33321 Defensie Cyber Strategie

Nr. 11 **VERSLAG VAN EEN COMMISSIEDEBAT**
Vastgesteld 24 juli 2024

De vaste commissie voor Defensie heeft op 12 juni 2024 overleg gevoerd met mevrouw Ollongren, minister van Defensie, over:

- de brief van de minister van Defensie d.d. 18 april 2024 inzake openbaar jaarverslag 2023 van de Militaire Inlichtingen- en Veiligheidsdienst (Kamerstuk 29924, nr. 260);

- de brief van de minister van Defensie d.d. 20 december 2023 inzake jaarplanbrief MIVD 2024 (Kamerstuk 29924, nr. 255);

- de brief van de minister van Defensie d.d. 5 juni 2024 inzake impact toepassing regeling met CTIVD inzake bulkdatasets (Kamerstuk 36263, nr. 41);

- de brief van de minister van Defensie d.d. 26 februari 2024 inzake toepassing regeling met CTIVD inzake bulkdatasets (Kamerstuk 36263, nr. 38);

- de brief van de minister van Defensie d.d. 30 mei 2024 inzake optreden Defensie in het cyberdomein (Kamerstuk 33321, nr. 10).

Van dit overleg brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De fungerend voorzitter van de commissie,

De Roon

De griffier van de commissie,

De Lange

Voorzitter: De Roon

Griffier: Manten

Aanwezig zijn acht leden der Kamer, te weten: Boswijk, Dassen, Erkens, Kahraman, Nordkamp, Pool, De Roon en Tuinman,

en mevrouw Ollongren, minister van Defensie.

Aanvang 13.04 uur.

De **voorzitter**:

Ik open dit commissiedebat van de commissie voor Defensie met de minister van Defensie. Het onderwerp van vandaag is MIVD en cyber. Op dit moment tel ik zeven woordvoerders van de kant van de Kamer. We hebben maar twee uur de tijd. Dus in de eerste termijn heeft iedereen drie minuten en maximaal één interruptie, als het nodig is. Meneer Tuinman.

De heer **Tuinman** (BBB):

Voorzitter, daar doen we het voor. Afgelopen zaterdag was de 80ste verjaardag van D-day, Operatie Overlord in Normandië. Dat was de start van het einde van de Tweede Wereldoorlog. Deze operatie benadrukt het belang van informatie, inlichtingen, deceptie en de informatieomgeving. Wist u bijvoorbeeld dat de Duitsers angst hadden voor het niet-bestaande First US Army Corps van generaal Patton? Spionnen in een dubbelcrossnetwerk, neplegers, duizenden opblaasbare tanks, crypto, enigmacodes en ultra-informatie waren cruciaal om de geallieerden op het Europese vasteland te krijgen. Het Amerikaanse leger heeft zelfs tot 1996 geheimgehouden dat het hierbij om een nepleger ging.

Voorzitter, ik kom to the point. Ik ben blij dat Nederland en de NAVO informatiegestuurd en multidomein-optreden versneld omarmen. Daarnaast ben ik tevreden dat de Tweede Kamer een tijdje terug op mijn initiatief een rondetafel heeft georganiseerd over data science, informatiegestuurd optreden en multidomein-optreden. Een terugkerend advies was daarbij: experimenteren, experimenteren en experimenteren. De landmacht heeft in 2021 geëxperimenteerd met het LIMC en heeft ook aan iedereen duidelijk

gemaakt dat er haken en ogen zitten aan het juridische regime met betrekking tot het verzamelen, categoriseren, analyseren en rapporteren van informatie buiten een oorlogssituatie. De commissie-Brouwer heeft ook aanbevelingen opgesteld. Het rapport laat zien dat de regering worstelt met de fase tussen vrede en oorlog, de grey zone, waar Rusland en China, en ook wel Iran, ons keer op keer uitdagen. In deze schemerzone gelden andere formele en informele regels. De Tijdelijke wet cyberoperaties voor bulkdatasets en de vernieuwing die eraan komt van de Wet op de inlichtingen- en veiligheidsdiensten, de Wiv, zijn stappen om Nederland weerbaarder te maken in het informatiedomein in de schemerzone van het conflict.

Voorzitter. De situatie is niet meer zoals in 1944. De informatieomgeving is veranderd. Het heeft impact op hoe we willen, kunnen en mogen optreden in de informatieomgeving. Daar heb ik drie vragen over. Hoe wordt gegarandeerd dat de Commandant der Strijdkrachten over de inzetopties van het Defensie Cyber Commando blijft beschikken als het Defensie Cyber Commando met de MIVD meer en meer in Cyber Mission Teams gaat samenwerken?

Voorzitter. Dan mijn tweede vraag. Hoe staat het met de uitwerking van de actielijnen en de aanbevelingen van de commissie-Brouwer? Daar komt ook de volgende vraag uit voort. Hoe staat het met het aangekondigde onderzoek dat bij de Nederlandse Defensie Academie is uitgezet?

Voorzitter. Dan mijn laatste vraag aan de minister. Voldoen de drie hoofdtaken zoals we die geformuleerd hebben voor Defensie nog bij informatiegestuurd optreden en wat zouden we daar eventueel in moeten aanpassen?

De **voorzitter**:

Dank, meneer Tuinman van BBB. Dan is het woord aan de heer Pool van de PVV.

De heer **Pool** (PVV):

Dank u zeer, meneer de voorzitter. Onze Militaire Inlichtingen- en Veiligheidsdienst vervult een belangrijke rol in het beschermen van onze nationale veiligheid. Zonder het belangrijke werk van de MIVD zou Nederland blind zijn voor de vele dreigingen waarmee wij geconfronteerd worden. De PVV spreekt dan ook haar grote waardering uit voor de inzet van al onze MIVD-medewerkers.

Voorzitter. Ik heb vandaag nog wel wat vragen. Op pagina 21 van het jaarverslag van de MIVD stelt de dienst meer zicht te hebben gekregen op kritische geluiden over Defensie uit rechts-extremistische kringen. Deze

kritiek richt zich bijvoorbeeld op het door Defensie gevoerde diversiteitsbeleid. De MIVD werkt eraan om rechts-extremisme bij Defensie te weren. Dat is natuurlijk goed. Maar ik heb een vraag aan de minister. Wat verstaat de MIVD onder de term "rechts-extremisme"? Betreft dat iedereen die niet staat te juichen als Defensie weer de regenboogvlag hijst of een dragqueen invliegt om onze militairen voor te lezen? Of hanteert de MIVD de partijlijn van deze D66-minister, waarbij onze partij, de PVV, stelselmatig onterecht wordt weggezet als extreemrechts? Zo noemde de partijleider van de minister de PVV vorige week bij WNL nog extreemrechts. Als deze minister die partijlijn ook hier doorvoert, moet de MIVD namelijk wel een hele grote groep mensen onderzoeken. We zijn immers de grootste partij van Nederland. Graag een reactie, voorzitter.

Voorzitter. Terwijl hier dus rapporten vol over worden geschreven, lees ik nergens iets over de oproepen tot intifada, die nu door de Nederlandse straten schallen. Het lijkt de PVV toch van belang dat onze MIVD hier een nauwlettend oog op houdt, gezien intifada staat voor een gewelddadige opstand. Wel wordt er kort gesproken over de verhoogde dreiging van jihadistisch terrorisme. Er bestaat een reële kans dat er een aanslag zal plaatsvinden in Nederland. Kan de minister verdere toelichting geven op deze dreiging en de acties die de MIVD nu neemt om deze dreiging het hoofd te bieden?

Voorzitter. Het kernwoord in dit debat moet wat de PVV betreft dan ook "realiteitszin" zijn. We kunnen het ons simpelweg niet veroorloven om de jacht te openen op mensen met kritiek op diversiteitsbeleid, terwijl jihadisten de grootste terroristische dreiging zijn voor Nederland.

Voorzitter. Tot slot over de Chinese inbraak bij Defensie. De MIVD maakte recent voor het eerst een technisch rapport over de werkwijze van Chinese hackers openbaar, nadat er malware was aangetroffen op een losstaand computernetwerk bij de krijgsmacht. Een vraag aan de minister: kan zij een actuele stand van zaken geven als het gaat om de Chinese hackpogingen bij Defensie en de wijze waarop de MIVD hier weerstand aan biedt? Dat is namelijk geen gemakkelijke taak als je ziet op wat voor schaal China hackers inzet. Dus graag een reactie.

Voorzitter, dank u wel.

De **voorzitter**:

Dank, meneer Pool. Er is een interruptie van de heer Erkens. Gaat uw gang.

De heer **Erkens** (VVD):

Een groot deel van de inbreng ging over rechts-extremisme en hoe de MIVD dat monitort en wat daar allemaal onder valt. Het lijkt mij niet dat het draait

om een mening die aan de rechterkant van het politieke spectrum zit, maar in Duitsland zagen we vorig jaar dat er door de inlichtingendiensten zelfs een staatsgreep voorkomen was door die monitoring op rechts-extremisme. Is de PVV wel van mening dat we met de juiste definitie moeten blijven monitoren op rechts-extremisme?

De heer **Pool** (PVV):

Jazeker, daarom noemde ik het in mijn spreektekst goed dat daar aandacht voor is. Ik wil alleen wel van de minister weten wat er precies mee wordt bedoeld. Als we het hebben over de nauwe definitie, namelijk dat het mensen zijn die bereid zijn geweld te gebruiken, snap ik het volledig. Alleen, wanneer we de definitie gebruiken van de partij waar deze minister van is, D66, dan gaat het ook, compleet onterecht, over onze eigen partij. Dat lijkt mij niet de bedoeling. Daarom heb ik een verhelderende vraag aan de minister.

De **voorzitter**:

Meneer Erkens nog? Niet?

De heer **Erkens** (VVD):

We hebben maar één interruptie, zei u, voorzitter.

De **voorzitter**:

Uw interruptie heeft u dan nu gehad, maar u kunt altijd een vervolgvraag stellen. Zo ben ik in het kader van interrupties dan ook wel weer. Maar goed, u gaat verder met uw eigen bijdrage namens de VVD-fractie. Gaat uw gang.

De heer **Erkens** (VVD):

Dank u, voorzitter. De cyberdreiging tegen Nederland en zijn bondgenoten is onverminderd groot en vraagt om een sterke krijgsmacht met een sterke cyberpoot. De tijdelijke wet zal hopelijk zorgen voor meer juridische ruimte voor de inlichtingendiensten om slagvaardig en snel te kunnen handelen.

Voorzitter. In dit korte debat heb ik een aantal punten. Ten eerste. De veiligheidsonderzoeken die nodig zijn om bij Defensie aan te slag te gaan, lopen meer en meer vertraging op. Berichtgeving toont aan dat Defensie hierdoor ook mensen kwijtraakt aan andere werkgevers. Gegeven de personeelsschaarste bij Defensie is dit onacceptabel. Wat is in werking gezet om deze vertragingen te voorkomen, zo vraag ik het kabinet. We gaan de

komende jaren immers alleen nog maar meer mensen moeten aantrekken bij Defensie. Dit zal mogelijk een herziening en verdere automatisering van het proces vergen, aangezien een enkelzijdige focus op meer werknemers lastig zal zijn in deze krappe arbeidsmarkt. Wat gaat het kabinet hieraan doen? Wanneer komt de herziening van de Wet veiligheidsonderzoeken naar de Kamer? Biedt deze ook extra oplossingen voor de oplopende wachttijden?

