigingsbeeld Statelijke Actoren* (DBSA) (Bijlage bij Kamerstuk 30 821, nr. 124) stelt, vormt de Chinese inzet van zowel legale als illegale middelen en (digitale) spionage een

ernstige dreiging voor de Nederlandse economische veiligheid. Met name de Nederlandse topsectoren en kennisinstellingen (inclusief universiteiten) zijn interessante spionagedoelwitten voor China vanwege de hoogwaardige infrastructuur, technologie en kennis die zij bezitten. Deze dreiging beperkt zich niet uitsluitend tot Nederlandse bedrijven of instellingen die een afdeling in China hebben, maar heeft betrekking op alle Nederlandse bedrijven en instellingen met waardevolle kennis. Ongewenste kennisoverdracht kan ook plaatsvinden via (academische of commerciële) samenwerkingsverbanden. Dergelijke samenwerking kan in sommige gevallen ook leiden tot ongewenste overdracht van kennis en technologie en tot ongewenste afhankelijkheden.

De leden van de D66-fractie erkennen dat cyber inmiddels een ontzettend belangrijk domein is geworden voor de mensheid, zo ook in oorlogsvoering. Deze leden vragen hoe de MIVD de rol van cyber inschat bij een mogelijk volgend conflict? Is dit domein inmiddels net zo belangrijk als conventionele domeinen? Dezelfde leden vragen ook of de MIVD, of Defensie in bredere zin, in reactie op de vele hybride conflicten van de afgelopen jaren met name van Russische zijde, inmiddels een strategie heeft ontwikkeld tegen hybride oorlogsvoering? Zo nee, waarom niet? Zo ja, is dit in samenwerking met NAVO-bondgenoten? Deze leden vragen ook of de huidige strijd tegen de Islamitische Staat gezien kan worden als een hybride conflict, aangezien het om een niet-statelijke actor gaat die beweegt tussen verschillende landen.

3. Antwoord

Cyber is inmiddels een volwaardig domein van militair optreden en het digitale domein zal in elk toekomstig conflict een belangrijke rol spelen. De MIVD beschouwt potentiële digitale verstoringen van de vitale infrastructuur en vitale sectoren/bedrijven als een van de grootste (digitale) dreigingen voor Nederland en zijn bondgenoten.

Daarnaast speelt cyber een grote rol in het schemergebied tussen vrede en oorlog: de grijze zone. Bij deze hybride vorm van conflictvoering is sprake van de geïntegreerde inzet van diplomatieke, informatie, militaire, economische, financiële, inlichtingen- en juridische instrumenten, onder het niveau van gewapend conflict. Hierin is het digitale domein (cyber) zowel middel als doel. Ons Koninkrijk heeft continu te maken met aanvallen in het cyberdomein en met ongewenste beïnvloeding door buitenlandse mogendheden.

De MIVD constateert dat een belangrijk element in het Russische veiligheidsbeleid is dat het zijn politiek-strategische doelstellingen volgens het concept van hybride conflictvoering, in de grijze zone tussen vrede en oorlog, tracht te verwezenlijken. Deze middelen worden door Rusland op geïntegreerde wijze ingezet om de nationale en supranationale besluitvormingsprocessen en eenheid in het Westen te ondermijnen.

Aangezien een hybride dreiging domeinoverstijgend is, vraagt deze ook om een domeinoverstijgende, of rijksbrede, aanpak. De kamerbrief voortgang aanpak Statelijke Dreigingen van 3 februari, die de Minister van Justitie en Veiligheid namens het kabinet stuurde, kan dan ook als de contrahybride aanpak van

het kabinet worden gezien.[1] Defensie vormt een integraal onderdeel van deze aanpak. In de Defensievisie-2035 (Kamerstuk 34 919, nr. 71) staat langs welke lijnen Defensie zich zou moeten ontwikkelen om een antwoord te hebben op de nieuwe dreigingen, waaronder hybride. De verwachting is dat er steeds vaker een beroep op het militair vermogen van Defensie zal worden gedaan en Defensie dient hierop voorbereid te zijn, zowel nationaal als internationaal. Om de meer permanente hybride dreigingen het hoofd te bieden verdiept Defensie de geïntegreerde benadering van militaire en civiele middelen. Dit valt onder inrichtingsprincipe 6 van de Defensievisie «Multidomein en geïntegreerd optreden». Onderlinge samenwerking met partners bij onder meer hybride dreigingen staat ook centraal in de brief van de Ministers van Justitie en Veiligheid en van Defensie van 26 juni 2020 over Civiel-Militaire Samenwerking.[2] Dat betekent in voorkomend geval trouwens ook dat civiele partijen Defensie en onze bondgenoten ondersteunen.

De aanpak van hybride dreigingen is in de eerste plaats een nationale verantwoordelijkheid, maar ook de NAVO heeft sinds 2015 een Strategie over het tegengaan van hybride conflictvoering. De NAVO zet hierbij in op voorbereiding (door bijvoorbeeld oefenen), afschrikking (door bijvoorbeeld strategische communicatie) en verdediging (door militaire en niet-militaire tegenmaatregelen). Staatshoofden en regeringsleiders van NAVO-bondgenoten spraken tijdens de Leaders Meeting eind 2019 af om meer te doen tegen cyberaanvallen en hybride tactieken.[3] Ook het recent gepubliceerde rapport «NATO 2030: United for a New Era» van de onafhankelijke reflectiegroep die aanbevelingen heeft gedaan aan de Secretaris-Generaal van de NAVO, onderkent het belang van een weerbare NAVO ten aanzien van huidige en toekomstige uitdagingen waaronder hybride dreigingen.[4]

Op de vraag van de leden van de D66-fractie of de huidige strijd tegen ISIS ook gezien van worden als een hybride conflict is het antwoord nee, niet volgens de definitie die de Nederlandse staat daarvoor hanteert.[5] Volgens deze definitie kan alleen een statelijke actor een hybride tegenstander zijn, omdat alleen een staat in samenhang over alle bovengenoemde instrumenten van hybride conflictvoering kan beschikken. Dat neemt niet weg dat ISIS zeer actief is in het gebruik van internet via verschillende sociale media voor zijn propagandadoeleinden, waarbij de nadruk ligt op de ondergrondse en asymmetrische strijd.

