Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

33 321 Defensie Cyber Strategie

Nr. 4

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 21 mei 2014

De vaste commissie voor Defensie, de vaste commissie voor Buitenlandse Zaken, de vaste commissie voor Binnenlandse Zaken en de vaste commissie voor Veiligheid en Justitie hebben op 26 maart 2014 overleg gevoerd met Minister Hennis-Plasschaert van Defensie over:

- **de brief van de Minister van Defensie d.d. 26 augustus 2012 inzake de stand van zaken Defensie Cyber Strategie (Kamerstuk 33 321, nr. 2);**
- **de brief van de Minister van Defensie d.d. 17 maart 2014 houdende informatie over de ontwikkeling van offensieve cybercapaciteiten van Defensie (Kamerstuk 33 321, nr. 3);**
- **de brief van de Minister van Defensie d.d. 27 juni 2013 inzake de defensiestrategie voor het opereren in het digitale domein (Kamerstuk 33 321, nr. 1);**
- **de brief van de Minister van Buitenlandse Zaken d.d. 6 april 2012 houdende de kabinetsreactie inzake het gezamenlijk advies van de Adviesraad Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke vraagstukken (CAVV) over digitale oorlogvoering (Kamerstuk 33 000 X, nr. 79);**
- **de brief van de Minister van Defensie d.d. 7 februari 2012 inzake het advies van de Adviesraad Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV) over digitale oorlogvoering (Kamerstuk 33 000 X, nr. 68);**
- **de brief van de Minister van Defensie d.d. 17 juni 2012 houdende de lijst van vragen en antwoorden over het gezamenlijk advies van de Adviesraad Internationale Vraagstukken en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken over digitale oorlogvoering (Kamerstuk 33 000 X, nr. 99);**
- **de brief van de Minister van Defensie d.d. 24 februari 2014 houdende een reactie op het artikel «Ook cyberaanval telt voor de NAVO straks als militaire aanval» in dagblad Trouw van 20 februari jl. (Kamerstuk 28 676, nr. 196).**

kst-33321-4
ISSN 0921 - 7371
's-Gravenhage 2014

Van dit overleg brengen de commissies bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de vaste commissie voor Defensie,
Ten Broeke

De voorzitter van de vaste commissie voor Buitenlandse Zaken,
Eijsink

De voorzitter van de vaste commissie voor Binnenlandse Zaken,
Berndsen-Jansen

De voorzitter van de vaste commissie voor Veiligheid en Justitie,
Jadnanansing

De griffier van de vaste commissie voor Defensie,
Van Leiden

Voorzitter: Maij
Griffier: Van Leiden

Aanwezig zijn zes leden der Kamer, te weten: Jasper van Dijk, Eijsink, Knops, Maij, Sjoerdsma, Vuijk,

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

Aanvang 14.00 uur.

De **voorzitter**: Ik heet de mensen op de publieke tribune, de mensen die meekijken via internet, de Minister en haar ondersteuning, de collega-Kamerleden en de ondersteuning van de Kamer van harte welkom bij dit algemeen overleg. Wij voeren dit overleg met de Minister van Defensie. De Minister van Buitenlandse Zaken zou er ook bij zijn, maar die is geëxcuseerd. De spreektijd in eerste termijn bedraagt vijf minuten, met twee interrupties per fractie.

De heer **Jasper van Dijk** (SP): Voorzitter. Wij spreken over digitale oorlogvoering. Ik stel vast dat Defensie haast heeft met de ontwikkeling van de cyberstrategie voor digitale oorlogvoering. Plannen worden vervroegd uitgevoerd. Het Defensie Cyber Commando (DCC) zal al dit jaar deels operationeel zijn. Steeds meer organisaties van buiten Defensie worden bij de opbouw van dit apparaat betrokken, zoals kenniscentra, het bedrijfsleven en allerlei consultants. In brieven van de Minister is sprake van een ambitieuze aanpak. De SP ziet uiteraard dat oorlogvoering moderniseert. Wij hebben zelf in onze ICT-nota gepleit voor digitale middelen voor Defensie. Dat neemt niet weg dat de regels duidelijk moet zijn. Maximale transparantie en parlementaire controle vergroten het draagvlak en verkleinen de argwaan. Deelt de Minister die mening?
Digitale oorlogvoering roept nieuwe vragen op. Die worden uitstekend geadresseerd in een artikel in Vrij Nederland deze week, genaamd Het Nederlandse cyberleger. Daar wordt bijvoorbeeld de heer Albert Benschop in aangehaald, schrijver van het boet Cyberoorlog. Een citaat: «Het belangrijkste aan de Nederlandse cyberstrategie ontbreekt nog: we weten niets over de aard van de offensieve wapens en de precieze voorwaarden waaronder die gebruikt mogen worden. Daar zijn absoluut nog geen geen uitgewerkte richtlijnen voor.» Hoe gaat de Minister hiermee om? Zij wijs naar het oorlogsrecht en naar de zogenaamde «Tallinn Manual». Dat is echter nog geen vertaling naar praktische gevechtsregels. Wij hebben nog altijd geen doctrine ontvangen, terwijl de ontwikkelingen voortgaan. Defensie werkt aan inzetscenario's, maar houdt die voor zichzelf, lezen wij in Vrij Nederland. Waarom kan de Kamer hier niet over beschikken? Waarom deze geheimzinnigheid? Het staat in het artikel, dat vandaag is verschenen. De Minister kan het van mij krijgen.
De juriste Boukje Pieters van het Rode Kruis waarschuwt ervoor dat het onderscheid tussen militaire en civiele doelen bij het gebruik van cyberwapens vervaagt. Je legt bijvoorbeeld digitaal een energievoorziening plat. Wat heeft dat voor gevolgen voor een ziekenhuis? Daarvoor moeten richtlijnen komen, lijkt mij.
Ik kom nu op de taakverdeling. Veel gebeurt vanuit geheime diensten en dan is het al snel schimmigheid troef. Denk aan de Stuxnet-aanval. De Kamer weet niet goed waar Defensie mee bezig is. Welke cyberwapens worden ontwikkeld met welke richtlijnen? De dubbelrol van cybermilitairen wordt ook genoemd in het artikel. Enerzijds verzamelen zij inlichtingen en anderzijds kunnen zij ook aanvallen uitvoeren. Hoe gaat de Minister daarmee om? Er is ook zorg over de intensieve samenwerking tussen Defensie en het bedrijfsleven. Bedrijven hebben er belang bij om de markt te vergroten, bijvoorbeeld door de vermeende gevaren van

digitale oorlogen aan te dikken. Wij houden de risico-inschatting liever in eigen hand. Ziet de Minister dit risico ook? Welke stappen zet zij om deze botsende belangen uit elkaar te houden? Ik ontvang graag een reactie op het artikel uit de Vrij Nederland. Dat mag ook schriftelijk.
Ik ga nog specifiek in op de versterkte rol van de geheime diensten. Digitale oorlogvoering maakt het bijna onvermijdelijk dat er een grotere vermenging plaatsvindt van civiele en militaire instituties. Die vermenging wordt ook beschreven in de Nationale Cyber Security Strategie (NCSS). Een praktische casus is de nauwe samenwerking tussen de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Ook de commissie-Dessens houdt een sterk pleidooi voor uitbreiding van de bevoegdheden van de diensten om kabelverkeer te kunnen afluisteren. Die activiteiten zullen zich grotendeels in het geheim voltrekken. Het is niet ondenkbaar dat de diensten met hun nieuwe samenwerkingsverbanden een zeer ruime interpretatie van hun bevoegdheden gaan hanteren. Dat is ook het geval gebleken bij de National Security Agency (NSA), zoals wij van Edward Snowden hebben kunnen leren. Is de Minister het ermee eens dat de uitbreiding van de bevoegdheden van de diensten vergezeld moet gaan met uitbreiding van de parlementaire controle?
Een ander gevaar betreft volkenrechtelijke implicaties van digitale oorlogvoering. De Commissie van advies inzake volkenrechtelijke vraagstukken (CAVV) van de Adviesraad Internationale Vraagstukken (AIV) stelt in haar rapport dat het onwaarschijnlijk is dat een toekomstige oorlog uitsluitend in het digitale domein wordt uitgevochten. Ook artikel 5 van het NAVO-verdrag is van toepassing op het digitale domein. Een cyber-Pearl Harbor is niet direct aan de orde, maar het is waarschijnlijk dat digitale aanvallen een rol spelen bij het initiëren van een conventionele oorlog. Een digitale aanval met eenzelfde soort gevolgen als een conventionele aanval, zoals grote aantallen slachtoffers, kan volgens de schrijvers van het rapport worden beschouwd als een daad van agressie die onder het VN-Handvest een tegenaanval rechtvaardigt. Is de Minister het eens met deze omschrijving?
In haar reactie op het rapport onderschrijft de regering in dit verband het probleem van de attributie. Het lijkt ons dat in de schimmige digitale wereld het opsporen van de dader van een aanval problemen kan veroorzaken. De daders van de aanval met Stuxnet op de Iraanse nucleaire installaties werden alleen bekend doordat een groot aantal andere landen werd getroffen door hetzelfde virus. Een geval van digitale collateral damage. Het kabinet wil in dit verband ook de mogelijkheid hebben om niet-statelijke actoren als vijand te beschouwen. Wat zijn hiervan de implicaties? Houdt dit in dat een land kan worden aangevallen op grond van de aanwezigheid van zulke groeperingen op zijn grondgebied? Ik hoor graag een verduidelijking.

De heer **Knops** (CDA): De heer Van Dijk heeft veel vragen gesteld aan de Minister over gevolgen, implicaties, enzovoorts. Hoe staat de SP zelf tegenover het opgaan van het pad dat cyberoorlog heet en het je daartegen wapenen?

De heer **Jasper van Dijk** (SP): Zoals ik al zei, hebben wij een ICT-nota geschreven. Daarin stellen wij dat ook Nederland vanzelfsprekend moet meegaan in die ontwikkeling. Je bent natuurlijk een gekke henkie als je zegt dat je je op digitaal gebied niet gaat ontwikkelen. Dus ik ben het ermee eens. Ik ga daarin mee. Ik heb echter wel een heel aantal vragen gesteld over hoe het met de parlementaire controle en de transparantie zit. Digitale oorlogvoering roept nieuwe vragen op en daar moet de Minister helderheid over verschaffen.

Mevrouw **Eijsink** (PvdA): Ik ben ontzettend nieuwsgierig naar de ICT-nota van de SP. Ik weet niet of die online te vinden is. Ik zou hem graag eens lezen. Ik weet niet of die onder de term «digitale oorlogvoering» of onder een andere term staat. Ik ben heel nieuwsgierig – het is niet eens een politieke vraag – hoe de SP staat ten opzichte van het digitale domein. Daar zijn prachtige definities van. Het gaat veel verder dan de twee kabels waar wij vanochtend over spraken in het overleg over sourcing bij Defensie. Het heeft ook alles te maken met Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv) en de bevoegdheden daarin. Ik ben heel nieuwsgierig of in die ICT-nota van de SP ook een verdere doorkijk staat. Digitale oorlogvoering en de offensieve cybercapaciteit, de onderwerpen waarover wij vandaag spreken naar aanleiding van de brief van de Minister van 13 maart, hebben daar immers alles mee te maken.

De heer **Jasper van Dijk** (SP): De ICT-nota van de SP is uitsluitend op papier verkrijgbaar. Nee, dat is een grapje. Hij staat uiteraard ook op internet. De nota is van augustus 2012 en is van mijn collega Gesthuizen. Ik moet eerlijk zeggen dat de zij niet heel diep is ingegaan op de problematiek zoals die de laatste tijd naar boven is gekomen, in verband met Snowden, de NSA, et cetera. Er wordt niet ingegaan op die specifieke problematiek die mevrouw Eijsink, overigens terecht, aanhaalt rond de Wet op de inlichtingen- en veiligheidsdiensten. De Minister rept daar ook over. Alle vragen die ik heb gesteld rond transparantie en parlementaire controle moeten ook in dat verband worden gezien. Daar zou je dus ook de wet op moeten aanpassen.

Mevrouw **Eijsink** (PvdA): Ik begrijp heel goed wat de heer Van Dijk zegt. Het AIV-rapport van december 2011 rept hier echter al over. Daarin wordt in feite aangegeven dat we daarnaar zouden moeten kijken als het over het grenzeloze van cyber gaat. Begrijp ik goed dat de SP ook van mening is dat wij ook goed moeten kijken naar wat de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) hierover zegt? Het is natuurlijk niet de eerste keer dat wij in deze commissie spreken over de mogelijkheden van digitale oorlogvoering, offensief, en cybercapaciteiten. Dat hebben wij voorheen ook al gedaan, naar aanleiding van SIGINT (Signals Intelligence) en alle rapporten van de MIVD en het CTIVD hierover.

De heer **Jasper van Dijk** (SP): Wij zijn daar als fractie buitengewoon voorzichtig mee. Dat mag duidelijk zijn. Ook mijn collega's hebben zich daar vaak over uitgelaten. Ik heb mijn inbreng nieuwe vragen opgeworpen die met dit onderwerp aan de orde zijn. Wij zijn terughoudend en parlementaire controle staat voorop.