Voorzitter. Defensie moet de komende jaren de slagkracht in het cyberdomein vergroten. Welke intensiveringen in het domein zijn er de komende jaren gepland? Hoe zorgt het kabinet dat er voldoende kundige mensen aangetrokken en behouden worden bij zowel de MIVD als ook de andere cybercapaciteit? Onder andere nieuwe huisvesting is daarbij van belang. Hoe staat het met het verder uitbreiden van het aantal cyberreservisten bij Defensie? Welke afspraken worden gemaakt met grote private spelers in dit domein, zodat Defensie voldoende toegang heeft tot deze vaardige cyberspecialisten gedurende een mogelijk conflict?

Voorzitter. Zoals al vaker besproken leven we niet in een oorlogssituatie, maar ook niet echt in vredestijd. We zien dit al helemaal in het cyberdomein, waarin onze tegenstanders elke dag proberen om posities te verwerven in onze systemen, posities die schadelijk zijn voor onze nationale veiligheid. Defensie moet in deze tussenfase de juiste bevoegdheden hebben om de samenleving veilig te houden alsook om zelf sterk te staan tegenover potentiële tegenstanders. Hoe staat het met het onderzoek naar een wettelijke grondslag in de vorm van een wet op de gereedstelling? Hoe zit het hierbij met de mogelijkheid tot bijvoorbeeld terughacken?

Voorzitter. Dan mijn laatste punt: het belang van openbaarmaking van cyberoperaties van onze strategische tegenstanders waar dat kan zonder operationele posities te beschadigen. De MIVD heeft onlangs een grootschalige operatie vanuit China blootgelegd -- een collega had het er ook over. Volgens mij is dat heel goed, want het vergroot de maatschappelijke bewustwording van de dreiging waarmee we op dit moment te maken hebben. Mijn vraag aan het kabinet is dan ook hoe uitvoering wordt gegeven aan de motie die we op dit vlak hebben aangenomen als Kamer.

Dank u, voorzitter.

De **voorzitter**:

Dank u wel, meneer Erkens. Er is een vraag van de heer Dassen. Begreep ik dat goed? Ja? Gaat uw gang.

De heer **Dassen** (Volt):

Dat klopt. De heer Erkens triggerde mij met een vraag die ik dadelijk ook aan de minister ga stellen. Je hebt de grey zone. Je bent wel in conflict maar nog

niet in oorlog en er zit -- hoe zeg je dat? -- eigenlijk een juridisch tekort in het internationaal recht. De AIV heeft net een rapport uitgebracht waarin zij zeggen dat het kabinet daarmee aan de slag moet gaan. Ik ga er dadelijk ook een paar vragen over stellen. Ik was benieuwd hoe de heer Erkens daarnaar kijkt.

De heer **Erkens** (VVD):

Dit is volgens mij een meer dan terecht punt van de heer Dassen. Die ruimte moet er komen. Ik kon in de brief lezen dat er een wet op de gereedstelling gemaakt wordt. Volgens mij moet die wet inderdaad meer ruimte gaan bieden in het grijze gebied. Alleen weet ik niet of die van toepassing gaat zijn op het cyberdomein; volgens mij nog niet op dit moment. Mijn vraag aan het kabinet, die ik dan met u deel, is: is dat misschien een logische route om meer ruimte te gaan bieden, zodat Defensie in het cyberdomein, alsook in het grijze gebied, meer ruimte krijgt en we inderdaad niet met beide handen gebonden op de rug die strijd moeten aangaan met onze tegenstanders?

De heer **Dassen** (Volt):

Precies. Ik denk namelijk ook dat het belangrijk is dat we dit verder ontwikkelen in het internationaal recht: wanneer ga je daadwerkelijk ook een juridische grens over in plaats dat je met elkaar in die grey zone blijft zitten? Een korte vervolgvraag. In dat advies komt naar voren dat we ook kritisch moeten kijken naar de hoofdtaken van Defensie zoals ze nu beschreven zijn in de Grondwet. Die vraag wil ik dadelijk ook aan de minister stellen, juist om te zorgen dat dit daar beter ingekaderd wordt. Ik was benieuwd of de heer Erkens het met mij eens is dat we dat moeten onderzoeken. Willen we daar inderdaad kritisch naar kijken? En moet het kabinet, de minister samen met juristen, misschien eens kritisch naar deze beschrijving gaan kijken?

De heer **Erkens** (VVD):

Dat is een goede vraag. Ik denk dat het goed is om er kritisch naar te kijken welke ruimte daarvoor nodig is en ook wat er herijkt moet worden. Ik zou wel oppassen dat je niet in een zwart-witscenario terecht gaat komen waarin je het onderscheid nog groter maakt: of het is oorlog of het is geen oorlog. Volgens mij zitten we nu precies in een tussensituatie waarin je een soort opschalingsladder wil hebben en Defensie meer bevoegdheden krijgt naarmate de situatie serieuzer wordt. Ik zou die richting steunen. Ik zou oppassen met het verder zwart-wit maken van: wat is die grey zone dan en wanneer ben je in oorlog of niet? Want het kan ook het effect hebben dat we juist minder ruimte krijgen om te handelen.

De **voorzitter**:

Dan gaan we luisteren naar de heer Boswijk van het CDA voor zijn inbreng.

De heer **Boswijk** (CDA):

Dank u wel, voorzitter. Voor de weerbaarheid van onze samenleving is het van belang dat we onze vitale infrastructuur beschermen. Het gaat om fysieke infrastructuur zoals op de Noordzee, maar ook om de veiligheid van onze digitale infrastructuur. Onze digitale footprint wordt met de dag groter, en informatie die in die voetafdruk hoort is van cruciaal belang voor onze veiligheid en voor ons maatschappelijk verkeer. Elke dag zijn er 100.000 Chinese hackers bezig met het ondermijnen van onze netwerken. Op dit moment is de Nederlandse burger net zo goed beschermd als de Chinese en Russische burger. Dat maakt het voor de inlichtingendiensten ingewikkeld.

Dat onze digitale infrastructuur kwetsbaar is, zagen we onder andere deze week toen de MIVD en het Nationaal Cyber Security Centrum bekendmaakten dat een Chinese statelijke hackersgroep in 2022 en 2023 toegang kregen tot minstens 20.000 systemen wereldwijd, onder andere van de Nederlandse krijgsmacht. Defensie kent binnen het cyberdomein drie aandachtsgebieden, waaronder cyberveiligheid; met andere woorden, het beschermen van onze eigen systemen, processen, operaties en personeel. De MIVD heeft hiervoor kabeltoegang nodig. De tijdelijke wet moet de MIVD in staat stellen om sneller op te treden en dreigingen het hoofd te bieden en om gebruik te maken van kabelinterceptie om relevant berichtenverkeer en malware te onderscheppen in het belang van de nationale veiligheid en de cybersecurity. Op 1 juli moet deze tijdelijke wet in werking treden. Kan de minister aangeven in hoeverre deze wet kan bijdragen om de dreigingen vanuit China, Iran en Rusland tegen te gaan? Wat is volgens de minister eventueel meer nodig om deze dreigingen het hoofd te kunnen bieden? Hoe kijkt de minister naar de bijzondere bevoegdheid van de MIVD? Ziet zij net als het CDA de noodzaak en dat het met de huidige internationale dreigingen belangrijker is om de diensten in staat te stellen voorspellend en met een intelligencebril te laten kijken naar de bevoegdheden? Nu kijken we namelijk vaak terug, onder andere met de toezichthouder, terwijl we eigenlijk juist vooruit moeten kijken. Hoe kijkt de minister hiernaar? Is de minister het daarom met het CDA eens dat de MIVD kabeltoegang nodig heeft om zijn rol voor cyberveiligheid te kunnen vervullen?

Voorzitter. De Adviesraad Internationale Vraagstukken schreef vorige week ook een adviesrapport over de hybride dreiging en de maatschappelijke weerbaarheid. De AIV stelt daarin onder andere dat de NAVO een studie zou moeten doen naar de wijze waarop artikel 5 al dan niet ingeroepen dient te worden bij cyberaanvallen. Tevens zou volgens de AIV artikel 3 navolging moeten krijgen ten behoeve van het versterken van de collectieve

weerbaarheidsdoelen, zowel militair als niet-militair. Wat is de reactie van de minister op deze voorstellen van de AIV?

Voorzitter, ten slotte. Afgelopen december liet de minister weten dat de plannen voor de gezamenlijke huisvesting voor de AIVD en de MIVD op de Frederikkazerne in Den Haag worden stopgezet. Kan de minister al aangeven hoe de plannen voor de nieuwbouw er nu voorstaan?

Ten slotte, voorzitter, wil ik me aansluiten bij de dankwoorden en de waardering die collega Pool net uitte richting alle medewerkers van de MIVD.

De **voorzitter**:

Dank u wel, meneer Boswijk. Dan gaan we nu luisteren naar de heer Kahraman van Nieuw Sociaal Contract.

De heer **Kahraman** (NSC):

Dank u wel, voorzitter. We moeten ons bewuster worden, bewuster van het feit dat oorlog vandaag de dag niet meer een ver-van-ons-bedshow is, maar een gegeven waar we op termijn allemaal mee te maken krijgen, one way or another. In een podcast, Samen Sterker, licht kolonel Han Bouwmeester toe dat er tegenwoordig geen wapens en munitie meer nodig zijn om een samenleving te ontwrichten. Denk bijvoorbeeld aan een stroomuitval tijdens een operatie in het ziekenhuis. Dit kan levens kosten. Denk aan de chaos die ontstaat als we zonder mobiele telefoons, laptops en elektrische auto's komen te zitten. Onze krijgsmacht wordt regelmatig getergd door cyberattacks en -spionage. Zo werd bijvoorbeeld afgelopen februari -- daar refereerden mijn collega's ook allemaal aan -- door de MIVD Chinese cyberspionage ontdekt op software van Defensiecomputers. Deze hack blijkt nu meer gevolgen te hebben gehad dan in eerste instantie gedacht. De vraag is hoeveel hackactiviteiten er nog niet ontdekt zijn.

Voorzitter. Tijdens het vragenuur van 14 mei jongstleden heb ik vragen gesteld over de Russische vissersboten in de Eemshaven. Daarbij zei de minister toe dat de Russische schepen geweerd worden uit de Eemshaven. De NSC-fractie heeft signalen ontvangen dat er nog steeds Russische vissersboten aanmeren, misschien nu onder de Noorse vlag. Herkent de minister deze signalen? Kan de minister aangeven of de MIVD zicht heeft op Russische spionage in Nederland en welke maatregelen er inmiddels worden genomen?

Voorzitter. China is al langere tijd bezig met de ontwikkeling als regionale en mondiale grootmacht en bouwt hard aan een dominante positie op het gebied van militaire technologie, onder andere in cyberspionage. Dit gaat met een snelheid die nauwelijks bij te houden is. Nederland is een aantrekkelijk doelwit door het hoge niveau van de aanwezige kennis op het

gebied van onder andere halfgeleiders, kwantumtechnologie en lucht- en ruimtevaart.

Voorzitter. De minister heeft in haar jaarplan 2023-2024 aangegeven dat er gekeken wordt naar welke acties en investeringen nodig zijn om diensten op te bouwen die de Chinese dreiging buiten de deur houden. Kan de minister toelichten welke acties en investeringen al uitgevoerd zijn?

