Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

33 321 Defensie Cyber Strategie

Nr. 7 **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 15 maart 2016

Voorwaarts in het cyberdomein

Het lijdt geen twijfel dat de snelle ontwikkeling en mondiale verspreiding van digitale technologie tot de meest ingrijpende veranderingen van onze tijd behoren. Ook Defensie heeft nadrukkelijk met deze verandering te maken, waarbij zich zowel kansen als risico's voordoen. Ik hecht groot belang aan de verdere versterking van het vermogen van Defensie om zich in het cyberdomein te weer te stellen, militair-operationeel op te treden en inlichtingen te verzamelen. Tijdens het algemeen overleg van 21 april 2015 over de actualisering van de Defensie Cyber Strategie (Kamerstuk 33 321 nr. 5) heb ik toegezegd u op de hoogte te houden van de uitvoering van deze strategie. Met deze voortgangsrapportage kom ik mijn toezegging na en maak ik duidelijk wat Defensie de komende periode te doen staat.

Aan het begin van deze kabinetsperiode heb ik besloten tot een versnelling van ontwikkeling van cybercapaciteiten bij Defensie. Dit heeft onder meer geleid tot de oprichting van de *Joint Sigint Cyber Unit* (JSCU) van de MIVD en AIVD in 2014 en het Defensie Cyber Commando (DCC) in 2015. In de begroting voor 2015 is extra geld uitgetrokken voor de uitvoering van de Defensie Cyber Strategie. De ontwikkeling van en investering in cybercapaciteiten in landen om ons heen onderstrepen dat we voorwaarts moeten blijven gaan en dat stilstand geen optie is. Naar het oordeel van het kabinet moet Nederland, met zijn hoge internet-dichtheid en als mondiaal knooppunt van digitaal verkeer, op dit gebied internationaal tot de voorhoede behoren.

Het scheppen van de voorwaarden voor succes

Zoals uit de rapportage blijkt, heeft Defensie het afgelopen jaar opnieuw vorderingen gemaakt met de opbouw van cybercapaciteiten. De geactualiseerde Defensie Cyber Strategie legt het accent op het scheppen van de voorwaarden voor het succesvol opereren in het cyberdomein. Hieraan

kst-33321-7
ISSN 0921 - 7371
's-Gravenhage 2016

hebben de defensieonderdelen het afgelopen jaar, op zichtbare en minder zichtbare manieren, hard gewerkt. «Cyber» staat immers niet op zichzelf, maar raakt alle lagen en activiteiten van Defensie.

Defensie besteedt in de beleidsagenda bij de begroting 2016 specifiek aandacht aan het omgaan met en inspelen op kort-cyclische, «klein-schalige» innovaties. Met het oog hierop ontplooit Defensie diverse initiatieven die in het bijzonder van belang zijn in het cyberdomein. De doorlooptijden en bestedingslimieten in het verwervingsproces behoren tot de grootste belemmeringen voor snelle en effectieve innovatie in het cyberdomein. Daarom worden de mogelijkheden onderzocht om sneller van behoeftestelling tot de inzet van het materieel te komen.

Ook onderzoekt Defensie hoe het hooggekwalificeerde *cyberprofessionals* kan boeien en binden. Hiertoe wisselt Defensie ervaringen uit met partners binnen en buiten de overheid, worden samenwerkingsmogelijkheden verkend en is in het buitenland gekeken naar ervaringen van andere defensieorganisaties. Defensie zal concrete maatregelen nemen ter versterking van de aantrekkingskracht van Defensie op *cyberprofessionals*. Hierop vooruitlopend is Defensie al gestart met het in kaart brengen van loopbaanpatronen.

Defensie heeft het afgelopen jaar veel geïnvesteerd in de samenwerking binnen Defensie en met partners in binnen- en buitenland. De colocatie van de AIVD en de MIVD op de Frederikkazerne in Den Haag, voorzien voor 2022 (Kamerstuk 30 977 nr. 134), bevordert de bundeling van schaarse kennis en capaciteit op cybergebied. Het voornemen is ook het DCC op deze locatie te vestigen. Voorts heeft Defensie de samenwerking met private partners, kennisinstellingen en de academische wereld geïntensiveerd. Zo is een brigade-generaal van de Militair Juridische Dienst van het Commando Landstrijdkrachten, die was benoemd tot hoogleraar *Cyber Warfare* aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie, dit jaar tevens aangesteld als bijzonder hoogleraar *Military Law of Cyber Operations & Cyber Security* aan de Universiteit van Amsterdam.

