Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

33 321 Defensie Cyber Strategie

Nr. 6

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 4 juni 2015

De vaste commissie voor Defensie heeft op 21 april 2015 overleg gevoerd met Minister Hennis-Plasschaert van Defensie over:

– **de brief van de Minister van Defensie d.d. 23 februari 2015 over de actualisering Defensie Cyber Strategie (Kamerstuk 33 321, nr. 5).**

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

De voorzitter van de vaste commissie voor Defensie,
Ten Broeke

De griffier van de vaste commissie voor Defensie,
Van Leiden

kst-33321-6
ISSN 0921 - 7371
's-Gravenhage 2015

Voorzitter: Eijsink
Griffier: Mittendorff

Aanwezig zijn zes leden der Kamer, te weten: Vuijk, Knops, De Roon, Hachchi, Jasper van Dijk en Eijsink,

en Minister Hennis-Plasschaert van Defensie die vergezeld is van enkele ambtenaren van haar ministerie.

Aanvang 16.30 uur.

De **voorzitter**: Ik heet de Minister van Defensie en haar medewerkers van harte welkom, net als iedereen op de publieke tribune en de mensen die wellicht elders het debat volgen. Ook heet ik de collega's welkom. Ter voorbereiding op dit algemeen overleg heeft op 8 april jongstleden een technische briefing plaatsgevonden. Wij bespreken vandaag de Kamerbrief van 23 februari jongstleden over de actualisering van de Defensie Cyber Strategie. Ik kijk naar de leden. Dit overleg is gepland tot 18.30 uur. We hebben er dus twee uur voor. Ik denk dat u met zes minuten spreektijd heel ver kunt komen; we zullen het zien. Het woord is aan de heer Vuijk van de VVD-fractie.

De heer **Vuijk** (VVD): Voorzitter. Vorige week bezochten de leden van de vaste commissie voor Defensie de internationale cybertop in Den Haag. Dit AO is vanwege die top naar vandaag verplaatst. Het biedt een goede gelegenheid om cyber, in de betekenis van digitale oorlogsvoering, nog eens met de Minister te bespreken. De dreiging van digitale spionage tegen Defensie is groeiend en agressief, zo las ik vandaag in het jaarverslag van de MIVD. Ik begin dan ook met de constatering dat voor een effectieve verdediging een voortdurende investering in digitale veiligheid en in het veiligheidsbewustzijn van het personeel nodig is. Dat lees ik ook in de stukken. De vraag aan de Minister is aan de orde of die verdediging effectief is en in hoeverre wij ook offensief kunnen optreden als dat nodig is. Hoe staat het met het verder ontwikkelen van militaire cybercapaciteiten, met ICT als een belangrijk wapensysteem?
De Defensie Cyber Strategie van 2012 heeft focus gegeven aan de ontwikkeling van defensieve en offensieve inlichtingencapaciteit in het digitale domein. Met deze actualisering ontwikkelt Defensie zich verder tot een slagvaardige, op innovatie gerichte organisatie die cyberprofessionals kan boeien en binden, zo zegt de Minister. Maar slaagt zij erin om voldoende professionals aan te trekken en vast te houden? Hoe werft zij op dit moment? Ik zie tv-spotjes over verschillende wapensystemen, maar ik zie nog geen spotjes over cyber. Maar dat kan ook komen doordat ik mogelijk niet meer tot de doelgroep voor deze spotjes behoor. Kan de Minister hier iets over zeggen?
Een belangrijk deel van de actualisering gaat over het Defensiepersoneel, waarbij de agenda voor de toekomst van het personeelsbeleid bij Defensie het uitgangspunt is. Het is bijvoorbeeld goed te volgen dat in het cyberdomein specifieke kennis en competenties zodanig van belang zijn dat beperkingen die voortkomen uit het plaatsingsbeleid van militairen – ik noem de beperkte plaatsingsduur, functietoewijzingen en het systeem van rangen en salarisschalen – zo veel mogelijk worden vermeden. Deze richting komt op de leden van de VVD-fractie vertrouwenwekkend over, maar de concrete uitwerking zal uiteindelijk doorslaggevend zijn voor het politieke oordeel. De VVD steunt het voornemen van de Minister om het aantal cyberreservisten verder uit te breiden.
Tijdens de technische briefing hebben wij al gesproken over de effecten van het plaatsingsbeleid. Ik leg die vraag hier opnieuw neer. Is de Minister niet bang dat je, vanwege alle aspecten van het plaatsingsbeleid, zoals de plaatsingsduur, de functietoewijzing, het systeem van rangen en

salarisschalen, een soort wereldje binnen Defensie krijgt met allerlei afwijkende regelingen voor de eenheden die zich met cyber bezighouden? Is de Minister dus niet bang dat men zich gaat gedragen als in een eigen wereldje?
In hoeverre maakt de Minister nu al gebruik van reservisten die werken bij professionele ICT-bedrijven en die gemilitariseerd inzetbaar zijn als de situatie daarom vraagt? In hoeverre zijn bedrijven als KPN, IBM, Atos en Fox-IT bereid om personeel de mogelijkheid te bieden om als reservist te dienen? Ook grote multinationals als Airbus en Lockheed Martin beschikken over professionele cybersecurity-organisaties om bedrijfsgegevens te beveiligen. In hoeverre zijn zij bereid om hun mensen de vrijheid te geven, om het maar zo te noemen, om als reservist binnen Defensie te dienen? Mogen zijn vanuit hun bedrijfsmatige omgeving uit de la van het bureau een groene of anders gekleurde baret pakken om als reservist op te treden? Hoe werkt dat? In hoeverre maakt Defensie gebruik van de kennis en de ervaring van deze organisaties?
Dan een ander punt. Uit het F-35-dossier komt de vraag naar voren hoe veilig militaire informatie is bij de defensie-industrie. Dit kwam eerder aan de orde bij een overleg met Lockheed Martin. Daarin werd aangegeven dat onzorgvuldig omgaan met gerubriceerde bedrijfsgeheimen verlies van orders, en dus verlies van werkgelegenheid, kan betekenen. Uit het bedrijfsleven komt de informatie dat vanuit het buitenland 24/7 ingebroken wordt in digitale systemen van de defensie-industrie. Vandaag konden we dat ook lezen in het jaarverslag van de MIVD. Ik maak het iets specifieker. Wat mij betreft gaat het om de vraag of de ABDO-regeling (Algemene Beveiligingseisen voor Defensieopdrachten) effectief is. Hoe weerbaar is de defensie-industrie? Is de ABDO-regeling op het punt van het organiseren van cyberweerbaarheid effectief, of verdient deze regeling een actualisatie? Daar komt een vraag achter vandaan, namelijk: hoe kan de Kamer de effectiviteit van die ABDO-regeling controleren en beoordelen? Wat kan de Minister hierover in de openbaarheid zeggen?
Ik heb nog een laatste opmerking. Afgelopen vrijdag bezocht een delegatie van de vaste commissie voor Defensie de oefening Lowland Torch in Schaarsbergen. Dat was een leerzaam bezoek, waarbij wij kennismaakten met Joint Intelligence, Surveillance, Target Acquisition and Reconnaisance Commando (JISTARC). Dit zijn de vooruitgeschoven mannen en vrouwen die met sensoren in het veld onder moeilijke omstandigheden inlichtingen verzamelen en analyseren. Mijn complimenten aan de Minister: het was een mooi werkbezoek. Het was goed om het te zien en er kennis mee te maken.

De heer **Knops** (CDA): Voorzitter. Estland heeft in 2007 aan den lijve ondervonden dat de toegenomen assertiviteit van Rusland niet beperkt blijft tot retoriek. Het werd bijna twee weken platgelegd met een digitale blitzkrieg, een cyberaanval die het verdedigingssysteem van het kleine land voor een groot deel lamlegde. Het is niet de eerste cyberaanval, en zeker niet de laatste. Amerikaanse experts waarschuwen al jaren voor een elektronisch Pearl Harbor en een digitale 9/11. Veel aanvallen die nu al plaatsvinden, zijn te herleiden tot China en Rusland; landen die in de cyber warfare vooroplopen. Terwijl andere landen inmiddels bezig zijn om speciale defensieafdelingen op te richten om zich tegen deze oorlogsvoering te kunnen wapenen, blijft het in Nederland stil.
Deze tekst sprak ik uit in december 2009. Het was voor mij aanleiding om een motie in te dienen waarin werd verzocht om te komen tot een cyberstrategie. Het is nu 2015. De Minister heeft de strategie, die door haar voorganger is opgezet, geactualiseerd. Wat ons betreft is dat een goede zaak, want de ontwikkelingen op het gebied van cyber gaan razendsnel. Het is voor Defensie van groot belang om met deze ontwikkelingen mee te kunnen gaan. Ik zal in mijn inbreng dan ook ingaan op de toegenomen dreiging en het vermogen van Defensie om hiermee om te

gaan. Daarnaast zal ik een appreciatie geven van de strategie, en ingaan op de vraag of Defensie genoeg doet en op de retorische vraag of er meer nodig is.
Over de dreiging van cyber kan niemand meer naïef zijn. Rusland, China, criminelen en terroristische organisaties: ze zijn er in toenemende mate bedreven in, inclusief de barbaren van ISIS, die zich niet beperken tot het afhakken van hoofden en ook hacken. Onlangs gebeurde dat nog bij een Frans televisiestation. Zelfs het thuisfront van militairen wordt via social media bedreigd door de ISIS-aanhang. Ook de spionage neemt toe. De MIVD constateert dat de dreiging van digitale spionage «significant, groeiend, steeds vaker geavanceerd en agressief van aard» is. Netwerken van Defensie waren het doelwit van grootschalige spionageaanvallen. Voor zover bekend is geen van deze aanvallen succesvol geweest, wordt eraan toegevoegd. De vraag is: hoelang is dat nog zo? Er wordt veel goed werk verricht bij Defensie. Nederland zou zelfs tot de cyberkopgroep binnen de EU en de NAVO behoren. Dat is een compliment waard. Nederland moet namelijk weerbaar zijn. Onze open economie is wellicht kwetsbaarder dan die van andere landen. Ook wordt de wereld instabieler; het is al vaak gezegd. Dat betekent dat we moeten investeren in Defensie, in cyber als vijfde domein en natuurlijk ook in de andere domeinen land, zee, lucht en ruimte.
De cyberstrategie ziet er op papier mooi uit, maar de vraag is natuurlijk hoe het in de praktijk gaat.

De heer **Vuijk** (VVD): Ik vind het betoog van de heer Knops interessant. Hij gooit de vraag op tafel of er meer naartoe moet. Ik ben geïnteresseerd in de opvatting van de heer Knops zelf. Over cyber en de cyberstrategie wordt in de stukken geschreven: investeer in mensen en materieel. Als de heer Knops vindt dat er meer moet gebeuren, kan hij dan iets meer zeggen over wat er precies meer moet gebeuren?

De heer **Knops** (CDA): Dat is op zich een logische vraag, maar mijn pleidooi is vooral gericht op het feit dat we in al die domeinen meer en sneller zullen moeten reageren. Het is niet Defensie, niet Nederland dat het tempo bepaalt. Opponenten, waar ze ook vandaan komen – vaak is ook niet bekend wie het precies zijn – bepalen of onze verdediging goed op orde is of niet. Als je daar niet hetzelfde tempo in betracht qua ontwikkelingsgang, qua technologische ontwikkeling en qua inspanningen die je ervoor levert, loop je grote risico's. Onze maatschappij is daar, meer dan andere, kwetsbaar voor.

De heer **Vuijk** (VVD): Ik had gehoopt op iets meer concreets. Is er concrete aanleiding om te zeggen: ik vind dat we meer moeten doen? De Minister legt hier een strategie neer en actualiseert die ook. Mijn appreciatie is dat we in ieder geval op de goede weg zijn. Is de heer Knops het met mij eens dat het een goede weg is, of vindt hij het te langzaam gaan? En hoort daar ook nog iets concreets bij?