De leden van de D66-fractie hebben enkele vragen over contraproliferatie. Deze leden vinden het goed dat er een contraproliferatie strategie is en vragen of er op dit vlak ook nieuwe dreigingen zijn? Zo wordt Syrië genoemd bij de lijst met landen die op zoek blijven naar kennis en goederen voor gebruik in hun eigen wapenprogramma's. Zijn er duidelijke signalen dat dit land een nucleaire ambitie heeft? Gaat dit dan om ontwikkeling of eerder om de handel in kernkoppen? Zijn er met

---

[1] Zie Kamerbrief «beleidsreactie DBSA en voortgang aanpak statelijke Dreigingen», Kamerstuk 30 821, nr. 125.

[2] Kamerstuk 34 919, nr. 68.

[3] Kamerstuk 28 676, nr. 331.

[4] Reflection Group «Nato 2030: United for a New Era» Zie: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

[5] «Een duiding van het fenomeen «hybride dreiging», NCTV, Ministerie van J&V, 18 april 2019.

betrekking tot dit soort landen ook risico's met betrekking tot niet-statelijke actoren?

4. Antwoord
De MIVD doet onderzoek naar landen die ervan worden verdacht dat zij in strijd met geldende verdragen werken aan het ontwikkelen van massavernietigingswapens en hun overbrengingsmiddelen of daar al over beschikken. De zogenoemde CBRN[6]-dreiging is mede door technologische ontwikkelingen aan verandering onderhevig en neemt mogelijk toe, met name op het gebied van chemische en biologische middelen. In dit kader doet de MIVD onderzoek naar de productie, gebruik en inzet van zenuwgassen door het Syrische bewind. De MIVD beschikt niet over inlichtingen dat Syrië op dit moment de ambitie heeft om kernenergie op te wekken of kernwapens te ontwikkelen. Ditzelfde geldt voor niet-statelijke actoren.

In het Jaarplan 2020 lezen de leden van de D66-fractie dat de MIVD de inzet op spionage, beïnvloeding en sabotage op dit vlak heeft vergroot. Kan er al worden gesproken van concrete resultaten die deze verhoogde inzet teweeg hebben gebracht? Heeft deze inzet alleen betrekking tot activiteiten buiten de Nederlandse samenleving? Wordt er op dit vlak ook samengewerkt met Europese of Atlantische bondgenoten?

5. Antwoord
Zoals in de brief aan de Kamer over de hoofdlijnen van het MIVD jaarplan 2020[7] is vermeld, plande de MIVD voor 2020 op het vergroten en verdiepen van het onderzoek naar de militaire, hybride, spionage en cyberdreiging door de Russische Federatie en China. Dit werd mogelijk door de versterking van de MIVD, waar de brief ook aan refereert.

Het gaat wat spionage, beïnvloeding en sabotage betreft om zogenaamd contra-inlichtingen onderzoek naar dreiging tegen defensiebelangen in Nederland en in het buitenland. Over de voortgang van de onderzoeken rapporteert de MIVD via de geëigende kanalen. De informatiepositie is als gevolg van de investeringen verbeterd. Daarnaast is een concreet resultaat van de verhoogde inzet het *Dreigingsbeeld Statelijke Actoren* dat de MIVD samen met de AIVD en NCTV heeft uitgebracht.

De MIVD werkt op verschillende gebieden samen met Europese en Atlantische bondgenoten. Hier biedt de Wiv 2017 een grondslag voor. Dit wordt in de beantwoording van de volgende vraag nader toegelicht.

De leden van de D66-fractie lezen dat de Wiv voor enige problemen heeft gezorgd bij de MIVD, met name de implementatiefase en met betrekking capaciteit. Hoe staat het hier nu mee? Zijn er nog steeds capaciteitsproblemen? Er wordt in het kader van de Wiv ook gesproken over internationale samenwerking. De leden van de D66-fractie vragen de Minister in te gaan op wat hiermee wordt bedoeld?

6. Antwoord
De implementatie van de Wiv 2017 heeft de afgelopen twee jaar bij de MIVD hoge prioriteit gekregen en heeft veel van de dienst gevraagd. Daarbij is onder meer van belang dat de MIVD te

[6] Chemisch, Biologisch, Radiologisch en Nucleair.
[7] Kamerstuk 29 924, nr. 196.

kampen heeft met ICT uitdagingen die de invoering van de Wiv 2017 bemoeilijkt. De invoering van de nieuwe wet heeft geleid tot aanpassing van de opzet en werking van talrijke werkprocessen, extra opleiding van personeel en aanpassing van IT-systemen. Dit heeft geleid tot extra beslag op de beschikbare capaciteit en tot verdringing van operationele activiteiten.

De impact van de Wiv 2017 op de operationele slagkracht van de diensten staat centraal in het nog te verschijnen rapport hieromtrent van de Algemene Rekenkamer.