Voorzitter. Ik had het in mijn bijdrage ook over het tekort bij de dienst die de screening doet bij de MIVD. De heer Erkens heeft de vragen die ik wilde stellen eigenlijk al gesteld; dank daarvoor. Ik ben heel benieuwd naar de beantwoording van de minister hiervan.

Als laatste wil ik de minister ook vragen hoe zij aankijkt tegen samenwerking met commerciële bedrijven om onze cyberweerbaarheid beter te maken. Werken we ook samen met commerciële bedrijven om ons als Nederland echt te weren tegen cyberaanvallen?

Dank u wel, voorzitter.

De **voorzitter**:

Dank u wel, meneer Kahraman. Er is een vraag voor u van de heer Boswijk.

De heer **Boswijk** (CDA):

Ik was even benieuwd. Voor de rest ben ik het helemaal eens met de inbreng van de heer Kahraman. Ik heb het alleen in andere debatten ook vaker gehad over veiligheid en hoe technologie ons daarbij kan helpen. Dan merkte ik toch vaak dat NSC heel terughoudend en ook erg wantrouwend is tegenover nieuwe technologie. Ik hoor nu ook een opmerking over het betrekken van commerciële bedrijven. Ik denk dat we in een weerbare samenleving zo veel mogelijk partijen erbij moeten betrekken. Hoe kijkt NSC zelf naar het betrekken van commerciële bedrijven bij het helpen bij onze cyberveiligheid?

De heer **Kahraman** (NSC):

We moeten als Nederland alles doen om onszelf weerbaarder te maken. Ik denk dat het onontkoombaar is dat we ook met commerciële partijen gaan samenwerken. Uiteindelijk hebben die de meeste mensen in dienst die kennis hebben van deze materie. Als de nood echt aan de man is, zullen we ook die bedrijven moeten bijschakelen. Voor mij is het, denk ik, onderdeel van onze weerbaarheid. Als Nederland moeten we dan ook Nederlandse bedrijven kunnen betrekken bij het weerbaarder maken van onze samenleving.

De heer **Boswijk** (CDA):

Daar ben ik het mee eens, maar ik hoor toch dat er heel vaak spanning zit tussen enerzijds veiligheid en anderzijds privacy. Ik hoor dat collega Kahraman naar de veiligheidskant hangt, terwijl ik merk dat NSC vaak heel erg naar de privacykant hangt. Is de heer Kahraman zich ervan bewust en is hij het ermee eens dat als het die kant op gaat, wat volgens mij onvermijdelijk is, de consequentie kan zijn dat we iets moeten inleveren op het gebied van onze privacy, waardoor onze samenleving wel weer veiliger wordt? Zou dat een probleem zijn voor NSC?

De heer **Kahraman** (NSC):

Voor ons zijn privacy, het juist toepassen ervan en de bescherming van onze eigen burgers ook heel belangrijk. We begrijpen natuurlijk dat we de hele samenleving moeten beschermen, maar bij een aantal processen mag het belang van een individu niet aangetast worden. Volgens mij moet je dus echt een balans zoeken. Ik wil dus niet zeggen dat het een het ander volledig moet uitsluiten, maar het moet wel goed in balans zijn. Daar moet ook toezicht op zijn. Voordat we dergelijke zaken gaan inrichten, moeten die ook duidelijk gecommuniceerd zijn naar Kamerleden.

De **voorzitter**:

Dan is het woord aan de heer ... Meneer Nordkamp, u wilt ook een interruptie? Gaat uw gang.

De heer **Nordkamp** (GroenLinks-PvdA):

De heer Kahraman had het over samenwerking met commerciële bedrijven op bijvoorbeeld het gebied van cyber en inlichtingen, omdat we daar zelf de handen of kennis niet voor hebben. Is het wellicht bespreekbaar om te kijken in hoeverre we de samenwerking met andere landen en hun diensten opschalen, in plaats van of naast een samenwerking met commerciële bedrijven? Ik vraag dat vanuit dezelfde redenering, namelijk dat er voor onszelf vanwege het gebrek aan handjes en kennis wellicht de noodzaak is om samen te werken. Kunnen we dus naast of in plaats van naar commerciële bedrijven te kijken ook over onze landsgrenzen heen kijken?

De heer **Kahraman** (NSC):

Het lijkt me noodzakelijk dat we juist ook op dit domein gewoon in NAVO-verband elkaar versterken en met elkaar samenwerken, net zoals bij alle

andere defensiedomeinen. Er is wat mij betreft dus geen enkele discussie over dat we ook op dit domein moeten samenwerken in NAVO-verband.

De **voorzitter**:

Dan is het woord aan de heer Nordkamp namens zijn fractie, GroenLinks-Partij van de Arbeid.

De heer **Nordkamp** (GroenLinks-PvdA):

Dank, voorzitter. We lezen dat de MIVD en de AIVD ook in 2024 hun focus blijven richten op China. De MIVD waarschuwt voor de snelle en assertieve ontwikkeling van China. Dit omvat verschillende ontwikkelingen, zoals aanzienlijke investeringen in kunstmatige intelligentie en kwantumcomputers. De ontwikkeling die China doormaakt, is volgens de MIVD voor het Westen haast niet bij te houden. De vraag hoe we ervoor zorgen dat we zo goed mogelijk bijblijven, is uiteraard interessant, maar ik wil ook graag weten wat hiervan de oorzaken zijn geweest, zodat we daar lering uit kunnen trekken en die lessen kunnen toepassen op andere terreinen. De inlichtingendiensten onderzoeken momenteel welke acties en investeringen nodig zijn om goed zicht te krijgen op de dreiging van China. Onze vraag is in hoeverre samenwerking met andere landen een oplossing biedt, bijvoorbeeld op het gebied van kennisdeling en investeringen. Kunnen we bekijken hoe we daarin nog intensiever met andere landen kunnen optrekken?

Ook de ondersteuning van de inzet van onze krijgsmacht in missiegebieden is een belangrijke taak van de MIVD. Er wordt steeds meer internationaal samengewerkt. Denk bijvoorbeeld aan de ontwikkeling met betrekking tot het New Force Model van de NAVO. Hoe ziet het werk van de inlichtingendiensten bij gezamenlijke missies eruit? Wat zijn de gedachten daarover? Moeten we niet ook op dat vlak nog meer samenwerken? Welke kansen ziet het kabinet daarbij? Wat zijn de risico's wanneer we onze nationale autonomie weghalen en bovennationaal samenwerken?

Dan kom ik bij cyber. Ik had onlangs een interessant gesprek met een militair historicus over de rol van cyber en het gebruik van data bij oorlogsvoering. Op een slagveld is vrijwel niets meer te verbergen. Daarnaast wordt er veel informatie uit openbare bronnen gehaald. Daarmee kan de tegenstander ook op een dwaalspoor worden gezet, vooral in deze tijd, waarin beeldvorming een steeds grotere rol speelt. Ik kwam tot het inzicht dat het hebben van veel informatie echt iets anders is dan het beschikken over goede inlichtingen. Hoe gaan onze inlichtingendiensten om met de steeds groter wordende invloed van cyber?

Zoals gezegd wordt de rol van cyber steeds groter. Het is een van de voornaamste ontwikkelingen op oorlogsgebied. We kunnen hierbij ook in

aanraking komen met voor ons nieuwe situaties op het gebied van oorlogsvoering. Denk bijvoorbeeld aan commerciële satellieten die gebruikt worden voor informatievoorziening. Onlangs zag ik ook een voorbeeld van een kind in Oekraïne dat handig is met drones en het leger aan het front helpt. Is dat kind met zijn kennis en kunde straks een burgerslachtoffer of niet? Dit speelt niet in Nederland, maar ik zeg het even om aan te geven hoe snel die ontwikkelingen gaan. Hoe passen we onze wet- en regelgeving aan op deze snelle ontwikkelingen op het gebied van cyber?

Dan rechts-extremisme en anti-institutioneel extremisme. We lezen dat ook in 2024 het doel wordt gesteld om de verspreiding van extremistisch of radicaliserend gedachtegoed en gedrag vroegtijdig te signaleren en te weren. De MIVD ziet wereldwijd een opleving van rechts-extremisme en constateert dat er vanuit deze gelederen interesse is voor een baan bij Defensie. Voor GroenLinks-PvdA en ook voor mij persoonlijk zijn rechts-extremisme en anti-institutioneel extremisme twee van de grootste zorgen met betrekking tot de weerbaarheid en stabiliteit in onze samenleving. Zoals ik ook bij de ...

De **voorzitter**:

We zijn al over uw spreektijd heen.

De heer **Nordkamp** (GroenLinks-PvdA):

Dan stel ik mijn laatste vraag.

De **voorzitter**:

De laatste vraag. Gaat uw gang.

De heer **Nordkamp** (GroenLinks-PvdA):

Welke acties worden ondernomen als dit soort gedachtegoed binnen Defensie gesignaleerd wordt? Kunnen we nog meer waarborgen in onze processen opnemen om dit met nog meer zekerheid te voorkomen?

De **voorzitter**:

Dank u wel, meneer Nordkamp. Dan is het woord aan de heer Dassen van de partij Volt.

De heer **Dassen** (Volt):

Dank, voorzitter. We hebben dagelijks te maken met cyberdreigingen. Uit het jaarverslag van de MIVD evenals uit het jaarplan 2024 wordt duidelijk dat de dreigingen uit met name Rusland en China toenemen. Maar ook Iran, Noord-Korea en proxy's komen voorbij. We zagen onlangs, zoals de collega's ook al aanhaalden, dat China tot diep in onze systemen is doorgedrongen. Volgens de AIV is het hoofddoel hiervan het zaaien van angst en onzekerheid en het ondermijnen van het vertrouwen in de instituties en de medemens. Is de minister het met de AIV eens? Is de minister van mening dat we dit nu voldoende onder controle hebben? Kan de minister ook toelichten welke delen van onze samenleving het meest onder druk staan? Gaat het om cruciale infrastructuur, zoals onze energievoorziening, of bijvoorbeeld ook om ziekenhuizen of het bedrijfsleven? Of zit de dreiging veel meer in de hoek van grootschalige desinformatiecampagnes om de samenleving instabieler en gepolariseerder te maken? Waar zitten de grootste uitdagingen om dit tegen te gaan? Is dat mankracht, kennis, kunde of zijn dat de middelen? Wat moet de overheid doen en wat ligt bij de samenleving?

Voorzitter. De minister zei op een NAVO-bijeenkomst dat we van woorden naar daden moeten gaan. Ik vraag me af wat zij daar precies mee bedoelde. Het klinkt mij in de oren alsof we wel stappen nemen, maar nog lang niet voldoende voorbereid zijn. Wie is dan waarvoor verantwoordelijk? Dan doel ik dus op het bedrijfsleven, de samenleving en de overheid. Natuurlijk ondersteunen we de oproep van de minister dat we onze verdediging in NAVO-verband moeten versterken, net zoals we dat in Europees verband moeten doen. Maar daar zie ik nog een risico. We lijken namelijk juist terug te vallen in onze nationale eilandjes. Inlichtingen en veiligheid zijn nationale aangelegenheden. Kan de minister toelichten welke concrete acties Nederland moet nemen in NAVO- en EU-verband om de ontwikkelingen vanuit China en Rusland bij te kunnen benen? Zijn onze diensten en krijgsmacht op het moment voldoende toegerust om in NAVO- en EU-verband te leveren? En welke impact gaan de plannen uit het hoofdlijnenakkoord hierop hebben?