De heer **Knops** (CDA): Voorzitter. Waar in vroeger dagen vooral het getal telde – hoeveel soldaten, hoeveel tanks, hoeveel vliegtuigen – om aan te geven wie er oppermachtig was, is dat anno 2014 heel anders. Om als land dat aangevallen wordt proportioneel te kunnen reageren, is het noodzakelijk om te weten wie de agressor is – dat is het attributievraagstuk waar de heer Van Dijk over sprak – over welke middelen hij beschikt en wat effectieve en proportionele tegenmaatregelen zijn. Zolang je dat niet weet, is het als boksen in dichte mist: het is weinig effectief en de kans dat je onnodig klappen oploopt, is levensgroot. De effectiefste aanval is anno 2014 een aanval waarbij weinig of geen doden vallen en waarbij de aanvaller onbekend of onzichtbaar is, waardoor het vraagstuk van legitimiteit van en draagvlak voor een tegenaanval wegvalt of onduidelijk is. Als er ook nog enige tijd overheen gaat voordat uiteindelijk wel duidelijk wordt wie de aanvaller of de bron is, een statelijke actor of een niet-statelijke actor, worden eventuele represailles minder effectief en is er ook minder draagvlak voor. Een recent voorbeeld is Oekraïne. Daar

hebben de Russen met paramilitairen van onduidelijke afkomst en heel kleine cyberaanvallen de Krim ingenomen. Dat is een voorbeeld van nieuwe oorlogsvoering: precies, met weinig collateral damage, maar heel effectief.
De ambtsvoorganger van de Minister heeft in 2012 als reactie op de motie van mij en een aantal collega's uit 2009 cyber echt als speerpunt van beleid genoemd en er extra middelen voor vrijgemaakt. Dat was eigenlijk de eerste keer dat echt effectief het belang van cyber in Nederland werd onderkend. Het was natuurlijk internationaal al langere tijd een vraagstuk, maar het werd nog niet vertaald in concrete actie. Zelf ben ik in 2008, ik meen met mevrouw Eijsink, in Tallinn geweest. Daar is toen het NATO Cooperative Cyber Defence Centre of Excellence opgericht – dat waren toen niet meer dan een paar barakken met wat pc's – als reactie op die cyberaanval van Rusland, die naderhand iets anders bleek te zijn.
Inmiddels was ook de film Die Hard 4.0 uitgekomen, die een scenario schetst van een cyberterrorist die de hele Verenigde Staten platlegt. Dat zorgde ervoor dat iedereen bepaalde beelden had van effectiviteit en van wat er zou kunnen kunnen gebeuren. Ik denk dat ook politiek, Kamerbreed, het belang van cyber is onderkend. De regering is ook aangemoedigd om met acties te komen. Wij spraken vanmorgen over ambities die wat achterlopen in de tijd. Hier hebben wij het over wat zaken die vooruitlopen. Ik ben blij dat de Minister dit ook zo oppakt en de organisatie daarvoor opbouwt.
Ik ben blij met het rapport van de AIV en met het rondetafelgesprek dat wij mochten hebben. Daarin kwam heel scherp naar voren waar de dilemma's, de problemen en de uitdagingen liggen. Het maken van plannen van aanpak en het opbouwen van de organisatie is slechts een eerste stap op een lange weg van het ontwikkelen van cyber en het denken over hoe je met de uitdagingen ervan omgaat. Alles wat je doet rondom cyber, zo is mij inmiddels duidelijk, leidt weer tot tegenreacties, die op hun beurt weer tot tegenreacties leiden. Het is dus niet statisch, maar continu in ontwikkeling. De snelheid waarmee het zich ontwikkelt, is enorm.
De ambitie van Nederland is om voorop te lopen. Wij kregen vorige week het mooie bericht dat er weer een cyberdienst naar Den Haag komt. Dat past daar heel mooi in. Wij willen die kennis borgen. De vraag is hoe de Minister die kennisopbouw borgt. Hoe zorgt zij ervoor dat met het bescheiden budget die positie kan worden waargemaakt? Hoe ziet zij het vraagstuk rond het delen van kennis? Uit het rondetafelgesprek kwam onder andere naar voren dat kennis delen op beperkte schaal kan. Hetzelfde geldt voor de inlichtingendiensten. Als je de kennis met te veel mensen deelt, erodeert die wellicht en kan een bedreiging ontstaan. Je wilt kennis voor jezelf houden, maar wel delen binnen de NAVO. Hoe gaat dat nu in de praktijk? Hoe verhoudt zich dat tot het vraagstuk van de inlichtingendiensten? Dat lijkt mij heel ingewikkeld, zeker voor een land als Nederland. Wij zijn een bescheiden land met bescheiden budgetten en kunnen niet alles zelf. Uiteraard gaat het dan ook over de samenwerking met het bedrijfsleven, waar wij een aantal heel mooie voorbeelden van hebben gezien en waar ook de Minister in haar nota aandacht aan schenkt.
Als je je wilt verdiepen in verdedigingstactieken, manieren om jezelf te wapenen tegen aanvallen van buitenaf van wie dan ook, is het belangrijk om zelf een tactiek te ontwikkelen die je kunt inzetten als een soort tegenmaatregel. Offensieve capaciteit dus. Wij zijn er erg voor dat de regering kiest voor beide componenten, defensief en offensief. Ik heb inmiddels de overtuiging, ook op basis van de gesprekken, dat als je je verdiept in de offensieve capaciteiten en die voor jezelf ontwikkelt, je die ook kunt gebruiken om je te wapenen tegen aanvallen van buitenaf.
Enige weken geleden was ik samen met collega Eijsink ...

Mevrouw **Eijsink** (PvdA): We zijn wel veel weg.

De heer **Knops** (CDA): Ja. Dat doen wij na dit debat. Dat is niet voor de openbaarheid.

De **voorzitter**: Niet al te uitgebreid meer, mijnheer Knops.

De heer **Knops** (CDA): Ik was dus op pad met collega Eijsink. Wij spraken met Peter Singer, een bekend deskundige op het gebied van cyber. Hij werkt voor Brookings Institution. Hij zei iets over de manier waarop de Verenigde Staten het probleem van cyber aanpakken. Zij doen het op een militaire manier: je richt een commando op en daarmee denk je – ik zeg het een beetje wat zwart-wit en kort door de bocht – dat je je gewapend hebt. Dat is volgens hem niet effectief. De vraag is wat wij leren van de Amerikaanse aanpak. Doen wij het op een zodanige manier dat wij niet de fouten maken die de Amerikanen in de ogen van Singer wel hebben gemaakt?
De heer Van Dijk heeft al iets gezegd over inlichtingen. Schat de Minister in dat de uitbreiding van de bevoegdheden noodzakelijk is en, zo ja, op welke wijze wordt dat geborgd? Ik heb daar wel een idee over, maar ik ben benieuwd naar de opvatting van de Minister. Het vraagstuk van de internationale rechtsorde is ook door de heer Van Dijk aangehaald. Daar kan ik mij kortheidshalve bij aansluiten. Een andere vraag is wanneer die doctrine nu beschikbaar komt voor de Kamer. Op welk niveau wordt de Kamer daarover geïnformeerd? Ik kan mij namelijk voorstellen dat daar ook zaken in staan die niet voor de openbaarheid zijn.

De heer **Vuijk** (VVD): Voorzitter. Wij spreken over digitale oorlogvoering. Onze maatschappij is afhankelijk van digitale diensten. Incidenten zoals die met DigiNotar tonen aan dat vanuit het buitenland aanvallen op onze infrastructuren worden uitgevoerd. Dat zijn incidenten met ontwrichtende effecten als gevolg. In de hoorzittingen kwamen onder andere de stroomvoorziening en het waterbeheer aan de orde. Dat zijn toch zaken waarmee wij in ons land bijzondere risico's lopen. Ik heb in de stukken gelezen dat wij door offensieve kwaliteit te ontwikkelen ook leren om ons te verdedigen. De Minister noemt cyber in haar nota In het belang van Nederland een nichecapaciteit. Dat juicht de VVD zeer toe.
Ook voor liberalen ligt de zwaardmacht bij de overheid. Daar hebben wij het hier over, over de cyberzwaardmacht in dit geval. Het zorgen voor veiligheid is een kerntaak van de overheid. Een individu kan dit niet alleen, ook bij cyber niet. Deze redenering rechtvaardigt het ook dat belastinggeld wordt uitgegeven voor digitale oorlogsvoering. Het roept echter wel een principiële vraag op. Kan de Minister nog eens toelichten hoe met name de zwaardmacht, het geweldsmonopolie, zich verhoudt tot cyberwapens en de inzet daarvan? Wat is het geweldsaspect bij cyberwapens?
Ik wil hier nog een opmerking bij maken, wellicht om het wat toe te lichten. Wat ik zelf wat ingewikkeld vind, ook bij de hoorzittingen, is dat wij spreken over cybercrime, cyberinlichtingen en cyberwarfare. Voor zover ik het nu snap, gaat het bij cybercrime om strafrecht en strafprocesrecht. Een verdachte moet eventueel worden vervolgd als er een incident plaatsvindt. Bij cyberinlichtingen, waarbij het gaat om spionage en verstoren, spreken wij over privacy van mensen en bij cyberwarfare spelen staatsnoodrecht, zelfverdediging en een internationaal mandaat een rol. Als je het op die manier strak uit elkaar trekt, spreken wij hier over digitale oorlogvoering. Daarbij speelt in mijn opvatting privacy als zodanig niet echt een rol. Ik ben erg nieuwsgiering naar de opvatting van de Minister hierover.
De VVD herkent de dreiging van die uitgaat van cyber en stemt in met het versneld oprichten van het Defensie Cyber Commando. Kan de Minister vertellen wanneer het DCC nu precies operationeel is? Welke capaciteiten

zijn dan inzetbaar en wat krijgt de Kamer daarvan te zien? De Minister heeft ook kunnen zien dat bij werkbezoeken de Kamerleden in groten getale komen opdagen. Wij zijn buitengewoon geïnteresseerd in wat daar gebeurt. Voor het vullen van het Defensie Cyber Commando zoekt de Minister IT-specialisten, die dan militair worden. Kan zij aangeven hoe de werving verloopt? Hoe groot is de belangstelling en in hoeverre speelt concurrentie met het bedrijfsleven een rol? Op wat voor manier leidt dat nog tot problemen? Volgens mij vissen namelijk bedrijven en de overheid in dezelfde vijver.
Ik heb begrepen dat de militaire doctrine in 2015 beschikbaar komt. Dat roept bij ons, zeker naar aanleiding van de werkbezoeken, de vraag op hoe zo'n cyberaanval eruit ziet. Wat zien wij daarvan, als buitenstaanders? Wat wij op de werkbezoeken zien, is dat die zich vooral afspelen in het cyberdomein en dus voor het grootste deel onzichtbaar zijn. Het gaat echter met name om zaken waarvan de ontwrichtende effecten wel zichtbaar worden in de maatschappij. Hoe ziet dat beeld er nu uit? In hoeverre kunnen onze troepen, bijvoorbeeld voor de kust van Somalië en zo meteen in Mali, voor militaire operaties al gebruikmaken van de nu beschikbare capaciteit?
De Minister schrijft dat voor offensieve cyberoperaties en digitale inlichtingenvergaring veelal vergelijkbare technieken en methoden worden gebruikt, zij het met een ander oogmerk en binnen een ander wettelijk kader. Ik heb daar in het begin van mijn betoog al een paar opmerkingen over gemaakt. Betekent deze constatering dat de parlementaire controle op de inzet van cyberwapens via de CTIVD zou moeten gaan verlopen? Volgens mij sluit dit aan bij vragen van de heer Knops en de heer Van Dijk.
De grens tussen cybercriminaliteit en cyberwarfare lijkt niet scherp. Hoe trekt de Minister de lijn waar het gaat om militaire zelfverdediging? Waar ligt de grens? Onder welke omstandigheden gaat bestrijding van criminaliteit onder leiding van het Openbaar Ministerie via de tussenstap van nationale bijstand over in verdediging van onze belangen onder leiding van de Commandant der Strijdkrachten? Hoe gaat het over van civiel naar zuiver militair? Wij hebben daar veel over gesproken. Ik heb zelf dat beeld nog steeds niet helemaal scherp.
In de hoorzitting bleek dat Defensie voor bijzondere werkzaamheden soms leunt op het bedrijfsleven. Het bedrijfsleven ziet lacunes in de regelgeving en acht zich kwetsbaar. Kan de Minister aangeven of en, zo ja, hoe zij de positie van het bedrijfsleven gaat versterken? Is het nodig en, zo ja, is er een beeld van de wijze waarop dat zou moeten?
De concentratie van de cyberactiviteiten van de NAVO zie ik als een bevestiging dat de ambities van de Minister op het gebied van cyber en internationale samenwerking goed verlopen. Ik ben nog wel nieuwsgierig of zij iets van een doorkijk kan geven in hoe deze ontwikkeling verder uitgebouwd zou kunnen worden.

Mevrouw **Eijsink** (PvdA): Voorzitter. Terwijl afgelopen week veel mensen werkzaam waren om ervoor te zorgen dat de Nuclear Security Summit (NSS) goed zou verlopen, kregen wij ook het bericht dat de cyberafdeling van de NAVO naar Den Haag komt. Of het met elkaar te maken heeft, weet ik niet. Het was echter een mooi en goed bericht, ook voor Den Haag als internationale stad voor vrede en veiligheid.
Wij hebben een werkbezoek gehad met betrekking tot digitale oorlogsvoering op 10 maart. Kolonel Folmer was daar onder andere bij. Ik vond het een uitstekend werkbezoek. Als ik er al confuus naartoe ging als het ging over definities, dan kwam ik er nog confuser vandaan. Ik heb op die dag in elk geval geleerd – voor een deel wist ik dat al – dat cyber grenzeloos, onnavolgbaar en ongrijpbaar is. Je moet het dus grijpbaar maken. Het is ook onzichtbaar, direct en indirect. De vraag is hoe je het zichtbaar gaat maken. De vraag is welke doctrine daarop past, welke

maatregelen, welk plan van aanpak en welke U-bochten. We hebben de metadata mogen zien. Wij hebben het over interceptie en detectie gehad. Om vier uur 's middags moest ik het even laten bezinken, om te begrijpen waar het over gaat. Toen ging ik weer in de Kamerstukken lezen, want zo doen wij dat. Wat is de definitie van «het digitale domein»? De Nationale Cyber Security Strategie duidt het digitale domein, cyberspace, aan als het geheel van digitale informatie, informatie-infrastructuren, computers, systemen, toepassing en interactie tussen informatietechnologie en de fysieke wereld waarover communicatie en informatie-uitwisseling plaatsvindt. Dat is inderdaad ingewikkelder dan de twee kabels en de ICT waar wij vanmorgen over spraken. De vraag is wat Defensie daarin betekent, als het gaat om de offensieve cybercapaciteit. De definitie zegt dat Defensie moet beschikken over kennis en capaciteiten. Die moet zij ter beschikking hebben ter ondersteuning van militaire operaties en zij moet offensief kunnen optreden in het digitale domein. Het gaat hierbij om het ontwikkelen van kennis over complexe en hoogtechnologische middelen en technieken die er specifiek op gericht zijn het eigen militaire vermogen te vergroten. Tot zover de definities.