De Wiv 2017 biedt het kader voor uitwisseling van informatie en samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten. Dit kader kent verscheidene waarborgen voor internationale samenwerking. Het betreft wettelijke vereisten voor toestemming, vastlegging en verantwoording bij het verstrekken van gegevens of het leveren van ondersteuning aan buitenlandse diensten. Voordat een samenwerkingsrelatie met een buitenlandse inlichtingen- en veiligheidsdienst wordt aangegaan, wordt onderzoek gedaan om te bepalen of en zo ja, in welke mate, met de betreffende dienst kan worden samengewerkt. Dit onderzoek wordt verricht aan de hand van wettelijke criteria, die vastgelegd zijn in artikel 88, derde lid, van de Wiv 2017. Een voorbeeld van een criterium waaraan wordt getoetst is de professionaliteit en betrouwbaarheid van de desbetreffende dienst.

In zogeheten *wegingsnotities* worden de resultaten van dat onderzoek en de daaruit voortkomende voorwaarden voor de samenwerking vastgelegd. Voor de implementatie en de verankering van deze waarborgen in de (deels geautomatiseerde) werkprocessen van de MIVD, is capaciteit vrijgemaakt.

De leden van de D66-fractie hebben meermaals hun zorgen geuit over een subcultuur bij defensie die gegrond is in rechts-extremisme. Er is hier eerder uitvoerig over gedebatteerd en de MIVD heeft een onderzoek gestart binnen Defensie. Hoe staat het hier mee? Zijn er harde bewijzen gevonden dat rechts-extremisme inderdaad een gevaar vormt in de cultuur van Defensie? Zijn er personen geïdentificeerd die dit kwalijke gedachtengoed vertolken? Hoe wordt de awareness en understanding gecreëerd, waar de brief naar verwijst?

7. Antwoord
De MIVD blijft alert op signalen die mogelijk wijzen op het aanhangen van rechts-extremistisch gedachtegoed en heeft haar onderzoek geïntensiveerd. De MIVD heeft geen aanwijzingen gevonden dat rechts-extremisme een gevaar vormt in de cultuur van Defensie. Door het geven van «awareness»-briefings draagt de MIVD bij aan de bewustwording van het gevaar van rechts-extremisme binnen de defensieorganisatie.

De leden van de D66-fractie begrijpen dat er een gevaar schuilt in de autorisatie en auditie van aanbestedingen. De uitvoeringsorganisaties die hiervoor verantwoordelijk zijn dienen volgens deze leden van hoge kwaliteit te zijn. Hoe zorgt de MIVD ervoor dat hier geen lekken ontstaan? Heeft de steeds verder gaande Europese defensiesamenwerking gezorgd voor nieuwe instanties die bij dit proces betrokken zijn? Heeft de MIVD hier een duidelijk beeld van?

8. Antwoord
In het kader van aanbestedingen beoordeelt de MIVD de (potentiële) opdrachtnemers teneinde vast te kunnen stellen dat zij voldoen aan de gestelde beveiligingsnormen. Nationaal gebeurt dit aan de hand van de, contractueel bedongen, Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) die recentelijk nog zijn aangescherpt met betrekking tot cyberveiligheid. Na gunning van het contract wordt het bedrijf met regelmaat door de MIVD bezocht en geauditeerd op correcte implementatie van de beveiligingsmaatregelen, met inbegrip van screening van het betrokken personeel. Internationaal gebeurt een en ander in samenwerking met een aantal gelijkgestemde partnerlanden die, op grond van een juridische overeenkomst de auditerende taak namens de MIVD uitvoeren.

De leden van de D66-fractie lezen over de dreigingen van de COVID-19 pandemie. Zij vragen of er kan worden ingegaan op de concrete dreigingen die hieruit voortkomen? Worden hier aanvallen op de Nederlandse vitale infrastructuur bedoeld?

9. Antwoord
In het recent uitgebrachte *Dreigingsbeeld Statelijke Actoren*, een gezamenlijke analyse van de AIVD, MIVD en NCTV, wordt geschetst welke nationale veiligheidsbelangen geschaad (kunnen) worden door statelijke actoren. Een aantal dreigingen die voortkomen uit de COVID-19 pandemie staat hierin beschreven.

Verder doet de MIVD onderzoek naar dreigingen richting de vitale infrastructuur in relatie tot Defensie(belangen). De MIVD werkt samen met de AIVD nauw samen met ketenpartners om dreigingen tegen de Nederlandse veiligheidsbelangen te duiden en te delen met relevante afnemers teneinde bevordering van veiligheidsbewustzijn en weerbaarheid. De AIVD en de MIVD informeren indien nodig organisaties en bieden ondersteuning in verhoging van weerbaarheid.

Tot slot vragen de leden van de D66-fractie naar het personeel en het materieel. In de Jaarplannen 2020 en 2021 wordt gesproken over de moeite die de dienst heeft met het aantrekken van expertise. Dit blijft een grote uitdaging, daarom vragen deze leden de Minister of hier een duidelijk plan voor is? Is er voor alle activiteiten van de MIVD goed en genoeg materieel zodat de officieren hun werk op het allerhoogste niveau kunnen uitvoeren? Aansluitend willen deze leden vragen hoe de internationale samenwerking van de MIVD met andere diensten is. Zijn er vaste partners waar veel mee wordt samengewerkt? Is er ook een Europese instantie waar steeds meer mee wordt gedeeld en samengewerkt?