Hybride dreigingen vinden plaats, nog voordat de juridische grens van een gewapend conflict is overschreden. Hoe zet de minister zich in voor rechtsontwikkeling op dit gebied? Hoe wordt daarbij rekening gehouden met de rechten van de mens? Daarbij wil ik ook graag de vraag stellen die ik net stelde aan de heer Erkens, namelijk hoe we dat op dit moment op internationaal vlak aanjagen. Is de minister bereid om naar de beschrijving van de hoofdtaken van de krijgsmacht als zodanig te kijken, omdat hybride dreigingen daar volgens de AIV niet voldoende onder vallen? Ik vraag me af of we daar nog eens kritisch naar moeten kijken met elkaar om te zorgen dat we er zeker van zijn dat dat voldoende meegewogen is, zeker ook omdat de hoofdtaken stammen uit, uit m'n hoofd genoemd, 2000. Toen waren hybride dreigingen nog een stuk kleiner.

Voorzitter, ik sluit af. Ik zie ook dreigingen die nieuw zijn voor mij, namelijk die van Venezuela voor het Caribisch deel van het Koninkrijk. Hoe acuut en reëel zou de minister die dreigingen omschrijven? Welke maatregelen neemt

zij nu al om die tegen te gaan? Is het voorlopig onderzoeken, of gaan we al verder?

Dank u wel.

De **voorzitter**:

Dank u wel, meneer Dassen. Er is een vraag voor u van de heer Tuinman.

De heer **Tuinman** (BBB):

Dat was een goed betoog van de heer Dassen. Dat spreekt mij aan. Hij heeft het in elk geval over inlichtingen op nationaal niveau. Ik snap ook wat de partijlijn is van Volt. Je moet het vooral in Europa en in de NAVO harmoniseren. De heer Dassen spreekt in zijn eerste interruptie ook over het idee dat je aan de ene kant oorlog en een andere kant vrede hebt. Daar zit een soort grey zone of een schemerzone tussen. Maar stel dat we nou naar de NAVO kijken. Dat is mijn pijler. Dan hebben we het over artikel 5. Dan kun je wel daadwerkelijk allemaal willen samenwerken, maar al die inlichtingenorganisaties werken eigenlijk allemaal al samen voor artikel 5. Voor artikel 5 werkt iedereen op basis van een nationaal juridisch mandaat. Het is best wel krachtig dat allerlei verschillende landen in Europa, maar ook daarbuiten, verschillende juridische constructen en mandaten hebben in die voorfase. Zij kunnen allemaal dingetjes doen. Dat valt dan niet onder de NAVO, maar uiteindelijk kunnen we daarmee wel een inlichtingenplaat opbouwen met wat Rusland en China aan het doen zijn. Dat kunnen we juist omdat we een divers palet hebben van juridische grondslagen op het gebied van de inzet van inlichtingenorganisaties. Mijn vraag aan de heer Dassen is dan ook als volgt. Zoals ik het begrijp, streeft u naar harmonisatie. Wilt u dan een richting op waarbij we een soort Europese wet op de inlichtingen hebben, waarmee elk land dezelfde juridische grondslag heeft om zijn inlichtingendiensten en -activiteiten te kunnen faciliteren? Of ziet u ook nog wel wat heil in een meer pluriform stelsel?

De heer **Dassen** (Volt):

Een mooie vraag van de heer Tuinman en ook fijn dat ik dat kan verduidelijken. Ik denk niet dat we alles moeten harmoniseren, maar we moeten er wel voor zorgen dat we alle puzzelstukjes op de juiste momenten bij elkaar kunnen leggen. Mijn zorg is soms wel dat wij in Nederland bepaalde kennis hebben en dat ze in Duitsland en Spanje bepaalde kennis hebben, maar dat die kennis onvoldoende bij elkaar komt, zodat we niet de hele puzzel zien. We moeten kijken hoe we dat nog verder kunnen verbeteren, want ik denk dat we elkaar daardoor versterken in plaats van dat we alles zelf moeten gaan doen, want dan zouden we alles op Europees niveau

moeten beleggen. Maar ik denk wel dat er mogelijkheden zijn om te zorgen dat we de puzzel beter in beeld krijgen met elkaar.

De heer **Tuinman** (BBB):

Dat stelt mij gerust. Mijn vraag richt zich nu een beetje op de NAVO, want dat vind ik wel een interessante. Bij de NAVO heb je bijvoorbeeld het NIFC, het NATO Intelligence Fusion Centre, waarin uiteindelijk alle producten van al die diensten met al die verschillende grondslagen bij elkaar komen in een fusion. Dan heeft het iets van waarde voor de NAVO en ook voor de lidstaten. Zoekt de heer Dassen het dan daar? Vindt hij dat je de verzamelde informatie uiteindelijk daar bij elkaar moet brengen of gaat het meer over de bevoegdheden en de harmonisatie van activiteiten? Waar vindt hij dat we nog een slag moeten maken?

De heer **Dassen** (Volt):

Dit gaat over de NAVO, maar bij de EU heb je EU INTCEN. Daar zou je ook met elkaar kunnen kijken of data op de juiste manier met elkaar worden gedeeld en of het begrijpelijk en toepasbaar is. Waar moeten dan inderdaad de bevoegdheden liggen? Ik denk dat het ook nog wel een uitdaging is om te bepalen welke inlichtingen je met elkaar deelt. Daar zit soms toch wel wat spanning, want misschien is dat wel informatie die je op dit moment met sommige landen binnen de Europese Unie wellicht niet wilt delen. Ik ben benieuwd hoe we dat toch met elkaar kunnen verbeteren en of daar dan ook bevoegdheden bij horen. Met andere woorden: kun je het op een andere manier toch beter toepasbaar maken?

De **voorzitter**:

Dank u wel. Ik kijk even naar de minister: is tien minuten genoeg?

Minister **Ollongren**:

Nee, ik zou heel graag tot 14.00 uur schorsen.

De **voorzitter**:

Dat is wel heel lang, maar kennelijk is daar bij de Kamer voldoende begrip voor. We gaan daarom nu tot 14.00 uur schorsen.

De vergadering wordt van 13.37 uur tot 14.02 uur geschorst.

De **voorzitter**:

We gaan snel verder met het tweede deel van deze sessie en wel met de eerste termijn van de minister. Eén interruptie per fractie. Het woord is aan de minister.

Minister **Ollongren**:

Voorzitter, dank. De leden van de commissie hebben een veelheid aan onderwerpen aangeroerd, waarvoor natuurlijk dank. We bespreken vandaag dan ook een belangrijk onderwerp. Het gaat over veel en er is natuurlijk ook nog een ander debat uitgesteld tot na de zomer, namelijk het jaarlijkse debat met beide commissies en beide bewindslieden over de inlichtingen- en veiligheidsdiensten. Ik denk dat het onvermijdelijk is dat een deel van de discussie daar ook weer terug zal komen. Maar ik ben eigenlijk wel dankbaar dat we het vandaag ook kunnen bespreken, want de veiligheidssituatie in de wereld en in Europa, de geopolitieke dreiging en de inderdaad door velen genoemde zogenaamde "grey zone" vragen daarom.

De dreiging in met name het cyberdomein is natuurlijk heel reëel in het werk van Defensie, het werk van de krijgsmacht en het werk van de MIVD. Dat werk is cruciaal om onze nationale belangen en natuurlijk ook de belangen van onze bondgenoten te beschermen. Het is ook belangrijk dat de samenleving weerbaarder wordt tegen deze dreiging, die niet altijd zichtbaar is. Die dreiging zichtbaar maken is dus deel van het werk en ik denk dat zo'n debat daaraan bijdraagt. Het is overigens gewoon een deel van het werk van de diensten. Ik weet dat beide diensten zich aangemoedigd voelen door de Kamer om dat te blijven doen.

Het is zonet ook gedaan door een aantal woordvoerders, maar ook ik wil graag via de voorzitter mijn dank uitspreken aan al die mensen, militairen en burgers, die zich iedere dag inzetten voor onze veiligheid en die hun werk vaak in beslotenheid doen. Ze doen dat om onze open samenleving veilig te houden en dat is belangrijk.

Voorzitter. Ik heb geprobeerd de vragen en dus ook de antwoorden te structureren door te gaan spreken over het dreigingsbeeld, de weerbaarheid van Defensie, het uitvoeren van militaire cyberoperaties, de wettelijke kaders en, wat breder, de weerbaarheid van Nederland en zijn bondgenoten. Ik hoop zo alle gestelde vragen aan de orde te laten komen.

Ik begin met het dreigingsbeeld. De woordvoerder van BBB, de heer Tuinman, haalde terecht D-day aan, want na de mooie herdenkingen die we hebben bijgewoond, zijn we ons er extra van bewust dat er 80 jaar na D-day weer een grootschalige oorlog op ons Europese continent is. Je moet altijd leren van het verleden, maar ook constateren dat sommige dingen zich

herhalen, maar nooit op dezelfde manier. De dreiging is nu inderdaad toegenomen. Het gaat dan om een oorlog die deels lijkt op oorlogen uit het verleden, maar waarbij er nu sprake is van hybride conflictvoering in die zone tussen oorlog en vrede.

Dergelijke conflictvoering, eigenlijk onder de grens van het gewapende conflict, is aan de orde van de dag. Er zijn statelijke en niet-statelijke actoren die er niet voor schuwen om onze open en vrije samenleving te bedreigen. We weten bijvoorbeeld dat er voorbereidingen worden getroffen voor sabotage van kritieke infrastructuur. Dat kan tal van landen overkomen en zeker ook Nederland. Het is eigenlijk gewoon een tijd van geopolitieke competentie, die ook van onze diensten vraagt dat zij steeds slimmer werken, steeds sneller werken en de dreiging vooral tijdig onderkennen. Ze moeten dat niet pas doen wanneer het te laat is. Ze moeten het tijdig onderkennen, zodat wij ook in staat zijn om te handelen en op te treden.

Een belangrijk voorbeeld van waar we dat doen is de Tijdelijke wet cyberoperaties. Het is de bedoeling dat de wet op 1 juli aanstaande in werking treedt. Het is een hele belangrijke stap in reactie op de steeds assertievere en eigenlijk ook wel agressievere landen die met offensieve cyber werken en daarbij niet worden gehinderd door een normaal stelsel van waarborgen, zoals wij dat wel kennen. Er wordt achter de schermen ontzettend hard gewerkt aan de voorbereidingen voor de herziening van de Wet op de inlichtingen- en veiligheidsdiensten. Ik weet dat daar in het hoofdlijnenakkoord ook plannen voor zijn en ik ga ervan uit dat het nieuwe kabinet daar heel voortvarend mee aan de slag gaat, zodat de Kamer daar ook snel over kan spreken.