Ik probeer mij dan een voorstelling te maken van wat het operationele domein inhoudt. Wat betekent dat nu voor onze missie in Mali? Wat betekent het concreet in de voorbereiding van onze militairen die wij op missie sturen? Wat betekent dat in kennis en kunde? Wat is het begrip van cyber? Naast het werkbezoek zijn er hoorzittingen geweest. Die waren overigens ook erg plezierig. Wij hebben veel kennis opgedaan over waar wij het nu over hebben. Mijn eerste vraag aan de Minister – ik erken meteen dat het lastig is – betreft samenwerking in Europees verband. Dat doen wij natuurlijk in Mali. Daar werken wij samen. Wij zijn daar modulair aanwezig. De aanpak daar is modulair. Als wij daar samenwerken, welke spelregels hebben wij dan? De heer Van Dijk noemde het artikel in Vrij Nederland al, waar kolonel Folmer een van de informanten voor was. Het gaat natuurlijk over draagvlak, over awareness. Weten wij waar het over gaat? Er wordt gesproken over cybersoldaten. Hoe werkt dat nu, als wij mensen uitsturen naar Mali? Ik zou het zeer waarderen als de Minister daar wat meer beeld en geluid bij zou willen geven. Ik kan het zelf ook bedenken. Het gaat over kennis en kunde en over opleiding, maar ook over de juridische randvoorwaarden. Als er ter plekke door onze commandant een cyberoffensief wordt gesignaleerd of informatie wordt ontvangen die invloed heeft op een wapensysteem van ons dat wordt ingezet en op inlichtingen die wij hebben, hoe moet ik mij dat dan voorstellen? Hoe gaat het dan met de juridische mogelijkheden? Hoe zit het met de beperkingen vanuit inlichtingenwerk?

Wij sturen mensen uit. Dat is internationaal. Wij gaan weer naar het nationale niveau als het gaat om de richtlijnen en de wetgeving. Ik noem de Wet op de inlichtingen- en veiligheidsdiensten 2002. Mogelijk komen daar nog discussies over. Die liggen ook voor de hand. De spelregels van 2002 gelden, als het gaat om SIGINT, voor alle verantwoordelijkheden over interceptie via de kabel, et cetera. Zou de Minister daar eens op willen reageren?

Ik ga nog even terug naar de definities en de Europese Raad. In december jongstleden heeft de Raad 22 conclusies aangenomen. In één daarvan staat dat er een cyberstrategie komt. Hoe moet ik dat voor mij zien? Wij hebben tijdens de hoorzitting van de heer Luiijf een prachtig document gekregen over de negentien cyberstrategieën. Als je ziet wat er aan definities wordt gebruikt in de verschillende landen, komen wij nog niet gelijk bij elkaar. Ik heb me ook laten vertellen dat als je het over strategie hebt, je het nog niet over de directe samenwerking hebt. Daar zit nog heel veel tussen.

Defensie zelf geeft aan dat het digitale domein naast land, zee, ruimte en lucht het vijfde domein is. Daar gaat de komende tijd natuurlijk veel op gebeuren. Mijn fractie is blij met de voortvarende aanpak van de Minister,

van de regering. Wat wel lastig is, is dat in deze Kamer vier commissies over het digitale domein gaan. Het het zal ook aan de Kamer liggen dat ik hierover moet spreken. De commissies voor Buitenlandse Zaken, Veiligheid en Justitie, Defensie en Binnenlandse Zaken gaan hierover. Morgen is er een algemeen overleg over de Nationale Cyber Security Strategie 2. Alles heeft met elkaar te maken. Wie is nu at the end verantwoordelijk voor de inzet en de capaciteiten, nationaal en internationaal?
Mijn laatste punt betreft het uitdaging rapport van de AIV van december 2011. Dat is wat mij betreft nog ongewijzigd van toepassing op vandaag, met alle informatie die erin staat. Een opmerking uit dat rapport is dat er geen reden is waarom een digitale aanval op een computerinformatiesysteem niet zou kunnen gelden als een gewapende aanval. De heer Knops zei het ook al. Wij hebben natuurlijk een voorstelling van hoe een fysieke aanval eruit ziet, maar met cyberaanvallen hebben wij nog weinig of geen ervaring. Ik wil even terug naar de regelgeving. Ik hoor daar graag een reactie op van de Minister.

De heer **Jasper van Dijk** (SP): Wij zien dus aan de ene kant dat er voortvarend wordt gewerkt aan een cyberstrategie. Daar valt ook heel veel voor te zeggen. Aan de andere kant blijven de spelregels rond die oorlogvoering echter wat achter. Er zou eind 2013 een doctrine komen, maar die is nu naar 2015 verschoven. Hoe beoordeelt mevrouw Eijsink dat? Vindt zij dat de ontwikkelingen gewoon door mogen gaan of wil zij toch dat wat meer tempo wordt gemaakt met die spelregels?

Mevrouw **Eijsink** (PvdA): Dat is inderdaad een heel interessante discussie die de heer Van Dijk wederom aan de orde stelt. Ik heb daar het antwoord niet op. Op pagina 20 van het AIV-rapport van 2011 staat nadrukkelijk – dat sluit aan bij de vraag van de heer Van Dijk – dat het instrumentarium dat wij hebben van toepassing is en van toepassing blijft, ook juridisch gezien en ook waar het gaat om artikel 51 van het VN-Handvest. Die zin triggerde mij meteen. De AIV – daar zitten toch mensen die wel iets van Defensie weten – zegt eigenlijk dat er door de tijd heen, of het nu gaat over de jaren vijftig, zestig, zeventig of tachtig, altijd technologische vooruitgang is geweest. Die technologische vooruitgang was echter in onze beleving veel zichtbaarder, waardoor wij er voor ons gevoel meer grip op hadden. Nu zetten wij een stap naar iets wat ongrijpbaarder is, het grenzeloze dat niet kan worden gedefinieerd. Net als de heer Van Dijk, vind ik dat best lastig. De AIV zegt in zijn rapport dat het van alle tijden is, maar dat het een andere manier van werken vergt. De AIV zegt dat zaken als het VN-Handvest en artikel 5 van het NAVO-verdrag het instrumentarium vormen dat wij hebben en dat wij het daar mee gaan doen. Het is trial and error, dus proberen en zien hoe wij dan verder besluiten nemen. Dat geldt ook voor onze eigen rules of engagement, het toetsingskader en de artikel 100-brieven. Ik heb dus geen antwoord op de vraag van de heer Van Dijk. Ik ben echter met hem, en ik denk met velen, aan het nadenken.

De heer **Sjoerdsma** (D66): Voorzitter. Naast land, lucht, zee en ruimte is er in toenemende mate sprake van een vijfde dimensie waarin sprake kan zijn van militair optreden: de digitale dimensie. Digitale aanvallen, cyberaanvallen, vormen een bedreiging waar Nederland zich tegen moet weren. Daar is iedereen, aan deze kant van de tafel en volgens mij ook aan de andere kant ervan, het van harte mee eens. Ook de digitale vijanden zijn bekend. Het zijn actoren die te relateren zijn aan China, Rusland, Iran en in beperktere mate Syrië. Ik denk dat bij velen van ons DigiNotar nog in het geheugen gegrift staat. Daarom is het nuttig en nodig dat Nederland cybercapaciteit ontwikkelt en daarin ook voorop wil lopen.
Toch heeft mijn fractie, net als een aantal andere fracties, nog steeds een aantal vragen, zelfs na het werkbezoek en het rondetafelgesprek. Ik

probeer, net als al mijn collega's, grip te krijgen op wat nu precies de aard is van de offensieve cyberwapens, wat de precieze voorwaarden zijn waaronder die mogen worden ingezet en wie er dan eindverantwoordelijk is voor die inzet. Die drie onderwerpen wil ik er graag uitlichten
Ik begin met de eindverantwoordelijkheid. Daar is al het een en ander over gezegd. Wat is nu precies de rol van Defensie binnen het grotere geheel van cyberverdediging en cyberaanval? Ik zet het op een rijtje. De verdediging van dijken en sluizen valt onder de Minister van Infrastructuur en Milieu, die van de stroomvoorziening onder de Minister van Economische Zaken en die van de bankensector onder de Minister van Financiën. Dan hebben wij ook nog het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie. Ook de Minister-President vervult nog een rol. Waar ligt nu precies de grens? Wanneer gaan wij van bestrijding van cybercriminaliteit naar die van cyberaanvallen? Wanneer gaan wij van cyberverdediging, die wellicht passief is, naar cyberaanval, die wellicht actief is? Hoe ziet de chain of command eruit in de verschillende scenario's? Misschien is het het beste om het in scenario's te beschrijven, zodat het voor ons duidelijker wordt hoe het precies werkt.
Ik kom nu op de offensieve inzet en de randvoorwaarden. Er ligt weliswaar een Defensie Cyber Strategie, maar die vind ik eerlijk gezegd wat weinig strategisch. Ik zie dat Defensie aan de ene kant heel hard gaat met de uitvoering, met het oprichten van organisaties en het trainen van mensen. Aan de andere kant lijkt er juist op de doctrine wat vertraging te zijn. Waarom is die doctrine eigenlijk vertraagd? Waarom komt die pas in 2015? Zou dat niet eerder kunnen en misschien ook eerder moeten?
Dan de operationele inzet van het cyberwapen. Wij hebben gezien dat het gaat van informatievergaring tot blokkeren en van misleiding tot manipulatie. Bij al die vormen is de vraag hoe het middel wordt ingezet, met welk doel en onder welke voorwaarden. De vraag is misschien ook wel hoe de Kamer daarover wordt geïnformeerd. Daarom heb ik enkele vragen. Wat zijn de randvoorwaarden voor de inzet van het cyberwapen? Onder welk recht vallen deze activiteiten? Soldaten vallen immers onder het oorlogsrecht en spionnen – ik zeg het maar even heel plat – onder de Wet op de inlichtingen- en veiligheidsdiensten. Hoe verhoudt dat zich nu tot elkaar? Wanneer ga je nu van het ene gebied naar het andere? Hoe wordt de Kamer geïnformeerd bij inzet? Is dat vooraf of is dat achteraf? En als het grootschalig is, hoe past het dan binnen onze eigen artikel 100-procedure? Kan de Minister aangeven – ik ben daar echt benieuwd naar – of het cyberwapen op dit moment offensief wordt ingezet en, zo ja, op welke manier?
Het is goed dat Nederland voorop wil lopen. Dit is een domein dat alleen maar aan importantie zal winnen. Daarbij moeten wij echter ook kijken naar de verhoudingen, internationaal. Wij geven per jaar 50 miljoen uit aan de ontwikkeling van de cybercapaciteit. Het cybersecurityplan van het Pentagon voor vijf jaar was 23 miljard. Wij trainen 200 soldaten en de Chinezen hebben inmiddels 20.000 van die cybersoldaten. Dat geeft volgens mij maar één ding aan. Wij kunnen, gezien deze verhoudingen, alleen maar een echte vuist maken als wij ook op dit terrein effectief samenwerken, zowel binnen de Europese Unie als binnen de NAVO. De Minister heeft in eerdere overleggen al iets gezegd over hoe zij dat ziet. Ik moedig haar graag aan om ook de samenwerking binnen de NAVO en de Europese Unie te versnellen en meer vorm te geven.
D66 ziet het belang van die cybercapaciteit. Daar keren wij ons niet tegen. Wij willen wel graag die heldere randvoorwaarden, of het nu gaat om de verdediging van Nederland en de Nederlandse belangen of om het actief aanvallen van anderen en misschien zelfs het voeren van oorlog. Ik krijg graag heldere antwoorden op de vragen die ik heb gesteld.

De **voorzitter**: Hiermee is een einde gekomen aan de inbreng van de Kamer in eerste termijn. Wij schorsen kort om de Minister in de gelegenheid te stellen om haar beantwoording voor te bereiden.

De vergadering wordt van 14.38 uur tot 14.43 uur geschorst.

De **voorzitter**: Voordat de Minister begint aan haar beantwoording in eerste termijn, meld ik dat mevrouw Eijsink iets voor 16.00 uur moet vertrekken. Dat geldt ook voor de heer Sjoerdsma. Wij gaan dus proberen te koersen op 15.55 uur.

Minister **Hennis-Plasschaert**: Voorzitter. Ik zal proberen te koersen op zo spoedig mogelijk, maar er zijn wel veel vragen gesteld. Ik zal daar doorheen gaan. Ik zal eerst ingaan op de juridische kaders van het cyberdomein, want dat punt hoorde ik eigenlijk in alle bijdragen terugkomen. Mevrouw Eijsink merkte terecht op dat de AIV en de CAVV in hun advies over digitale oorlogvoering hebben gesteld dat het van belang is om te beseffen dat wij voor alle handelingen die wij verrichten in het cyberdomein al regels hebben. De regels in het cyberdomein zijn eigenlijk niet anders dan die in de fysieke wereld. Dat zijn regels voor het toepassen van geweld door staten, regels voor optreden tijdens een gewapend conflict, regels voor inlichtingenvergaring en speurneuzen en regels voor strafrechtelijk handelen. Waar het gaat om het strafrechtelijk handelen, moet ik onmiddellijk verwijzen naar mijn collega van Veiligheid en Justitie. Dat is zijn verantwoordelijkheid. Hierover vindt morgen een overleg plaats. Het is dus allemaal niet nieuw. Met name de offensieve cybercapaciteit staat nog in de kinderschoenen. De regels die wij kennen in de fysieke wereld passen wij ook toe in het cyberdomein.
De MIVD is dagelijks bezig met inlichtingenvergaring, zowel in het fysieke als in het digitale domein. Dat doet hij inderdaad – dat werd terecht opgemerkt – binnen de kaders van de Wiv 2002. Daarnaast zijn natuurlijk onze eigen IT'ers dagelijks bezig met het draaiende houden van onze eigen netwerken. Er zijn in relatie tot de Wiv 2002 vragen gesteld – al werd het niet direct zo benoemd – over kabelgebonden en niet-kabelgebonden. Hierbij wil ik verwijzen naar het debat naar aanleiding van het rapport van de commissie-Dessens dat eraan zit te komen. Daar moet het debat hierover plaatsvinden, niet hier. Het kabinet heeft nog heel even de tijd genomen om te bepalen hoe het wil omgaan met het technologieneutraal maken van de wet, de voorwaarden die daarbij om de hoek komen zeilen en wat dat betekent voor de parlementaire controle. Daar zijn wij nog even op aan het studeren. Heel binnenkort heb ik volgens mij dit debat al met de Kamer, samen met Minister Plasterk. Dat vraagstuk wil ik dus even vooruitschuiven in de tijd.
De MIVD handelt dus binnen de kaders van de Wiv. Mogelijk zegt iemand dat de diensten ook wel eens handelen net buiten de kaders van de Wiv. Daarvoor hebben wij de CTIVD, die de rechtmatigheid toetst. Als er een onrechtmatigheid wordt geconstateerd, zijn er drie manieren waarop de MIVD kan handelen: de werkwijze aanpassen, de werkwijze nog een keer uitleggen en alsnog een akkoord vinden met de CTIVD of überhaupt met de werkwijze stoppen. Dat hebben wij eerder met elkaar gedeeld, maar ik wilde het nogmaals aan de orde stellen.
De Minister van Veiligheid en Justitie is verantwoordelijk voor de coördinatie van cybersecurity in Nederland. Hiervoor heeft hij het NCSC tot zijn beschikking, het Nationaal Cyber Security Centrum, dat tot taak heeft verstoringen in het digitale domein te voorkomen en te beperken. Het NCSC fungeert eigenlijk als een soort spin in het web. Verschillende organisaties, zoals de politie, de inlichtingendiensten, de vitale infrastructuur, Defensie en de private sector, werken hierin heel nauw samen om dreigingen het hoofd te bieden. Dit staat ook zo beschreven in de Nationale Cyber Security Strategie en in de brief van de Minister van