De heer **Knops** (CDA): Nu ik zo luister naar de heer Vuijk, denk ik dat hij mij niet helemaal goed begrepen heeft. Waar ik zei dat er meer moet gebeuren, gaat het meer in zijn algemeenheid over de inspanningen van Defensie. Het kan geen verrassing zijn voor de heer Vuijk om dat uit mijn mond te vernemen. Dus daar hoort ook cyber bij. Tot nu toe ben ik in mijn inbreng buitengewoon positief over de inzet van Defensie. Ik heb wel nog een aantal vragen over de risico's die ook een beetje in lijn zijn met de vragen die de heer Vuijk zelf gesteld heeft. Het gaat namelijk niet vanzelf en dit is een heel andere materie dan de conventionele situaties waar Defensie de afgelopen decennia mee te maken heeft gehad.
Een van mijn zorgpunten rond cyber betreft de vraag hoe een en ander in de praktijk gaat. Defensie heeft zijn eigen ICT niet op orde en een

Kamermeerderheid vindt dat de Minister niet in control is. Hoe verhoudt zich deze problematiek tot de cyberinspanningen? Klopt het dat een deel van de computers van Defensie nog op Windows XP draait? Dat is toch hetzelfde als aan internetverkeer deelnemen zonder gordel? Verder ben ik benieuwd te vernemen hoe het zit met de uitbesteding van vitale en kwetsbare ICT-infrastructuur waar het gaat om cybergevoeligheid. Wanneer je praat over sourcing van dit soort vraagstukken en je dat buiten Nederland zou brengen, loop je buitengewoon grote risico's. Ik ben benieuwd naar de reactie van de Minister op dat punt. Is er en wordt er overigens voorzien in een voldoende adequaat beschermingsniveau van de ICT-infrastructuur? Wordt voorzien in periodieke controles en stresstests in oefeningen, ook internationaal? Gaan ook oefenaanvallen plaatsvinden op de eigen systemen teneinde die te testen, zodat we ook echt weten of ze werken?
Permanente innovatie is nodig en de vraag is hoeveel ruimte daarvoor is. Generaal De Kruif trok aan de alarmbel en had het erover dat Defensie in het rood draait en onvoldoende kan innoveren. Dat heeft natuurlijk allemaal met geld te maken. Als je te weinig geld hebt, kun je ook op het gebied van innovatie te weinig doen. De Minister erkent dat een volledig waterdichte digitale verdediging onhaalbaar is. Op welke wijze wordt voorzien in gevolgenbestrijding in het geval van een geslaagde aanval? Dan nog een opmerking over de mooie passage over het binden en boeien van personeel. Ook bij cyber is de mens namelijk de cruciale factor. De desbetreffende voornemens zien er op papier goed uit. Defensie als aantrekkelijke werkgever, zo staat het geformuleerd. De werkelijkheid is dat het personeel al meer dan 700 dagen zonder een cao zit en al jaren op de nullijn zit. En dan is er nog het Wul-drama enz. enz. Bovendien loopt de loonontwikkeling achter en is er een braindrain gaande. Wat gaat de Minister doen om die cyberbraindrain te voorkomen? Mooie woorden en mooie intenties, maar gaat dit ook allemaal werken? De Minister zet zich in voor modernisering van de arbeidsvoorwaarden, maar de vraag is waarom ze zich niet inzet voor verbetering van de arbeidsvoorwaarden van de militairen die al jaren op de nullijn zitten. Dat geldt ook de militairen die geworven moeten worden in een organisatie voor cyber.
In aansluiting op de heer Vuijk heb ik nog de vraag wat de reservisten kunnen betekenen voor cyber. Dat lijkt mij heel veel te zijn, maar het is dan wel goed om inspanningen op een goede manier te benutten. Ik ben dan ook benieuwd hoe Defensie dat wil doen.
Verder wil de Minister inzetten op offensieve capaciteiten. Dat is wat ons betreft helemaal terecht. Sommige fracties willen hier niet over praten in dit parlement, maar de idee dat je alleen maar jezelf behoeft te verdedigen en niet proactief zou moeten aanvallen, maakt allemaal onderdeel uit van het spectrum. Dat moet je dus ook kunnen doen. De vraag is wel hoe dat juridisch, internationaalrechtelijk zit. De Geneefse Conventie stamt uit 1949 en de vraag is dan hoe het zit met begrippen als «collateral damage». Hoe is het onderscheid tussen strikt militaire doelen en civiele objecten te maken?
Onze fractie heeft dus nog wat vragen. Dat geldt ook voor de SMART-formulering in de brief. Ik heb er in de technische briefing ook al naar gevraagd. De vraag is toch wat, hoe en wanneer de Minister dat wil bereiken. Alleen als de doelstellingen SMART geformuleerd zijn, kan de Kamer controleren.
Tot slot. De Minister doet haar best met de beperkte middelen en binnen de te krappe begroting. Ze trekt een bedrag van oplopend 9 miljoen euro extra uit voor cyber vanaf 2017 en de vraag is of dat genoeg is, zeker gezien de analyses van de MIVD waarin gemeld wordt dat het digitale domein echt een punt van aandacht is voor de komende jaren. Ik sprak in het begin al over de snelheid waarmee een en ander gepaard zou moeten gaan. Als ik dat dan afzet tegen de reactiesnelheid van Defensie ten aanzien van de aangenomen motie-Van der Staaij in de Tweede Kamer,

dan vraag ik mij af of dat tempo wel voldoende is om dit soort ontwikkelingen bij te houden. Ik zou de Minister dus willen vragen om daar uitgebreid op te reflecteren.

De heer **De Roon** (PVV): Voorzitter. De PVV is blij met de toegenomen aandacht voor het onderwerp cyber warfare bij Defensie, maar we vragen ons wel af of Defensie over voldoende middelen daarvoor beschikt. De Minister spreekt in haar brief over een digitale revolutie, maar we zien nog niet heel veel gevolgen daarvan op de Defensiebegroting. Ik heb gelezen dat er op termijn 9 miljoen euro bijkomt voor cyber-warfare-doeleinden. Dat is een heel aardig bedrag maar het is hetzelfde bedrag als wat het kost om een Joint Strike Fighter een jaar lang te onderhouden. Dus als ik dat met elkaar vergelijk, moet ik concluderen dat we straks nog niet zo heel veel uitgeven aan cyber warfare. Nu zeg ik niet van «pomp er maar zo veel mogelijk geld in», want ik weet ook wel dat als je dat bij een startend bedrijfsonderdeel doet, het meestal niet goed afloopt, maar met die 9 miljoen zullen we er in de toekomst zeker niet zijn.
Uit het jaarverslag van de MIVD dat waarschijnlijk niet geheel toevallig net gisteren uitkwam, blijkt dat cyberspionage een groot en groeiend probleem is, geavanceerd en agressief van aard. Als er nu spionage wordt geconstateerd bij Defensie gaat de MIVD natuurlijk proberen om die spionage te stoppen. Kan zo'n detectie van spionage ook een aanleiding zijn voor Defensie om van zich af te bijten en om dus gewoon terug te slaan, in de zin dat niet alleen de spionage wordt gestopt maar dat ook een stuk ICT-infrastructuur van degene die achter die spionage zit, is te treffen met een aanval?
Het is duidelijk dat alles staat of valt met het hebben en behouden van goed personeel dat ook gemotiveerd moet blijven. Gekwalificeerde cybersoldaten zijn van essentieel belang. Defensie wil, om dat te bereiken, flexibel omgaan met het personeelsbeleid. Dat lijkt mij op zich heel verstandig. Ook het idee dat je een flink deel van het cyberpersoneelsbestand van Defensie in de vorm van reservisten hebt, vind ik logisch. De Verenigde Staten doen dat ook, zo las ik. Nou las ik toevallig van de week ook een stuk over hoe men er in de Verenigde Staten mee omgaat. De kop van dat artikel was «The army is sharing its top cyber warriors with Hollywood and Wall Street». Ik weet niet of de Minister het voor Nederland ook zo interessant kan maken, maar wat ik wel weet is dat Hollywood en Wall Street forse salarissen betalen. Hoewel in dat artikel niet staat wat men in Amerika dan aan dat soort mensen gaat betalen, rijst bij mij wel de vraag tot hoever de Minister dan wil gaan als het gaat om salaristegemoetkomingen voor cyber warriors in Nederland. Ik mag toch hopen dat de balkenendenorm in ieder geval in acht zal worden genomen. Graag verneem ik hierop de reactie van de Minister.
Dan de offensieve inzet van cybercapaciteit. Ik had er al iets over gevraagd naar aanleiding van eventueel geconstateerde spionage. De Minister en ik hebben in een eerder overleg al gewisseld dat we allebei blij zijn met het idee van het ontwikkelen van offensieve cyberwapenmogelijkheden. Die wapens moeten snel en effectief kunnen worden ingezet. In de actualisering van de cyberstrategie lees ik dat de cyberwapens alleen mogen worden ingezet tegen militaire doelen. Is dat traditionele onderscheid tussen militaire doelen en niet-militaire doelen nog wel van toepassing? We hebben in deze tijd immers te maken met allerlei niet-statelijke actoren die geweld en wellicht cybergeweld toepassen. Dat zal in ieder geval in de toekomst van steeds grotere betekenis kunnen worden. Dus betekent de term «militaire doelen» in dit verband nou ook dat in voorkomende gevallen ook de IT-infrastructuur van niet-statelijke actoren kan worden aangevallen als daar aanleiding toe is? Graag krijg ik hierop een reactie van de Minister.
De ontwikkeling van cyberwapens is nuttig en noodzakelijk, maar binnen welke kaders kunnen we die inzetten? We zouden van de Minister begin

2015 een doctrine ontvangen op dit punt, maar uit de brief de we op 23 februari van de Minister hebben gekregen blijkt dat die doctrine eigenlijk nog verder ontwikkeld moet worden. Daar kan ik mij heel veel bij voorstellen, maar dan is mijn vraag wel of de Minister er een bepaalde planning voor heeft. Wanneer kunnen we nu wel een afgeronde doctrine tegemoetzien?
Waar het gaat om het voeren van een cyberoorlog dient een complement daarvan op z'n minst te zijn adequate mogelijkheden van elektronische oorlogsvoering. Wat is het standpunt van het kabinet ten aanzien van het onderwerp elektronische oorlogsvoering en het offensieve gebruik daarvan, al dan niet complementair aan cyber warfare? Ik denk dat het ontwikkelen van cyberwapens hand in hand moet gaan met de verdere ontwikkeling van aanvallende capaciteiten voor elektronische oorlogsvoering. Andere landen doen dat ook. Ik vraag mij af of de Nederlandse regering dat ook van plan is. Ik zie dat mijn tijd om is, voorzitter, dus ik stop er nu mee.

Mevrouw **Hachchi** (D66): Voorzitter. Vandaag spreken wij over de Defensie Cyber Strategie. Ik denk dat we met elkaar kunnen vaststellen dat cyber en cybersecurity, digitale veiligheid, een hot topic is, ook gelet op de Global Conference on CyberSpace van vorige week. Voordat ik inga op de rol die Defensie speelt op het gebied van cyber, benadruk ik dat het voor mijn partij ontzettend belangrijk is dat we de balans weten te vinden tussen aan de ene kant het internet als publieke kern of het vrije internet en aan de andere kant de belangen die er terecht zijn op internationaal niveau maar ook op het niveau van nationale staten. Het is belangrijk om die balans steeds voor ogen te houden.
Ik zoom in op de rol van Defensie op het gebied van cyber. We hebben het ook over cyber warfare. Een echt grootschalige cyberoorlog is er nog niet geweest, maar we kunnen niet zeggen dat het nooit kan gebeuren. D66 vindt het goed dat Defensie cybercapaciteit ontwikkelt. Zeker gelet op het feit dat in het jaarverslag van de MIVD staat dat Defensie het doelwit is van grootschalige spionageaanvallen, is het goed dat we hierin investeren. Dat is ook gebeurd naar aanleiding van de begrotingsafspraken. Er is structureel 9 miljoen euro bij gekomen. Dat is toch bijna een verdubbeling van het budget.
Mijn fractie snapt niet helemaal waarom het Defensie Cyber Commando (DCC) is belegd binnen de landmacht. Is cyber nou echt een vijfde domein? Of is het de bedoeling dat cyber wordt geïntegreerd binnen de bestaande krijgsmachtonderdelen? Hoe is dan de samenwerking met de luchtmacht en de marine?
Ik ga eerst in op de defensieve kant van cyber. De vraag die eigenlijk voorligt is: wat is het Nederlandse cybergrondgebied? Met andere woorden: wat moet Defensie verdedigen? Kan de Minister daarop reflecteren? Ik heb vorige week verschillende mensen hierover gesproken. Waarom is Defensie terughoudend om die grotere rol te spelen in de bescherming van de vitale infrastructuur van Nederland?
Vorige week riep de Minister van Buitenlandse Zaken op tot een hackverbod voor vitale onderdelen van het internet. Onderstreept de Minister van Defensie dit pleidooi? Hoe moeten we dat dan zien? Betreft het een niet-aanvalsverdrag tussen landen? Of is het ook gericht tegen hackers? Ik vraag mij af of dat überhaupt mogelijk is. Kun je dit afspreken met hackers? Tegelijkertijd wijs ik de Minister op het feit dat de rechter recentelijk een uitspraak heeft gedaan waaruit blijkt dat een hacker zelfs malware mag installeren op systemen van een ziekenhuis om zwaktes aan te tonen in die systemen. Kortom: je hebt het ook nodig om die systemen veiliger te maken. Hoe moet ik de uitspraak van Minister Koenders nu precies plaatsen?
Ik kom op de offensieve kant. Offensieve inzet is alleen mogelijk als je de kwetsbaarheden in software opspoort of koopt op de witte of zwarte

markt. Daar is een bloeiende handel in. Dat kunnen we lezen in het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) over internet. Dat is overigens een uitstekend rapport. Om aanvallen te kunnen doen, moet je de kwetsbaarheden intact laten tot het moment dat je een aanval wilt doen, in plaats van die kwetsbaarheden op te lossen en het internet veiliger te maken. Oftewel: je laat ze bestaan voor een later moment. Bovendien kunnen ook anderen er gebruik van maken als ze die kwetsbaarheden opsporen of hebben gekocht. Dat kan worden gedaan door criminelen of de vijand, wie dat dan ook mag zijn. Dat heeft natuurlijk impact op mensen en overheden, die hier slachtoffer van kunnen worden. De kern van mijn vraag is: hoe wenselijk is dat? Wil de Minister samen met haar collega van V en J de Kamer per brief hierover informeren? Kan zij in die brief reflecteren op de wenselijkheid van het opsparen van de kwetsbaarheden in software en het dilemma dat daardoor ontstaat? Dan heb ik het over de spanning tussen offensief en defensief. Met name het defensieve is immers bedoeld om aanvallen op te sporen en de veiligheid te garanderen. Ik wil hier graag een helder antwoord van de Minister op horen. Als zij dat niet kan geven omdat zij afhankelijk is van haar collega van V en J, dan zou ik daar graag een brief over ontvangen. Zou de Minister daarin ook kunnen ingaan op de vraag hoe de bloeiende handel het beste kan worden aangepakt? Dat zul je wel in internationaal verband moeten doen.

Ik kom op de samenwerking, want Defensie kan het niet alleen. Juist in het cyberdomein is samenwerking met publieke en private partners noodzakelijk. In de brief van de Minister ontbreekt echter één cruciale partner, namelijk de hacker community. Op welke wijze zoekt de Minister naar samenwerking daarmee?