Dan een verdieping op een aantal punten. De heer Dassen vroeg specifiek naar China. Hij relateerde dat overigens aan het AIV-rapport. Dat kent u natuurlijk. Het kabinet kent het ook. Het heeft nog geen kabinetsreactie gekregen; die volgt nog. Maar in algemene zin kan ik hier wel zeggen dat ik het natuurlijk eens ben met de AIV dat de Chinese cyberdreiging heel hoog is, dat dat veel vraagt van onze diensten en dat we daar dus ook fors op moeten inzetten. We weten gewoon dat China veel cyberaanvallen uitvoert. Die aanvallen zijn geavanceerd van aard. Ze zijn gericht tegen Nederland, tegen onze belangen. Daar waarschuwen de diensten overigens al heel lang voor. Het komt omdat we een hoogwaardige kenniseconomie zijn. We zijn daarmee een aantrekkelijk doelwit. We hebben bedrijven, kennisinstellingen en specifiek, natuurlijk, onze defensie-industrie. Het is dus heel belangrijk dat we die geavanceerde aanvallen tijdig onderkennen. Dat heeft voor de MIVD ook prioriteit. De dienst werkt daar dus aan met technische kennis en met de middelen die ervoor nodig zijn, zoals de bekende kabelinterceptie. Daarvoor hebben we ook die tijdelijke wet gemaakt, anders kunnen wij niet voldoende inzet plegen en zicht houden op de Chinese dreiging. Het is dus heel belangrijk dat die tijdelijke wet in werking gaat. Het is, denk ik, ook belangrijk dat de wetswijziging van de Wiv daar ook in de komende kabinetsperiode weer vorm aan geeft.

Ik ga heel specifiek in op de casus van afgelopen maandag, de zogenaamde FortiGate-hack. De melding die afgelopen maandag is gedaan, was eigenlijk een update van de eerdere melding. Die vond plaats omdat de dienst heeft geconstateerd dat de besmetting groter is dan eerst gedacht en ook niet zo heel gemakkelijk te verwijderen is voor alle spelers die ermee besmet zijn: er zijn meer dan 20.000 besmettingen bij allerlei organisaties. Daarover in de openbaarheid treden moet ten eerste bijdragen aan meer bewustwording -- dat was de vorige keer ook al het motief om ermee naar buiten te treden -- maar is ook bedoeld om de organisaties die ermee te maken kunnen hebben, te helpen om zich ertegen te wapenen en te weren.

Dat ligt, denk ik, heel erg in het verlengde van de motie-Erkens. Het is jammer dat de heer Erkens er net niet is; hij vroeg ernaar. Ik denk dat dat precies is wat hij beoogde, namelijk om het daar waar het kan -- je moet altijd een goeie afweging maken vanuit het belang van de dienst en het onderzoek -- openbaar te maken. Dat helpt natuurlijk enorm. Zo zien mensen dat het niet alleen maar mooie woorden in het jaarverslag van de diensten zijn, maar dat het ook gewoon aan de orde van de dag is en daadwerkelijk gebeurt.

China is nu het voorbeeld, maar dit geldt natuurlijk niet alleen voor China. Ook andere landen hebben een offensieve cyberstrategie. Het is ook niet alleen het werk van de diensten; het is eigenlijk rijksbreed. Daarom is er ook een rijksbreed responskader voor statelijke dreigingen. Het kabinet treft diverse maatregelen, voor verhoging van de weerbaarheid en om risicovolle afhankelijkheden, waarvan we hebben geconstateerd dat we die hebben, af te bouwen. Ik noem ook het toepassen en maken van wet- en regelgeving ter bescherming van onze belangen, zoals bijvoorbeeld de Wet veiligheidstoets investeringen, fusies en overnamen, de Wet vifo. We zijn bij Defensie aan het werk met een nieuwe wet, die we voorlopig even de Wet op de defensie-industrie noemen. Die willen we namelijk in het bijzonder beschermen tegen deze actoren.

Het AIV-rapport gaat, zoals ik al zei, op tal van zaken in, onder andere op de hybride dreiging. Nogmaals, ik verwijs wel ook naar de kabinetsreactie, die natuurlijk nog moet komen. Maar als de vraag is of we meer moeten doen, bijvoorbeeld de wetgeving hiervoor verbeteren of versterken, dan geldt in het algemeen dat iedere vorm van inzet gewoon valt onder het handhaven van de internationale rechtsorde zoals die in de Grondwet is verankerd. Dat geldt bij alle inzet van de krijgsmacht, dus ook als het in het domein is waar humanitair oorlogsrecht van toepassing is. Zo is ook de naleving van mensenrechten geborgd. De basis, het fundament voor het verankeren daarvan, is dus eigenlijk wel aanwezig. De vraag is of de wijziging van de dreiging, die een andere vorm aanneemt dan we al kenden, nog noopt tot aanpassingen of verbeteringen. Dat is nog onderwerp van gesprek.

Terrorismedreiging. Daarover ging een vraag van de heer Pool. Ik mag hem misschien ook verwijzen naar het nieuwste DTN. Dat is dinsdag 11 juni uitgegaan. Daar staat een globale analyse in van de terroristische

gewelddadige extremistische dreiging tegen Nederland en Nederlandse belangen in het buitenland. Het is belangrijk dat dit DTN periodiek onder coördinatie van de NCTV wordt uitgebracht. De dreiging is nog steeds reëel. De diensten en de MIVD leveren input voor dat DTN, waarbij wij ons bij de MIVD concentreren op de dreigingen voor de krijgsmacht, op de dreigingen van de democratische en internationale rechtsorde vanuit die hoek.

De **voorzitter**:

Ik voeg nog even toe dat DTN staat voor Dreigingsbeeld Terrorisme Nederland.

Minister **Ollongren**:

Ja, precies: DTN.

De **voorzitter**:

Ik zeg dat even voor de toehoorders.

Minister **Ollongren**:

Heel goed. Dank u wel.

In het blokje weerbaarheid van Defensie wil ik graag ingaan op de vragen die gesteld zijn over personeel, kennis, vgb's, huisvesting en al die zaken. Terwijl we ons bezighouden met de ontwikkelingen in de wereld -- ik kom net weer terug van twee dagen in Oekraïne -- en terwijl we weten dat die cyberoperaties in volle gang zijn, dat die een prominente en integrale rol zullen spelen in toekomstige gewapende conflicten en dat die dus echt complementair zijn aan conventionele oorlogsvoering, is het belangrijk dat we ons bewust zijn van het feit dat dat in geen enkel land, geen enkele organisatie, alleen maar een militair antwoord kan vragen. Dat vraagt om een integraal antwoord. Dat betekent dat de hele samenleving daarbij betrokken is en de hele industrie daarbij een rol heeft te spelen. Het gaat ten slotte over meer dan de veiligheid in fysieke zin. Dat is heel erg verbonden met de cyberwereld. De mate van collectieve weerbaarheid, onze maatschappelijke weerbaarheid hiertegen, zal ook bepalen hoe succesvol landen met een offensieve cyberstrategie in ons land kunnen zijn.

We hebben het tegenwoordig veel over weerbaarheid. Ik denk ook dat dat heel belangrijk is. Daar moeten we hard aan werken. Daarbij moeten we leren van voorbeelden uit andere landen. In een andere vergadering met een deel van deze commissie ging het ook veel over voorbeelden uit

Scandinavische landen: Finland, Zweden. Daar moeten we ook aan werken zodat het ook in ons DNA gaat zitten.

Om wat concreter te worden: we hebben ook gewoon mensen nodig. We moeten bijvoorbeeld meer cyberreservisten aantrekken bij Defensie en afspraken maken met private partijen. We hebben voor cyberreservisten heel concrete doelstellingen. We hebben er nu 110. We willen naar 150 cyberreservisten. We spreken inderdaad met private partijen. Dat vroeg de heer Erkens nog. Het gaat zowel over individuele reservisten als ook over de bedrijven waar je afspraken mee moet maken, omdat die bedrijven er soms in slagen om mensen met de juiste kennis en expertise uit deze hele schaarse groep aan te trekken, bijvoorbeeld door hele goede arbeidsvoorwaarden, hoge salarissen en dergelijke te bieden. Maar die mensen zijn wel degelijk geïnteresseerd om bij te dragen aan onze nationale veiligheid, om te werken bij Defensie. De route van reservist is dan een aantrekkelijke route. Op zich ben ik in die zin hoopvol dat de mensen dit willen doen, maar dat ook de private partijen het zien als hun maatschappelijke rol om die mogelijkheid te bieden aan hun werknemers.

De heer **Dassen** (Volt):

Even een vraag om even iets meer gevoel te krijgen bij het aantal van 150 dat de minister nu noemt. Ik geloof dat China iets van 110.000 hackers heeft. Dat zijn bijna zo veel mensen als een middelgrote stad in Nederland. Ik probeer even een beeld te krijgen van de verhoudingen en van waar dat getal van 150 vandaan komt. Acht de minister dat voldoende? Ik moet daar zelf nog wat beter een gevoel bij krijgen, merk ik.

Minister **Ollongren**:

Dat begrijp ik heel goed. Het is natuurlijk niet zo dat dat de enige groep is waar die kennis zit. Er werken veel meer mensen bij Defensie, bijvoorbeeld bij de diensten, bij de verschillende krijgsmachtonderdelen of bij het Defensie Cyber Commando. We hebben dus een veel grotere groep deskundigen en experts, maar we willen juist de flexibele schil vergroten. Daar zit de groep van cyberreservisten in. Dit is wat we nu hebben aan cyberreservisten. Ik denk dat we dat kunnen laten groeien, zodat we ook kunnen gaan werken aan schaalbaarheid waar dat nodig is.

Ik begrijp de vergelijking met China heel goed, maar daar kunnen we ons natuurlijk nooit mee vergelijken. Dat is zo'n oneindig veel groter land. Zij hebben inderdaad bijna oneindig de beschikking over dit soort expertise. Wat wij wel kunnen, is ervoor zorgen dat wij het ontzettend goed kunnen. Wie niet sterk is, moet slim zijn. Daar moeten wij het hier echt van hebben. Ten eerste door er zelf voor te zorgen dat we de allerbeste mensen aan ons kunnen binden en ten tweede door samen te werken met andere diensten, met

andere landen en ook met het bedrijfsleven. Dat was ook een vraag van een aantal van u. We kunnen dit niet zonder het bedrijfsleven. Daar zit ook heel veel kennis. Dat zien we ook in de oorlog in Oekraïne. Commerciële partijen spelen gewoon een rol en beschikken over heel veel informatie en kennis. Die moeten we gewoon op een slimme manier aanboren en aan ons binden.

De **voorzitter**:

Dank u wel. Dan is er nog een vraag van de heer Erkens.

De heer **Erkens** (VVD):

Dank aan de minister voor de beantwoording. Laten we doorgaan op de cyberreservisten en het aantrekken van de juiste mensen. Kijk, qua salaris zal je voor deze uitmuntende individuen waarschijnlijk niet kunnen concurreren met de private sector. Een cyberreservistmodel is best logisch om die mensen wel nog op een of andere manier te binden aan de krijgsmacht. Wordt er ook gekeken naar de optie om mensen deeltijd in dienst te laten nemen, bijvoorbeeld doordat je twee dagen per week werkt voor de MIVD en drie dagen per week voor een bedrijf als ASML? Daarmee kun je misschien wel het beste van twee werelden krijgen met elkaar. Worden die modellen ook verkend? Of is het: ik ben een reservist óf volledig in dienst van Defensie? Want ik denk dat een tussenvariant misschien juist heel aantrekkelijk kan zijn voor deze individuen.

Minister **Ollongren**:

Meestal is de wijze van inzet van reservisten anders en nemen we ze voor een specifieke periode over met een opdracht, als onderdeel van een inzet, als onderdeel van een project of gewoon als extra capaciteit in een bepaalde periode. Ik zal hier ook even naar kijken. Ik kan zo een-twee-drie niet zeggen of het al gebeurt. Ik zou zeker ook niet willen zeggen dat het niet zou kunnen. We gaan dus nog even goed bekijken of dat al gebeurt en anders gaan we er zeker naar kijken.