Veiligheid en Justitie van 12 december 2013 over de versterking van het NCSC. Daarover vindt morgen een algemeen overleg plaats.
Het is evident dat Defensie niet zozeer de firewall van Nederland is of overal aan bijdraagt. Uiteindelijk zijn dat de sectoren zelf, zoals ook benoemd door de heer Sjoerdsma. Op verzoek en onder aansturing van civiele autoriteiten kan Defensie wel hulp bieden bij cyberincidenten. Hiervoor gelden weer dezelfde regels als voor de fysieke militaire bijstand die wij bijna dagelijks leveren. De Kamer weet immers net zo goed als ik dat een derde van onze capaciteit dag in, dag uit wordt ingezet voor de nationale veiligheid.
Bij een ernstig incident dat niet als een gewapende aanval kan worden beschouwd, kan de nationale crisisbeheersingsstructuur in werking treden. Onder coördinatie van de Minister van V en J worden dan maatregelen genomen om de impact van het incident te beperken en de dreiging af te wenden. Ook hierbij is weer een mogelijkheid om de hulp van Defensie in te roepen, op grond van zijn derde hoofdtaak: de civiel-militaire samenwerking. Ook hiervoor gelden de vaste juridische kaders voor militaire bijstand of steunverlening. Zolang er geen sprake is van een aanval met het effect van een gewapende aanval, zal de reactie plaatsvinden op grond van het strafrecht en heeft Defensie niet meer bevoegdheden in het cyberdomein dan de politie heeft.
Mocht er wel sprake zijn van een cyberaanval die als een gewapende aanval beschouwd kan worden, ook de AIV en de CAVV gaan daar uitgebreid op in, dan valt dat onder onze grondwettelijke eerste hoofdtaak: het verdedigen van het nationaal en bondgenootschappelijk grondgebied. Het is in zo'n situatie een besluit van de regering om met een beroep op zelfverdediging tot maatregelen over gaan. Er kan dan in voorkomende gevallen een beroep worden gedaan op artikel 5 van het NAVO-verdrag. De Kamer weet dat dit altijd een politiek besluit betreft.

Mevrouw **Eijsink** (PvdA): Wat de Minister nu schetst, heb ik zo ongeveer voor mij liggen als een soort van overzicht wie waarvoor verantwoordelijk is. Dat is heel interessant. Ik ga ervan uit dat het dan werkt zoals het moet werken. Interessant is natuurlijk de vraag wie bepaalt wanneer een cyberaanval als een gewapende aanval kan worden beschouwd. De Minister gaf net de structuur weer. Op welk moment wordt dat bepaald, in een split second? Wie is verantwoordelijk, wie bepaalt en wie vraagt wie? Wij hebben daar tijdens ons werkbezoek ook over gesproken en toen is de structuur een beetje geschetst. Uiteindelijk is de vraag – dat sluit aan bij de vraag wanneer de politiek wordt geïnformeerd – wie bepaalt of een cyberaanval als een gewapende aanval kan worden beschouwd.

Minister **Hennis-Plasschaert**: Zoiets beslis je niet in een split second. Daar gaat heel vaak wat tijd overheen. 9/11 is daarvan een goed voorbeeld. Volgens mij wordt het ook genoemd in het artikel van Vrij Nederland, dat ik nog niet tot drie cijfers achter de komma heb gelezen maar wel heb gescand. Ik kom er nog op terug. Het is uiteindelijk een politiek besluit, een besluit van het kabinet. Dat is hoe het werkt, ook in de fysieke wereld.

Mevrouw **Eijsink** (PvdA): Met een split second bedoel ik 24 uur. Volgens mij is dat in de politiek al heel lang voor zoiets. Ik begrijp uiteraard goed wat de Minister zegt. Het gaat mij erom welke definitie geldt. Ik heb net niet voor niets definitie voorgelezen van bijvoorbeeld «het digitale domein» uit de Nationale Cyber Security Strategie, en wat daar binnen past. Ik vind het voor de discussie interessant om te weten welke definitie de regering hanteert voor het aanmerken van een cyberaanval als een gewapende aanval. Is dat dezelfde als beschreven in artikel 5 van de NAVO? Welke definitie hanteren wij?

Minister **Hennis-Plasschaert**: Ik ben echt net begonnen met mijn beantwoording. Er zijn een heleboel vragen gesteld, waaronder deze. Ik kom daar gewoon nog op terug. Ik heb net al gezegd dat als er sprake is van een aanval, het altijd een politiek besluit betreft, ook als er een beroep wordt gedaan op artikel 5 van het NAVO-verdrag. Dan heeft Defensie natuurlijk de rol om de aanval af te slaan. Ik heb net al gezegd dat Defensie niet de firewall is van heel Nederland. Als er een fysieke aanval plaatsvindt op Nederland, is nog steeds de brandweer verantwoordelijk voor het blussen van de branden en is nog steeds de ambulance bezig met het ophalen van gewonden. Dat is in het digitale domein niet anders. Het is primair aan de civiele netwerkbeheerders en autoriteiten om hun systemen te beschermen en te verdedigen. Ook de Nationale Cyber Security Strategie onderstreept dat private en publieke partijen in Nederland zelf verantwoordelijk zijn voor de veiligheid van hun systemen en netwerken.
Op het moment dat wij bij zelfverdediging geweld gebruiken, zijn wij uiteraard gebonden aan de regels van het humanitair oorlogsrecht. Kortom, het is wederom precies hetzelfde als in de fysieke wereld. Als ten slotte wordt besloten om cybermiddelen in te zetten voor onze tweede hoofdtaak, de inzet ten behoeve van de internationale rechtsorde, geldt de artikel 100-procedure waarover wij met enige regelmaat over spreken. De inzet moet dan een adequaat volkenrechtelijk mandaat hebben en moet voldoen aan de regels van het humanitair oorlogsrecht en de voor die missies afgegeven rules of engagement. Ook dit is niet anders dan een besluit om fysiek militaire middelen in te zetten. Dat is even om het overzicht te bewaren, ook voor mijzelf. Mevrouw Eijsink sprak in haar inbreng ware woorden toen zij zei dat de inzet van offensieve cybercapaciteit nog in de kinderschoenen staat en dat er nog een heleboel zaken in ontwikkeling zijn.
De heer Van Dijk vroeg mij of ik met de SP van mening ben dat wij transparant moeten zijn. Ja, in de zin dat wij proberen om de Kamer zo veel mogelijk proberen mee te nemen in wat er gaande is en wat de stappen zijn die door Defensie worden gezet. Betekent dat dat ik helemaal het achterste van mijn tong kan laten zien, of eigenlijk het achterste van de tong van Defensie kan laten zien als het gaat om de manier waarop die cybercapaciteit exact wordt vormgegeven? Zover zijn wij nog niet. Het antwoord op die vraag is ook nee, want daarmee zou je ook de mensen die het minder gezellig met je voorhebben informatie geven. Ik zal de Kamer blijven informeren over de stand van zaken en het is haar vrij om mij te blijven bevragen. Ik probeer echt zo transparant mogelijk te opereren.
De heer Van Dijk vroeg ook naar inzicht in de inzetscenario's. De inzet van cybermiddelen, hoe die er dan ook precies uit zou moeten zien, is natuurlijk wel afhankelijk van de uitkomst van het planningsproces van de operationele commandant. Ook voor mij geldt dat ik mij in dat geval moet baseren op het militair advies van de Commandant der Strijdkrachten. Afhankelijk van de gewenste effecten, bepaalt de commandant natuurlijk welk middel waarvoor ingezet wordt. Defensie gaat cyberinzet inbrengen in oefeningen. Wij moeten ermee gaan oefenen. De resultaten zullen weer leiden tot mogelijke scenario's. Oefeningen en scenario's hoeven niet per se een-op-een overeen te komen met de werkelijkheid. Met heel veel inzet en ook creatieve geesten kunnen een heleboel scenario's worden bedacht. Vervolgens zullen wij een keuze gaan maken en bezien welke scenario's realistisch zijn. Er wordt op dit moment een aantal scenario's met Veiligheid en Justitie besproken – dat staat allemaal echt nog in de kinderschoenen – en doorgewerkt. Daarbij wordt met name gekeken naar de verdeling van de verantwoordelijkheden. Dat is precies wat alle sprekers hebben gevraagd: waar ligt nu de grens? Die is nog best schimmig. Waar liggen de verantwoordelijkheden, tussen V en J en Defensie, en hoe krijgen wij dat helderder? Dat is precies waar wij nu mee

bezig zijn. Wij willen ook vooral duidelijk krijgen wanneer de verantwoordelijkheid, als er straks iets gebeurt, overgaat van V en J naar Defensie. Ik realiseer mij goed dat ik de heer Van Dijk hiermee geen antwoord geef, want hij wil een pasklaar antwoord. Het is echter nog in beweging. Ik zal de Kamer zo veel mogelijk informeren.

De heer **Jasper van Dijk** (SP): De Minister zegt heel helder dat het in de kinderschoenen staat. Het wordt ontwikkeld, dus kun je natuurlijk nog niet alles af hebben. Dat is duidelijk. Daarnaast is zij ambitieus en dat valt alleen maar te prijzen. Ik constateer echter ook dat de Minister in een eerdere brief heeft beloofd dat er eind 2013 een doctrine zou zijn en dat die nu net iets is vertraagd. De ontwikkeling van de cyberwarfare gaat dus heel rap, maar de doctrine is wat vertraagd. Erkent zij met mij dat er een spanning kan ontstaan als je allerlei instrumenten aan het ontwikkelen bent, en misschien ook activiteiten, terwijl de spelregels achterblijven?

Minister **Hennis-Plasschaert**: Ik begrijp heel goed wat de heer Van Dijk zegt. Een doctrine voor het militair optreden – dat heb ik volgens mij al in een brief geschreven – is vorig jaar op hoofdlijnen tot stand gekomen. Ook die is nog in ontwikkeling. Dit jaar werken wij die doctrine verder uit. Dat is dus parallel aan de ervaring die wij opdoen. Wij proberen die doctrine ook te toetsen tijdens de oefeningen waarin cyber wordt geïntegreerd. Naar verwachting is medio 2015 de doctrine echt gereed. Het is wel een proces waarin wij met vallen en opstaan en al doende leren. Wij moeten de plaat nog helemaal compleet krijgen.

De heer **Jasper van Dijk** (SP): Dank. Gaat de Minister in de doctrine ook in op de punten die ik heb genoemd rond de vervagende grens tussen civiele en militaire doelen – het ziekenhuis dat wordt uitgeschakeld als je een energiecentrale uitschakelt – de dubbelrol van cybermilitairen en de spanning tussen het bedrijfsleven, dat een bepaalde agenda heeft, enerzijds en Defensie anderzijds? Die drie punten heb ik genoemd.

Minister **Hennis-Plasschaert**: Je wilt de neveneffecten, of je nu met fysieke of met digitale wapens opereert, altijd zo beperkt mogelijk houden. Dat luistert inderdaad heel nauw. Er zijn voorbeelden uit het verleden waarbij de neveneffecten aanzienlijk waren. Dat is een van de grootste aandachtspunten in de ontwikkeling van offensieve cybercapaciteiten. Het tweede punt van de heer Van Dijk was de dubbelrol. De MIVD is binnen de kaders van de wet bezig met inlichtingenvergaring. Daarbij worden bepaalde methoden gebruikt die interessant kunnen zijn voor de ontwikkeling van offensieve cybercapaciteiten. Dat betekent niet per definitie dat hij een dubbele pet opheeft en dat daarmee grenzen aan het vervagen zijn. Het is ook voor ons van belang dat wij heel duidelijk weten binnen welke kaders wij handelen: namen en rugnummers, wie is waarvoor verantwoordelijk en wie is waarop aanspreekbaar. Dat is voor mij, net als voor de heer Van Dijk, een heel belangrijk aandachtspunt. De spanning tussen het bedrijfsleven en Defensie zie ik niet helemaal. Als het gaat om cyber, hebben de private sector en de publieke sector elkaar heel hard nodig. Misschien kan de heer Van Dijk mij op dit punt nog even op weg helpen.

De **voorzitter**: Mijnheer Van Dijk, misschien wilt u uw vraag nog even wat meer inkleuren.

De heer **Jasper van Dijk** (SP): Bij cyberwarfare is de samenwerking tussen het bedrijfsleven en Defensie intensief. Ik heb gezegd dat bedrijven er natuurlijk een eigen agenda op na kunnen houden. Zij hebben er bijvoorbeeld belang bij om de angst voor de cyberdreiging aan te zetten.

Ik heb liever dat de Minister het risico inschat dan dat een bedrijf dat voor haar doet.