Verder ontwikkelen van cybercapaciteiten

Behalve het scheppen van de voorwaarden voor succes, zal Defensie op de ingeslagen weg voortgaan en de defensieve, operationele en inlichtingencapaciteiten verder ontwikkelen. In het kader van het meerjarige perspectief op de ontwikkeling van de krijgsmacht is hiervoor nadrukkelijk aandacht. Verder is de totstandkoming in 2016 van de nieuwe Wet op de inlichtingen- en veiligheidsdiensten, waarin het achterhaalde onderscheid tussen kabel- en niet-kabelgebonden communicatie wordt opgeheven, een voorwaarde om de ambities in het cyberdomein te kunnen verwezenlijken.

De rapportage laat zien dat Defensie binnen de mogelijkheden goed op weg is met de opbouw van cybercapaciteiten, maar ook dat de snelheid van de ontwikkelingen in het cyberdomein een onafgebroken inspanning vereisen. Zoals ik heb aangekondigd in de actualisering van de Defensie Cyber Strategie is in 2016 de start van een beleidsdoorlichting van deze strategie voorzien. Daarin zal ik zowel de opbouw van cybercapaciteiten bezien als de rol van deze capaciteiten bij de bescherming van Nederland

als veilige plaats om te wonen, werken en leven. Ik ben ervan overtuigd dat Defensie met deze aanpak de komende jaren haar cybercapaciteiten verder zal versterken.

De Minister van Defensie,
J.A. Hennis-Plasschaert

Voortgangsrapportage Defensie Cyber Strategie

Inleiding

Deze voortgangsrapportage beschrijft de verdere ontwikkeling van de capaciteiten in het cyberdomein sinds de actualisering van de Defensie Cyber Strategie (de strategie) in februari 2015. De strategie bevat zeven speerpunten waaraan Defensie nadrukkelijk aandacht besteedt:

- Het boeien, binden en ontwikkelen van *cyberprofessionals;*
- De noodzaak van snelle innovatie;
- Krachten bundelen en samenwerking intensiveren;
- Verbreden en verdiepen van de kennis in de organisatie;
- De digitale weerbaarheid van Defensie;
- Het inlichtingenvermogen van Defensie in het cyberdomein;
- Cybercapaciteiten als integraal onderdeel van het militaire optreden.

Deze rapportage schetst per speerpunt de stand van zaken en benoemt de belangrijkste aandachtspunten voor de komende periode.

1. Het boeien, binden en ontwikkelen van cyberprofessionals

De belangrijkste «capaciteit» waarover Defensie moet beschikken zijn slimme, kundige en gemotiveerde *cyberprofessionals*. Diepgaande kennis van het domein is onontbeerlijk en deze schuilt hoofdzakelijk in mensen. Het boeien, binden en ontwikkelen van *cyberprofessionals* vraagt voortdurend aandacht. De strategie beklemtoont de noodzaak van een flexibel personeelsbeleid om aantrekkelijk te zijn voor deze doelgroep. Daarbij dienen talentvolle *cyberprofessionals* zich niet altijd via de ons vertrouwde kanalen aan. Om meer zicht te krijgen op wat *cyberprofessionals* specifiek boeit en aan de organisatie bindt, is een werkgroep ingesteld. De bevindingen van de werkgroep zullen moeten uitmonden in concrete maatregelen ter versterking van de aantrekkingskracht van Defensie op *cyberprofessionals*.

Vooruitlopend op de definitieve conclusies van de werkgroep start Defensie ook met het in kaart brengen van loopbaanpatronen. Dit moet op korte termijn leiden tot meer inzicht in de doorstroommogelijkheden voor zowel burgers als militairen binnen Defensie. Doorstroommogelijkheden bevorderen het soepel wisselen van functies in het cyberdomein, waardoor er minder gaten in de organisatie vallen als personeel vertrekt en de kennis voor Defensie behouden blijft. Loopbaanpatronen in het cyberdomein bevorderen de uitdaging in de dagelijkse werkzaamheden, het uitzicht op een carrière bij Defensie, kennisuitwisseling tussen medewerkers en de bredere inzetbaarheid van medewerkers. Op individuele basis is de uitwisseling van personeel bij defensieonderdelen die met cyber te maken hebben al mogelijk. Ook behoren flexibele plaatsingsduur en functietoewijzing tot de mogelijkheden. Daarnaast staan partners buiten Defensie open voor vormen van samenwerking ten behoeve van de ontwikkeling van medewerkers. Hierbij wordt gedacht aan het uitwisselen en detacheren van medewerkers.