10. Antwoord
De MIVD is door specifieke arbeidsmarktcommunicatie en gericht beleid in staat om op verantwoorde wijze te groeien. Het aantrekken van expertise wordt bijvoorbeeld gedaan met behulp van wervingscampagnes specifiek gericht op de MIVD, zoals *«Zie jij wat anderen niet zien».* Speciale aandacht gaat daarbij uit naar schaarse categorieën, zoals IT-expertise. Om de MIVD compliant en toekomstbestendig te maken heeft dit kabinet een eerste investering gedaan ten behoeve van de IT bij de dienst. Het belang van goede en *up-to-date* IT bij de MIVD wordt aangetoond door meerdere rapporten van toezichthouder Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) en de

Algemene Rekenkamer. Ook de bevindingen van de Evaluatiecommissie Wiv 2017 onderstrepen dit.
Internationale samenwerking is voor de taakuitvoering van de MIVD essentieel. Samenwerking met buitenlandse diensten draagt significant bij aan de informatiepositie van de dienst. Het partnerveld van de MIVD is divers en kent vaste partners waar intensief en breed mee wordt samengewerkt. De MIVD verstrekt gegevens aan het inlichtingenbureau van de militaire staf van de EU (EUMS-int).

GroenLinks

De leden van de GroenLinks-fractie vragen of inmiddels een definitief een besluit is genomen over de verplaatsing van de satellietschotels te Burum, aangezien het voornemen is dat de 3,5Ghz frequentie die deze schotels gebruiken in 2022 beschikbaar komt voor gebruik voor 5G. Deze leden vragen of de Minister bereid is de vaste commissie voor Defensie, respectievelijk de vaste commissie voor Binnenlandse Zaken, al dan niet vertrouwelijk, te informeren over de nieuwe locatie van door de MIVD gebruikte interceptiecapaciteit en daarbij behorende juridische kaders voor internationale samenwerking. Zo nee, waarom niet? De leden van de GroenLinks-fractie vragen of het, voor het verplaatsen van interceptiewerkzaamheden van de MIVD naar het buitenland, niet noodzakelijk is om een verdrag te sluiten met het betreffende land, en of een dergelijk verdrag niet aan de Kamer zou moeten worden voorgelegd ter goedkeuring.

11. Antwoord
Het Kabinet heeft in 2019 besloten om voor de interceptie van de 3,5 GHz een internationale oplossing te treffen om satellietinterceptie na de invoering van 5G in Nederland, voorzien in september 2022, voort te kunnen zetten.[8] Ik kan vanwege de in dit verband vereiste vertrouwelijkheid verder geen uitspraken doen over de precieze invulling van deze internationale samenwerking.
De Tweede Kamer wordt zoals te doen gebruikelijk via de geëigende kanalen geïnformeerd op welke wijze de internationale oplossing wordt gerealiseerd.

De leden van de GroenLinks-fractie vragen de Minister te bevestigen dat interceptie door de MIVD via stations in het buitenland ook onder de volledige werking van de Wet inlichtingen- en veiligheidsdiensten 2017 valt.

12. Zie antwoord vraag 13
Vragen 12 en 13 worden gezamenlijk beantwoord.

De leden van de GroenLinks-fractie vragen de Minister uiteen te zetten hoe het toezicht van de TIB en CTIVD, zowel formeel als op praktisch niveau, is geregeld bij interceptie via in het buitenland gestationeerde satellieten.

13. Antwoord
Zoals op 14 juni 2019 reeds aan uw Kamer toegezegd[9], zal de Wiv 2017 en de bijbehorende waarborgen van toepassing zijn op de internationale samenwerking die in het kader van een alternatief voor satellietinterceptie in Burum zal worden aangegaan. De

[8] Kamerstuk 24 095, nr. 459 en Kamerstuk 24 095, nr. 478.
[9] Aanhangsel Handelingen II 2018/19, nr. 3091.

CTIVD houdt conform artikel 97 van de Wiv 2017 volledig toezicht op het handelen van de diensten. Daar valt ook bovengenoemde internationale samenwerking onder.

Met betrekking tot contra-proliferatie en andere wapenwedloop constateren de leden van de GroenLinks-fractie dat de MIVD in haar jaarverslag en jaarplannen terecht aandacht besteed aan het gevaar van proliferatie van kernwapens. Ook in de ontwikkeling van andere soorten wapens, zoals drones en offensieve cybertechnologie, zien deze leden een gevaar voor de internationale rechtsorde en de vrede. De leden van de GroenLinks-fractie vragen in hoeverre de inwinning van inlichtingen door de MIVD over de ontwikkeling van (kern)wapensystemen in het buitenland ook wordt afgestemd op strategische besluiten die defensie moet nemen over de verwerving van eigen defensiematerieel. Als voorbeeld noemen deze leden de verwerving van nieuwe onderzeeboten, waarvan de militaire relevantie grotendeels samenhangt met de internationale ontwikkelingen op het gebied van technologie waarmee onderzeeboten kunnen worden opgespoord.

14. Zie antwoord onder vraag 15
Vragen 14 en 15 worden gezamenlijk beantwoord.

Een ander relevant voorbeeld is wat de leden van de GroenLinks-fractie betreft de verwerving van nieuwe fregatten. Deze leden vragen of de MIVD expliciet naar informatie zoekt die relevant kan zijn voor besluiten om fregatten bijvoorbeeld uit te rusten met middelen ter bestrijding van ballistische en hypersone raketten, die voor DMO relevant kan zijn.

15. Antwoord
De MIVD doet onderzoek naar wapensystemen die nu of in de toekomst een dreiging vormen voor de huidige en toekomstige wapensystemen van de krijgsmacht of voor haar bondgenoten. De door de MIVD geschetste dreiging wordt afgewogen en meegenomen in de behoeftestellingen voor nieuwe wapensystemen voor de krijgsmacht.