Minister **Hennis-Plasschaert**: Ik neem aan dat de heer Van Dijk bedoelt dat het bedrijfsleven vanwege financiële belangen het misschien erger voorstelt dan het is. De digitale ontwikkeling gaat in een zeer rap tempo. Ik laat mij niet zo snel leiden door een lobbyist, of het nu gaat om kavels of om de ontwikkeling van offensieve capaciteiten. Het gaat erom dat wij ons allemaal – daar hebben wij vanochtend op een heel andere wijze met elkaar over gesproken – laten voorlichten door experts, door specialisten die er verstand van hebben. Dat kunnen mensen zijn uit de publieke sector en mensen uit de private sector. Uiteindelijk is het aan het kabinet en ook aan Defensie om een eigen afweging te maken. Dat doet het bedrijfsleven niet voor ons.

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

Minister **Hennis-Plasschaert**: Ik probeer niets over te slaan. Dat is helemaal niet eenvoudig, want ik word er gelijk aan gehouden. Ik heb net al iets gezegd over het rapport van de commissie-Dessens, waarbij ik heb gezegd dat het me niet verstandig lijkt om dat nu te bespreken.
Er is gesproken over statelijke en niet-statelijke actoren. Wanneer is iemand de vijand? Dat hoef ik de Kamer natuurlijk niet te vertellen, want zij weet net zo goed als ik dat in het kader van het VN-Handvest een aanval door niet statelijke actoren kan worden ingezet. Dat is ook door de AIV en de CAVV gezegd. Ik noemde net 9/11 al als voorbeeld. Er is natuurlijk geen vrijbrief voor groeperingen of wie dan ook om landen willekeurig aan te vallen. Dat is precies waar ik net op doelde. Dan kom je weer terug bij het politieke besluit. Als de staat waar de groepering zich bevindt niet in staat is om zelf in te grijpen, is een optreden tegen een groepering in een ander land mogelijk. Daarbij moet natuurlijk weer worden voldaan aan de eisen van noodzakelijkheid en proportionaliteit. Het is vrij complex. Dat zal ik niet ontkennen. Dit is wel hoe wij al eerder hebben gewerkt en afspraken hebben gemaakt.
De heer Knops vroeg hoe wij de kennisopbouw borgen. De snelheid waarmee de ontwikkelingen gaan is, zoals ik al zei, echt enorm. Dat stelt ook heel hoge eisen aan het adaptieve en innovatieve vermogen van Defensie. Wij moeten over kennis blijven beschikken om relevante ontwikkelingen te kunnen volgen en er hier en daar ook snel en doeltreffend op in te kunnen spelen. Wij richten hiervoor het Defensie Cyber Expertise Centrum (DCEC) op. Dat is een centraal punt voor kennisontwikkeling, borging en verspreiding op het gebied van cybersecurity. Dit werkt weer nauw samen met andere Defensieonderdelen, waaronder de MIVD, en andere spelers in het cyberdomein. In het kader van innovatie en onderzoek wordt er nationaal en internationaal intensief samengewerkt met de private sector en kennisinstituten, maar ook binnen de NAVO en de Europese Unie. Daarnaast doen wij dat uiteraard interdepartementaal, vooral met V en J.
De heer Knops verwees naar Peter Singer. Ik heb hem niet ontmoet en ik weet ook niet wat hij precies met de heer Knops heeft gedeeld. Hij was in elk geval niet te enthousiast, begrijp ik uit zijn bijdrage. De realiteit is dat op het gebied van cyber nog niet alles wordt gedeeld, net als in de inlichtingenwereld niet alles wordt gedeeld. Defensief zijn wij geneigd om wel kennis te delen en te faciliteren. Wat betreft offensief zie je dat de landen nog heel erg op slot zitten. Dat is ook niet zo heel erg raar. Als je te veel details prijsgeeft over een bepaalde cybercapaciteit, kan die immers gelijk weer worden afgeschreven voor inzet. Wat natuurlijk wel wordt gedaan, zeker in geval van een incident, is ervaringen delen. Daarmee leren wij van elkaars fouten. Als ik terug ben op het departement zal ik nog eens extra kijken naar de uitspraken van Peter Singer en ze in hun

context plaatsen. Voor zover wij nu inschatten, is de ontwikkeling van cybercapaciteiten binnen Defensie in Nederland echt anders belegd dan in de VS. De integrale aanpak staat centraal. Dat heb ik de hele tijd al proberen aan te geven. Wij doen het echt met alle Defensieonderdelen. Kennis wordt intern heel goed gedeeld. Duplicatie van capaciteiten wordt zo veel mogelijk voorkomen.
De heer Knops noemde 20.000 cybersoldaten in China of miljarden dollars in Amerika. Daar ben ik natuurlijk jaloers op. Ik zeg er wel gelijk bij dat 20.000 cybersoldaten helemaal niets zegt over het niveau van kennis en kunde. Ik ben volgende week in China, dus dan ga ik het maar eens navragen. De heer Knops brengt mij op een idee. Hij vroeg ook nog wanneer de doctrine openbaar wordt. Ik heb al gezegd dat dat medio 2015 zal zijn.
De heer Vuijk vroeg heel specifiek naar de zwaardmacht die bij de overheid ligt. Het geweldsmonopolie van de overheid strekt zich natuurlijk uit over zowel het militaire als het justitiële domein. Het ligt bij de Staat, niet bij een specifiek ministerie en dus ook niet bij Defensie. Wat betreft de inzet van cyberwapens in het kader van een gewapend conflict of een vredesmissie, ligt het monopolie voor het gebruik van geweld wel weer bij Defensie. De politie kan ook cybermiddelen inzetten binnen de voor haar geldende juridische kaders. Ik heb in mijn inleiding al geprobeerd om dat hele overzicht te schetsen.
De heer Vuijk en ook anderen vroegen naar het versneld oprichten van Defensie Cyber Commando. Het is eind 2015 operationeel. Dan ook is het DCC in staat om een operationele commandant te ondersteunen en te adviseren over de mogelijkheden en kwetsbaarheden van onze eigen systemen, over de manier waarop wij cybermiddelen kunnen inzetten en over de effecten die wij ermee kunnen bereiken. Dat is dus nog in ontwikkeling. Het is dus niet zo dat wij nu met één druk op de knop al in die capaciteiten kunnen voorzien.
Ik heb net al tegen de heer Van Dijk al gezegd dat ik de Kamer zo veel mogelijk zal meenemen en zo transparant mogelijk wil opereren. Het moet echter wel duidelijk zijn dat de ontwikkeling en de inzet van cybermiddelen gepaard gaat met de nodige geheimhouding, omdat je je anders wel heel erg kwetsbaar maakt voor de tegenstander. Wij beschikken nu nog niet over operationele digitale middelen, maar hopelijk straks wel. Ik zal die informatie echter niet in een algemeen overleg als dit met de Kamer kunnen delen. Ik zal nog even kijken of wij dat wel op een andere manier kunnen doen, via andere lijnen in de Kamer.
Er werd ook gevraagd naar de werving. Wij hebben verschillende projecten opgezet voor de opleiding van het eigen personeel en de werving van nieuw personeel. In 2013 heeft er een Cyber Challenge plaatsgevonden binnen Defensie, voor het eigen personeel. Ik vond dat zelf heel geslaagd. 400 militairen hebben eraan meegedaan. Daarvan zijn er nu slechts 13 geselecteerd voor een opleiding tot technisch cyberspecialist bij een vooraanstaand cybersecuritybedrijf. Dat is echt heel goed, omdat zij worden meegenomen in de opleiding en ook direct worden geconfronteerd met de praktijk. De werving voor de operationele cyberadviseurs loopt. Daar bestaat ontzettend veel belangstelling voor. Natuurlijk is er concurrentie met het bedrijfsleven. Gezien de vervulling van cyberfuncties, denk ik niet dat er reden is tot zorg. Gelukkig spreekt Defensie, zeker als het hierom gaat, nog steeds tot de verbeelding.
Ik zei net al dat het DCC nog niet is opgericht. Wij kunnen dus nog niet, zo zeg ik tegen mevrouw Eijsink en de heer Vuijk, rekenen op capaciteit van het DCC waar het gaat om militaire operaties. Natuurlijk ondersteunt de Taskforce Cyber, die er wel is op dit moment, de operationele planning. Ook bij oefeningen wordt gekeken waar gebruik kan worden gemaakt van cyberreservisten. Er is een cyberadviseur geplaatst bij de planning voor Mali. Dat is echter niet waar wij nu met elkaar over spreken. Dat laat echt nog even op zich wachten.

Mevrouw **Eijsink** (PvdA): Ik heb een heel praktische vraag over de personele bezetting en alle opleidingen. De Minister sprak al even over de cyberreservisten. Wij zijn nog steeds met haar in gesprek over een reservistenbeleid. Als ik de brieven goed heb begrepen, vallen deze cyberreservisten daar ook onder. Wat betekent dat nu verder voor de inzet van deze reservisten? Er zijn vragen over de bedrijven die mensen vrijmaken om reservist te zijn, over de dagvergoeding en de juridische regelingen daarvoor. Kan de Minister daar iets meer over zeggen?

Minister **Hennis-Plasschaert**: Hebben wij niet binnenkort een algemeen overleg over de reservisten?

Mevrouw **Eijsink** (PvdA): Als de Minister een algemeen overleg over reservisten wil, kan de Kamer daar best over overleggen.

Minister **Hennis-Plasschaert**: Sorry, ik weet dat echt niet uit mijn hoofd. Wij zijn het reservistenbeleid, zoals bekend, enorm aan het uitbreiden en verder aan het optuigen. Er zijn allerlei gesprekken gaande. Ik heb nu echt niet op mijn netvlies hoe het zit met de vergoedingen et cetera. Daar kom ik dus op terug. Volgens mij hebben wij een afspraak om binnenkort met elkaar te praten over reservisten.

Mevrouw **Eijsink** (PvdA): Ik refereer gewoon aan een brief die wij vandaag bespreken, waarin wordt gerept over cyberreservisten. Ik neem dan aan dat het beleid verder ontwikkeld is. Cyber ontwikkelt zich heel snel, net als de actie en de reactie en de snelheid van werken. Daar moeten wij natuurlijk beleid voor hebben. Zegt de Minister nu dat dit beleid zo spoedig mogelijk naar de Kamer komt? Ik ben er niet van op de hoogte dat dat komt. Wij hebben een algemeen overleg personeel staan, maar daar staat nog niet de uitgewerkte reservistennota op de agenda. Dit heeft natuurlijk direct impact op het inzetten van de mensen die de Minister cyberreservist noemt. Het zijn gewoon reservisten die cyber gaan doen.

Minister **Hennis-Plasschaert**: Zo is het ook. Ik krijg net ingefluisterd dat de reservistennota, waarover ik eerder met de Kamer over heb gesproken, in juni naar de Kamer komt. Daar doelde ik net op. Ik had het even niet paraat. Of het nu een reservist is die gisteren is ingezet tijdens de NSS of een cyberreservist, het gaat erom welke kaders wij met elkaar willen afspreken en welke vergoedingen er zijn. Daarbij maakt het niet uit of iemand een cyberreservist is of voor een andersoortige taak wordt ingezet. Begrijpen wij elkaar dan goed?

Mevrouw **Eijsink** (PvdA): Ik begrijp de Minister voor een deel. Ik kan mij voorstellen dat voor cyberreservisten toch iets andere regels gelden, ook wat betreft clearing en toegang tot informatie, dan voor de reservisten die gisteren bij het Hilton Hotel zijn neergezet voor bewaking. Ik krijg graag nadere informatie van de Minister. Dit gaat iets verder dan alleen maar ergens staan om iets of iemand te beschermen. Dit gaat tot ver in de informatiekrochten van de AIVD en de MIVD en van andere delen van de organisatie.

Minister **Hennis-Plasschaert**: Wij hebben vele reservisten met vele soorten expertise op veel verschillende terreinen. De een is bewaker, een ander is chauffeur, een volgende is cyberspecialist en nog een ander is jurist. Daar gelden ook verschillende clearances voor. Daar komen wij op terug in de reservistennota. Ik denk dat wij elkaar dan voldoende begrijpen.
De heer Vuijk vroeg naar de inzet van cybermiddelen in het kader van inlichtingenvergaring. Op dit moment is het zo geregeld – ook daarover

gaan wij het volgens mij het gesprek aan in een ander debat – dat de controle plaatsvindt via de commissie voor de Inlichtingen- en Veiligheidsdiensten, met toezicht door de CTIVD. Zodra wij cybermiddelen offensief gaan inzetten, is in feite de normale parlementaire procedure voor inzet van militaire middelen van toepassing. Ik hecht daar ook aan, omdat je daarmee de transparantie krijgt waar de heer Van Dijk op hamert.
Wij hadden het net al even over de grensvervaging tussen V en J en Defensie, over de vraag wie wat doet. De ontwikkelingen op dat terrein zijn nog gaande. Daar werken wij nog aan. De heer Vuijk vroeg specifiek naar de grens tussen cybercriminaliteit en cyberwarfare. Ook daarvoor hebben de IAV en de CAVV in hun advies een aantal criteria gegeven aan de hand waarvan kan worden bepaald of een cyberaanval kan worden beschouwd als een gewapende aanval in de zin van het VN-Handvest. Dat hoef ik allemaal niet uit te leggen. Wij proberen zo veel mogelijk te kijken naar de regels die gelden in de fysieke wereld en die passen wij een-op-een toe op de digitale wereld. Ik heb ook al gezegd dat er nog zaken in ontwikkeling zijn. V en J en Defensie werken daar momenteel aan.
De concentratie van cyberactiviteiten van de NAVO in Den Haag vind ik ook goed. Wij hebben ons best gedaan om dat binnen te halen. Het is vooral onderzoek. Het is wel van belang om dat verder een boost te geven.
Ik heb al gezegd dat het DCC nog niet operationeel is in de zin die wij zo graag zouden willen zien. Dat gebeurt pas in 2015. Dat betekent ook dat wij nog niet specifiek capaciteiten in bijvoorbeeld Mali inzetten. In Mali worden alle activiteiten, van welke aard dan ook, uitgevoerd binnen het mandaat van de missie en de rules of engagement die daarvoor gelden. Dat geldt dus ook voor de inzet van cybermiddelen. Die zouden dan worden meegenomen in de rules of engagement. Waar het gaat om inlichtingenactiviteiten moeten wij steeds weer terug blijven vallen op de Wiv 2002, waarover wij binnenkort een gesprek hebben.
Ik denk dat ik al voldoende heb gezegd over de taakverdeling tussen mij en de Minister van V en J. Ik was toen ik in de Kamer zat woordvoerder cyber en ben toen zelf enigszins in verwarring geraakt omdat toen ineens Donner als Minister van Binnenlandse Zaken het debat voerde over DigiNotar. Ik denk dat het aan dit kabinet is om heel duidelijk te zijn over wie welke rol heeft en wie waarvoor verantwoordelijk is. Wat voor iedereen klip-en-klaar moet zijn, is dat V en J die coördinerende rol heeft en daar ook op aanspreekbaar is.