Hoe staat het met de vulling van het Defensie Cyber Commando? Ook collega's hebben daarnaar gevraagd. Lukt het om de juiste mensen te vinden? Op verschillende universiteiten worden masterprogramma's ontwikkeld en gestart. Wordt daar ook mee samengewerkt? De Minister is in de stukken weinig concreet over de samenwerking met het bedrijfsleven, maar wellicht kan zij hier vandaag nog wat concreter ingaan op de vraag hoe de samenwerking met het bedrijfsleven wordt gezocht en hoe die plaatsvindt.

Ik gaf net al aan dat cyber per definitie een internationaal onderwerp is. Je kunt immers geen hekje plaatsen om het Nederlandse onlinedomein. Effectieve cyberwapens vereisen ook een internationale aanpak, binnen de Europese Unie maar ook binnen de NAVO. Als ik echter lees wat zowel de EU als de NAVO doet op het gebied van cyber, voelt het als langetermijnwerk. Daarom stel ik de Minister de volgende vragen. Is cyber een thema voor de Minister tijdens het aankomend EU-voorzitterschap? Hoe staat het met cyber binnen het GVDB, het gemeenschappelijk veiligheids- en defensiebeleid? Hoe staat het met de uitvoering van het EU Cyber Defence Policy Framework? Welke mogelijkheden ziet de Minister om cyber op de agenda's van de EU en de NAVO een hogere plek te geven?

Ik weet dat mijn spreektijd bijna om is, voorzitter. De ontwikkelingen inzake het cyberdomein gaan razendsnel. De Minister constateert zelf in haar strategie dat het problemen oplevert op het gebied van verwerving en innovatie. Kan de Minister concreet toelichten wat zij daarmee gaat doen en hoe dit zich verhoudt tot Europese aanbestedingsregels?

Ik sluit af. De Defensie cyberdoctrine is nog in ontwikkeling. Hoe wordt die ingebed in de Nederlandse Defensiedoctrine? Wordt de Defensie cyberdoctrine ook openbaar gemaakt?

Over de inzet van Defensiecybercapaciteiten hebben we van het ministerie een goede briefing gehad met een scenariocontext. Ik weet ook wat de AIV (Adviesraad Internationale Vraagstukken) en CAVV (Commissie van advies inzake volkenrechtelijke vraagstukken) hierover hebben gezegd, namelijk dat het niet anders is dan dat het bij de huidige bestaande militaire capaciteiten gaat. We hebben de Defensiecybercapaciteit nog niet

ingezet, maar als blijkt dat er uitzonderingen zijn of dat cyber toch een andere betrokkenheid van het parlement vergt of wat dan ook, wil ik dat de Minister ons daarover informeert. Ik denk dat de grootste uitdaging is dat de geesten rijp gemaakt worden voor de inzet van cybercapaciteit tijdens missies.

De heer **Jasper van Dijk** (SP): Voorzitter. We lezen in de media dat er steeds meer cyberaanvallen zijn. Netwerken van Defensie zijn doelwit van grootschalige digitale spionageaanvallen. De MIVD meldt dat het mogelijk gaat om China en Rusland. Cyberaanvallen zijn dagelijkse kost, maar gelukkig zijn ze vaak niet succesvol. Kan de Minister meer zeggen over de grootschalige aanvallen van Rusland en China? Zijn er ook aanvallen van bondgenoten, zoals Edward Snowden heeft aangetoond?
Cyberveiligheid staat in de belangstelling. Zie de cybertop van vorige week. Maar ik heb daar nog wel wat vragen over. Wat zijn nou precies de voorwaarden waaronder cyberwapens gebruikt mogen worden? Er zijn eigenlijk geen duidelijke richtlijnen over. Dat heb ik bij het vorige algemeen overleg ook al gezegd. De Minister heeft toen toegezegd om op een artikel in Vrij Nederland te reageren. Dat staat ook netjes in de begroting. In de brief van februari wordt er ook wel wat over gezegd, maar nergens wordt concreet ingegaan op dat artikel. Dat had ik eigenlijk wel een beetje gehoopt. Misschien kan de Minister hier nog iets over zeggen.
De Minister schrijft wel dat de juridische kaders niet anders zijn dan die voor de inzet van conventionele middelen en dat er een volkenrechtelijk mandaat moet zijn. Ook schrijft zij: we bekijken verder wel per operatie wat we gaan doen. Het volgen van het oorlogsrecht is één ding, maar minstens zo belangrijk zijn uitgewerkte richtlijnen voor militairen. Dat zegt ook Sergei Boeke, die hiernaar onderzoek deed in opdracht van Defensie. Wellicht kent de Minister zijn onderzoeksrapport, anders heb ik het hier. Want een commandant moet toch weten wanneer hij welke wapens kan inzetten en hoe? Hoe pak je niet-statelijke actoren aan? Wat is proportioneel gebruik? Wat is de verhouding tussen civiele en militaire doelen? Welke richtlijnen zijn er dienaangaande? Het Rode Kruis wijst daar ook op en stelt dat de regels van het humanitair oorlogsrecht van toepassing zijn op cyber in een gewapend conflict. Dan moet je dus ook het verbod erkennen om directe aanvallen te plegen tegen burgers en burgerobjecten. Vanwege de nauwe verwevenheid tussen militaire en civiele digitale netwerken is het onderscheid daartussen moeilijk. Dat wordt ook wel interconnectedness genoemd. Als je de energievoorziening digitaal aanvalt, kun je dus ook een ziekenhuis aanvallen. Daar komt het concreet op neer. Volgens mij is dat niet de bedoeling. Is het mogelijk om een betere scheiding te maken tussen civiele netwerken en militaire netwerken? Is het zinvol om daar onderzoek naar te doen op digitaal gebied? Kunnen computernetwerken gezien worden als vitale infrastructuur in dit verband, net als bijvoorbeeld nucleaire installaties?
In 2012 is voor het eerst een doctrine aangekondigd. Wanneer kunnen we deze verwachten? De collega's vroegen het ook al. Een doctrine zou toch de basis van het beleid moeten zijn? Ook de richtlijnen ten aanzien van het inwinnen van inlichtingen kwamen in het VN-artikel aan de orde. Wij lezen dat Defensie investeert in een hoogwaardige inlichtingenpositie en dat de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) gemoderniseerd moet worden. Dan gaat het ook om kabelgebonden telecommunicatie. Kan de Minister toelichten waar voor het kabinet de grenzen liggen? Waar wordt de privacy op een ontoelaatbare manier aangetast? Hoe staat het met het idee om ook kabels af te tappen?
De Minister doet veel, met name op het gebied van technische ontwikkelingen en digitale oorlogsvoering. Daar valt heel veel voor te zeggen, maar er zit ook een moreel aspect aan. Dat is eigenlijk de kern van mijn inbreng. Wat mij betreft, ontbreekt het nog aan een concrete uitwerking

daarvan. Je kunt immers niet zeggen: dat zien we wel op het moment dat we een operatie doen, zoals de Minister schreef op pagina 11. Dat vind ik echt een beetje te makkelijk. Ik zou zeggen: ook cyberoorlog is te belangrijk om aan militairen over te laten.

De **voorzitter**: Mag ik de heer De Roon wederom vragen om even de voorzittershamer van mij over te nemen, zodat ik mijn eigen inbreng kan doen? Ik zeg de heer De Roon toe dat ik nauwlettend mijn eigen spreektijd in de gaten zal houden.

Voorzitter: De Roon

De **voorzitter**: Daar ga ik zonder meer van uit. Het woord is aan mevrouw Eijsink.

Mevrouw **Eijsink** (PvdA): Voorzitter. Ik herinner mij nog heel goed dat we vorig jaar op 26 april overleg voerden met de Minister over toen nog de brief die heette: offensieve cybercapaciteit Defensie. Wij spreken vandaag over de Defensie Cyber Strategie. Uiteraard sluiten beide bij elkaar aan. Een dag of twee dagen na het vorige overleg kwam er een artikel in de krant over de vraag of cyber nu wel of niet onder artikel 5 van de NAVO valt. Ik denk dat daardoor een goede discussie is ontstaan, met name op de briefing – ik dank de Minister overigens voor die briefing – die we hierover hadden op 8 april. Het wordt steeds duidelijker wat die offensieve cybercapaciteit is en hoe we die mogelijk kunnen inzetten.
De brief van 23 februari, die we vandaag bespreken, behelst zeven speerpunten. Boeien, binden en ontwikkelen. Wie kan daar tegen zijn? Het verruimen van mogelijkheden. Daar kun je natuurlijk ook niet tegen zijn. Wat vandaag hier niet aan de orde is, omdat het niet op de agenda staat en omdat we er nog een apart overleg over hebben, is het jaarverslag van de MIVD dat we gisteren ontvangen hebben van de Minister. Daar komt nog een briefing over. Dat sluit zeer aan bij een van die zeven punten, namelijk het inlichtingenvermogen van Defensie in het digitale domein. Dat geeft voor mijn fractie meteen aan dat de discussie rondom cyber – mevrouw Hachchi zei het ook – natuurlijk veel breder is dan Defensie alleen. Ik zou het eigenlijk goed vinden als de Kamer een wat breder overleg had over cyber. Daar hebben we het de vorige keer ook over gehad, naar aanleiding van de brief van 17 maart vorig jaar. Het beperkt ons als vaste commissie van Defensie nog weleens dat wij alleen met de Minister van Defensie spreken. Defensie geeft al langer aan dat cyber, het digitale domein, als het vijfde domein voor militair optreden wordt gezien, naast land, lucht, zee en de ruimte. Dat is niet nieuw en dat bespreken we vandaag opnieuw. Wellicht wil de Minister zelf ingaan op de suggestie dat het misschien beter is om cyber op verzoek van de Kamer in een breder verband te bespreken, ook in commissies? Wij bespreken nu alleen het kleine stukje cyber Defensie, terwijl het meer en veel breder is.
Er zijn al veel vragen gesteld, waar ik mij gemakshalve bij aansluit zonder ze te herhalen. Met name over de personele gevolgen hebben de heer Knops en de heer Vuijk al breed gesproken. Dat geldt ook voor de reservisten. Een punt dat ik extra wil inbrengen, sluit aan bij een punt uit het betoog van mevrouw Hachchi, namelijk de EU-cyberstrategie. Wij weten dat dit een van de 22 punten was naar aanleiding van de Raad van december 2013 en dat de EU toen afgesproken heeft dat er een EU-cyberstrategie zou komen. Binnen de NAVO is er ook een cyberstrategie. De vraag is natuurlijk hoe een en ander praktisch, operationeel aansluit. Tijdens de briefing op 8 april hebben we die vraag ook gesteld en te horen gekregen dat een aantal landen op dit moment geen inlichtingen wenst te delen daarover, terwijl een aantal andere landen misschien wel zou willen samenwerken. Om weer terug te gaan naar een operationeel

niveau: op welke wijze wordt informatie gedeeld? Ik moet eerlijk zeggen dat ik daar geen beeld van heb.
Net als de collega's ben ik vorige week naar verschillende cyberbijeenkomsten geweest, maar ik zal u eerlijk zeggen dat ik nog niet goed inzicht krijg in hoe inlichtingen gedeeld zullen worden. De heer Knops verwees terecht naar 2009, toen we hier debatteerden met de voorganger van deze Minister, voormalig Minister Hillen. Nee, het was niet Minister Hillen, het was toenmalig Minister van Middelkoop. Hij deed in 2009 de eerste aanzet. Vervolgens kwam onder Minister Hillen de eerste strategie naar de Kamer. We zijn opgeschoten. Uiteraard zijn er ontwikkelingen geweest in het denken hierover. Het is echter ook voor de Kamer van belang hoe we dat operationeel kunnen inpassen. Terecht werd verwezen naar het werkbezoek van vrijdag, waar dit ook in verweven zit. Dat zei de heer Knops terecht. Daarom sluit ik mij ook aan bij de vraag hoe je binnen de fysieke systemen alles gaat inrichten.
Als laatste een opmerking – en dan ben ik heel erg binnen mijn tijd gebleven, zeg ik tegen de voorzitter – over de fysieke termen. We gaan in Iran alleen maar een paar gebouwen bezetten of opblazen. We gaan niet proberen om dominantie over het Iraanse luchtruim of zeegebied te krijgen. Zou de Minister daarop willen reageren? Dat gaat natuurlijk over de offensieve inzet. Ik probeer in de termen van Defensie beeld en geluid te krijgen bij wat dit nu betekent en op welk moment er besluiten genomen worden. In de briefing is daar heel goed op ingegaan. Wellicht dat de Minister dat hier nogmaals kan doen.

Voorzitter: Eijsink

Schorsing 17.08 uur tot 17.18 uur

De **voorzitter**: Ik stel voor dat de leden maximaal twee keer interrumperen. Mocht er meer nodig zijn en mocht daarvoor de tijd beschikbaar zijn, dan benutten wij die natuurlijk graag.