Ook de werving en inzet van cyberreservisten is een speerpunt in de strategie. In het afgelopen jaar is vanuit het bedrijfsleven veel enthousiasme getoond om mensen de kans te geven cyberreservist bij Defensie te worden. De prioriteit ligt momenteel bij het werven van reservisten met specifieke kennis van het cyberdomein. Defensie brengt in kaart op welke plekken in de organisatie de kennis en deskundigheid van de reservisten het hardst nodig is.

Tot slot zijn de omstandigheden waaronder *cyberprofessionals* hun werk moeten doen van invloed op de werkbeleving. Belangrijke voorwaarden zijn onder andere het op peil houden van het kennisniveau van de medewerkers en het werken met de nieuwste technologie in flexibele organisatievormen. De speerpunten in de volgende paragrafen hebben voor een belangrijk deel betrekking op het creëren van de optimale werkomstandigheden.

2. De noodzaak van snelle innovatie

Innovatie staat bij Defensie hoog op de agenda. Dit geldt ook voor innovatie in het cyberdomein. De reguliere processen, waaronder controles vooraf en bestedingslimieten, zijn ingericht om verwervingstrajecten zorgvuldig te laten verlopen. Ze kosten hierdoor echter wel veel tijd. In het cyberdomein gaan de ontwikkelingen razendsnel en is er vaak sprake van innovatiecycli van maanden in plaats van jaren. De ontwikkeling van digitale technologie laat zich bovendien moeilijk voorspellen. Tot de grootste belemmeringen voor snelle en effectieve innovatie in het cyberdomein behoren dan ook de doorlooptijden in de verwervingsketen. Defensie wil het mogelijk maken om sneller van de behoeftestelling tot de inzet van materieel te komen, zonder aan zorgvuldigheid in te boeten. Het verwerven van materieel dat nodig is om de strategie uit te voeren maakt hier nadrukkelijk deel van uit.

Innoveren is niet alleen noodzakelijk in het cyberdomein maar ook op andere terreinen. Innovatie heeft daarom een prominente plek in de beleidsagenda bij de begroting van Defensie. Defensie beziet op dit ogenblik aan welke voorwaarden zij moet voldoen om innovatief en adaptief te kunnen zijn en welke initiatieven daarvoor nodig zijn. Hiervoor leggen medewerkers werkbezoeken af aan publieke en private partners en interviewen zij de belangrijkste betrokkenen bij Defensie en daarbuiten.

3. Krachten bundelen en samenwerking intensiveren

De cyberstrategie van Defensie berust op een geïntegreerde aanpak en bundelt zoveel mogelijk schaarse cyberkennis, middelen, personeel en capaciteiten. Voorts is nauwe samenwerking met nationale en internationale partners van wezenlijk belang om de doelen in het cyberdomein te bereiken.

In 2015 is uw Kamer geïnformeerd over het voornemen de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) gezamenlijk onder te brengen op de Frederikkazerne in Den Haag (Kamerstuk 30 977, nr. 134). Dit moet leiden tot meer samenwerking en meer uitwisseling van kennis en informatie. Er wordt ook gedacht aan het onderbrengen van andere cyberorganisaties in hetzelfde pand, zoals het Defensie Cyber Commando (DCC). De mogelijkheden en de gevolgen worden op dit ogenblik onderzocht. Het gezamenlijk huisvesten van organisatieonderdelen die vergelijkbare werkzaamheden uitvoeren en vergelijkbare middelen nodig hebben, bevordert het geïntegreerde werken bij Defensie en met partners.

Het bundelen van krachten gebeurt ook op andere manieren, zoals met bijeenkomsten voor alle *cyberprofessionals* bij Defensie. In deze bijeenkomsten praten zij elkaar bij over de laatste ontwikkelingen en wisselen ze nieuwe ideeën uit. Ook op het hoogste niveau staat cyber hoog op de agenda. Dit blijkt onder andere uit de reguliere bijeenkomsten met alle commandanten van onderdelen die met cyberactiviteiten te maken hebben. Deze bijeenkomsten bevorderen coherente beleidsvorming en -uitvoering.