Mevrouw **Eijsink** (PvdA): Ik begrijp goed wat de Minister zegt over die coördinerende rol, over wie in de driver's seat zit. Ik heb toch een vraag over de besluitvorming. De Minister van V en J zit in de driver's seat. Die besluit, maar dat is op nationaal niveau. Cyber is grenzeloos, ook de aanvallen. Het heeft toch met Mali te maken. Hoe moet ik mij voorstellen dat de regering dit gaat oppakken? Het is immers niet ondenkbaar dat er iets gebeurt. Wat gebeurt er dan? Wie informeert wie en binnen welk tijdbestek? Wij kennen voorbeelden waarbij het rond de informatieposities binnen de regering niet allemaal goed ging. Ik probeer gewoon even een beeld te krijgen van hoe dit dan verloopt, binnen de afspraken.

Minister **Hennis-Plasschaert**: Bij DigiNotar is het wel goed verlopen, behalve dat er even wat verwarring was doordat er door BZK verantwoording werd afgelegd in de Kamer. Ik kan mij nog herinneren dat op het moment van het incident, om het zo maar te noemen, onmiddellijk iedereen werd opgeroepen die opgeroepen moest worden en die mensen bij elkaar werden gezet. Het was vervolgens aan het kabinet om te handelen. Bij een incident in een missiegebied is natuurlijk Defensie als eerste aan zet. Bij een incident in Nederland is de coördinerend bewindspersoon, in dit geval Minister Opstelten, als eerste aan zet. Er zullen altijd

experts bij elkaar komen om te bepalen wat er aan de hand is. Daarvoor is echt iets meer tijd nodig dan die split second waar wij net over spraken. In geval van een gewapende aanval is er vaak zelfs veel meer tijd nodig dan de 24 uur die werd genoemd.

De heer **Sjoerdsma** (D66): Ik probeer het toch nog iets concreter te krijgen. De Minister zei eerder tijdens dit overleg dat het nog in de kinderschoenen staat. Ze zei: de verdeling tussen V en J en Defensie is schimmig, dat geef ik toe.

Minister **Hennis-Plasschaert**: «Schimmig» zei ik volgens mij niet.

De heer **Sjoerdsma** (D66): Dat waren de letterlijke woorden. Ik heb ze even genoteerd. Nu is het klip-en-klaar. Ik wil het nog hebben over de verantwoordelijkheden. Stel nu dat er binnen de MIVD in dit cyberkader iets fout gaat. Is dan de Minister van V en J daarvoor verantwoordelijk of de Minister van Defensie?

Minister **Hennis-Plasschaert**: Kunt u uw vraag nog eens herhalen?

De heer **Sjoerdsma** (D66): Stel nu dat er binnen de MIVD binnen dit cyberkader door iemand van de MIVD een fout wordt gemaakt. De Minister zegt dat de Minister van V en J verantwoordelijk is in de algehele coördinatie. Ik neem echter aan dat in dit geval zij verantwoordelijk is.

Minister **Hennis-Plasschaert**: Zeker. Ik ben verantwoordelijk voor de MIVD. Dus dat blijf ik ook in dat geval. Het woord «schimmig» had ik misschien niet moeten gebruiken. Ik ben mijn beantwoording begonnen met een uiteenzetting van bijna een kwartier van wie waarvoor verantwoordelijk is op dit moment. Dat er nog wat in beweging is tussen V en J en Defensie waar het gaat over de exacte rolverdeling, dat daar nog specifieker naar wordt gekeken en dat er op dit moment aan wordt gewerkt, is een tweede. Het is heel duidelijk dat er één coördinerende bewindspersoon is voor cybersecurity, namelijk de Minister van V en J.

De heer **Sjoerdsma** (D66): Het is dus niet schimmig, maar er is nog wel het een en ander in beweging tussen V en J en Defensie over wie dan wat doet. Wat is er dan nog precies in beweging? Waar wordt op dit moment naar gekeken?

Minister **Hennis-Plasschaert**: Ik kom daar zo even op terug, aan het einde van mijn beantwoording. Ik ben namelijk mijn blaadje kwijt naar aanleiding waarvan ik dat zei. Als de heer Sjoerdsma mij daar even de tijd voor geeft, kom ik daar in tweede termijn op terug.
Ik denk dat het goed is om even door te gaan met de beantwoording van de vragen van mevrouw Eijsink. Zij vroeg specifiek of ik zou kunnen duiden hoe een cyberaanval op Nederland eruit zou kunnen zien en wat onze respons dan zou kunnen zijn. Dat is heel moeilijk, want cyberaanvallen kunnen nogal verschillend van aard zijn. Het kan gaan van een aanval op de vitale infrastructuur – dat kan heel zichtbaar worden, bijvoorbeeld als de sluizen worden opengezet – tot iets dat minder grijpbaar is. Het Nationaal Cyber Security Centrum van Nationaal Coördinator Terrorismebestrijding en Veiligheid is verantwoordelijk als coördinator van cybersecurity in Nederland. Dat komt dan bijeen en zal in reactie hierop coördineren in samenwerking met alle partners in het digitale domein. Daar zit ook precies de kracht, omdat er niet één iemand verantwoordelijk is voor alle systemen in Nederland. Er zal worden onderzocht of het gaat om een aanval of een technische storing. Mocht het om een aanval gaan, moet worden gekeken of duidelijk is wie de dader is. Pas als het om een ernstige cyberaanval gaat waarvan de

effecten vergelijkbaar zijn met die van een gewapende aanval, kan het recht op zelfverdediging worden ingeroepen en kan eventueel worden besloten tot een militaire respons. Ik herhaal wat ik net al zei: het is altijd een politiek besluit. Ik denk ook dat wij hier eerlijk in moeten zijn. Meestal zullen cyberaanvallen helemaal niet beschouwd kunnen worden als een gewapende aanval. In dat geval heeft de Minister van V en J de justitiële middelen tot zijn beschikking en kan Defensie wel worden ingezet in het kader van de civiel-militaire samenwerking. Ik denk dat ik het hiermee zo goed als mogelijk heb geschetst. Ik kom zo nog even bij de heer Sjoerdsma terug op wat ik net heb bedoeld met de lijnen tussen V en J en Defensie.
De heer Sjoerdsma vroeg of er op dit moment al cyberwapens offensief worden ingezet. Het antwoord daarop is nee.

De **voorzitter**: Ik zie dat mevrouw Eijsink nog een vraag heeft.

Mevrouw **Eijsink** (PvdA): Ik zou het op prijs stellen als wij een volgende keer als wij over dit onderwerp spreken toch door kunnen praten over de definitie van een cyberaanval met het effect van een gewapende aanval. Ik begrijp wat de Minister zegt, namelijk dat zij nu naar behoren informatie wil geven. Ik ben echter benieuwd naar de definitie van een aanval in het cyberdomein die aangemerkt kan worden als gewapende aanval. De Minister heeft zelf gezegd dat het lastig is. Wie bepaalt wanneer dat het geval is? Ik zou daar graag wat meer duidelijkheid over krijgen.
Ik vraag de Minister ook om mijn vraag over de Europese Raad en de strategie te beantwoorden. Of komt dat nog?

Minister **Hennis-Plasschaert**: Nee, ik ben klaar.

Mevrouw **Eijsink** (PvdA): Dan zou ik de Minister willen vragen om die vraag nog te beantwoorden.

Minister **Hennis-Plasschaert**: Ik zou mevrouw Eijsink willen vragen om die vraag nog even te herhalen, want die heb ik niet op mijn netvlies.

Mevrouw **Eijsink** (PvdA): In december heeft de Europese Raad 22 conclusies aangenomen. Een van de conclusies was dat er een cyberstrategie komt op Europees niveau en dat die in juni 2014, dus nog dit jaar, naar buiten gebracht zal worden. Daar hebben wij ook over gesproken in het laatste algemeen overleg hierover. Hoe moeten wij kijken naar definities? Internationaal lopen definities – daar hebben wij ook in de hoorzitting over gesproken – niet volledig gelijk aan elkaar. Ik verwees naar de studie over de negentien cyberstrategieën van de heer Luiijf die wij hebben besproken tijdens die hoorzitting. Dat was mijn eerdere vraag.

Minister **Hennis-Plasschaert**: Dat is een van de punten die worden geadresseerd in het aanlopen van de strategie. Daar zijn wij nu mee bezig. De Kamer heeft volgens mij in mijn laatste terugkoppeling een overzicht gekregen van alle conclusies en de stand van zaken daarop. Als ik meer informatie heb over de manier waarop wij die definities verder invullen en meer gelijk krijgen, wordt de Kamer daar uiteraard over geïnformeerd. Dat spreekt voor zich.

Mevrouw **Eijsink** (PvdA): Kan de Minister nog reageren op mijn verzoek ten aanzien van de gewapende aanval?

Minister **Hennis-Plasschaert**: De definitie van een gewapende aanval heb ik net al een paar keer proberen te geven. Die staat ook geformuleerd in het rapport van de AIV en heeft een relatie met het VN-Handvest. Uiteindelijk komt het altijd neer op een politiek besluit.

De heer **Sjoerdsma** (D66): De Minister zegt dat er op dit moment geen sprake is van offensieve inzet. Bij fysieke militaire operaties wordt altijd een afweging gemaakt over potentiële nevenschade. Dat kun je relatief goed doen. Hoe wordt dat gedaan bij de inzet van digitale wapens? Neem bijvoorbeeld Stuxnet. Dat was bedoeld, door wie het ook heeft ontwikkeld, om de Iraanse nucleaire reactoren uit te schakelen. De nevenschade daarvan was buitengewoon groot, ongetwijfeld niet geheel voorzien. Hoe kan de Minister van Defensie een correcte inschatting maken van de potentiële nevenschade van de inzet van cyberwapens? Daar ben ik benieuwd naar.

Minister **Hennis-Plasschaert**: Dat is een heel terechte opmerking van de heer Sjoerdsma. Dat is ook precies waarom het zo veel tijd kost om tot de ontwikkeling van offensieve cybercapaciteiten te komen. Je wilt immers heel precies zijn in waar ze voor worden ingezet, wat het beoogde effect is en wat de eventuele neveneffecten zijn. Dat is precies waarom wij bijvoorbeeld de inlichtingenvergaring nodig hebben voor de ontwikkeling van offensieve cybercapaciteiten. Je moet immers weten over welke systemen het gaat, wat daarvan de kwetsbaarheden zijn, hoe je daarop kunt inspelen en hoe je de neveneffecten zo beperkt mogelijk kunt houden. Onder andere om die reden kan er pas in 2015 daadwerkelijk worden gesproken van offensieve cybercapaciteit.

De heer **Vuijk** (VVD): Ik was even in vertwijfeling of de Minister een van mijn vragen al had beantwoord. Wij hebben er in de hoorzitting over gesproken dat Defensie voor bijzondere werkzaamheden soms leunt op het bedrijfsleven. Het bedrijfsleven ziet lacunes in de regelgeving en acht zich kwetsbaar. Ik refereer even aan opmerkingen van de heer Prins van Fox-IT. Hij zegt dat zijn bedrijf soms wordt ingehuurd voor klussen en dat hij dan niet weet of zij wel goed juridisch zijn afgedekt. Nu is dat ongetwijfeld in de Nederlandse verhoudingen wel zo. Hij zei echter zoiets als: ik weet niet of ik daarna nog in het land waar het om gaat op vakantie kan gaan, omdat ik dan wel staatsrechtelijk afgedekt ben maar niet civielrechtelijk. In het rondetafelgesprek werd er onder andere op gehint of het dan niet mogelijk is om mensen die bij zo'n bedrijf werkzaam zijn niet onder een civiel contract te laten werken, maar ze te militariseren. Dat waren wat suggesties. Ik was even nieuwsgierig of daar nog iets over te zeggen is.

Minister **Hennis-Plasschaert**: Mag ik daar zo in tweede termijn op terugkomen? Ik moet heel even mijn hersens kraken.

De **voorzitter**: Dan komt daarmee een einde aan de beantwoording van de Minister in eerste termijn. Ik geef de leden graag de gelegenheid voor een korte tweede termijn, met een spreektijd van twee minuten.

De heer **Jasper van Dijk** (SP): Voorzitter. Ik dank de Minister voor haar antwoorden. Het debat is nog volop in ontwikkeling en wij zullen hier ongetwijfeld nog vaker over spreken. Mijn conclusie is vooralsnog dat de ontwikkeling van de cybercapaciteiten is versneld, terwijl de ontwikkeling van de spelregels daaromtrent is vertraagd. Dat is een vaststelling die vraagt om waakzaamheid. Ik zal dat in elk geval zorgvuldig in de gaten houden.
Ik waardeer het dat de Minister een snelle eerste reactie heeft gegeven op het artikel in Vrij Nederland, maar volgens mij kan er wel meer over worden gezegd. De richtlijnen zijn natuurlijk het belangrijkst. De Minister zei dat zij niet alles hier aan de Kamer kan vertellen, maar dat zij zou nadenken over een vorm waarin ze dat dan wel kan overbrengen. Daar ben ik erg benieuwd naar. Dat moeten wij misschien goed in de gaten

houden als commissie, met name waar het gaat over de vermenging van publieke en militaire doelen.
De Minister zegt vooralsnog dat zij de dubbelrol en de dubbele pet van cybermilitairen, die enerzijds inlichtingen vergaren en anderzijds aanvallen kunnen uitvoeren, goed in de gaten zal houden, als ik haar antwoord goed interpreteer. Dat lijkt me iets waar wij heel erg goed op moeten letten, evenals op de verstrengeling van bedrijfsleven en Defensie. De Minister stelde mij op zich gerust, met de opmerking dat zij de besluiten over risico's et cetera neemt. De rol van het bedrijfsleven is echter groter in dit dossier en dus de invloed ook. Om een lang verhaal kort te maken: is de Minister bereid om nog schriftelijk te reageren op het artikel in Vrij Nederland, waarin deze vraagstukken aan de orde komen? Aan de hand van die brief kunnen wij er dan in een later debat nog op terugkomen.