Overigens is het misschien wel goed om op te merken dat de MIVD zeker niet te klagen heeft over belangstelling. Er is veel animo om bij de dienst te komen werken. Ik begrijp dat ook heel goed. Het is ongelofelijk interessant en belangrijk werk. De groeidoelstellingen van de MIVD van vorig jaar zijn echt ruimschoots gehaald. De dienst groeit verder. We verwachten ook dat de doelen voor dit jaar worden gehaald. We zijn dus heel actief aan het werven. Dat levert ook resultaat op. We hebben natuurlijk niet alleen maar cyberspecialisten nodig bij de dienst, maar ook allerlei andere kennis en talent.

Dan de veiligheidsonderzoeken. Daar was inderdaad toch sprake van een knelpunt. Ik heb steeds gezegd en met de Kamer gewisseld: veiligheidsonderzoeken zijn belangrijk en kunnen we niet overslaan. Dit gaat over mensen die werk gaan doen waarbij vertrouwelijke informatie wordt gebruikt en gehanteerd. Het is dus heel belangrijk dat die veiligheidsonderzoeken wel worden uitgevoerd. Maar het is ook belangrijk dat ze niet zo lang duren dat mensen afhaken. Dat gaat nu wat beter, want we hebben ingezet op het vergroten van de personele capaciteit van de organisatie die hiermee is belast. We hebben ingezet op het moderniseren van de manier van werken bij de veiligheidsonderzoeken, onder andere door automatisering en uniformering van de processen bij de AIVD en MIVD. Bovendien wordt er ook gewerkt aan de wijziging van de Wvho, de Wet veiligheidsonderzoeken, waarin een locatiegebonden vgb wordt geïntroduceerd. Dat is overigens een beperkte wijziging, maar ook dat kan helpen. Het nader rapport zal binnenkort voor advies naar de Raad van State gaan. Mijn collega van BZK en ikzelf verwachten dat we daarna door kunnen en dat het nieuwe kabinet, als ze dat willen, dat na het zomerreces aan uw Kamer zou kunnen aanbieden. Ik vind het vooral belangrijk om te zeggen dat we dus een aantal aanpassingen hebben gedaan in het proces en dat dat dus leidt tot een verbetering en een verkorting van de termijnen.

Ook de huisvesting is een vraagstuk dat weer opkwam. Ik begrijp dat goed. In mijn vorige functie heb ik natuurlijk ook met die huisvesting te maken gehad. Het is gewoon lastig. Het idee van gezamenlijke huisvesting is volgens mij een heel goed idee; deze twee diensten werken ontzettend goed samen en dan ligt het erg voor de hand om te proberen om dat op één plek voor elkaar te krijgen. Maar tegelijkertijd heb je te maken met twee diensten die enorm aan het groeien zijn en waarvoor specifieke randvoorwaarden gelden vanwege de aard van het werk. Je moet dus iedere keer zoeken naar een oplossing. De plannen die gemaakt zijn, pasten gewoon niet meer bij de omvang van de diensten. Ik denk dus dat de minister van BZK en ik dan moeten zeggen dat de plannen zoals zij waren niet meer passen bij wat de diensten nu zijn. We willen nog steeds het maximale doen om te zorgen dat beide diensten zo veel mogelijk bij elkaar en met elkaar kunnen werken. Er loopt een project huisvesting MIVD Frederikkazerne, dat het reguliere traject doorloopt. De staatssecretaris van Defensie zal de Kamer hier verder over informeren. We zullen zorgen dat er in de nieuwbouw van de MIVD ruimte is; in de planvorming voor de MIVD wordt er ruimte gemaakt voor de AIVD, om zo de samenwerking te kunnen borgen.

Voorzitter. Dan alles rondom de vragen over militaire cyberoperaties. Inmiddels is allang door Defensie onderkend dat cyber een volwaardig operationeel domein is dat nodig is om allerlei militair-strategische effecten te kunnen bereiken. Militaire cyberoperaties kunnen samenhangen met militaire activiteiten in een ander domein of met andere machtsmiddelen die kunnen worden ingezet, bijvoorbeeld diplomatie of rechtshandhaving. Het is natuurlijk duidelijk op het moment dat er een oorlogssituatie is, maar ook in

de grey zone hebben we mogelijkheden, onder andere omdat we de Wiv hebben, die daarin voorziet. Militaire cyberoperaties hebben vaak lange aanlooptijden, die heel erg afhankelijk zijn van onze inlichtingen en onze technische mogelijkheden in cyberspace. Daarom werkt het Defensie Cyber Commando heel nauw samen met de MIVD. Dat gebeurt inderdaad in zogenoemde multidisciplinaire cyberteams. Dat is ook nodig. Alleen in die gezamenlijke aanpak kunnen we de effecten bereiken die nodig zijn. We hebben te maken met het domein tussen vrede en oorlog in, de grijze zone, de grey zone, maar we weten dat ook als er gewoon militaire operaties op het slagveld zijn, cyber een essentiële rol heeft in het bewerkstelligen van militaire effecten op tactisch niveau. Dus tijdige inlichtingen en ruimte om te kunnen opereren in cyberspace zijn noodzakelijk.

De ontwikkeling van tactische capaciteit voor cyberoperaties heeft dus echt prioriteit. De opdracht om dat te doen ligt bijvoorbeeld bij het nieuw geïntegreerde Cyber & Electromagnetic Activities bataljon.

Dan de vraag van de heer Tuinman -- ik dacht dat de heer Dassen er ook naar vroeg -- over IGO: Informatie Gestuurd Optreden. Ik neem even een aanloopje. Dit kabinet heeft de commissie-Brouwer ingesteld. Die commissie is met aanbevelingen gekomen. We hebben gezegd dat dat heel waardevolle aanbevelingen zijn en zijn ermee aan de slag gegaan. Het Informatie Gestuurd Optreden was natuurlijk iets wat al liep; we hebben de commissie-Brouwer daar eigenlijk opgelegd en gezegd: je moet dit betrekken bij de ontwikkeling van je informatiegestuurde optreden. Dus al die aanbevelingen van Brouwer zijn erin meegenomen. Onze CIO werkt er ook dagelijks mee. Dat betekent dat we eigenlijk in beeld aan het brengen zijn welke beleidsmatige en ook juridische implicaties dit alles heeft.

De heer Tuinman vroeg naar het onderzoek van de NLDA. Dit is inmiddels afgerond. De uitkomsten daarvan worden ook weer betrokken bij de verdere uitwerking van Informatie Gestuurd Optreden. We moeten nog even de weging maken welke beleidsmatige conclusies we eraan verbinden en welke juridische wijzigingen we dan eventueel zouden willen. Daarbij kijk je of het eigenlijk al kan binnen de kaders die we hebben en we het alleen maar slimmer of anders moeten inrichten, of dat het nodig is om hier nog andere stappen in te zetten. Intensiveringen in dat domein vinden ook al plaats. We hebben in de maatregelennota van Defensie gezegd -- daarover had de heer Erkens trouwens een vraag gesteld -- dat we twee dingen in ieder geval moeten doen: het vergroten van de cyberreadiness en het doorgroeien van het DCC, het Defensie Cyber Commando. We gaan daarmee ook fors uitbreiden: er worden ongeveer 450 fte toegevoegd. We hebben het budget aangepast en we voorzien eigenlijk ook alle relevante eenheden binnen Defensie -- want het zit natuurlijk op tal van plekken -- van investeringsbudget, zodat ze kunnen investeren in de opleiding en relatief kleine uitgaves kunnen doen in hardware of bepaalde licenties die ze nodig hebben. Dat zit dus heel breed door de organisatie heen, niet alleen bij de

MIVD en het DCC, maar bijvoorbeeld ook bij de KMar, SOCOM en andere onderdelen.

De **voorzitter**:

Een vraag van de heer Tuinman.

De heer **Tuinman** (BBB):

Hartelijk dank voor de uiteenzetting. Ik heb daar toch nog een vraag over. Het is "train as you fight", maar natuurlijk ook "you fight as you're being trained". Als we het DCC, waarvan het idee is dat dat daadwerkelijk in een oorlog moet kunnen optreden, continu onder de Wiv laten trainen en daar ervaring in laten opdoen, bent u dan niet bang dat ... Het is zoals het ontwikkelen van een auto. Het DCC mag hem designen en bouwen, maar krijgt niet de brandstof om er een rondje in te rijden. Heel af en toe mag het van de Wiv een rondje rijden, maar daadwerkelijk experimenteren met die auto in de jungle -- dat is trouwens wel lastig, hoor -- of in een woestijn, in Europa of bij de poolcirkel ... U snapt wel een beetje waar ik naartoe wil. Ziet u daar risico's in? Denkt u dat het DCC onder de Wiv met de MIVD in een legale structuur terechtkomt waarin het eigenlijk juist weg beweegt van daar waar we het willen hebben, namelijk dat het ten tijde van oorlog de anderen daadwerkelijk met al die cyberwapens om de oren kan slaan?

Minister **Ollongren**:

Ik vind dit een hele relevante vraag. Dit is natuurlijk ook een dilemma. Ik wil de vraag echt langs twee lijnen beantwoorden. Eén. Zojuist was er de vraag hoe we nou zorgen dat het DCC voldoende kan doen of, omgekeerd, dat wat het nu ook in het kader van de Wiv door die samenwerking met de MIVD kan doen, voldoende is. Ik denk dat het wel belangrijk is dat we dat mogelijk maken en dat we daarom door moeten gaan met het inbedden en onder de MIVD krijgen van de taskforce militaire cyberoperaties, die er is. Daardoor creëren we eigenlijk interdisciplinaire teams van het DCC en de MIVD. De CDS heeft natuurlijk ook de ruimte om daar opdrachten voor te verlenen. Maar tegelijkertijd moeten we inderdaad kijken of dat voldoende is.

Daarmee kom ik eigenlijk op de aanzet tot een wet op de gereedstelling, want ik denk dat die de oplossing hiervoor kan bieden. Als de heer Tuinman en de voorzitter het goedvinden, wil ik kijken of ik met mijn antwoorden over die wet op de gereedstelling ook de interruptievraag van de heer Tuinman beantwoord.

We zijn nog niet in de fase van het voorstel van een wet, maar we zijn wel in de fase dat we bezig zijn in lijn met de commissie-Brouwer, die gezegd heeft

dat Defensie in dat grijze gebied tussen oorlog en vrede effectief, maar ook op basis van de juiste passende juridische kaders en waarborgen moet kunnen oefenen en optreden; dat is precies het punt van de heer Tuinman. Hierbij behoren bevoegdheden die een beetje afhankelijk zijn van waar je bent in je gereedheidstatusfase. Met andere woorden: kan Defensie voldoende meebewegen tegen de dreigingen waartegen we ons moeten wapenen? Als die worden verhoogd, zijn wij daarin dan ook op tijd opgeschaald? En als ze weer verlaagd worden, kunnen we misschien ook weer afschalen. Daarvoor loopt nu dus, zoals ik de Kamer ook heb gemeld, de opdracht om te onderzoeken of we dat zouden kunnen doen via een specifieke wettelijke grondslag, bijvoorbeeld een wet op de gereedstelling, zoals ik het maar heb genoemd.