Minister **Hennis-Plasschaert**: Voorzitter. De heer Knops verwoordde het heel mooi: over de dreiging van cyber kan niemand meer naïef zijn. Zo is het. Defensie bereidt zich er daarom al een tijdje op voor. Het is overigens niet zo dat het eventjes geregeld is. Voordat je die kennis hebt opgebouwd, ben je zomaar een hele tijd verder, of het nu gaat om het defensief of om het offensief vergaren van inlichtingen.
Laat ik allereerst wat zeggen over de reservist. Defensie maakt bij voorkeur met regelmaat gebruik van de reservist. In de Kamer leeft net als bij mij de wens om de inzet van reservisten te vergroten. Dat doet overigens niets af aan het feit dat je natuurlijk zelf over een kern moet beschikken, maar daar waar mogelijk worden reservisten ingezet. Bij Def-Search zijn op dit moment bijvoorbeeld twee reservisten ingezet. Vorige week zijn ook reservisten ingezet bij het Defensie Cyber Expertise Centrum (DCEC). Wij zijn altijd in overleg, zeker ook op dit terrein, met grote en kleinere bedrijven om te bekijken of wij elkaar kunnen versterken bij het beschikbaar stellen van cyberreservisten. Ik zeg er gelijk bij dat dat ook weer allerlei vragen met zich meebrengt, bijvoorbeeld over de drive van bepaalde bedrijven en werknemers. Verhoudt het zich tot de werkzaamheden waarvoor de cyberreservist wordt aangesteld? Dat heeft ook weer te maken met integriteit, beïnvloeding en dat soort zaken. Het is bekend dat er een onderzoek loopt, dat er vooralsnog rustig uitziet. Maar goed, ik kan helemaal niet vooruitlopen op de uitkomsten daarvan. Het is een vraagstuk dat je niet kunt negeren. Waar mogelijk willen wij natuurlijk zo veel mogelijk gebruikmaken van de expertise van reservisten. Afhankelijk van de aard van een incident of de benodigde expertise zal daarvan gebruik worden gemaakt. Dat doen wij nu al en dat zullen wij waar mogelijk in de toekomst intensiveren.

De heer Vuijk vroeg of niet de neiging ontstaat om een cyberwereldje binnen de organisatie te creëren. Nee, want uiteindelijk probeer je waar mogelijk maatwerk te leveren, ook als dat in het belang is van het aantrekken van bepaalde expertise. Op op zichzelf staande wereldjes binnen de organisatie van de krijgsmacht zit ik absoluut niet te wachten. De kracht van de krijgsmacht is juist dat iedereen elkaar weet te vinden en dat iedereen complementair is. Wel heb ik aangegeven dat er een aantal aanpassingen nodig zijn, zowel op personeelsgebied als bij de verwerving van materieel. Het moet allemaal snel. De technologie staat niet bepaald stil. Het moet lager in de organisatie kunnen worden belegd. Net als je voor medici bepaalde regelingen treft, moet je ook bekijken of dat voor cyber mogelijk is.
Dat brengt mij op de opmerking van de heer Knops dat het onvoldoende smart zou zijn. Het is een strategie, het geeft richting. Het hoeft niet per se supersmart te zijn geformuleerd, ook omdat op dit gebied dingen heel erg snel gaan. Je kunt nu smart formuleren waar je over twee jaar wilt zijn, maar daarmee kun je over een jaar alweer bedrogen uitkomen. Het geeft richting en het wordt verder ingevuld. Dat is volgens mij ook tijdens de technische briefing met de Kamer gedeeld aan de hand van de hoeveelheid actieplannen, die nu verder worden opgesteld. Voor 2015 zijn al een heleboel concrete acties gepland. Ik kan er daarvan een aantal met de Kamer delen, bijvoorbeeld projectfuncties extra personeel bij het DCC. Ik noem ook het extra personeel en materieel bij de Koninklijke Marechaussee. Ik denk aan het systeem en personeel bij de MIVD, het uitbreiden en onderhouden van de heimelijke wereldwijde infrastructuur, het uitvoeren van search in cyberspace for target reconnaissance and target development, het verkrijgen van duurzame toegang tot systemen, het uitvoeren van digitaal forensisch onderzoek. Er is nog een ander actieplan betreffende het operationele van de technologieafdeling van het DCC na instroom van de eerste techneuten in mei. Het hoofdkwartier van het DCC wordt op de Frederikkazerne ingericht. Ik noem ook de voorbereiding van en de deelname aan internationale oefeningen. Dat zijn er nogal wat, bijvoorbeeld van de Cyber Coalition van de NAVO, maar ook van de individuele krijgsmachtdelen. Zo kan ik nog wel even doorgaan. Er is een grote hoeveelheid acties gepland. Er zal steeds meer invulling worden gegeven aan die cyberstrategie. Als de actieplannen verder zijn opgesteld, zal ik bekijken of het zich ervoor leent om met de Kamer te delen. Ik heb op zichzelf niks achter te houden, anders dan dat ik ook ruimte wil houden voor de organisatie om voldoende flexibel te zijn bij de invulling van dit domein.

De heer **Knops** (CDA): Ik begrijp het antwoord van de Minister wel, maar hoe kun je beoordelen of je voldoende geëquipeerd bent om de dreigingen het hoofd te bieden? Je kunt misschien niet alle plannetjes smart formuleren, maar wij zouden in de kopgroep zitten. Hoe kunnen wij beoordelen of de planning van de implementatie van allerlei cyberplannen op schema ligt? Hoe kunnen wij beoordelen of Defensie in het juiste tempo op de juiste planning ligt? Hoe competitief is Defensie?

Minister **Hennis-Plasschaert**: In 2016, 2017 komt er een beleidsdoorlichting. Dat lijkt mij een goed haakje om hier verder handen en voeten aan te geven. De realiteit is dat Nederland het defensief goed doet als het gaat om het vergaren van inlichtingen. Het offensieve aspect staat nog in de kinderschoenen. Wij zijn nog bezig met het oprichten van het DCC, wij zijn nog bezig met de vulling daarvan, wij zijn nog bezig met het samenstellen van die technische kern. Vanaf 1 mei zullen hierin belangrijke stappen worden gezet. Tijdens de technische briefing heeft de Kamer een heel interessant scenario gehad. Ik vond dat heel realistisch, maar wel toekomstmuziek. De MIVD kan inbreken op netwerken. Van die expertise zullen wij gebruikmaken. Daar zullen het DCC en de MIVD van leren.

Offensief zullen wij, als het goed is, de komende jaren grote stappen voorwaarts gaan zetten. Met de beleidsdoorlichting zullen wij antwoord kunnen geven op de vragen die nu worden gesteld. Ik zal daar in de volgende update of de volgende jaarlijkse brief – ik weet niet wat wij daarover hebben afgesproken – wat meer op vooruitlopen, zodat de Kamer het beter kan gaan volgen en kan afzetten tegen de activiteiten van andere landen. Niet iedereen laat altijd het achterste van zijn tong zien in dezen, maar in de NAVO en de Europese Unie wordt Nederland erkend als een vooroplopend land.

De heer **Knops** (CDA): Dat is volgens mij de kern. De Kamer wil weten of de ter beschikking staande middelen voldoende zijn voor de plannen die de Minister nu heeft ontvouwd. Ik weet dat wij geen 100% garantie kunnen krijgen, maar ik wil wel het gevoel hebben dat het voldoende is voor datgene wat nodig is. Als het niet voldoende is, moet dat aan de Kamer gemeld worden. Er zijn allerlei interpretaties over die 9 miljoen. Kan de Minister het met dit budget doen en kunnen wij daarmee de dreiging het hoofd bieden?

Minister **Hennis-Plasschaert**: Een andere woordvoerder had het in dit verband over het absorptievermogen. Dat is een heel reëel punt. Je kunt iemand gelijk volstorten met geld, maar dan verdrinkt diegene daarin. Het absorptievermogen speelt zeker een rol. Het bedrag is niet 9 miljoen. Tot en met mei 2015 is een fors bedrag geïnvesteerd. Daarnaast zien wij een structureel totaalbedrag van 30 miljoen, waarvan 9 miljoen investering. Het is dus geen verdubbeling, maar wel een zeker bedrag. Ik ga er echt van uit dat wij in de toekomst meer geld nodig hebben. Het domein zal groeien en steeds meer aandacht vragen. Ik loop daarmee niet vooruit op noodzakelijke intensiveringen, maar dat er binnen dit domein intensiveringen zullen plaatsvinden, is wat mij betreft evident.
De heer Vuijk en ook andere woordvoerders vroegen of ik wel voldoende mensen kan krijgen. Nog steeds is het mooie van de krijgsmacht dat het een unieke organisatie is met een unieke werkomgeving. Jazeker, zo zeg ik ook tegen de heer Knops, we zijn bezig met het moderniseren van de arbeidsvoorwaarden. Daarin zit wat mij betreft ook ruimte voor loonontwikkeling. Dat heb ik ook eerder al tegen de Kamer gezegd. Ik kan hier alleen geen percentages noemen. We hebben zojuist het eerste deelakkoord gesloten en gaan nu verder met de bonden spreken, met nadruk niet alleen maar aandacht voor het zuur, maar ook voor het zoet, om het zo maar even te zeggen. Er moet een juiste balans zijn. Net als medewerkers van andere sectoren binnen de rijksoverheid hebben de militairen lang genoeg op de nullijn gestaan. Dit is wat ik in zijn algemeenheid kan aangeven.
Dan kom ik op werving specifiek voor het cyberdomein. Ik heb net al aangegeven dat je kunt spelen – alhoewel, «spelen» is misschien niet het goede woord – met een aantal zaken waarmee je de aantrekkingskracht van Defensie nog verder kunt vergroten voor professionals. Bij de werving van specialisten kijken we ook heel erg naar wat er intern beschikbaar is. Er is ontzettend veel belangstelling, ook intern, voor functies in het cyberdomein. Als organisatie zijn we erachter gekomen, en dat is heel leuk, dat heel veel mensen over onvermoede kwaliteiten beschikken. Zij geven zich op voor en doen mee aan zogenoemde «cyber challenges», online testen en cursussen die worden georganiseerd. Op dit moment doen 700 Defensiemedewerkers mee aan een cyberzelfstudieprogramma. Daarnaast heeft het Defensie Cyber Expertise Centrum een Defensiecybercommunity opgezet, waarbij voor geïnteresseerden workshops worden georganiseerd en waarbij dezen op de hoogte worden gehouden van de ontwikkelingen in het cyberdomein. De commissie weet dat we een programma hebben met een bedrijf, een cybersecurityfirma, voor het opleiden van specialisten. Zij voltooien heel binnenkort, volgende maand,

hun cyberopleiding. Op dit moment zijn we met dat bedrijf in gesprek om vanaf september daar een tweede groep te plaatsen. Ook hebben we regelmatig stagiairs van civiele opleidingen bij het DCEC, met als doel om hen echt te interesseren voor de Defensiewerkomgeving. We kunnen dus heel veel maatregelen nemen, maar dit vind ik al heel aardig.
De heer Knops had het ineens over een braindrain op dit specifieke punt. Dat herken ik dan weer niet, een uitstroom van mensen met cyberexpertise. Ik ben er echter wel op gebrand, zoals ik net al zei, om zonder een eigen wereld binnen de krijgsmacht te ontwikkelen wel een op het verder interesseren van mensen toegesneden pakket te hebben. We werken natuurlijk ook samen met andere departementen, zodat mensen bijvoorbeeld kunnen gaan switchen tussen ministeries. Dat geldt ook voor het uitwisselen van werknemers met bijvoorbeeld bedrijven, het plaatsen van burgers op militaire stoelen en het creëren van stoelen met een flexibele rang en schaal. Naar dat soort dingen wordt gekeken. Dat wordt ook verder uitgewerkt, inclusief de arbeidsmarkttoelage die we ook voor andere schaarse categorieën hanteren.
Ik kom op de ABDO-regeling. Inderdaad komt die uit 2006, zo zeg ik tegen de heer Vuijk. De regeling wordt op dit moment herzien. Actualisering en verbetering van de bescherming tegen de cyberdreiging is daarbij een van de belangrijkste aspecten. Dat past ook binnen de doelstellingen van onze cyberstrategie, waarbij we in de preventieve sfeer steeds meer aandacht schenken aan awareness van cyberdreiging en -security. Ook wordt nagedacht over een systeem waarmee de defensie-industrie tijdig wordt geïnformeerd over bijvoorbeeld aanstaande dreigingen. Verder zullen de security audits moeten worden geïntensiveerd. Het is niet anders. Kortom, ik weet dat die regeling op dit moment wordt herzien. Ik kan de commissie niet even uit mijn hoofd vertellen wanneer dat traject moet worden afgerond en of vervolgens de uitkomsten daarvan met de Kamer kunnen worden gedeeld, maar dat ga ik na. De Kamer zal hier nader over worden geïnformeerd.
Een aantal woordvoerders sprak over het onderscheid tussen civiele en militaire doelen. Ik ben daar in de brief ook op ingegaan. Zoals we het nu doen, is het niet anders dan bij conventionele oorlogvoering. Ik ben even aan het zoeken. Uiteindelijk is het altijd een militair doel: commandocentra, aanvoerlijnen en dat soort zaken. Een goede inlichtingenpositie is ook in het cyberdomein cruciaal. Ik zeg altijd: zonder inlichtingen geen inzet. Ik ga maar even terug naar het scenario dat met de commissie is gedeeld tijdens de technische briefing. Dat is echt een heel mooi voorbeeld van hoe het in de toekomst zal gaan. Je gaat niet over één nacht ijs. Er is een grote hoeveelheid afwegingen te maken. Dat geldt voor de reguliere wapeninzet maar ook voor offensieve cyberinzet.
Nu kunnen we bij cybers...

De **voorzitter**: Er is een interruptie van de heer Van Dijk. Uw eerste interruptie, mijnheer Van Dijk.

De heer **Jasper van Dijk** (SP): Nou, het hangt ervan af. Het zou namelijk kunnen dat de Minister net begon aan een zin die hier nog betrekking op heeft. Of is dat niet zo?

De **voorzitter**: U twijfelt, zo begrijp ik. Wilt u wachten of wilt u nu uw vraag stellen?

De heer **Jasper van Dijk** (SP): Ik stel de vraag.

De **voorzitter**: Gaat uw gang, mijnheer Van Dijk. U bent een snelle beslisser.