De heer **Knops** (CDA): Voorzitter. Cyber is in zekere zin onontgonnen terrein. Werkende weg wordt er gewerkt aan strategie en technieken om een antwoord te geven op de dreiging die wel van vandaag is. Tegelijkertijd hebben wij te maken met humanitair oorlogsrecht. Landen zijn daaraan gehouden, maar terroristen en schurkenstaten laten zich daaraan niets gelegen liggen. Bij de ontwikkeling van cyber en de uitdagingen die daarmee samengaan, moeten wij manoeuvreren, zowel in aanval als verdediging, tussen de regels van het humanitair oorlogsrecht door. Dat zorgt ervoor dat het wat ingewikkeld is en dat wij niet allemaal op dit moment een beeld hebben van hoe het nu verder moet. Het lijkt me goed als de Minister daar in verdere rapportages uitgebreid op terugkomt. Ook in het rondetafelgesprek kwam dit punt aan de orde.
Ik steun de Minister wel op haar ambitieuze weg om hier snel een positie in te verwerven. Het feit dat ook de NAVO heeft gemeend om de cyberdienst te vestigen in Den Haag is wat dat betreft een goed punt. Dat betekent wel – ik vraag de Minister om daarop in te gaan – dat er ook financiële inspanningen geleverd zullen moeten blijven worden in de komende jaren. Is de verwachting dat dat ingevuld kan worden in de relatie tot de ambities die er zijn?

De heer **Vuijk** (VVD): Voorzitter. Allereerst een compliment aan de Minister, haar medewerkers en het bedrijfsleven. Wij hebben een aantal rondetafelgesprekken en werkbezoeken gehad. Ik heb mensen van Fox-IT, KPN en TNO aan tafel gezien, samen met kolonel Folmer. Dat koppel, Defensie en het bedrijfsleven, geeft mij vertrouwen dat het met de veiligheid van Nederland op dit punt voorlopig wel goed zit. Ik zie mensen die buitengewoon slim en intelligent met IT om kunnen gaan en in één oogopslag tot in de grootste complexiteit kunnen zien welke enorme risico's er aan IT gekoppeld zijn. De militairen hebben een praktische «can do»-mentaliteit. Als het ingewikkeld wordt en er dingen gebeuren in Nederland die niet door de beugel kunnen, gaan zij gewoon ingrijpen. Dan gaat de militaire planningsmachine lopen en dan gaan zij gewoon aan de slag. Dat geeft mij er veel vertrouwen in dat het, hoewel het juridisch ingewikkeld en moeilijk is, op zich wel goed komt en dat wij voorop lopen. Ik vind overigens het feit dat de NAVO ervoor kiest om haar activiteiten in Den Haag onder te brengen, daarvan een bevestiging is.
Ik heb ook een vraag gesteld over de plek van het bedrijfsleven en de manier waarop je omgaat met het inhuren van bedrijven. De Minister heeft gezegd dat zij daar nog even naar gaat kijken. Dat hoeft wat mij betreft niet nu, want ik begrijp dat het een ingewikkelde kwestie is. Wij hebben er in het rondetafelgesprek ook over gesproken en toen kwamen de deskundigen er ook niet in één keer uit. Ik zou het bijna een wonder vinden als de Minister zegt: ik heb het nog even nageslagen en ik heb het antwoord. Ik kan mij voorstellen dat wij daar in de toekomst nog even goed naar kijken en het daar nog over hebben.

Mijn laatste opmerking betreft de kwalificatie van het operationele optreden. Hoe zit dat nu? Valt het formeel onder het straf- en procesrecht? Valt het onder de coördinerende rol van de Minister van V en J? Of gaat het zuiver over inlichtingen waarbij je dan weer kijkt naar de AIVD en de MIVD? Of gaat het over Defensie? Het komt op mij over alsof er een dominante stroming is die het voortdurend als het ware naar het midden trekt, naar het straf- en procesrecht, en dan heel moeilijk kijkend zegt dat het allemaal heel ingewikkeld is. Ik zou graag toch nog een keer echt de rol van Defensie daarin willen bespreken, want volgens mij spelen dan heel andere zaken dan straf- en procesrecht en het zoeken naar een dader. Dan praat je echt over militair optreden. Ik zou tegen Defensie willen zeggen – dat is ook mijn uitleg van wat de heer Knops zei – dat zij echt een eigen rol moet claimen in dit domein. Maak ons en de buitenwacht echt duidelijk dat het hier om Defensie gaat en militair optreden. Hoewel er best samenhang zal zijn met inlichtingenwerk en met cybercrime, gaat het hier echt om een heel specifieke tak van sport waar het geweldsmonopolie sec op van toepassing is.

Mevrouw **Eijsink** (PvdA): Voorzitter. Ik dank de Minister voor de heldere beantwoording. Zij heeft de mogelijkheden en onmogelijkheden geschetst van het verstrekken van informatie. Zij heeft echter ook toegezegd zo transparant mogelijk te zijn en zo veel als mogelijk met ons te delen.
De AIVD en de MIVD gaan binnenkort samen in de Joint SIGINT Cyber Unit (JSCU) in Zoetermeer. Wij hebben ook gelezen dat daar mogelijk wat moeilijkheden zijn wat betreft personeel. Er is een rechtszaak aangespannen vanuit de medezeggenschapsraad. Kan de Minister daarop reageren? Ik wil, net als de heer Vuijk, graag vertrouwen uitspreken, maar ook dit soort zaken gebeurt op de werkvloer. Ik verneem graag van de Minister wat de stand van zaken is en hoe dit verder gaat.
Ik heb nog een vraag over het informeren van de Kamer. De Kamer spreekt vandaag voor het eerst in tweeënhalf jaar met de Minister over cyber en digitale oorlogvoering. Ik vraag de Minister of het mogelijk is om de Kamer halfjaarlijks op de hoogte houden. Dat mag dan in een rapportage of een brief zijn, dat vind ik op zich niet zo interessant. Gezien de complexiteit van de discussie die ik ervaar, de vragen die er zijn en de snelheid van handelen, zou ik het op prijs stellen als de Minister de Kamer halfjaarlijks op de hoogte houdt. Voor alle duidelijkheid: ik vraag niet om een nota of een rapportage, maar ik vraag de Minister om de Kamer in welke vorm dan ook op de hoogte te houden. Ik vraag haar om ervoor te zorgen dat wij, gezien de ontwikkelingen, met elkaar blijven optrekken in die snelheid. Ik hoor hier graag een reactie op van de Minister.
Ik ondersteun de Minister vanuit de PvdA-fractie in haar snelheid van aanpak en ontwikkeling op dit moment zoals zij die voorstaat in de brief aan de Kamer. Ik wens haar daar veel succes bij. Ik geloof niet dat het altijd makkelijk is, gezien de spaghetti van informatie iedere keer. Het gaat niet alleen om de snelheid van handelen, maar ook om het vermogen om kennis, kunde en snelheid in de organisatie weg te zetten.
De heer Knops verwees naar de financiële kant. Daar ben ik ook in geïnteresseerd. Die kan ook in zo'n rapportage of brief worden meegenomen. Ik ben met name geïnteresseerd in de personele werving en selectie ten aanzien van cyber. Dat zullen niet de reservisten zijn die cyber kunnen inbrengen. Dit moet op verschillende niveaus worden ingebracht. Het gaat ook om de deskundigheid over cyber in de organisatie zelf, in combinatie met de private aanpak. Daar hebben wij ook in de hoorzitting over gesproken. Ik heb veel waardering voor de mensen van Defensie en uit de private sector die wij hebben gehoord. De samenwerking, de verbinding, kan wellicht nog beter. Ik denk dat het niet zozeer meer in de kinderschoenen staat. Ik denk dat die schoenen al wat groter zijn geworden, gehoord de hoorzitting. Daarvan wil ik graag op de hoogte gehouden worden.

De heer **Sjoerdsma** (D66): Voorzitter. Ik dank de Minister voor haar beantwoording in eerste termijn. Zij besteedde, zoals zij zelf zei, vijftien minuten aan de uitleg van de verantwoordelijkheden en de rolverdeling. Dat schetst een beetje de complexiteit van dit thema en misschien ook waar de mogelijke valkuilen zitten. De Minister zou nog terugkomen op de vraag waar het nu precies op hangt tussen Defensie en V en J. Daar ben ik zeer benieuwd naar. Ik ben ook wel benieuwd naar hoe het nu werkt bij de Joint SIGINT Cyber Unit. Die hangt organisatorisch tussen de Ministeries van Defensie en Binnenlandse Zaken in, maar Algemene Zaken heeft er ongetwijfeld ook nog een rol in. Welk ministerie is wat betreft die unit ons aanspreekpunt?
De Minister heeft gezegd dat er op dit moment geen sprake is van offensieve inzet en dat eigenlijk pas van offensieve cybercapaciteit kan worden gesproken in 2015. Zegt zij daarmee ook dat er geen offensieve inzet zal zijn voordat die doctrine bij de Kamer ligt? Mag ik dat zo uitleggen? Of zegt ze: nee, wij bouwen die capaciteit en die is in 2015 operationeel, ongeacht die doctrine?
Ik wil toch nog iets zeggen over internationale samenwerking. De Minister zegt dat er wel 20.000 cybersoldaten zijn in China, maar dat wij nog maar moeten zien wat die capaciteit inhoudt. Als ik haar eigen Commandant der Strijdkrachten mag geloven en ook het dreigingsbeeld van China dat wordt beschreven, is zowel de kwantiteit als de kwaliteit van de capaciteit in China op dit terrein niet onaanzienlijk. Is er gezien die behoorlijke capaciteit van China en ook van Rusland geen ruimte, ondanks de gevoeligheid van samenwerking op dit terrein, om toch nog meer samen te werken binnen de NAVO dan wij nu al doen? Ik zeg dat ook omdat, zoals de Minister al zei, ook een digitale aanval kan worden opgevat als iets wat onder artikel 5 valt. Dat is een politiek besluit. Een reactie – wij moeten maar zien of die reactie digitaal is of fysiek – zou dan ook gezamenlijk moeten worden uitgevoerd. Dan hoop je dat niet alleen aan de defensieve kant wordt samengewerkt, maar dat wij ook aan de offensieve kant capaciteiten hebben die goed op elkaar aansluiten. Ik hoor daar graag nog iets over.
In de «echte wereld» is het relatief makkelijk om te achterhalen wie wie aanvalt. Dat is in de digitale wereld niet het geval. Ik neem Estland maar even als voorbeeld. Daar werd in eerste instantie Rusland verdacht van een grote cyberaanval, maar die bleek uiteindelijk afkomstig te zijn van een Estse student van Russische afkomst. Met welke zekerheid kunnen wij de herkomst van zulke aanvallen achterhalen? Hoe wordt ermee omgegaan als je je hebt vergist? Ook dat kan ik mij namelijk voorstellen in die digitale wereld.

De **voorzitter**: De Minister kan gelijk antwoorden. Ik geef haar daartoe het woord.

Minister **Hennis-Plasschaert**: Voorzitter. Hoe ga je om met gevallen waarin je je hebt vergist? Ik mag vanzelfsprekend hopen dat wij nooit in zo'n situatie terechtkomen. Je moet er alles aan doen om zeker te weten wie je voor je hebt voordat je tot een aanval overgaat. Dat is ook precies waarom het niet mogelijk is om in een split second of in 24 uur een besluit te nemen. Dat luistert inderdaad allemaal heel nauw. Het is in bepaalde omstandigheden helemaal niet eenvoudig om te achterhalen van wie de aanval komt. Het voorbeeld dat de heer Sjoerdsma aanhaalt, is natuurlijk heel sprekend. De hele wereld had al een oordeel klaar en toen bleek dat het toch wat anders in elkaar stak.
Verschillende woordvoerders hebben gesproken over samenwerking binnen de NAVO en de EU. Ik denk dat inmiddels duidelijk is dat ik een groot voorstander ben van het vergroten van ons militaire handelingsvermogen door verregaande internationale samenwerking. Dat geldt ook voor cyber, maar daar past nog wel wat meer zorgvuldigheid dan bij de