Defensie werkt veel samen met nationale partners, waaronder het Nationaal Cyber Security Centrum (NCSC). Onder coördinatie van het NCSC levert Defensie bijdragen aan een gezamenlijk beeld van digitale dreigingen, op grond waarvan jaarlijks het Cyber Security Beeld Nederland wordt uitgebracht. Ook de inlichtingen- en veiligheidsdiensten werken intensief samen. Naast de voorgenomen colocatie, is de *Joint Sigint Cyber Unit* (JSCU) een belangrijk voorbeeld van de samenwerking tussen de MIVD en de AIVD.

De Koninklijke Marechaussee (KMar) zet samen met de gezagsdrager, de Minister van Veiligheid en Justitie, stappen om voldoende toegerust te zijn in het cyberdomein. Om de rechtshandhavingsketen volledig te sluiten werkt de KMar ook samen met de Nationale Politie. Daartoe moet de KMar op een aantal taakvelden in het cyberdomein investeren, zoals de militaire politietaak, de politietaak op luchthavens en de grenstoezichttaak. Samen met de Nationale Politie beziet de KMar hoe de voorziene nieuwe bevoegdheden, zoals omschreven in het voorstel tot aanpassing van de strafwetgeving («Wet Computer Criminaliteit 3»), in de praktijk kunnen worden vormgegeven.

Defensie werkt steeds intensiever samen in internationaal verband. Defensie zoekt bilateraal naar samenwerking met gelijkgestemde landen en multilateraal in EU en Navo-verband. Daarnaast neemt Nederland actief deel aan het *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) in Estland.

Naast publieke partners in binnen- en buitenland, werkt Defensie samen met private partners, kennisinstellingen en de academische wereld. Een voorbeeld van de geslaagde samenwerking is de relatie van de Nederlandse Defensie Academie en de Universiteit van Amsterdam. Zo is een brigade-generaal van de Militair Juridische Dienst van het Commando Landstrijdkrachten hoogleraar *Cyber Warfare* aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie, en tevens bijzonder hoogleraar *Military Law of Cyber Operations & Cyber Security.* Hij zal zich in verband met het juridische karakter van de leerstoel onder andere bezighouden met veiligheid in het cyberdomein en met de rol van de krijgsmacht en de legitimiteit van overheidsoptreden. Ook met private partners werkt Defensie succesvol samen. De opleiding voor *cyberprofessionals* die Defensie samen met Fox-IT verzorgt, is hiervan het voornaamste voorbeeld. De eerste lichting heeft de opleiding reeds doorlopen en onlangs is een tweede groep met de opleiding gestart.

4. Verbreden en verdiepen van de kennis in de organisatie

Het breed verspreiden van kennis over het cyberdomein binnen Defensie is van groot belang, omdat alle medewerkers zich bewust moeten zijn van de kansen en kwetsbaarheden die daarmee gepaard gaan. Meer kennis bij medewerkers verhoogt ook de digitale weerbaarheid van Defensie. Daarom moet Defensie in opleidingen, trainingen en oefeningen structureel aandacht schenken aan het fenomeen «cyber». Om het cyberbewustzijn van de defensiemedewerkers te vergroten organiseert Defensie regelmatig bewustwordingsprogramma's.

5. De digitale weerbaarheid van Defensie

Zowel in militaire operaties als in de reguliere bedrijfsvoering is Defensie sterk afhankelijk van hoogwaardige communicatie- en informatiesystemen, genetwerkte wapensystemen en logistieke systemen. Daarnaast neemt de hoeveelheid data die besloten ligt in bijvoorbeeld sensoren, wapensystemen en commandosystemen (SEWACO-systemen) en

netwerken exponentieel toe. Defensienetwerken en -systemen zijn voorts gevoelig voor manipulatie tijdens de ontwikkeling en de productie en gedurende transport en onderhoud. Niet alleen de beveiliging van systemen en netwerken, maar ook die van de informatie zelf is van wezenlijk belang. Hierbij staan de exclusiviteit, de integriteit en de beschikbaarheid van informatie voorop.