De heer **Jasper van Dijk** (SP): Dank u wel, voorzitter. De vraag is: kun je het militaire en het civiele scheiden op internet? Zou dat niet ook legitiem zijn, in navolging van het humanitaire oorlogsrecht, op grond waarvan je geen burgers wilt raken? In de fysieke wereld zou ik me daar iets bij kunnen voorstellen, maar zou je vanwege de digitale oorlogvoering, die zo in opkomst is, niet ook daar moeten bekijken of je die zaken kunt scheiden? Ik kan me heel goed voorstellen dat de Minister zegt: dat is nogal lastig, want internet is één groot geheel. Maar zou ze dat op zijn minst kunnen onderzoeken?

Minister **Hennis-Plasschaert**: Zeker. Ik denk dat het goed is dat ik daar in een volgende rapportage op terugkom. Ik weet, nogmaals, niet of we hebben afgesproken dat ik jaarlijks rapporteer over de uitvoering van de Defensie Cyber Strategie. Mocht ik dat nog niet met de commissie hebben afgesproken, dan stel ik dat bij dezen voor. Ik zal erop terugkomen in de volgende rapportage. We kunnen het scheiden. Dat kan niet in alle gevallen, maar ook daarvoor geldt, zoals ook geldt voor de reguliere inzet: iedere keer maak je de afweging wat de gevolgen van de beoogde inzet zijn en in hoeverre dat acceptabel is. Deze vragen komen steeds terug. Ik denk daarom dat het goed is dat we het cyberdomein zo veel mogelijk net zoals de andere domeinen behandelen en dat ik in de volgende rapportage over de voortgang van de Defensie Cyber Strategie daar wat meer aandacht aan besteed. Er is namelijk onderscheid te maken. Enerzijds moet je het, zoals gezegd, zo veel mogelijk behandelen als de andere domeinen. Anderzijds is het wel veel abstracter, minder tastbaar, wat het wat lastig maakt om er op dit moment zo over te spreken. Ik kom er dus op terug, maar de afweging is altijd: de gevolgen overzien en daarop de afweging baseren. Dat is ook met de commissie besproken tijdens de technische briefing.

De heer **Jasper van Dijk** (SP): Het is heel fijn dat de Minister daarop terugkomt. Misschien kan ze nog iets specifieker zeggen op welke manier en wanneer ze dat zal doen. Mijn vervolgvraag is: is de Minister ook bereid om computernetwerken onder het humanitair oorlogsrecht te definiëren als vitale infrastructuur, vergelijkbaar met dammen en nucleaire installaties?

Minister **Hennis-Plasschaert**: Ik vrees dat ik daar niet in mijn eentje over ga. Ik ga er heel even op kauwen en dan kom ik er in tweede termijn nog even op terug.

De heer **Jasper van Dijk** (SP): En wat betreft de eerste vraag: hoe gaat de Minister precies terugkomen op ...

De **voorzitter**: Mijnheer Van Dijk, u wilde nog een vraag tussendoor stellen, zo begrijp ik. Gaat uw gang. U stelt echter wel een heleboel nieuwe vragen. De Minister heeft zich voorbereid op de vragen die in eerste termijn zijn gesteld. U stelt nu een heleboel nieuwe vragen. De Minister heeft natuurlijk tijd nodig om de beantwoording van een aantal vragen voor te bereiden. Gaat u nu een nieuwe vraag stellen? De Minister heeft namelijk nog niet uw eerste vraag kunnen beantwoorden. Wat gaat u nu herhalen?

De heer **Jasper van Dijk** (SP): Nee, u doet het helemaal perfect, voorzitter. Ik wachtte nog even op het antwoord op mijn eerste vraag: wanneer kunnen we precies wat verwachten? Ik stelde die vraag omdat de Minister zei: ik kom erop terug. De Minister had het over «de volgende rapportage». Maar wat gaat de Minister dan precies doen? Gaat ze dan onderzoeken hoe die scheiding wordt gemaakt tussen humanitair en civiel? Of gaat ze toelichten hoe dat onderscheid wordt gemaakt?

De **voorzitter**: Tegen de Minister zeg ik het volgende. Deze Kamercommissie krijgt jaarlijks een brief van u over de voortgang van de Defensie Cyber Strategie.

Minister **Hennis-Plasschaert**: Fijn, dan krijgt de commissie in februari 2016 een update. Ik schrijf daarin dan een aparte paragraaf over het onderscheid tussen civiele doelen en militaire doelen. Ik heb net echter al aangegeven dat bij een reguliere inzet civiele doelen nooit een doel zijn. Het gaat altijd om militaire doelen. Die afspraken hebben we met elkaar. Die gelden ook voor het cyberdomein. In dat opzicht moeten we het cyberdomein niet anders willen behandelen dan de andere domeinen. Het is echter vrij abstract, zeker als het gaat over het cyberdomein. Daarom lijkt het me goed om daar in de volgende rapportage, de volgende actualisatie van de strategie, even apart aandacht aan te besteden, zodat daarover geen misverstand meer kan bestaan. Ik heb dat nu gedaan, maar blijkbaar was dat te beperkt. Ik zal er dan dus nog wat nader op ingaan. Ik weet niet of u de technische briefing hebt bijgewoond – dat weet ik oprecht niet – maar die schijnt ook echt heel verhelderend te zijn geweest wat dat betreft.

Mevrouw **Hachchi** (D66): Ten aanzien van dit onderwerp heb ik een vraag gesteld over de uitspraken van Minister Koenders. Ik weet niet of de Minister daar nu meteen op doorgaat. Dan kunnen we in één keer een hieraan rakend onderwerp behandelen.

De **voorzitter**: Wellicht krijgt de Minister nu even de tijd om die vraag te beantwoorden.

Minister **Hennis-Plasschaert**: Doelt mevrouw Hachchi op de uitspraak van de heer Koenders over een vrij internet?

Mevrouw **Hachchi** (D66): Nee, Minister Koenders heeft het gehad over een hackverbod op vitale onderdelen; denk bijvoorbeeld aan de infrastructuur van ziekenhuizen. Vandaar dat ik heb gevraagd of de Minister het eens is met die uitspraak. Dit gaat namelijk ook over doelen die civiel zijn, maar wel vitaal, omdat een ziekenhuis bijvoorbeeld heel kwetsbaar is. Mijn eerste vraag was dus of de Minister het eens is met Minister Koenders. Mijn tweede vraag is hoe we dit dan moeten zien. Wordt er een soort niet-aanvalsverdrag tussen landen voorgesteld? Aangezien de Minister dit thema enigszins aanraakt, vraag ik haar of zij die antwoorden ook meteen kan geven.

De **voorzitter**: Ik wil dat de Minister even de gelegenheid krijgt om te antwoorden. U herhaalt nu de vragen uit uw eerste termijn, en volgens mij was de Minister net begonnen aan een aantal te beantwoorden vragen.

Minister **Hennis-Plasschaert**: Ik heb zonet duidelijk gezegd dat het oorlogsrecht aanvallen altijd beperkt tot militaire doelen. Nu zie ik niet zo goed in hoe een ziekenhuis kan verworden tot een militair doel. Ik ben dus even zoekende naar wat mevrouw Hachchi nu van mij wil horen.

Mevrouw **Hachchi** (D66): De Minister gaf zojuist al terecht aan dat het, zodra we het over cyber en de digitale wereld hebben, abstract en lastig te begrijpen wordt. In dit geval kan echter ook het netwerk van een ziekenhuis een doel zijn om de vijand te raken. Minister Koenders zegt dat niet voor niets. Daarom heb ik die vraag ook gesteld. Hij zegt dat er een hackverbod moet komen voor vitale onderdelen van het internet, bijvoorbeeld systemen waar ziekenhuizen op aangesloten zijn. Een ziekenhuis is geen militair doel, maar in de cyberwereld is het natuurlijk

wel een heel kwetsbaar doel, waarmee je de boel behoorlijk kunt ontregelen en schade kunt toebrengen.

Minister **Hennis-Plasschaert**: Defensie handelt tijdens een gewapend conflict wel conform het oorlogsrecht. De cyberconferentie van vorige week ging natuurlijk een heel stuk verder dan alleen het gewapende conflict en wat we daarvan kunnen toepassen in het cyberdomein. Dus ja, ik ben het eens met wat de heer Koenders zegt, maar ik herhaal wat ik zonet zei. Ik zie niet hoe een ziekenhuis kan verworden tot een militair doel. Dan moeten daar wel een heleboel voorwaarden aan verbonden zijn en afwegingen in worden gemaakt. Het risico dat mevrouw Hachchi nu schetst, dat we een ziekenhuis als target op de lijst plaatsen, herken ik gewoon niet.

Mevrouw **Hachchi** (D66): Voorzitter ...

De **voorzitter**: Mevrouw Hachchi, nu gaat de discussie heen en weer. Volgens mij is dit het antwoord dat de Minister wil geven. Ik wil u wel toestaan om uw vraag nog kort toe te lichten, maar dit moet geen debat tussen u tweeën worden.

Mevrouw **Hachchi** (D66): Maar als ik het antwoord van de Minister beluister, heb ik het idee dat ze mijn vraag niet goed heeft begrepen. Ik heb niet gezegd dat onze Defensie een ziekenhuis als militair doel ziet. Een ziekenhuis is echter wel een voorbeeld van een vitale infrastructuur van kwetsbare systemen, die aangevallen kunnen worden door de vijand. De uitspraak van Minister Koenders staat natuurlijk op zich.

Minister **Hennis-Plasschaert**: Ik zei zonet al dat ik het eens ben met de heer Koenders als hij ertoe oproept om dat vooral niet te doen, en in een conflict te handelen conform het oorlogsrecht. Dat betekent dat je je verre houdt van civiele doelen, bijvoorbeeld een ziekenhuis.

De **voorzitter**: U vervolgt uw betoog.

Mevrouw **Hachchi** (D66): Voorzitter, mijn interrupties tot nu toe gingen met name om verheldering. We komen nu tot een antwoord, waarop ik een vervolgvraag heb.

De **voorzitter**: Mevrouw Hachchi, ik waardeer uw creativiteit. U krijgt nog één kans van mij, maar volgens mij blijft u nu steken. De Minister geeft waarschijnlijk hetzelfde antwoord, maar u krijgt een laatste mogelijkheid.

Mevrouw **Hachchi** (D66): Dit was een ander antwoord. De Minister geeft aan dat zij het eens is met de uitspraak van Minister Koenders. Dan is mijn vraag: moeten we dit dan zo zien dat het Nederlandse kabinet pleit voor een niet-aanvalsverdrag tussen landen op dat vlak? Ik heb daarbij de vervolgvraag gesteld hoe de Minister dit dan voor zich ziet. Je kunt dit niet afspreken met hackers of met mensen die kwaad in de zin hebben. Ik heb ook als voorbeeld de uitspraak van de rechter genoemd dat het juist belangrijk is dat je kunt hacken op systemen van ziekenhuizen, omdat je daarmee die systemen veiliger maakt. Kortom, ik kom nu tot de vraag die ik gesteld had.

Minister **Hennis-Plasschaert**: Ik denk dat deze vraag aan de verkeerde Minister wordt gesteld. Ik zit hier als Minister van Defensie. Ik heb de oproep van de Minister van Buitenlandse Zaken hier voor me. Hij zei: «... specific elements of the cyber domain to be off limits for cyber-attacks, in the same way that hospitals cannot be attacked in times of war». Hij doet een oproep, die mevrouw Hachchi nu in een context plaatst waar wij

hier vandaag vooral niet over spreken. Ik denk dat het goed is om dit te scheiden. De oproep van de heer Koenders steun ik; dat zei ik al twee keer.

De **voorzitter**: De Minister vervolgt haar betoog.

Minister **Hennis-Plasschaert**: De heer De Roon vroeg of Defensie kan terugslaan bij cyberspionage. Ja, in die zin dat we spionage kunnen verstoren en we beschikken over middelen om in te breken op andere netwerken; althans de MIVD beschikt over die middelen. Dat betekent niet per definitie dat het wenselijk is om onmiddellijk over te gaan tot een soort cyberaanval, maar we kunnen best wat.
Mevrouw Hachchi vroeg iets over de zero-days, de kwetsbaarheden. Er is op 6 maart een brief gestuurd, ik meen ook aan deze Kamer maar in ieder geval aan de Eerste Kamer, waarin wordt ingegaan op het verzamelen door de MIVD van bijvoorbeeld militair relevante dreigingsinformatie, waarmee digitale kwetsbaarheden in kaart worden gebracht. Defensieonderdelen en Defensieorderbedrijven worden dan ook geïnformeerd om deze bedrijven, organisaties en onderdelen in staat te stellen om digitale dreigingen te reduceren. We werken natuurlijk erg nauw samen met het NCSC (Nationaal Cyber Security Centrum); dat zal de Kamer niet verbazen. We proberen om vanuit de eigen expertise zo goed mogelijk bij te dragen aan het vergroten van de weerbaarheid van de hele Nederlandse samenleving in het digitale domein. Het NCSC publiceert bij geconstateerde kwetsbaarheden ook veiligheidsadviezen op zijn website. Wat is er aan de hand, wat kun je eraan doen en ga zo maar door. Op deze wijze wordt door verschillende partijen, waaronder Defensie, bijgedragen aan de bescherming van de publieke kern van het internet. Het is een feit dat je, als je kwetsbaarheden signaleert, daar zo snel mogelijk naar wilt handelen en de relevante partners daarover wilt informeren. Bij hoge uitzondering doe je dat niet. Dat heeft dan bijvoorbeeld te maken met een specifiek onderzoek dat loopt. De regel is echter dat je die kwetsbaarheden zo snel mogelijk probeert te dichten en anderen daarop wijst ten behoeve van de weerbaarheid.
Ik kom op de hacker community. Dit is inmiddels een term die ontzettend veel definities kent. Hij kan slaan op programmeurs, maar wordt daar niet meer voor gebruikt; dat is een oude definitie. Hij kan slaan op mensen die legaal security testen en onderzoeken, maar ook op mensen die illegaal inbreken in de systemen. Er zijn vele legale communities die zichzelf hacker communities noemen. Daaraan nemen overigens ook Defensiemedewerkers deel. Zij werken daarin samen en er vinden geen illegale activiteiten plaats. Dat hoeft dus niet per se. Het zijn communities waarin bijvoorbeeld wordt samengewerkt met security researchers van gerenommeerde bedrijven en universiteiten. Ik denk dat het heel goed is om met deze niet-illegale activiteiten uitvoerende hacker communities zo veel mogelijk contact te hebben en daar zo veel mogelijk van te leren.
Mevrouw Hachchi vroeg ook wat het Nederlandse cybergrondgebied is. Wat moet Defensie nu eigenlijk verdedigen? Er is natuurlijk een onderscheid tussen beschermen en verdedigen. Beschermen doen we met zijn allen; verdedigen is een primaire taak van de krijgsmacht. Deze algemene verdedigingstaak ziet zowel fysiek als digitaal op de militaire verdediging van het Koninkrijk der Nederlanden en de bondgenootschappelijke verdediging in NAVO- en EU-verband tegen gewapende aanvallen. Dat geldt voor het gehele grondgebied. In NAVO-verband kan in een dergelijk geval artikel 5 van het verdrag worden toegepast. De Kamer weet dat de discussie over het politieke besluit of er sprake is van een aanval, volop gevoerd wordt binnen de NAVO. Zoals het er nu uitziet, zullen grote incidenten nog steeds onder de zogenaamde drempelwaarde van artikel 5 blijven vallen. Die discussie is echter nog lang niet afgelopen. Die zal zich steeds verder ontwikkelen naarmate het cyberdomein zich verder ontwikkelt en wij spreken over de vraag wanneer er welke assistentie