meer conventionele wapensystemen. Er worden schoorvoetend eerste stappen gezet. Dat heb ik net geschetst. Wat betreft inlichtingen, defensief en offensief, zie je grote terughoudendheid waar het gaat om offensief. Bij defensief zie je meer de neiging om te delen, te faciliteren et cetera. Ik ga ervan uit dat dat er de komende tijd stappen voorwaarts worden gezet, maar je moet het wel de tijd geven. De ontwikkelingen in het cyberdomein zullen een enorme vlucht nemen. Dat is onmiskenbaar waar en daar hoeven wij ook niet heel ingewikkeld over te doen. Nederland speelt daar een belangrijke rol in. Wij hebben in september een NAVO-top. Cyber zal daar een belangrijk onderwerp zijn en ook terugkomen in de deliverables. Ik weet niet of ik de heer Sjoerdsma al helemaal kan gaan bedienen op de meer offensieve capaciteit in het kader van de NAVO. Dat de NAVO-lidstaten en ook de EU-lidstaten de handen veel meer ineen moeten gaan slaan, is echter eigenlijk wel evident.
Er is gevraagd naar de doctrine en de capaciteit. Ik zei net al dat de offensieve capaciteiten op dit moment in ontwikkeling zijn. De doctrine is in hoofdlijnen in de steigers gezet en wordt nu verder uitgewerkt aan de hand van de oefeningen waarin capaciteiten worden getoetst. In feite is er dus sprake van een parallelle ontwikkeling. Er moet wel een doctrine zijn voordat de capaciteiten uiteindelijk daadwerkelijk worden ingezet. De heer Van Dijk sprak een paar keer over de spelregels en de doctrine. Ik acht de doctrine cruciaal, maar de spelregels worden natuurlijk ook bepaald door de kaders zoals ik die aan het begin van mijn beantwoording heb geschetst. Wie is waarvoor verantwoordelijk? Voor inlichtingen is de Wiv leidend. V en J is verantwoordelijk waar het gaat om strafrecht. Ook heb ik het humanitair oorlogsrecht genoemd, et cetera. Dat zijn natuurlijk vooral de spelregels waar we ons aan dienen te houden. We zijn dus al een heel eind.
De heer Vuijk vroeg heel specifiek iets over de bescherming van medewerkers uit de private sector die door de overheid zijn ingezet. Daar moest ik even over nadenken. Ik heb er even geen beeld bij. Ik wil me daar wat verder in verdiepen. Ik was van plan om later dit jaar, dus eind 2014, de cyberstrategie te actualiseren. Deze wil ik dan in het eerste kwartaal van 2015 gereed hebben. Daarmee zal ik de Kamer informeren. Het is ook de bedoeling dat bij deze actualisatie de doorontwikkeling wordt beschreven, inclusief de financiële kaders voor de toekomst. Dat lijkt mij een mooi moment om met elkaar het debat aan te gaan over de vraag waar wij staan. Aan de hand daarvan kunnen wij bijvoorbeeld een vast jaarlijks moment afspreken voor een update of een actualisatie van die cyberstrategie, juist omdat de ontwikkelingen snel gaan.
De heer Sjoerdsma wees mij terecht op mijn woordgebruik bij mijn uitleg over de verdeling van verantwoordelijkheden tussen V en J en Defensie. Ik ga weer terug naar mijn inleiding, waarin ik de kaders heb geschetst van wie waarvoor verantwoordelijk is. Ik moest zelf even teruggaan in de tekst. De discussie heeft met name te maken met de toegenomen verwevenheid tussen het civiele en het militaire domein. Wij zijn op dit moment met een gezamenlijke werkgroep de mogelijkheden voor die civiel-militaire samenwerking aan de hand van een aantal scenario's verder aan het uitwerken. Er zijn ook nog bepaalde governancevraag-stukken. Daar wordt gezamenlijk onderzoek naar verricht. Dit wordt gedaan door de Universiteit Leiden onder leiding van Beatrice de Graaf. Als ik daar meer informatie over heb, zal ik de Kamer nader informeren.
Er is gevraagd naar de JSCU, een onderdeel van de AIVD en de MIVD. De Ministers van BZK en Defensie zijn gezamenlijk verantwoordelijk voor deze unit. Mevrouw Eijsink had een vraag over problemen met het personeel. Die had ik gemist, maar ik krijg hem hier ingefluisterd.

De **voorzitter**: Misschien kunt u uw vraag nog even verduidelijken, mevrouw Eijsink.

Mevrouw **Eijsink** (PvdA): Er was een krantenbericht – volgens mij aan de kant van Defensie niet onbekend – dat een van de medezeggenschapsraden een rechtszaak heeft aangespannen tegen de samenwerking tussen de AIVD en de MIVD en de verhuizing naar Zoetermeer. Dat is niet onbelangrijk voor de dagelijkse werkwijze, neem ik aan.

Minister **Hennis-Plasschaert**: Nu weet ik waar het over gaat. Dat heeft alles te maken met een aanvullend veiligheidsonderzoek dat ineens van toepassing zou zijn op de MIVD'ers. Dat werd niet als prettig ervaren. Dat staat even los van de enorme wil die er is in beide organisaties om samen te werken, laat daar geen misverstand over bestaan. Inmiddels heeft de geschillencommissie gesproken. Het aanvullende veiligheidsonderzoek is de enige weg voorwaarts. Dat gaan wij doen. Probleem opgelost. Nu gaan wij de wil die er bij de organisaties is mooi vormgeven.

Mevrouw **Eijsink** (PvdA): Even pragmatisch. Als ik een beetje getalsmatig in mijn hoofd heb, gaat het om meer dan 800 medewerkers van de MIVD. Die moeten allemaal door een nieuw veiligheidsonderzoek. Wat gaat betekenen qua tijd? Hoe moet ik mij dat voorstellen? Om welke categorie veiligheidsonderzoek gaat het? Wat gaat het mogelijk betekenen voor de samenwerking en de daadwerkelijke aanwezigheid in Zoetermeer?

Minister **Hennis-Plasschaert**: Ik voorzie geen vertraging en geen grote gevolgen. Het gaat ook niet om een grootschalige nieuw onderzoek, maar om aanvullend onderzoek. Ik weet even niet om hoeveel fte het gaat. Dat kan ik navragen en de Kamer daarover informeren. Er was vooral in het gevoelen even een kleine ergernis ontstaan. Dat is nu geadresseerd. Wij gaan nu met goede moed en een goed humeur voorwaarts.

Mevrouw **Eijsink** (PvdA): Ik moet eerlijk zeggen dat ik het bericht heel erg opmerkelijk vond. Als je bij de AIVD of de MIVD werkt, moet je een verklaring van geen bezwaar hebben en moet je door een hele procedure heen. Maar goed, dat laat ik verder bij de regering.
Ik heb nog een vraag naar aanleiding van de toezegging van de Minister dat wij de cyberstrategie zullen ontvangen. Ik had gevraagd om de Kamer halfjaarlijks op de hoogte te houden. Ik begrijp dat de Minister dat niet direct enthousiast ontvangt. De stand van zaken ten aanzien van de cyberstrategie die wij nu bespreken is van 26 augustus 2013. Dat is ook alweer een halfjaar geleden. Ik vraag de Minister om in elk geval de Kamer in augustus weer te informeren. Anders loopt het te ver uit elkaar. Wij geven de Minister ruimte. Het staat in de kinderschoenen. Wij zeggen dat het snel gaat, dat het transparant moet en dat het complex is. Als wij die ruimte geven, vind ik het te laat als de Kamer pas begin 2015 wordt geïnformeerd. Nogmaals, ik vraag niet om een rapportage. Ik wil gewoon op de hoogte worden gehouden van financiële, operationele en personele ontwikkelingen. Ik wil dat de Kamer op de hoogte wordt gehouden van deze complexiteit, maar ook van de snelle ontwikkelingen en het plan van aanpak.

Minister **Hennis-Plasschaert**: Ik schetste net de planning die wij nu hebben uitgestippeld binnen het departement. Die ligt voor de hand, ook gezien de ontwikkelingen die gaande zijn. Het kost gewoon de nodige tijd. Het is volgens mij pas leuk om te rapporteren als er daadwerkelijk nieuwe stappen zijn gezet. De planning is om aan het einde van dit jaar de cyberstrategie te actualiseren. Die krijgt de Kamer dan begin 2015. Wij kunnen daarbij een jaarlijks moment afspreken om hierover te spreken. Daar ben ik graag toe bereid. Een halfjaar is echt te kort om het verschil te maken in de ontwikkelingen die er zijn. Ik ga dus aan het einde van het jaar actualiseren. De Kamer heeft begin 2015 die actualisatie met een doorkijkje naar de toekomst, ook als het gaat om de financiële kaders.

Mevrouw **Eijsink** (PvdA): Ik vind dat gewoon heel erg laat. Wij spreken hier nu over een notitie van vorig jaar augustus. Ik vraag de Minister nogmaals om de Kamer eerder te informeren. Het gaat nu over 2015 nota bene. Dan zijn wij echt een jaar verder. Dan wordt de Kamer pas weer een keer uitvoerig geïnformeerd over iets wat sterk in ontwikkeling is en kan zij daarover spreken met de Minister. Ik nodig de Minister toch nog één keer uit om de Kamer eerder te informeren.

De **voorzitter**: Ik heb nog een vraag. Er is op 17 maart ook een brief gestuurd. Is het dat soort brief waar u op doelt, mevrouw Eijsink? Volgens mij doelt u beiden op een verschillend niveau van informatie. Is dat het soort brief waar u om vraagt, mevrouw Eijsink?

Mevrouw **Eijsink** (PvdA): Nee, voorzitter. De brief van 17 maart ken ik. Daar was door de Kamer om gevraagd. Het gaat erom dat de Kamer gewoon langs de lijnen van het plan van aanpak, de doctrine, de financiën, de operationele capaciteiten en het personeel wordt geïnformeerd over de stand zaken in de uitwerking. Het lijkt mij niet heel erg lastig, maar ik kan niet voor de Minister spreken. De Kamer geeft de Minister veel ruimte in deze ontwikkeling. Dit is de eerste keer in tweeënhalf jaar dat de Kamer erover spreekt. Ik geef alleen maar aan – ik herhaal mezelf, helaas – dat de Kamer gezien de complexiteit wellicht eerder geïnformeerd zou kunnen worden. Ik denk dat dat goed is voor zowel de Kamer als de regering. Wij zitten immers in missies als die in Mali. Er vinden ontwikkelingen plaats. Meer redenen kan ik niet noemen.

De **voorzitter**: Ik zie dat de heer Sjoerdsma hier ook nog iets over wil zeggen.

De heer **Sjoerdsma** (D66): Niet over dit onderwerp, voorzitter.

De **voorzitter**: U wel, mijnheer Van Dijk?

De heer **Jasper van Dijk** (SP): Nee, ook niet over dit onderwerp.

De **voorzitter**: Ik denk dat het verzoek van de Kamer duidelijk is. Ik vraag u toch om te reageren op het verzoek van mevrouw Eijsink en om aan te geven of u daaraan zou willen voldoen, Minister.

Minister **Hennis-Plasschaert**: De ontwikkelingen gaan snel, maar ook weer niet zo snel. Voor het ontwikkelen van offensieve cybercapaciteiten is de nodige tijd nodig. Die capaciteiten moeten ook worden getoetst in oefeningen. Parallel daaraan wordt de doctrine verder uitgewerkt. Ik kan nu wel zeggen dat ik in augustus een update stuur, maar dan moet er wel iets te updaten zijn. Soms heeft iets meer tijd nodig. Vandaar mijn voorstel om eind 2014 de cyberstrategie te actualiseren. Ik zal dan de Kamer direct informeren. Dat zal dan begin 2015 zijn. Ik zei net nog dat ik dat in het eerste kwartaal zou doen, maar laat ik dan zeggen: in januari 2015. Het is helemaal geen onwil. Ik wil zo graag de Kamer ergens over kunnen informeren, in plaats van met een herhaling van zetten te komen en onnodige rapportagedruk.

De heer **Sjoerdsma** (D66): Het lijkt mij op zich niet onredelijk. De Minister heeft ook toegezegd dat de doctrine voorafgaat aan de offensieve inzet. Dat is volgens mij een duidelijke waarborg van de Minister, als zij toezegt dat wij wat horen als er wat te melden valt. Januari 2015 staat in mijn achterhoofd gegrift.
Ik heb nog een vraag over de JCSU. De Minister zegt dat daar eigenlijk twee Ministers voor verantwoordelijk zijn. Dat maakt het voor de Kamer wel heel lastig om daar iemand op aan te spreken. Als er twee Ministers

verantwoordelijk zijn, is er over het algemeen in de praktijk niemand verantwoordelijk. Hoe ziet de Minister dat?

Minister **Hennis-Plasschaert**: Dat is volgens mij precies waarover wij het debat met elkaar aangaan naar aanleiding van het rapport van de commissie-Dessens. Daar zou ik dit bij willen betrekken. De Minister van BZK en ik zijn beide verantwoordelijk, zeker voor de besluiten die worden getekend.

De heer **Jasper van Dijk** (SP): Ik heb de Minister nog gevraagd of zij nog schriftelijk gaat reageren op het artikel in Vrij Nederland en de daarin geschetste dilemma's.

Minister **Hennis-Plasschaert**: Excuses, die vraag was mij even ontschoten. Ik heb het artikel redelijk gelezen, net als de heer Van Dijk. Ik reageer normaliter met liefde op artikelen. Ik denk echter ook dat wij niet op ieder artikel een schriftelijke reactie hoeven te geven. Ik heb er een aantal dilemma's uitgepikt. Ik heb het artikel met belangstelling gelezen. Het geeft op zich een goed beeld van de huidige stand van zaken. Er wordt ook een aantal mogelijke inzetopties en dilemma's in behandeld. Dat zijn dilemma's die ook hier weer ter tafel komen. Er is wat meer tijd voor nodig om daarop te reageren. Dat spelregels ontbreken voor militair opereren in het cyberdomein, deel ik niet. Ik heb al een paar keer toegelicht waarom, namelijk omdat die regels in beginsel niet verschillen van die voor de inzet van andere wapensystemen. Wij hebben ook nog de rules of engagement die voor elke missie en inzet worden opgesteld. Ik zal het artikel – misschien is dat wel een leuk voorstel – bij mij houden, zeker bij het actualiseren van de cyberstrategie. De dilemma's die in het artikel worden geschetst, zal ik terug laten komen in de actualisatie van de cyberstrategie. Ik ga echter niet een aparte brief sturen aan de Kamer naar aanleiding van het artikel in Vrij Nederland.

De heer **Jasper van Dijk** (SP): Ik vind het een buitengewoon interessante formulering. Ik zal haar teruglezen als het verslag er is. De Minister gaat het artikel bij zich houden en het komt terug bij de actualisatie van januari 2015. Dat klopt toch?

Minister Hennis-Plasschaert: Ja.

De heer **Jasper van Dijk** (SP): Die staat ook in mijn achterhoofd gegrift, vanaf nu.

De **voorzitter**: Prima. Er zijn veel tatoeages toegevoegd vandaag. Ik dank de Minister voor de beantwoording in tweede termijn. De griffier heeft een aantal toezeggingen genoteerd. Die lees ik nog even op.
– Medio 2015 ontvangt de Kamer de doctrine voor het militair optreden in het digitale domein.

Minister **Hennis-Plasschaert**: Nee. Ik ga niet even de doctrine naar de Kamer sturen. Dat ga ik niet doen.

De **voorzitter**: Oké. Ik ga verder met te toezeggingen.
– In juni 2014 ontvangt de Kamer de reservistennota, inclusief passages over cyberreservisten.
– De Kamer ontvangt in januari 2015 de geactualiseerde cyberstrategie en neemt daarin de diverse punten mee zoals vandaag besproken, inclusief het artikel in Vrij Nederland.

Minister **Hennis-Plasschaert**: Voorzitter, niet overdrijven. Het is inclusief de dilemma's die worden geschetst in het artikel in Vrij Nederland.

De **voorzitter**: Ja, precies. Hiermee komt er een einde aan dit algemeen overleg. Ik dank iedereen voor de belangstelling. Ook dank aan de Minister en haar ondersteuning en uiteraard de ondersteuning van de Kamer.

Sluiting 15.55 uur.