Een van de doelstellingen van de gezamenlijke AIVD-MIVD Unit Contraproliferatie is het bijdragen aan het voorkomen van de uitvoer van gevoelige goederen naar kernwapenprogramma's in landen van zorg. Wanneer er relevante inlichtingen worden ingewonnen over dergelijke programma's dan worden zowel Defensie als andere belanghebbenden daarover geïnformeerd via de daarvoor bestemde kanalen.

Met betrekking tot het budget van de MIVD betreuren de leden van de GroenLinks-fractie het dat de Minister bij de afgelopen begrotingsbehandeling wederom niet is ingegaan op het verzoek van deze leden om transparant te zijn over de uitgaven aan de MIVD. Deze leden hebben begrip voor geheimhouding bij evident gevoelige informatie, maar zien niet direct aanleiding om aan te nemen dat het openbaar maken van het budget voor de MIVD, desnoods binnen bandbreedtes, een onacceptabel risico zou vormen. De leden van de GroenLinks-fractie vragen de Minister of zij dit nader kan beargumenteren, mede in het licht van het belang van de Kamer om invloed uit te kunnen oefenen op de besteding van overheidsmiddelen. Informatie die vertrouwelijk wordt verstrekt aan de CIVD komt immers niet terecht bij de woordvoerders die de bestedingen bij Defensie controleren, aldus de leden van de GroenLinks-fractie.

16. Antwoord
Het opnemen van het budget voor de MIVD in de Defensiebegroting zou inzicht geven in de capaciteiten, focusgebieden en onderzoeken van de MIVD. Daarom is het niet wenselijk het budget voor de MIVD openbaar te maken. De begroting van de MIVD wordt in de Kamer behandeld via de daarvoor geëigende kanalen. De Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) wordt geïnformeerd over de uitsplitsing van het budget over de verschillende onderzoeksgebieden van de MIVD. Ook wordt aandacht besteed aan de trends die relevant zullen zijn voor de nationale veiligheid in het aankomend jaar. Daarnaast worden de geheime uitgaven jaarlijks beoordeeld door de Algemene Rekenkamer.

SP

Met belangstelling en verbazing hebben de leden van de SP-fractie de Kamerstukken die voorliggen bestudeerd. Belangstelling om te speuren naar diepere lagen en dubbele bodems, we zijn niet voor niks in contact met een «geheime dienst». En met verbazing, vooral over de zaken die we van de CTIVD moeten leren en die niet in deze stukken staan. Het blijft naar het oordeel van de leden van de SP-fractie een groot probleem dat belangrijke onderdelen van Defensie en Buitenlandse politiek zwaar gefilterd moeten worden bediscussieerd en uit het principe van democratische controle moeten worden gecontroleerd.
In het Jaarverslag 2019 wordt gesteld dat er «een spanningsveld» is tussen publieke rapportage en het werk van een inlichtingen- en veiligheidsdienst. De leden van de SP-fractie zijn van mening dat het niet een spanningsveld is, maar een regelrechte tegenstelling. De toevoeging in het verslag dat dat de openheid «beperkt» is, is een eufemisme. De gang naar de rechter is het minimale middel van de burger. De CTIVD is het minimale middel van de volksvertegenwoordiging, aldus deze leden. Zij zijn nog steeds van mening dat daar nieuwe middelen voor openbaar debat over de MIVD moet worden gezocht. Er zijn te veel voorbeelden van zaken die in de media worden gemeld of besproken die door de Minister publiek onbespreekbaar worden verklaard. De leden SP-fractie herinneren aan het vorige algemeen overleg toen zij navraag deden naar berichten over het sluiten van de MIVD-post in Kaboel naar aanleiding van publicaties van een militair. Zowel de publicaties als de gevolgen voor de MIVD werden door de Minister voor het parlement zo klein mogelijk gemaakt. Een moeilijk te verdragen beleid omdat de details van dat beleid bekend zijn en ook een rol spelen in een groter verband, namelijk dat van operaties in Afghanistan. De leden van de SP-fractie vragen of de Minister alsnog bereid is toelichting te geven?

18. Zie antwoord onder vraag 19
Vragen 18 en 19 worden gezamenlijk beantwoord.

Het vorige algemeen overleg bespraken de leden van de SP-fractie de noodzaak voor het openbaar manier van de Aanwijzing SG A/978. De publicatie daarvan heeft een stimulans opgeleverd voor het bewustzijn van militairen dat ze het recht vrijuit te spreken, ook als het over zaken gaat die gevoelig liggen bij de MIVD of bij de CDS. Dat achten de leden van de SP-fractie een voordeel dat voortvloeit uit hun aanhouding over deze Aanwijzing. De leden van de SP-fractie verwachten een veel actiever opstelling van de regering over openheid.
Onlangs, op 20 januari 2021, stelde scheidend CDS admiraal Bauer dat geheime operaties geheim moeten blijven. De leden van de SP-fractie stellen dat ook hier het gesprek via de pers gaat. De admiraal komt niet in de Kamer debatteren. De Kamer staat altijd op achterstand als de Minister

dat geheime beleid van de CDS niet wil toelichten, aldus deze leden. Dat is naar het oordeel van de leden van de SP-fractie een relevante kwestie naar aanleiding van de uitspraak «inzet van geheime militaire eenheden is een principe». Tot nu toe heeft niemand in de Kamer dat principe onderuit gehaald. En deze leden achten democratie zeker een belangrijker principe. Al sinds 2000 is onder auspiciën van artikel 100, lid 2, Grondwet het beleid voor geheime operaties. Dat beleid dat ook door de WIV 2017 wordt gesteund, is nog nooit verantwoord. Kritiek op onderdelen wordt persoonlijk gemaakt (mariniers in De Punt, vliegeniers boven Irak/Syrië) door burgers, advocaten of sommige politici omdát het beleid hermetisch gesloten is. Dat moet veranderen, anders gaat het debat via de krant en komt het altijd een beetje beteuterd over. De leden van de SP-fractie vragen hierover een reactie van de Minister.