wordt verleend aan de «allies». Ik kan niet vooruitlopen op de uitkomsten daarvan. Die gesprekken zijn gaande. Volgens mij was dat de vraag die mevrouw Hachchi stelde.
Waarom is het DCC ingedeeld bij de Koninklijke Landmacht? Daarover hebben we eerder gesproken. Cyber is een vijfde domein. Krijgsmachtdelen worden niet per definitie per domein ingedeeld, maar het is een eenheid die te klein is om een eigen krijgsmachtdeel te krijgen. Maar je weet nooit hoe het in de toekomst loopt; ik sluit niets uit. Ik verwacht dat cyber groeit. DCC is een joint eenheid met ondersteuning van alle krijgsmachtdelen. Dat betekent dat de samenwerking gewoon goed is. De landmacht faciliteert en is het huis waarin DCC schuilt, maar uiteindelijk is het van alles en iedereen, want het is joint. Dat is de reden waarom het bij de landmacht zit.
De heer Knops in het bijzonder vroeg naar de staat van de IT. Ook enkele anderen vroegen daarnaar. Windows XP wordt niet meer gebruikt als computers op het internet zijn aangesloten. Ik heb het even nagevraagd omdat ik weet dat het uitgefaseerd wordt. Die verschrikkelijke beeldvorming kunnen we dus misschien een beetje achterwege gaan laten. De Algemene Rekenkamer heeft in 2012 een onderzoek naar de informatiebeveiliging van alle departementen gedaan. De Kamer was daar toen ook bij. Defensie werd toen als voorbeeld gesteld voor andere departementen. Dat was goed nieuws, dus dat herhaal ik nog maar even. Ik doel op het rapport Informatiebeveiliging en vertrouwensfunctie. Tegelijkertijd heb ik, ondanks deze goede behaalde resultaten uit het verleden, de Kamer gerapporteerd dat de technische staat van de IT onder de maat is en dat we daarom een hoeveelheid acties en maatregelen hebben genomen. Daarmee is Defensie weer in control gekomen, maar hebben we nog wel een aantal zaken uit te voeren. Dat is slecht nieuws. Tegelijkertijd zeg ik erbij dat de impact daarvan op de digitale weerbaarheid niet groot, ja zelfs beperkt is. Dat heeft weer te maken met de wijze waarop de beveiliging is opgebouwd, namelijk in verschillende schillen. De primaire beveiligingscomponenten waren niet verouderd of onder de maat. Bij de volgende schil, de beveiliging van de reguliere netwerken en de systeembeveiliging, is wel wat vernieuwing noodzakelijk. Ik begrijp de opmerking van de heer Knops en die is ook buitengewoon relevant. In de IT-strategie hebben we niet voor niets gezegd dat de cyberstrategie een duidelijke link heeft en dat er ook apart rekening wordt gehouden met de ontwikkelingen op dit vlak. Het is echter niet zo dat door de staat van de IT die ik eerder met de Kamer heb gedeeld – overigens hebben we nu een heleboel stappen in de juiste richting genomen – de digitale weerbaarheid onder grote druk is komen te staan. Verdient het allemaal de schoonheidsprijs? Nee, want anders hadden we al die actieplannen en maatregelen niet hoeven te nemen.
Ik kom op de aanvallen van Rusland en China. In het Cybersecuritybeeld Nederland, dat vrij recentelijk is gepubliceerd, en in het MIVD-jaarverslag wordt de cyberdreiging beschreven. De grootschaligheid heeft betrekking op de frequentie, de diversiteit, de methodes die gehanteerd worden, maar ook op de complexiteit van de aanvallen op de defensienetwerken en de defensie-industrie. Meer kan ik er in het openbaar niet over zeggen, naast wat er staat in het Cybersecuritybeeld en het jaarverslag. Ik kan wel in het openbaar zeggen dat er geen aanvallen van bondgenoten zijn vastgesteld.
Mevrouw Eijsink vroeg naar de samenwerking. Dat is een terechte vraag. We spraken net al over het verschil tussen beschermen en verdedigen. Defensie kan het nooit helemaal in haar uppie doen; we zijn er allemaal verantwoordelijk voor. De interdepartementale samenwerking is goed. Er wordt op nationaal niveau zeer intensief samengewerkt met V en J, in het NCSC en met Binnenlandse Zaken. Een ander voorbeeld is het Nationaal Detectie Netwerk, waarin niet alleen met andere departementen wordt gewerkt, maar ook met een aantal bedrijven uit de vitale sector.

Mevrouw Eijsink vroeg ook naar de EU-cyberstrategie en de NAVO-cyberstrategie. De realiteit is dat de EU laat wakker is geworden op dit terrein en nu een beetje een inhaalslag aan het maken is. De NAVO is al wat langer bezig. We nemen ook actief deel aan de verschillende oefeningen en aan het Cooperative Cyber Defence Centre of Excellence. Daarover is de Kamer eerder geïnformeerd. De aard van zowel de NAVO- als de EU-strategie is defensief, dus vooral niet offensief, al sluit ik niet uit dat daarover in de toekomst wordt gesproken, zeker binnen NAVO-verband. Van belang is nu om de activiteiten op cybergebied vooral af te stemmen en niet te veel overlap te laten zien.
Mevrouw Hachchi vroeg of ik dit als onderdeel wil meenemen voor het voorzitterschap van de Europese Unie. Daar ontkom ik niet aan en daar wil ik ook niet aan ontkomen. Cyber is een belangrijk domein dat zich in een razendsnel tempo ontwikkelt. Of ik het nou leuk vind of niet – gelukkig vind ik het leuk – ik zal het moeten meenemen tijdens het EU-voorzitterschap.
Ik krijg net door dat de ABDO-regeling eind dit jaar gereed is, zeg ik tegen de heer Vuijk. Hij is ook openbaar. De bevindingen van de audits zijn niet openbaar. Ik denk dat we naar aanleiding van de publicatie van de ABDO-regeling nog nader met elkaar komen te spreken. Ik zal haar in ieder geval meenemen in de actualisatie die de Kamer volgend jaar februari krijgt toegestuurd.
Volgens mij heb ik hiermee best veel vragen beantwoord, voorzitter.

De **voorzitter**: Volgens mevrouw Hachchi is er een vraag blijven liggen.

Mevrouw **Hachchi** (D66): Ja, volgens mij wel meer, voorzitter. Op een aantal zal ik terugkomen in mijn tweede termijn. De vraag die sowieso is blijven liggen, is de vraag over de Defensie cyberdoctrine. Ook zou ik graag een duidelijke uitspraak horen over de inzet van cybercapaciteit. Als daar wijzigingen in ontstaan – ik heb aangegeven dat het net zo gaat als bij de bestaande inzet van militaire capaciteiten – wil de Kamer daar zo snel mogelijk iets van horen. Ik heb ook vragen gesteld over het verwervingstraject en de innovatieprocessen, met name over de manier waarop dit opgelost kan worden in relatie tot de Europese aanbestedingsregels. Hoe denkt de Minister dit op te lossen? Ik heb ook vragen gesteld over de internationale samenwerking met de EU en de NAVO. Welke mogelijkheden ziet de Minister om het onderwerp hoger op de agenda te krijgen, kijkend naar wat er nu voorligt bij zowel de EU als de NAVO? Het zijn met name de langetermijnzaken die we terugzien. Vandaar die opmerkingen.

Minister **Hennis-Plasschaert**: De vraag over de cyberdoctrine heb ik inderdaad over het hoofd gezien. Sorry. Daar wordt aan gewerkt. Dat heb ik vorig jaar ook gezegd. Ik verwacht dat die eind 2015 gereed is. Ik heb tijdens het vorige AO gezegd dat ik die niet publiek wil maken, omdat dat de manier beperkt waarop je de doctrine invult. Als de Kamer vindt dat het publiek moet, zal het een heel beperkte doctrine zijn. Dan zie je dat de rest wordt uitgewerkt in allerlei onderliggende documenten en handboeken, zoals je ook bij andere doctrines ziet. Ik wil die doctrine liever zo volledig mogelijk laten zijn. Vanzelfsprekend ben ik bereid om de doctrine vertrouwelijk met de Kamer te delen, zodat de Kamer er ook een toelichting op kan krijgen. Dat proces zal zich dit jaar verder voltrekken. Aangezien de technologische ontwikkelingen in zo'n razendsnel tempo gaan, is het hoe dan ook een levend document. Als de Kamer eind dit jaar zo'n doctrine gepresenteerd krijgt, moet zij niet denken dat dat het is. Het is vooral niet in beton gegoten en het zal de komende jaren nog volop de aandacht krijgen.
Welke mogelijkheden zie ik om het in de internationale samenwerking hoog op de agenda te krijgen? Het staat al hoog op de agenda. Er gaat geen top voorbij of er wordt over gesproken. Wat mij veel meer zorgen

baart, is niet dat het niet op het netvlies van de Europese Unie of de NAVO zou staan, maar of er wel voldoende wordt geïnvesteerd en gedaan in de lidstaten zelf. Dat kan niet allemaal goedgemaakt worden door de Europese instellingen of door de sg van de NAVO die daar een mening over heeft. Uiteindelijk moeten de lidstaten die kar zelf gaan trekken. Dat is een veel ingewikkelder proces, omdat we in dat soort gremia niet aan naming-and-shaming doen; daar ben ik overigens ook geen voorstander van. Je kunt je echter wel afvragen hoe je die peer pressure wat kunt verhogen om het bewustzijn overal te laten toenemen. Dat is absoluut iets waar ik tijdens het Nederlands voorzitterschap aandacht aan wil geven. De indruk mag namelijk niet ontstaan dat de NAVO of de Europese Unie het bij falen van individuele lidstaten wel even overnemen. We hebben daar allemaal last van, want cyberdreiging is per definitie onbegrensd. Ik zal dus niet aarzelen om daarop te wijzen. Ik doe dat ook al. Er zijn binnen de EU en de NAVO 28 lidstaten. Ik voel me desalniettemin gesteund door de woorden van mevrouw Hachchi in dezen.
Op het afwijken van innovatie en verwervingstrajecten kom ik in tweede termijn terug, want die vraag heb ik niet meer scherp.

De **voorzitter**: Dank u wel. Ik zie dat de leden behoefte hebben aan het houden van een tweede termijn. Iedere woordvoerder krijgt daarin twee minuten spreektijd.

De heer **Vuijk** (VVD): Voorzitter. Ik dank de Minister voor alle antwoorden en voor de openheid waarmee zij heeft geantwoord. Dit is een lastige materie. Ik wil nog een paar zaken aanroeren. Het is overigens de vraag of ze nu allemaal helemaal moeten worden uitgediept, want we zullen hierover zeker vaker spreken.
We hebben gesproken over het reservistenbeleid en wat de positie van de reservist zelf is. Wat ik nog mis, is de rol van de werkgever. Hoe zit die er precies in? Is daarover iets te zeggen, of moeten we daar een andere keer verder over spreken? Ik hoor op werkbezoeken dat in het bedrijfsleven in toenemende mate expertise wordt opgebouwd op het vlak van het beschermen van bedrijfsgegevens. Dat werkt echter twee kanten op. In hoeverre is die werkgever bereid om zijn duurbetaalde mensen af en toe voor een aantal dagen, weken of een andere periode als het ware «weg te geven» aan Defensie? Hoe zit de werkgever daar precies in? Ik kan me ook voorstellen dat we op deze vraag terugkomen tijdens een AO dat specifiek over reservisten gaat.
De Minister zegt dat er geen apart wereldje van cyberspecialisten bij Defensie komt, maar dat er wel gebruik wordt gemaakt van uitzonderingen als die mogelijk zijn. Ik hoor de Minister spreken over specifieke toelages. Volgens mij is de mogelijkheid om specifieke groepen periodiek een toelage te verstrekken, al lang staande praktijk. Volgens mij heb ik dat wel goed begrepen.
Ik begrijp ook dat de werving wel goed gaat en dat Defensie wel mensen kan werven. Defensie blijft een unieke werkgever. Mensen willen nog steeds, ook vanuit specifieke motieven, graag bij Defensie werken. Als ik de Minister goed begrijp, kan Defensie dus voldoende mensen werven.
Hoe controleert de Kamer wat er precies gebeurt op het vlak van cybersecurity bij Defensie? Dat is lastige materie. Ik merk dat onder andere als wij hierover onder elkaar spreken. Hoe krijg je hier grip op? Ik vind het zelf met name lastig dat de controlemechanismen niet goed werken omdat dit onderwerp voortdurend wisselt van aard. Op het ene moment gaat het over iets wat zich binnen de werkingssfeer van de MIVD afspeelt. Dan kom je al snel op een terrein terecht waarbij je niet in het openbaar over de onderwerpen kunt spreken. Op een ander moment gaat het over militaire capaciteit. Heeft de Minister voldoende middelen en voldoende mensen? Hoe werkt dit precies? Wat koop je precies van die middelen? Dit blijft lastig. Het gaat hierbij niet om vliegtuigen en niet om

schepen. Het gaat hierbij niet om een gepantserd voertuig. Als het schiet, knalt het niet en geeft het ook geen rook. Hoe wordt het voor de Kamer wat tastbaarder? Ik vraag mij daarom af of wij niet nieuwe controlemechanismen moeten ontwikkelen om specifiek op dit terrein van cyber onze controlerende taak goed te kunnen uitvoeren.