Wat zou die wet nou bijdragen? Als er geen oorlog is, maar een soort tussenfase waarin we de samenleving veilig moeten houden en sterk willen staan tegen tegenstanders waarvan we weten dat ze dit doen, zou die wet kunnen helpen om de grondslag te creëren om te oefenen, te trainen en te werken met het gebruik van cybercapaciteiten, waaronder bijvoorbeeld terughacken. Als jij gehackt wordt door een tegenstander, moet je je daar echt tegen kunnen wapenen, niet alleen door je ertegen te beschermen maar door iets terug te doen. Dat moet je leren; daar moet je je op kunnen voorbereiden. Die grondslag in zo'n wet op de gereedstelling kan bijdragen aan ruimte om tijdens gereedstellingsactiviteiten in een informatieomgeving te werken zonder in problemen te komen, zoals destijds wél is gebeurd met de eisen die wij in Nederland stellen aan de privacy. Je creëert dus eigenlijk een balans tussen een aanvullende grondslag voor het uitvoeren van dat soort taken en de waarborgen die we graag zien voor bescherming van privacy en persoonlijke gegevens. We zijn daar dus mee bezig. We kijken eigenlijk vooral eerst wat er sowieso al kan binnen de huidige kaders en waarom je wat extra ruimte wil creëren in de wet op de gereedstelling. Die gaat dan overigens over nog veel meer, want die gaat niet alleen over het cyberdomein, maar ook over het fysieke terrein.

Voorzitter. In het verlengde daarvan had de heer Boswijk vragen over de tijdelijke wet. Ik denk dat die tijdelijke wet echt kan helpen. We hebben de afgelopen jaren gezien dat diensten te weinig mogelijkheden hadden om even snel te handelen tegen opponenten of landen die offensief hun gang gaan, zoals China. Het gaat er dus niet alleen om de dreiging te onderkennen, maar ook om vervolgens wendbaar te kunnen optreden in het cyberdomein. Wanneer er bijvoorbeeld steeds gewisseld wordt van server, kunnen we met de bestaande bevoegdheden onvoldoende uit de voeten. We willen bevoegdheden effectief kunnen inzetten, zodat we digitale spionage, hacks et cetera veel sneller kunnen onderkennen, kunnen volgen en zo mogelijk ook kunnen attribueren. Ik denk dat die tijdelijke wet daar belangrijk voor is.

In het verlengde daarvan was er de volgende vraag: helpt die dan ook om meer voorspellend vermogen te creëren, zodat we niet alleen maar achter de

dreiging of daadwerkelijke aanvallen aanlopen? Ja, dat denk ik wel. Als die tijdelijke wet is ingegaan, kunnen de diensten inderdaad meer voorspellend vermogen voor zichzelf creëren, omdat ze meer toegang zullen hebben tot de kabel. U zult daar in het volgende debat ongetwijfeld ook nog over spreken. Maar dat is in ieder geval de inzet, en de reden waarom we deze wet zo ontzettend graag wilden hebben. Dan sluiten we toch nog beter aan op technologische ontwikkelingen. Dat was al de bedoeling van de Wiv 2017, maar we hebben gewoon gemerkt dat die niet goed aansluit op de praktijk. We denken dat we dat probleem met de tijdelijke wet in ieder geval voor de komende tijd hebben opgelost.

De **voorzitter**:

Een vraag van de heer Boswijk.

De heer **Boswijk** (CDA):

De minister kijkt naar collega Erkens, die alleen maar naar zijn telefoon zit te kijken, maar ik had de vragen gesteld.

Minister **Ollongren**:

O, sorry.

De heer **Boswijk** (CDA):

Maakt niet uit.

De heer **Erkens** (VVD):

Heeft de heer Boswijk slecht geslapen, of zo?

De heer **Boswijk** (CDA):

Nee, nee. Een beetje luchtig doen op dit onderwerp moet nog wel kunnen!

Op zich ben ik blij met de antwoorden, maar ik heb nog wel een beetje zorgen. Het eerste debat dat ik heb gevoerd, ging over LIMC. Ik vond toen zelf dat de Kamer en de media, ondanks dat er fouten zijn gemaakt ... We wisten allemaal dat het niet expres was gedaan; het was allemaal met de beste intenties gedaan, voor onze gemeenschappelijke veiligheid. Ik merkte toen dat er ontzettende druk vanuit de samenleving en de politiek was. Als

we dit met de tijdelijke wet ook gaan doen -- ik ben daar groot voorstander van, want ik denk dat het hard nodig is -- ben ik er gewoon bang voor dat zo'n geval zich weer zal voordoen. Er werken mensen aan. Het is een nieuw terrein. Er kunnen fouten gemaakt worden. Hoe gaan we voorkomen dat we dan ineens weer in een kramp schieten en tien stappen achteruit worden geworpen, terwijl China en Rusland ondertussen honderd stappen vooruitzetten? Wordt daar ook rekening mee gehouden? Hoe kunnen we daar dan op anticiperen?

Minister **Ollongren**:

Tegen de heer Boswijk zou ik het volgende willen zeggen. Hij heeft gelijk, maar laten we toch even twee dingen uit elkaar trekken. LIMC betreft de commissie-Brouwer. Eén. De aanbevelingen van de commissie-Brouwer hebben ertoe geleid dat we hebben geconstateerd dat de krijgsmachtonderdelen best mogelijkheden hebben in het domein die nog niet helemaal werden benut. Twee. Je zou ook mogelijkheden willen hebben die nog niet kunnen. Daar zou je dan een wettelijke grondslag voor moeten creëren. Soms is de oplossing dat je dingen onder de Wiv kunt doen, maar dat lost inderdaad niet alles op. We hebben nu gezegd: dan vinden we dat we die ruimte toch moeten creëren in de wet op de gereedstelling. Daarnaast -- dat staat echt los van LIMC -- is die tijdelijke wet er gekomen omdat de diensten bij de uitvoering van hun bevoegdheden tegen knelpunten aanliepen. In de geest loste de Wiv 2017 die wel op, want die was juist bedoeld om nieuwe technologieën en technologische mogelijkheden het hoofd te kunnen bieden. Maar in de praktijk was vooral de toegang tot de kabel onvoldoende. Daarmee stonden we achter ten opzichte van de landen die er wel gebruik van kunnen maken. Dat hebben we nu gerepareerd met de tijdelijke wet, die natuurlijk nog moet ingaan, dus daarom kan ik nog niet zeggen of het voldoende is. Maar we hebben er natuurlijk lang en zorgvuldig naar gekeken en ook uitvoeringstoetsen gedaan. We hebben er dus vertrouwen in dat dit de diensten echt gaat helpen, dat zij veel meer relevante informatie van de kabel af zullen kunnen halen en dat zij bovendien veel sneller zullen kunnen meegaan met de wijze waarop de opponenten of statelijke actoren met offensieve cyberprogramma's zich in de cyberwereld bewegen, omdat we onze werkwijze hebben versneld. De wijze waarop het toezicht daarop werd uitgeoefend, nam erg veel tijd in beslag, waardoor je weer weken achterliep op degene die aan het hacken was. Ik denk dat dit nu is opgelost. Volgens mij zijn beide nodig voor het werk van de krijgsmacht, maar is er dus wel een onderscheid te maken tussen het werk van de diensten en de aanpassing via de tijdelijke wet, en de oplossingen die we nog voor andere krijgsmachtonderdelen moeten zoeken in de wet op de gereedstelling, met name om voorbereid te zijn en te kunnen werken in het cyberdomein.

De **voorzitter**:

Ik constateer dat we nog ruim twintig minuten de tijd hebben. Ik zal dus geen interrupties toestaan, tenzij we aan het eind van het debat nog tijd over hebben. Dan kan het natuurlijk weer wel. Minister, u gaat verder.

Minister **Ollongren**:

Voorzitter, ik heb al heel wat vragen kunnen beantwoorden, dus ik denk dat het moet lukken. Er is misschien nog wel een belangrijk thema, namelijk de weerbaarheid van Nederland en bondgenoten. Daarna heb ik nog een paar overige vragen, die ik al dan niet per ongeluk heb overgeslagen. Ik ga meteen even naar de vragen. Ik heb vraag over de AIV en de NAVO, een vraag over de EU en een vraag over Venezuela.

Laat ik die laatste eerst even pakken. Het is een vraag van de heer Dassen, die zei dat voor hem de dreiging vanuit Venezuela nieuw was. Ik denk dat het wel al eerder is gesignaleerd door de diensten. We doen in het kader van het dreigingsbeeld in het Caribisch gebied onderzoek naar politieke en militaire ontwikkelingen aldaar, omdat die natuurlijk een uitstralingseffect kunnen hebben richting het Koninkrijk der Nederlanden, en in het bijzonder natuurlijk Aruba, Bonaire en Curaçao. Daarover staat iets in het jaarverslag. Het ministerie van Defensie is natuurlijk een Koninkrijksdepartement en we hebben ook een operatieplan ter bescherming van de eilanden. Dat wordt continu geactualiseerd. Dus daarin wordt de dreiging vanuit Venezuela gewoon meegewogen.

Dan kom ik op de vragen van de heer Dassen over internationale samenwerking en in het bijzonder de NAVO en de EU als het gaat om cyberdreigingen. Misschien even vooraf: internationale samenwerking is ontzettend belangrijk. Als we het hebben over de diensten, dan gebeurt de internationale samenwerking tussen de diensten. Dat zijn dus nationale diensten die met elkaar samenwerken, informatie kunnen uitwisselen, elkaar kunnen waarschuwen et cetera. Daar heb ik het eigenlijk niet over. Ik wilde het naar aanleiding van de vraag van de heer Dassen vooral hebben over de vraag hoe we vanuit die twee voor ons belangrijke instellingen, namelijk de NAVO en de EU, werken aan cyberweerbaarheid. Want inderdaad, ik denk dat dit enorm kan helpen, omdat we allemaal in meer of mindere mate met dezelfde problematiek te maken hebben. Daarom doen we dat heel actief. Bij de NAVO zijn wij onderdeel van het Virtual Cyber Incident Support Capability. Dat is een mechanisme voor alle NAVO-bondgenoten, waarin je NAVO-steun kunt aanvragen. Daarbij kunnen wij dus ook anderen helpen. We nemen altijd deel aan de jaarlijkse cyberoefening -- die heet Locked Shields -- om de geallieerde weerbaarheid tegen cyber te versterken. We dragen bij aan de NAVO Cyber Defence Pledge. Die organiseert een effectieve samenwerking tussen bondgenoten en uitwisseling van best practices op het gebied van cyberweerbaarheid. We hebben die bijeenkomst afgelopen mei nog in Den

Haag gehad. Daar hebben we precies dat gedaan. We hebben gesprekken gevoerd met bondgenoten, en overigens ook met partnerlanden zoals Oekraïne, over cyberdreiging. Het staat ook heel regelmatig op de agenda van de ministeriële vergaderingen. Het staat op een agenda van de Washingtontop. Dit is echt een heel belangrijk onderwerp in de NAVO.

Hetzelfde geldt voor de EU. We hebben al langer een lopend PESCO-project over cyber. Dat heeft vooral tot doel cyberinformatie op te leveren ten behoeve van de militaire staf en de militaire planning. We leveren een bijdrage aan situational awareness. Het heet Cyber and Information Domain Coordination Center en dit hele project wordt gedragen door een aantal landen, waaronder Duitsland en Nederland. We hebben ook een Cyber Rapid Response Team dat kan worden ingezet op verzoek van de lidstaten. Ik heb al vaker gezien dat dit ook met succes gebeurd is. Het heeft eigenlijk de beschikking over een algemene cybercapaciteit, die kan worden ingezet als er cyberincidenten zijn. Dus als jij in jouw land te maken hebt met zo'n cyberincident, kan je het inzetten, maar je kan het ook als preventieve maatregel inzetten. Als een land in aanloop naar verkiezingen vreest dat het slachtoffer zou kunnen worden van cyberaanvallen, kan het preventief het team inzetten. Het is dus een heel effectief instrument vanuit de EU.