19. Antwoord

Transparant zijn waar het kan past bij een moderne inlichtingendienst. De MIVD probeert steeds meer inzicht te geven in de wijze waarop zij haar taken uitvoert. Hierbij valt te denken aan het publiceren van een openbaar jaarverslag en bijvoorbeeld het openbare *Dreigingsbeeld Statelijke Actoren*.

Tegelijkertijd is inherent aan operaties van de MIVD dat deze veelal geheim moeten blijven. Informatie die de werkwijze of het actueel kennisniveau van de MIVD kan prijsgeven, in strijd is met de wettelijk bepaalde bronbescherming of militaire operaties in gevaar kan brengen wordt daarom niet in het openbaar besproken. Evenmin kan worden ingegaan op individuele rechtszaken die nog worden behandeld door een rechter, persoonlijk vertrouwelijk zijn of de privacy van de betrokkene kunnen schaden. Hier is sprake van een spanningsveld tussen enerzijds het belang dat gelegen is in transparantie en anderzijds de wettelijke en operationele kaders waarbinnen het werk plaatsvindt.

De operaties van de MIVD vinden plaats binnen het veiligheidsbeleid dat onderhevig is aan publiek debat, zoals dat ook heeft plaatsgevonden over de Wiv 2017. Daarnaast wordt de uitvoering van het beleid via de geëigende kanalen gecontroleerd op een wijze die recht doet aan de principes van onze rechtsstaat. Voorts wordt de rechtmatigheid van de uitvoering, wanneer het gaat om de inzet van bijzondere bevoegdheden, getoetst door de Toetsingscommissie Inzet Bevoegdheden (TIB). Tot slot houdt de CTIVD toezicht op het handelen van de diensten. De toezichthouder kan ten behoeve van haar taak over alle informatie beschikken die zij daartoe noodzakelijk acht. De CTIVD brengt rapporten uit waarin aanbevelingen worden gedaan ten aanzien van de uitvoering van de wet. De Minister legt daar vervolgens verantwoording over af aan uw Kamer.

De leden van de SP-fractie waarderen het werk van de CTIVD en vragen de Minister te reageren op de kritiek. Vooral het punt dat de WIVD 2017 volgens deze leden nog steeds niet goed wordt toegepast, waarbij het gaat om het gebruik van «bulkdatasets». Afgelopen maanden heeft de CTIVD vastgesteld dat ook de MIVD de wet WIV 2017 niet goed uitvoert en dat de Minister opdracht krijgt daaraan te werken. De leden van de SP-fractie wat de rol en het belang van de MIVD is in het verzamelen van bulkdatasets en waarin de belangstelling verschilt van de AIVD? Deze leden vragen wat gaat de Minister gaat doen met de kritiek van de CTIVD.

20. Antwoord
Zowel de AIVD als de MIVD beschikken over algemene en bijzondere bevoegdheden om bulkdatasets rechtmatig te verzamelen. Evenals de CTIVD zijn de diensten van oordeel dat bulkdatasets grote waarde hebben voor de taakuitvoering van de AIVD en MIVD. Het betreft zowel de waarde voor de verdere analyse van gekende dreigingen als het kunnen onderkennen en identificeren van personen en organisaties en verborgen dreigingen. Het precieze belang van een specifieke bulkdataset is afhankelijk van de inlichtingenbehoefte, die volgt uit de vastgestelde Geïntegreerde Aanwijzing. Voor de MIVD zal dit vaker een militaire component bevatten, denk bijvoorbeeld aan het verzamelen van gegevens uit gebieden waar een militaire missie plaatsvindt.

In rapport 70 heeft de CTIVD zich uitgesproken over het verzamelen van bulkdatasets door inzet van de hackbevoegdheid en in rapport 71 heeft de CTIVD gerapporteerd over het verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen. De belangrijkste conclusies en aanbevelingen uit beide rapporten hebben betrekking op de verdere verwerking van bulkdata. In reactie daarop hebben de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie gezamenlijk aanvullende regels en waarborgen ingesteld,[10] die gelden voor de verdere verwerking van bulkdatasets. Met deze extra waarborgen volgen de diensten een groot deel van de aanbevelingen van de CTIVD op.

De leden van de SP-fractie nemen aan dat de aankondigde investeringen in de komende jaren in ICT ter waarde van 20 miljoen euro een ander beleidsveld is dan de 20 miljoen euro voor offensieve cyberacties. Of is dat niet het geval, zo vragen zij?

21. Antwoord
Deze aanname is correct.

De leden van de SP-fractie vragen de Minister toe te lichten wat de betekenis is van de «impact van COVID-19» op de informatiepositie van de MIVD. Wat zijn de risico's dat «de inlichtingenpositie op een verantwoord niveau» blijft. Gaat het om ziekte en dood door COVID van formele of informele medewerkers? Zo nee, wat dan, zo vragen deze leden?

22. Antwoord
Het functioneren van de MIVD is aangemerkt als vitaal proces en de werkzaamheden van de MIVD gaan met inachtneming van de maatregelen omtrent COVID-19 door. De inlichtingeninspanning ten behoeve van de nationale veiligheid en de ondersteuning van de krijgsmacht is op een verantwoord niveau doorgegaan.