De heer **Knops** (CDA): Voorzitter. Ik dank de Minister voor de beantwoording van de vragen. Ik moet echter een misverstand uit de wereld helpen. Ik had het over de braindrain. Dat is iets wat heel Defensie raakt. Mijn vraag was hoe de Minister voorkomt dat juist in dit specifieke vakgebied er straks ook sprake zal zijn van een braindrain. Dat heeft natuurlijk alles te maken met de mate waarin Defensie als werkgever aantrekkelijk is. We hebben daarover ook tijdens de technische briefing – waarvoor ik de Minister overigens dank – prima vragen kunnen stellen en daarop goede antwoorden gekregen. Soms is het echter goed om bepaalde vragen nog een keer in het openbaar te stellen en daarop een politieke reactie te krijgen.
De Minister heeft vooruitgekeken en had daarvoor heel veel woorden nodig. Eerst zei ze: ik ga ervan uit dat we in de toekomst meer geld nodig hebben. Dat lijkt mij een logische conclusie. De vraag is echter of de Minister dan ook bereid is om de consequentie daarvan te verbinden aan de uitwerking van de motie-Van der Staaij. Laat ik het nog maar een keer proberen. Zolang die motie nog niet is uitgevoerd, kan dit hierin allemaal worden meegenomen.
De Minister heeft in 2014 in GOV Magazine een uitspraak gedaan. GOV Magazine is een blad dat ik niet kende. Het gaat niet over geestelijke verzorging of iets dergelijks, maar het is een tijdschrift voor de digitale overheid. In dat blad heeft de Minister in 2014 geroepen dat we in het kader van offensieve acties ook bereid zouden moeten zijn om bijvoorbeeld een kernreactor uit te schakelen met cyber warfare. Ik vond dat een nogal interessante uitspraak. Ik schrik er niet zo van, maar ik zie mevrouw Eijsink bedenkelijk kijken. U bent neutraal, voorzitter. Ik schrik er niet zo van, maar ik vraag me wel af of dat nog steeds iets is waaraan de Minister denkt in het kader van de discussie die wij hier nu voeren. Denkt zij hier nog steeds aan als zij het heeft over offensieve acties?

De **voorzitter**: Ik glimlachte, mijnheer Knops. Als u een glimlach van de voorzitter neutraal vindt, zou ik zeggen: een glimlach van de voorzitter is altijd goed.

De heer **De Roon** (PVV): Voorzitter. Ik dank de Minister voor de beantwoording in de eerste termijn. Ik ben blij met de toezegging dat de doctrine eind 2015 gereed zal zijn en wij die dan mogen verwachten. Ik ben het namelijk wel met de heer Van Dijk eens: die doctrine moet je wel kennen en kunnen begrijpen om überhaupt te kunnen beoordelen of wat we aan cyberdefensie hebben of gaan ontwikkelen, is wat we willen. Als de Minister zegt dat zij die doctrine wel vertrouwelijk met de Kamer wil delen, dan kan ik dat alleen maar toejuichen.
Ik ben het eigenlijk ook wel eens met wat de heer Vuijk in zijn tweede termijn zei over cyberdefensie als iets wat niet knalt en niet rookt. Dat gevoel heb ik ook als we spreken over de capaciteit op het vlak van cyber. Ik spreek hierbij even helemaal voor mijzelf. Eigenlijk heb ik geen goed beeld van wat onze cyberdefensie nu eigenlijk kan, van wat de cyberdefensie zou moeten kunnen en van wat dat dan zou moeten kosten. Dat beeld is er gewoon niet. Ik hoop dat wij daarvan in de toekomst samen of – hoe moet ik het zeggen – aangestuurd door de Minister een beter beeld kunnen krijgen.
Ik heb in de eerste termijn ook nog een vraag gesteld over de salarisschalen. Ik lees in de brief van de Minister dat flexibel moet worden omgegaan met de salarisschalen om personeel te kunnen aantrekken en

behouden. Ik verwees daarbij naar de Amerikanen, die hiervoor samenwerken met Hollywood en Wall Street, waar de salarissen nogal hoog zijn. Dat was een beetje een kwinkslag, maar ik heb hier wel een concrete Nederlandse vraag aan verbonden. Ik vroeg waar dan de grenzen liggen bij dat flexibel omgaan met salarisschalen. Betekent dit, dat de Minister binnen de huidige salarisschalen zal opereren? Of is het straks ook mogelijk dat zij de balkenendenorm wil overschrijden omdat zij top warriors wil krijgen en behouden? Ik zie de Minister op dit moment al nee knikken. Nou, dan is dat duidelijk voor dit moment.

De **voorzitter**: Non-verbaal wordt er vandaag veel duidelijk.

Mevrouw **Hachchi** (D66): Voorzitter. De Minister gaf aan hoe belangrijk samenwerking is bij cyberdefensie. Het is dan ook positief dat zij de hacker community omarmt, dat ze vindt dat er op dat vlak iets moet gebeuren en dat dit moet worden geïntensiveerd. Ik heb nog niet gehoord in hoeverre de universiteiten op dit vlak zijn aangesloten bij Defensie. Daar worden op dit moment veel masterprogramma's voor cyber ontwikkeld.
We hebben het over samenwerking. Ik zou er daarom voor willen pleiten om te beginnen met goede samenwerking binnen het kabinet bij cyber. Ik heb namelijk vragen gesteld over de uitspraak van Minister Koenders. Natuurlijk zegt de Minister dat zij achter zijn uitspraak staat. Het gaat mij er echter met name om hoe wij dit moeten duiden. Het zou daarbij fijn zijn als ook de Minister van Defensie ons van antwoorden op dit vlak kon voorzien. Met de reactie op de vragen die ik hierover heb gesteld, ben ik dus iets minder tevreden.
Ik ben ook teleurgesteld over de antwoorden van de Minister op de vragen over offensieve capaciteit. Ik heb daarbij gewezen op de spanning die er ontstaat tussen offensieve capaciteit en defensieve capaciteit. Ik heb hiernaar met name gevraagd omdat de Minister zelf stelt dat Defensie ook offensieve capaciteit aan het ontwikkelen is. Ik kan het dan niet plaatsen dat de Minister ook stelt dat omwille van de veiligheid kwetsbaarheden in software worden opgespoord. Zij zegt: die kwetsbaarheden gaan we niet opsparen, maar oplossen, want we willen natuurlijk defensief onze cyber en onze systemen beschermen. Dat is in conflict met het verhaal over het ontwikkelen van de offensieve capaciteit. Ik zie dat de Minister mij vragend aankijkt. Kan zij ook op dit vlak samenwerken met haar collega van Veiligheid en Justitie, en de Kamer hierover een brief sturen? Dit punt wordt namelijk ook in het rapport van de WRR aangedragen. Ik ben bereid, te helpen bij het formuleren van het verzoek, zodat de Kamer in die brief de juiste informatie krijgt. Wellicht kan dit terugkomen bij de toezeggingen.
Wat is de laatste stand van zaken bij het EU Cyber Defence Policy Framework? Ik weet niet meer of de Minister daarop concreet is ingegaan. De Minister komt nog terug op de verwervings- en innovatieprocessen. Verder ben ook ik benieuwd naar de cyberdoctrine, die de Kamer eind dit jaar zal ontvangen.

De heer **Jasper van Dijk** (SP): Voorzitter, ik kom nog even terug op de toezegging dat de Minister zal terugkomen op het punt van de mogelijke scheiding tussen civiele en militaire netwerken. Het gaat over civiele en militaire netwerken. Is het mogelijk om die twee soorten netwerken misschien zelfs fysiek te scheiden? De Minister zei dat ze daarop terug zou komen in de rapportage. Wat bedoelt ze daar precies mee? Gaat ze die vraag in die rapportage beantwoorden? Wordt dit daarin dan uitgewerkt? Ik hoor graag een toelichting.

De **voorzitter**: Mag ik u iets vragen, mijnheer Van Dijk, om te voorkomen dat er mogelijk verwarring ontstaat? De Minister heeft in de eerste termijn

uw vraag beantwoord. Zij heeft u een toezegging gedaan die ging over de scheiding tussen militaire doelen en civiel-humanitaire doelen. Ik merk dit even op, want «doelen» is mogelijk iets anders dan «netwerken». U gebruikt nu zelf het woord «netwerken». U bent hierin uiteraard zeer nauwkeurig, maar wellicht is het goed om nog even te bezien wat u nu bedoelt. Dat is ook voor mij van belang, want ik wil voorkomen dat u straks tegen mij zegt dat de toezeggingen niet goed zijn geformuleerd. Dat zou ik natuurlijk niet kunnen verantwoorden naar u.

De heer **Jasper van Dijk** (SP): Heel goed, voorzitter. U verdient echt een prijs voor uw scherpte. Ik heb in de eerste termijn gevraagd of het mogelijk is om een betere scheiding te maken tussen netwerken, waardoor militaire netwerken los kunnen bestaan van civiele netwerken. Kan dat mogelijk worden onderzocht? Het punt is natuurlijk dat het militair oorlogsrecht al oud is. Hoe gaan we om met deze problematiek van de digitale wereld? Kun je wellicht zelfs een fysieke scheiding maken tussen militaire netwerken en civiele netwerken? Ik zie dat de Minister staat te springen om hierop een antwoord te geven.
Op mijn tweede vraag zou de Minister nog terugkomen. Ik vroeg of het mogelijk is om computernetwerken als vitale infrastructuur aan te merken, waardoor zij speciale bescherming kunnen genieten. Op deze twee punten hoor ik graag een reactie.

De **voorzitter**: Ik zie dat de Minister even tijd nodig heeft om haar antwoorden in de tweede termijn voor te bereiden. Ik schors de vergadering voor twee minuten.

De vergadering wordt enkele ogenblikken geschorst.

Minister **Hennis-Plasschaert**: Voorzitter. Wij zullen elkaar nog nader spreken over het reservistenbeleid. Ik heb laatst de werkgevers award weer uitgereikt. Ik zeg nu even uit mijn hoofd dat er vorig jaar 25 werkgevers vertegenwoordigd waren en er dit jaar ongeveer 90 waren. Je ziet dit dus groeien. Het gaat allemaal niet vanzelf en we moeten er flink aan trekken, maar het reservistenbeleid krijgt wel steeds meer vorm. Het krijgt ook steeds meer zijn beslag binnen zowel het bedrijfsleven als de overheid. Het is iets van lange adem, maar het is wel aardig. We komen hierover echter nog separaat te spreken.
Er is gesproken over meer geld. De motie-Van der Staaij wordt een soort fenomeen. Ik kan zeggen dat er nog steeds geen geldboom groeit op het Binnenhof of in de achtertuin van Jeroen Dijsselbloem. Ik kan nu niet voorspellen hoeveel geld er in de toekomst voor cyber nodig is. Ik verwacht echter dat dit moet worden geïntensiveerd, maar ik ga er nog geen prijskaartjes aan hangen en er geen definitieve uitspraken over doen. Het spreekt voor zich dat we, in het kader van de motie-Van der Staaij, ook kijken naar het cyberdomein.
Mijn uitspraak over de kernreactor is aangehaald. Ik heb een kernreactor als voorbeeld gegeven als dit een militair doel zou dienen. Daarmee komen we gelijk bij wat de heer Van Dijk zegt. In de ideale wereld kun je natuurlijk een militair netwerk van een civiel netwerk onderscheiden. Je kunt het op zo'n manier opzetten dat die twee typen netwerken volledig los van elkaar kunnen draaien. De praktijk is echter totaal anders. Je zult je soms op een militair doel moeten richten via een civiel netwerk. Die scheiding is niet te maken. Daarvoor zijn de zaken veel te veel met elkaar verweven. De heer Van Dijk noemt het interconnected, maar ik vind «verweven» ook een mooi woord, en het is Nederlands. Ik snap wel dat de heer Van Dijk op die verwevenheid wijst. Ik maak echter wel een heel duidelijk onderscheid tussen civiele doelen en militaire doelen. Dat zei de voorzitter heel terecht. De vraag hoe je tot dat doel komt, is natuurlijk weer van een andere orde. Neem je de snelweg of neem je een zandweg?