Dan kijk ik heel even of er nog dingen waren die ik was vergeten. Ja, die zijn er.

Ik heb om de een of andere reden niet meer het antwoord dat ik wilde hebben op de vraag van de heer Pool over rechts-extremisme. We hebben namelijk een definitie van rechts-extremisme, maar die heb ik hier niet bij de hand. Als iemand die nog heeft, wil ik die graag hebben. Ik wil wel heel precies zijn nu. Ik kom daar zo op terug. Ik vind het wel belangrijk om die vraag te beantwoorden, want ik vind het een beetje jammer om zo'n belangrijk onderwerp, dat voor de diensten en voor onze nationale veiligheid ontzettend belangrijk is, te gaan politiseren. Er is vrijheid van meningsuiting. Volgens mij mag iedereen politiek gezien etiketten plakken zoals die wil, maar vanuit de diensten zijn we heel zorgvuldig. Als er een dreiging is voor de nationale veiligheid en de democratische rechtsstaat vanuit groepen of individuen, is dat relevant voor de diensten. Dat speelt ook in de rechts-extremistische hoek. Zo wordt daarnaar gekeken. Als ik de definitie straks wel weer voor mijn neus heb, zal ik die voorlezen, maar dit is de kern van de zaak.

Voorzitter. Dan over de Eemshaven. Ik heb een mondelinge vraag daarover beantwoord. We hebben er toen heel goed naar gekeken. De heer Kahraman stelde die vraag. Ik heb toen namens de collega van IenW gezegd dat wij het inderdaad onwenselijk vinden dat Russisch gevlagde vissersschepen worden toegelaten tot de Eemshaven, en eigenlijk überhaupt tot havens waar ze eventueel kennis kunnen nemen van kritieke infrastructuur of militaire activiteiten. Ik heb nu laten navragen of en de bevestiging gekregen dat Russische vissersschepen niet meer worden toegelaten in de Eemshaven. Er

is bevestigd dat dat inmiddels ook uitgebreid is tot andere havens. Ik geloof dat de heer Kahraman zei dat hetzelfde schip met een andere vlag binnen was gevaren. Dat zal ik dan nog even moeten nagaan bij IenW, maar ik wil hem dus wel verzekeren dat wij juist op dit soort dingen ontzettend alert zijn.

De heer **Kahraman** (NSC):

Ik werd er inderdaad van op de hoogte gebracht dat een Russisch schip uit Rusland probeerde in Velsen aan te meren en is geweigerd. Heel goed. Het schip is onder een andere vlag teruggevaren en heeft toen wel een haven in Nederland kunnen binnenvaren. Als een onderzoeksjournalist dit kan volgen, is mijn vraag in hoeverre onze veiligheidsdiensten deze bewegingen van voertuigen, schepen en personen uit Rusland die Nederland binnenkomen in de gaten houden. Houden we die extra in de gaten of niet?

Minister **Ollongren**:

Ik stond op het punt om de heer Kahraman een betrekking aan te bieden bij de MIVD, maar ik begrijp nu dat het van een onderzoeksjournalist komt. Dan ga ik dus toch weer elders kijken! Ik maak er grappen over, maar het is natuurlijk heel serieus. Het is echt heel serieus en wij nemen dit ook echt heel serieus. Ik kan deze vraag nu niet beantwoorden. Daar gaan we natuurlijk naar kijken, maar het is niet voor niks dat wij vanuit Defensie en de diensten juist waarschuwen voor die activiteiten uit Rusland en dat we gezegd hebben dat het niet alleen gaat om schepen van de marine, maar dat het ook kan gaan om onderzoeksvaartuigen en commerciële voertuigen. We zijn daar niet naïef in. Ik vind het ontzettend belangrijk om dat in de gaten te blijven houden, vandaar ook dat we -- dat heb ik de vorige keer ook gezegd -- met de autoriteiten, dus de havenbedrijven van de verschillende havens in Nederland, samenwerken om dit te onderkennen en waar mogelijk tegen te gaan.

Voorzitter. Misschien dan toch nog een paar losse vragen. Daarna ben ik echt klaar. De heer Nordkamp vroeg nog wat de MIVD kan doen. We hadden het net al even over de definitie van het rechts-extremisme, maar zijn vraag ging meer over de situatie waarbij dat binnen de krijgsmacht voorkomt. We weten dat er een bepaalde aantrekkingskracht van de krijgsmacht uitgaat voor mensen die rechts-extremistisch gedachtegoed aanhangen. De MIVD doet inderdaad onderzoek naar de specifieke aard daarvan, de omvang daarvan en specifieke casussen. Als daar een aanleiding voor is, kan de MIVD de commandant door bijvoorbeeld het uitbrengen van een ambtsbericht waarschuwen dat er een dreiging is en informeren over wat er aan de hand is. In dat geval kunnen er ook gewoon rechtspositionele maatregelen worden getroffen. Daarbij kan er dus inderdaad sprake zijn van een dusdanig risico dat dat handelingsperspectief moet worden geboden. We kunnen natuurlijk

altijd veiligheidsonderzoeken uitvoeren of opnieuw uitvoeren. Dat kan soms aanleiding geven tot het weigeren of intrekken van een verklaring van geen bezwaar. Dat is natuurlijk een vereiste voor het werken dan wel blijven werken bij Defensie.

De **voorzitter**:

Een vraag van de heer Nordkamp hierover.

De heer **Nordkamp** (GroenLinks-PvdA):

Het is me duidelijk dat dat geconstateerd wordt. Maar zijn er nog meer mogelijkheden aan de voorkant, bijvoorbeeld een socialmediascreen, dus dat het daar een beetje gevolgd wordt? Is iets in die trant misschien ...

Minister **Ollongren**:

Ik zou wel met de heer Nordkamp willen meedenken. Bij voorkeur neem je die mensen helemaal niet bij de krijgsmacht aan. Het is namelijk veel ingewikkelder om via de inzet en de bevoegdheden van de dienst aan de slag te gaan dan om aan de voorkant een goed filter te hebben. Het is dus heel belangrijk dat we hier zowel bij de vacatures als bij VEVA, dus bij het hele aannametraject, al aandacht voor hebben en die mensen niet geschikt bevindt. Maar je kan natuurlijk niet uitsluiten dat er toch mensen doorheen komen, dan wel dat ze gedurende de tijd dat ze werkzaam zijn bij Defensie, ineens een switch maken en een vernieuwde of andere belangstelling krijgen. Daarom moet je toch beide blijven doen.

De **voorzitter**:

Kunt u verder met uw betoog of bent u klaar? Dan hebben we nog een punt van de heer Pool. Is daar al een antwoord op? Ik kijk even naar u, minister. U zou nog een definitie voorlezen.

Minister **Ollongren**:

Deze definitie staat overigens ook op de website, hoor. "Rechtsextremisme vormt een dreiging voor de nationale veiligheid en de democratische rechtsorde, omdat het antidemocratische doelen nastreeft, al dan niet met ondemocratische middelen." Dat is de definitie die bij de diensten wordt gehanteerd.

De **voorzitter**:

Dan de heer Pool voor een vraag.

De heer **Pool** (PVV):

Ik ben heel blij met de antwoorden van de minister. Dan is er namelijk maar één conclusie mogelijk: dat de PVV helemaal geen extreemrechtse partij is. De wijze woorden die de minister sprak, dus dat we dit begrip niet moeten politiseren en ook geen etiketjes moeten plakken, is dus gericht aan haar eigen partijleider, die dat dus ten onrechte doet tegenover de PVV. Dat vind ik een fijne en waardevolle afsluiting van dit debat.

De **voorzitter**:

De minister wil daar nog op reageren.

Minister **Ollongren**:

Ja, heel graag, hoewel ik geen vraagteken hoorde aan het eind van de reactie van de heer Pool. In mijn antwoord zei ik net: ik vind het echt belangrijk dat we het werk van de inlichtingen- en veiligheidsdiensten niet politiseren. Dat is echt cruciaal, wie er ook op deze stoel zit. Daarmee doen we de rechtsstaat en het werk van de diensten, die hun werk echt met hele grote zorgvuldigheid uitvoeren binnen de kaders die wij als wetgever daarvoor hebben gesteld, namelijk echt tekort. Dat moeten we dus echt niet doen. Ik vind een politiek debat ... Er is vrijheid van meningsuiting. Er mag heel veel worden gezegd of niet worden gezegd. Etiketten mogen worden geplakt. Maar het antwoord dat ik gaf, was heel feitelijk. Dat ging namelijk over hoe de diensten tegen dit fenomeen aankijken en waarom ze rechts-extremisten volgen. Nou, hierom! Er kan een dreiging van uitgaan voor de democratische rechtsstaat. Dat is een heel serieus punt. Er zijn voorbeelden gegeven van andere landen, waar letterlijk ontwrichtingen zijn geweest van de democratische rechtsstaat. Als het het geval is dat er een dreiging van uitgaat voor onze democratische rechtsstaat, dus voor onze nationale veiligheid, is het de taak en de plicht van de diensten om dat te volgen. Dat is niet politiek. Dat heeft alleen maar met onze veiligheid te maken.

De **voorzitter**:

Dan zijn we daarmee, denk ik, aangekomen bij het einde van dit debat. O, de toezegging die u uitsprak om nog iets na te zoeken over dat schip dat omgevlagd was. Kunnen we uw antwoord daarop binnen een bepaalde termijn verwachten?

Minister **Ollongren**:

Als de heer Kahraman dat heel graag wil. Ik zou 'm het liefst gewoon meenemen en de commissie ervan verzekeren dat we er echt bovenop zitten. Als er aanleiding is om iets te melden, zullen we erop terugkomen. Maar ik neem het uiterst serieus en de minister van IenW ook. Dank voor het signaal. Het was eigenlijk niet bedoeld als toezegging, alleen om de heer Kahraman een beetje gerust te stellen.

De **voorzitter**:

De heer Kahraman neemt daar genoegen mee. Ik zie dat meneer Erkens nog een punt heeft.

De heer **Erkens** (VVD):

Ik had nog één antwoord tegoed. De vraag ging over de mogelijkheid om mensen op deeltijdcontracten te laten werken, zowel voor de private sector als voor de dienst of de cybereenheden.

Minister **Ollongren**:

Voorzitter. Mij wordt verzekerd dat er door de dienst zelf naar wordt gekeken of deze mogelijkheid soelaas biedt, zowel voor het werk bij de dienst als voor deze specifieke doelgroep. Ook wat breder, in onze nieuwe aanpak van hr bij Defensie, heeft dit aandacht. Ik hoop dat ik de heer Erkens in ieder geval zeg dat we het een heel goed idee vinden. Er wordt namelijk dus al over nagedacht.

De **voorzitter**:

De heer Erkens lijkt daarmee tevreden.

Dan kunnen we nu overgaan tot de afsluiting van dit debat. Dank aan de leden voor hun inbreng en aan de minister voor de beantwoording.

Sluiting 14.52 uur.