Een van de toezeggingen in het algemeen overleg MIVD van 3 juli 2019 was te melden in het jaarverslag over 2019 hoeveel gevallen van rechts-extremisme er waren. «In 2019 heeft de MIVD een tweetal gevallen onderzocht van mogelijk rechts-extremisme. Dit heeft geen dreiging tegen de krijgsmacht aan het licht gebracht.» De leden van de SP-fractie vragen waarom van «mogelijk» rechts-extremisme wordt gesproken? Hoe zijn deze zaken afgehandeld? Kan de Minister stellen dat er geen rechts-extremisme in de krijgsmacht is?

[10] Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017.

23. Antwoord
Signalen die mogelijk wijzen op het aanhangen van rechts-extremistisch gedachtegoed door defensiemedewerkers zijn in de regel aanleiding tot nader onderzoek voor de MIVD. Zo lang onderzoek nog geen uitsluitsel heeft geboden wordt de term «mogelijk» gehanteerd. In de betreffende gevallen in 2019 bleek op basis van het ingestelde onderzoek geen sprake te zijn van rechts-extremisme.

De leden van de SP-fractie delen de noodzaak dat proliferatie van massavernietigingswapens zeer ongewenst is. Sinds enige tijd, 2019, bestaat de gezamenlijke Unit Contra Proliferatie (UCP) die onderzoek doet naar landen die worden verdacht in strijd met die verdragen te handelen. Deze leden vragen wat daarvan de resultaten zijn en wat de waarborgen zijn dat een geval van Nederlandse medewerking indertijd aan proliferatie van kernwapens van Pakistan, wordt voorkomen. De leden van de SP-fractie vragen de Minister dat toe te lichten.

24. Antwoord
Een van de aandachtsgebieden van de in 2008 opgerichte, Unit Contraproliferatie is het voorkomen van de uitvoer van gevoelige goederen naar kernwapenprogramma's in landen van zorg. Wanneer er relevante inlichtingen worden ingewonnen over dergelijke programma's dan worden verschillende afnemers daarover zo goed mogelijk geïnformeerd. Om de uitvoer van goederen te voorkomen wordt het Ministerie van Buitenlandse Zaken hierover geïnformeerd. Dit kan zowel op initiatief van de UCP, via ambtsberichten van de diensten, als op initiatief van BZ via vergunningsvoorleggingen. Jaarlijks worden meerdere verwervingspogingen voorkomen. Het blijft ondanks de inspanningen echter voorstelbaar dat er *dual-use* goederen via geraffineerde handelsconstructies hun weg vinden naar landen van zorg.

SGP

De leden van de SGP-fractie hebben met belangstelling kennisgenomen van de stukken bij het schriftelijk overleg over de MIVD. Zij hebben de volgende vragen en opmerkingen.
In de Jaarplanbrief MIVD 2021 staat dat spionage, beïnvloeding en sabotage een ernstige dreiging blijven voor Nederland en zijn bondgenoten. Daarbij worden Rusland en China expliciet genoemd. Is er sprake van een toename van vijandige activiteiten van genoemde landen op dit terrein, zo vragen de leden van de SGP-fractie? Welke doelen lijken hiermee voornamelijk te worden beoogd?

25. Antwoord
De spionagedreiging die uitgaat van de Russische Federatie richting defensie- en bondgenootschappelijke belangen is onverminderd hoog en is de afgelopen jaren veel zichtbaarder geworden. De Russische Federatie is op zoek naar informatie om zijn krijgsmacht te moderniseren, de economie te versterken of politieke besluitvorming te beïnvloeden. Het kan hierbij gaan om klassieke spionage, om digitale spionage of een combinatie van beide. Het DBSA stelt dat de belangrijkste potentiele dreiging voor de fysieke territoriale integriteit van Nederland en het NAVO-bondgenootschap komt uit Rusland. Rusland beschouwt de NAVO als de belangrijkste externe dreiging.

Bij de beantwoording van vraag 2 van D66 wordt antwoord gegeven op de vraag ten aanzien van China.

Het Jaarplan voor 2020 vermeldde dat de MIVD onderzoek doet naar Afghanistan, Syrië en Irak. Het Jaarplan voor 2021 noemt deze landen niet. De leden van de SGP-fractie vragen of dit een wijziging inhoudt van de geografische focus voor 2021, en zo ja, hoe dit zich verhoudt tot de mogelijkheid van een wederopstanding van terreurgroepen zoals IS in Irak en Syrië. Hoe wordt met een dergelijk scenario rekening gehouden?

26. Antwoord
In de Jaarplanbrief 2021 is uw Kamer geïnformeerd over de aandachtsgebieden van de MIVD. De genoemde landen blijven ook in 2021 onderwerp van onderzoek. Ten aanzien van ISIS geldt dat er geen sprake is van een wederopstanding omdat ISIS nog steeds aanwezig is maar geleidelijk is overgegaan op een guerrillastrijd. Wel is en blijft ISIS een grote bron van zorg omdat deze nog steeds ondermijnende activiteiten ontplooit, een dreiging vormt jegens Nederlandse troepen in de regio's waar ISIS actief is en vanuit Syrië en Irak een serieuze terroristische dreiging vormt tegen het Westen in het algemeen.

De MIVD en de AIVD doen samen onderzoek naar landen die ervan worden verdacht dat zij werken aan het ontwikkelen van massavernietigingswapens. In dit kader wijzen de leden van de SGP-fractie op het gevaar van de ontwikkeling van een nucleair wapen door Iran. Recent gaf de hoogste Israëlische legerbevelhebber zelfs aan paraat te zijn voor een aanval op Iran om nucleaire proliferatie te voorkomen. Hoe wordt de informatie van onze inlichtingendiensten betrokken bij het bepalen van de Nederlandse positie en (diplomatieke) inzet richting Iran, zo vragen de leden van de SGP-fractie? Wordt op dit thema samenwerking gezocht met bijvoorbeeld Israëlische en Amerikaanse diensten?