Moet je een zijpad nemen? Er leiden in dat opzicht meer wegen naar Rome. De afweging voor welke weg er wordt gekozen, wordt steeds binnen de rules of engagement gemaakt, conform het scenario dat met de Kamer is gedeeld.
De heer Van Dijk vroeg ook of wij de computernetwerken kunnen aanmerken als vitale infrastructuur. Daar zegt hij nogal iets. Computernetwerken zijn er in vele vormen, soorten en maten. Wat de heer Van Dijk vraagt, is ondoenlijk. Heel Nederland zou op die manier in één keer worden aangemerkt als vitale infrastructuur. Bij de inzet van Defensie gaat het om de vraag wat een civiel doel is en wat een militair doel is. Welke afwegingen worden gemaakt? Gaat het conform het oorlogsrecht? Wat zijn de rules of engagement en wordt er binnen die rules gehandeld? Ik begrijp wel dat hierover blijvend vragen worden gesteld. Daarom is hierover nu een klein stukje opgenomen in de actualisering van de strategie. Volgend jaar februari ontvangt de Kamer een rapportage van de voortgang die is gemaakt. Ik zou dat niet weer een actualisering willen noemen. Ik stel voor dat ik hierop dan wat nader inga.
Van offensieve inzet is nu geen sprake, althans niet van de scenario's die met de Kamer zijn gedeeld. Wij houden ons aan de regels die daarvoor gelden. Mevrouw Hachchi vroeg of ik het even zou kunnen melden als ik ervan ga afwijken. Dat spreekt voor zich. De leden vragen hoe zij invulling kunnen geven aan hun controlerende taak. Heel veel wat wij hier bespreken, gaat over bedrijfsvoering. De organisatie moet ook de ruimte krijgen om dat op te zetten. Als wij echter zouden gaan afwijken van de kern waar het allemaal om draait, dan zou ik dat uiteraard met de Kamer moeten delen. Ik kan haar echter direct al zeggen dat ik niet voornemens ben om ervan af te wijken.
Onder anderen de heer De Roon wilde wat meer een beeld krijgen bij waar het om gaat. Men zei: het knalt niet, er komt geen rook uit en je ziet het niet. Het is natuurlijk ook allemaal heel abstract, maar er worden wel verscheidene oefeningen mee gedraaid. Het is altijd heel verleidelijk om te gaan kijken bij een grote oefening waar veel materieel te zien is en veel wapens worden ingezet. Dat spreekt erg tot de verbeelding. Volgens mij is het echter ook wel aardig als ik eens ga zoeken naar een oefening die voor de Kamerleden interessant zou kunnen zijn. Daarbij zouden zij dan kunnen aanhaken. Daar zouden zij kunnen zien hoe het nu precies in de praktijk werkt. Dat levert misschien het beeld op waarnaar de heer De Roon en anderen op zoek zijn. Zo'n bezoek aan een oefening geeft veel meer beeld dan het hier blijven pingpongen met woorden. Ik zal op zoek gaan en wij zullen de commissie een voorstel doen. Als de Kamer dat ziet zitten, is het uiteraard aan de leden om te bepalen of zij die uitnodiging accepteren.

De heer **Jasper van Dijk** (SP): Ik volg de Minister. Ik vind «verwevenheid» ook een mooier woord. Ik wijs dus op die verwevenheid op het internet van die doelen of zaken. Het ziekenhuis is bij wijze van spreken verbonden aan de energievoorziening. Als dan je militaire doel op het internet de energievoorziening is, maar je raakt daarmee ook het ziekenhuis, is dat een uitkomst die je niet wilt. Mijn vraag is of kan worden onderzocht in hoeverre die netwerken te scheiden zijn. Dat vraag niet alleen ik, maar dat vraagt ook het Rode Kruis. Het lijkt mij een heel legitieme vraag. Ik zeg dus niet dat het nu te scheiden is of dat het nu moet worden gescheiden, maar ik vraag of de mogelijkheden kunnen worden onderzocht.

Minister **Hennis-Plasschaert**: Dat kan. Dat zou Defensie niet in haar uppie moeten doen. Dat is echt iets waarbij je samen moet oplopen. Ik zal nagaan hoe we dat het beste kunnen aanvliegen. De heer Van Dijk stelt namelijk voor om tot een soort noodvoorziening te komen, vergelijkbaar met bijvoorbeeld een noodvoorziening als plotseling de elektriciteit uitvalt, waardoor we toch nog door kunnen draaien. Dat is waar de heer

Van Dijk volgens mij om vraagt. Ik zal daarnaar kijken en ik kom erop terug. Het is echter niet iets waarvoor Defensie verantwoordelijk is of iets wat Defensie in haar uppie moet gaan doen. Ik had het zelf over de vraag hoe je een onderscheid maakt tussen civiele doelen en militaire doelen, en hoe je het militaire doel bereikt. We kunnen echter zeker even kijken naar de zaak waar de heer Van Dijk het nu over heeft.

De heer **Jasper van Dijk** (SP): Ik wil hier even heel precies in zijn. Wanneer gaat de Minister dit voor ons na? Wanneer kunnen wij dit verwachten?

De **voorzitter**: Ik heb de toezegging uit de eerste termijn hier voor mij liggen, mijnheer Van Dijk. Als ik het goed heb, zal de Minister hierop terugkomen bij de eerstvolgende actualisering.

De heer **Jasper van Dijk** (SP): Nee, voorzitter, de Minister zei: ik ga even na wat de mogelijkheden hiervoor zijn. Gaat het daarbij om dezelfde toezegging als de toezegging waarover de voorzitter het nu heeft?

Minister **Hennis-Plasschaert**: Bij voorkeur wel, want anders worden we een soort productiebedrijf dat op aparte momenten rapporteert. Volgens mij heb je hier ook wel even tijd voor nodig. In feite vraagt de heer Van Dijk hoe je de nevenschade beperkt. Die afweging wordt altijd gemaakt, bij iedere inzet. Dat doen we nu elke dag boven Irak. We bekijken goed hoe we het doel zo clean mogelijk kunnen uitschakelen. Dat is in het cyberdomein niet anders. De heer Van Dijk stelt echter nog een vraag. Volgens mij verdient die vraag wel wat meer aandacht dan alleen maar «even snel navragen». Als ik dit kan meenemen bij de eerdere toezegging, ben ik de heer Van Dijk dankbaar.
Mevrouw Hachchi vroeg of de universiteiten zijn aangesloten. Ja, dat is het geval. Met Eindhoven, Leiden, Delft en de VU in Amsterdam zijn op dit vlak goede contacten.
Is offensief mogelijk zonder zero-days? Het antwoord op die vraag is ja. Niet alle aanvalsmethoden zijn afhankelijk van die kwetsbaarheden in de software. Zoals gezegd worden de zero-days gedeeld, tenzij dat onwenselijk wordt geacht. Ik zie dit niet-delen bij voorkeur als uitzondering, omdat je daarmee niet echt bijdraagt aan de digitale weerbaarheid. Er zijn echter omstandigheden te verzinnen waarin het buitengewoon onverstandig is om die kwetsbaarheden onmiddellijk te delen met je partners. Ik vermoed echter zomaar dat hierover het laatste woord nog niet is gezegd. Ook hierover zal het debat nog worden gevoerd.

Mevrouw **Hachchi** (D66): Ik heb in mijn tweede termijn om een brief hierover verzocht. Ik begrijp dat het hierbij niet alleen om het Ministerie van Defensie gaat, maar ook om het Ministerie van Veiligheid en Justitie. Is de Minister bereid om, met haar collega van V en J, de Kamer te informeren over offensieve capaciteit en zero-days? Het gaat mij dus om het spanningsveld tussen offensief en defensief.

Minister **Hennis-Plasschaert**: Ik wil daar best op ingaan in de rapportage die de Kamer volgend jaar krijgt. Mevrouw Hachchi doet nu echter net alsof het een het ander uitsluit. Dat is natuurlijk helemaal niet zo. Ik kom hier graag op terug als het voor mevrouw Hachchi een belangrijk aandachtspunt is. Er is vanzelfsprekend een relatie tussen offensief en defensief, maar het gaat daarbij niet om de relatie die mevrouw Hachchi hier nu neerzet.

Mevrouw **Hachchi** (D66): Ik probeer niet technisch te worden. Dat heb ik ook niet gedaan in mijn inbrengen. Ik heb begrepen dat er sprake is van het opsparen van kwetsbare software om die offensieve capaciteit

daadwerkelijk te kunnen ontwikkelen. De Minister zegt nu dat er ook vormen van capaciteit bij Defensie zijn waarbij dit niet nodig is. Ik heb echter begrepen, ook uit de stukken, uit het rapport van de WRR en van de mensen die ik vorige week heb gesproken, dat er sprake is van dit opsparen van kwetsbare software om die offensieve capaciteit te kunnen ontwikkelen en te kunnen gebruiken. Dat is een dilemma en levert spanning op, omdat je met defensieve capaciteit het internet juist meteen veiliger wilt maken. Dat pleit ervoor om zulke kwetsbaarheden juist direct op te lossen. Ik zeg nogmaals dat ik volgens mij de Minister een handreiking doe als ik haar vraag om hierop samen met haar collega van V en J terug te komen. Wil zij op die manier de Kamer hierover informeren? In het WRR-rapport staat ook letterlijk dat er een bloeiende handel bestaat in kwetsbaarheden. Je zult dus ook in internationaal verband iets moeten doen om dit tegen te gaan. Ik wil graag dat de bewindslieden ook op dat vraagstuk ingaan in die brief.

Minister **Hennis-Plasschaert**: Ik ben even zoekende. Waarom moet ik nu een aparte brief met mijn collega van V en J naar de Kamer sturen? Er is een relatie, maar er is niet de relatie die mevrouw Hachchi nu neerzet. Het is aan de Kamer, te bepalen welke punten zij terug wil zien in de volgende rapportages. Ik neem het punt dat mevrouw Hachchi nu aanroert gewoon uitgebreid mee in die rapportages. Nu wordt echter het beeld geschetst dat alle kwetsbaarheden worden opgespaard ten behoeve van de ontwikkeling door Defensie van offensieve capaciteit. Dat beeld herken ik niet. Het ontwikkelen van offensieve capaciteit is ook geen verantwoordelijkheid van V en J. Laten we dit dus bij Defensie houden en meenemen in de rapportage. Daarmee doe ik de toezegging volledig gestand, maar dan in de vorm van een rapportage. Op die manier kunnen we de zaken ook een beetje bundelen en kunnen we het overzicht behouden.

De **voorzitter**: Op welke toezegging doelt de Minister precies?

Minister **Hennis-Plasschaert**: Dat ik de ontwikkeling van capaciteit in relatie tot de zero-days, dus in de woorden van mevrouw Hachchi gaat het over het opsparen van de kwetsbaarheden. Ja?

De **voorzitter**: Ik dank de Minister. Deze toezegging is dus meteen herhaald en ga ik niet meer herhalen. Hiermee zijn we gekomen aan het einde van de tweede termijn van de Minister.

Minister **Hennis-Plasschaert**: Nee, voorzitter, ik heb nog een puntje.

De **voorzitter**: Excuses.

Minister **Hennis-Plasschaert**: Nu wil ik ook álle vragen beantwoorden, voorzitter. Het laatste punt gaat over innoveren, verwerven en de kortere doorlooptijden. Ik kan natuurlijk niet de Europese aanbestedingsregels overboord zetten. Ook al zou je dat af en toe graag willen; zo werkt het niet. Die aanbestedingsregels moet je volgen vanaf bepaalde bedragen. Ik heb de bedragen nu even niet paraat waarbij je kunt spreken over bijvoorbeeld een directe aanbesteding en de bedragen waarbij je de regels voor Europese aanbesteding moet volgen. We kunnen dit dus niet overboord zetten. We zullen echter wel altijd kijken naar wat mogelijk is om het sneller te doen. Dat hebben we bijvoorbeeld gedaan in de Defensie Industrie Strategie. De realiteit is dat we te maken hebben met buitengewoon lange verwervingstrajecten bij de DMO. Dat willen we versnellen. We doen dat door een aantal taken voor verwerven en innovatie te beleggen op een lager niveau in de organisatie, bijvoorbeeld bij het JIVC, het DCC en de MIVD zelf. Daardoor kun je een en ander bespoedigen. Je kunt dus heel veel doen binnen de organisatie, maar je

kunt uiteindelijk de standaardregels niet zomaar overboord zetten. Ook daarover hoop ik de Kamer nader te rapporteren als we weer wat voortgang hebben geboekt.

De **voorzitter**: Ik dank de Minister voor haar beantwoording in de tweede termijn.
Er zijn tijdens dit overleg drie toezeggingen gedaan, maar op de eerste toezegging, over de ABDO-regeling, heeft de Minister al tijdens de eerste termijn gereageerd door een antwoord te geven. Ik zie op dit moment dat de heer Vuijk dat met mij eens is.
De tweede toezegging is de volgende.

– In de volgende actualisering van de Defensie Cyber Strategie geeft de Minister een uitwerking van de scheiding tussen militaire en civiel-humanitaire doelen/netwerken.

Ik zie aan de heer Van Dijk dat hij het eens is met deze formulering.
De derde toezegging is zojuist door de Minister herhaald. Die gaat over de relatie tussen zero-days, capaciteit en ontwikkeling.
Ik dank de Minister en haar medewerkers. Ik zie dat de Minister verzoekt om nog wat spreektijd.

Minister **Hennis-Plasschaert**: U had het over de volgende actualisering, voorzitter. Dat snap ik, maar het gaat misschien wat ver om ieder jaar de strategie te actualiseren. Het is meer een rapportage, als u dat goed vindt.

De **voorzitter**: Ik kijk hiervoor naar de leden. Volgens mij kunnen we elkaar zeker vinden in de formulering dat de jaarrapportage jaarlijks zal worden geactualiseerd. Zullen we het daarop houden?

Minister **Hennis-Plasschaert**: Fantastisch, voorzitter.

De **voorzitter**: Ik dank de Minister, haar medewerkers, de mensen op de publieke tribune en de mensen die elders het debat hebben gevolgd. Ik dank de leden voor hun bijdrage.

Sluiting 18.28 uur.