27. Antwoord
De MIVD en de AIVD informeren met grote regelmaat via de daarvoor geëigende kanalen verschillende afnemers over dit onderwerp. Het beantwoorden van vragen over samenwerkingsverbanden of herkomst van inlichtingen is een bevestiging of ontkenning van het bestaan van de samenwerkingsverbanden en kan daarmee inzicht geven in de werkwijze en het kennisniveau van de diensten. In voorkomende gevallen wordt uw Kamer daar via de daartoe geëigende kanalen over geïnformeerd.

De MIVD onderzoekt in 2021 spionage- en cyberactiviteiten van vreemde mogendheden tegen de Nederlandse Defensie-industrie. De leden van de SGP-fractie vragen wat in de praktijk de aard en omvang is van spionage of zelfs diefstal van hoogwaardige kennis en technologie bij de Nederlandse defensie-industrie door buitenlandse actoren. Deze leden vragen of een overzicht of indicatie kan worden gegeven. Heeft de MIVD tevens nadrukkelijk aandacht voor Nederlandse bedrijven die technologieën ontwikkelen die meer indirect gebruikt (kunnen) worden voor militaire- of veiligheidsdoeleinden, zoals surveillance? Zo nee, waarom niet, en bestaat er dan noodzaak de inzet in dezen alsnog te wijzigen?

28. Antwoord
Vanwege het vertrouwelijke karakter van de informatie doet de MIVD geen uitspraak over individuele zaken. Over het algemeen kan worden gesteld dat de Nederlandse defensie-industrie een hoogwaardige industrie is, en beschikt over geavanceerde kennis en technologieën waar China en Rusland in zijn geïnteresseerd.

Dit maakt de defensie-industrie een doelwit voor (economische) spionage, zowel fysiek als in het digitale domein. Het onderzoek naar cyberspionage – en sabotageactiviteiten wordt door de MIVD voortgezet.

De MIVD draagt bij aan de weerbaarheid en veiligheid van Defensie en de aan Defensie gerelateerde industrie. Voor zowel omvangrijke materieelprojecten als de uitvoering van bepaalde diensten, is Defensie afhankelijk van externe marktpartijen. Bedrijven die belast zijn met de uitvoering van gerubriceerde of vitale defensieopdrachten zijn gehouden aan de regeling Algemene Beveiligingseisen voor Defensieopdrachten (ABDO). De MIVD autoriseert Defensieorderbedrijven voordat zij mogen werken aan gerubriceerde opdrachten voor Defensie. De MIVD controleert ook op de naleving van de beveiligingseisen door regelmatige audits en inspecties uit te voeren. Daarnaast adviseert de MIVD gedurende de looptijd van een autorisatie ABDO-bedrijven en Defensie over veiligheidsbevorderende maatregelen.

Vanwege de samenhang tussen binnenlandse en buitenlandse veiligheid achten de leden van de SGP-fractie de samenwerkingsagenda van de AIVD en MIVD van groot belang. In hoeverre spelen onder meer de opkomst van nepnieuws en «deep fake» videotechnologie een rol in de activiteiten van deze diensten? Bestaan er aanwijzingen dat ook statelijke actoren zich van dergelijke middelen bedienen teneinde de Nederlandse democratie en samenleving te beïnvloeden of ondermijnen? Heeft dit de aandacht in het kader van de aankomende Tweede Kamerverkiezingen, zo vragen de leden van de SGP-fractie?

29. Antwoord
Desinformatie als middel van heimelijke politieke beïnvloeding en samenhangende ontwikkelingen op technologisch vlak hebben de aandacht van de diensten. De MIVD heeft vastgesteld dat met name de Russische Federatie beïnvloedingsoperaties uitvoert en daartoe gebruik maakt van sociale media en digitale onderzoeksplatforms. De AIVD heeft zoals gemeld in het jaarverslag 2019 in Nederland pogingen gezien van Russische inmenging. Zo is er sprake van voortdurende (online)beïnvloedingsactiviteiten op sociale media vanuit Rusland, waarbij de beïnvloeding van de beeldvorming ten aanzien van de toedracht van de ramp met vlucht MH17 een grote rol speelt. Het land beschikt hiertoe over steeds meer geavanceerde technische capaciteiten maar maakt ook gebruik van individuen, die parallel aan hun eigen belang ook het belang van Rusland dienen. De impact op Nederland lijkt vooralsnog beperkt.
De Nederlandse inlichtingen- en veiligheidsdiensten dragen vanuit verschillende taakvelden bij aan het verloop van veilige en eerlijke Tweede Kamer Verkiezingen 2021, bijvoorbeeld via bijdragen aan diverse dreigingsbeelden. Momenteel gaat er, naar inschatting van de AIVD, een beperkte maar voorstelbare dreiging uit van statelijke actoren richting het verkiezingsproces in Nederland. De betrokken ministeries en inlichtingen- en veiligheidsdiensten staan doorlopend in nauw contact om informatie en signalen van mogelijke inmengingsactiviteiten te delen en te duiden en daarop zo nodig te acteren. Daarbij spelen de inlichtingen- en veiligheidsdiensten een rol bij het tijdig onderkennen van ongewenste buitenlandse inmenging, waar grootschalige, door statelijke actoren geïnitieerde desinformatiecampagnes een uitingsvorm van kunnen zijn.