De snelheid waarmee nieuwe digitale dreigingen zich manifesteren, vragen op meer vlakken om een intensieve aanpak. Om de digitale weerbaarheid te verhogen is in 2015 het Defensie *Computer Emergency Response Team* (DefCERT) versterkt en is begonnen met de oprichting van het *Security Operations Center* (SOC). In het SOC werken de beheerorganisaties samen om de netwerken en systemen van Defensie in Nederland en in operatiegebieden 24 uur per dag te beschermen. In 2016 zal Defensie het SOC voor een deel operationeel hebben. In 2017 moet het volledig operationeel worden.

De maatregelen om de eigen informatievoorzieningssystemen (IV-systemen) veilig te houden, maken deel uit van de diensten en producten die het Joint IV Commando (JIVC), waaronder het DefCERT, en de directie *Operations* van de Defensie Materieel Organisatie leveren. Belangrijk onderdeel van de bestaande aanpak is het voorkomen en beperken van acties van zogeheten *insider threats*.

Ondanks alle maatregelen is de voortdurende ontwikkeling van de digitale weerbaarheid geboden. Daarom ontwikkelt Defensie een *roadmap* voor verbeteringen in het IT-domein op het gebied van innovatieve beschermings-, detectie- en mitigatiemaatregelen. Omdat Defensie de beveiliging van haar systemen doorlopend moet vernieuwen, is in de *roadmap* specifiek aandacht besteed aan innovatie. Ook leveranciers worden in toenemende mate verplicht maatregelen te nemen om hun digitale weerbaarheid te verhogen. De maatregelen hebben bijvoorbeeld betrekking op de beveiliging van de IT-voorzieningen en het garanderen van een cyberveilige *supply chain* van toeleveranciers. In de modernisering van de Algemene Beveiligingseisen Defensie Opdrachten (ABDO) wordt digitale veiligheid een volwaardig onderdeel van de beveiligingseisen. Voor het toezicht hierop is met een team van cyber-revisoren specifieke deskundigheid voorhanden. Daarnaast wordt bedrijven geadviseerd om de door het NCSC beschreven algemene preventiemaatregelen in acht te nemen.

6. Het inlichtingenvermogen van Defensie in het cyberdomein

De dreiging van digitale spionage tegen Defensie, toeleveranciers, bondgenootschappelijke netwerken en producenten van militair-relevante producten is aanzienlijk (zie voor een uitgebreide analyse het Cybersecurity Beeld Nederland, Kamerstuk 26 643 nr. 369). Deze dreiging neemt in omvang toe, wordt steeds agressiever en geavanceerder en is vanuit het perspectief van de aanvaller ongeëvenaard succesvol. Waar buitenlandse inlichtingendiensten met alle risico's van dien[1] voorheen vooral gebruikmaakten van agenten, kan tegenwoordig veelal worden volstaan met een handeling vanaf een anonieme computer.

Aanvallen van statelijke actoren worden doorgaans niet gedetecteerd door commerciële producten. Daarom doet de MIVD daar zelf actief onderzoek naar. Met behulp van de MIVD slaat Defensie dagelijks aanvallen van statelijke actoren af. De onderzoeken komen bovendien de verdediging van de defensienetwerken ten goede. Door de deelneming

[1] Zoals valse paspoorten en identiteiten, kans op diplomatieke incidenten, fysieke veiligheid

van de MIVD aan het Nationaal Detectie Netwerk (NDN) draagt Defensie ook bij tot de bescherming van de rijksoverheid en het bedrijfsleven.

Mede als gevolg van de snel toegenomen dreigingen en de groeiende vraag naar producten, heeft Defensie verder geïnvesteerd in het inlichtingenvermogen in het cyberdomein. Voor het verder ontwikkelen van cybercapaciteiten zijn voorts investeringen nodig in geavanceerde beveiligingsmiddelen en onderzoeken naar de aanwezigheid en herkomst van vreemde actoren op netwerken. Bovenal is aanpassing van het wettelijke kader nodig. De wet op de Inlichtingen- en Veiligheidsdiensten 2002 (Wiv) stamt van voor de tijd dat de uitdagingen in het cyberdomein in beeld kwamen. Om de diensten in staat te stellen ook in dit domein hun taken naar behoren te kunnen vervullen werkt het kabinet aan het vernieuwen van de Wiv.

De strategie is verder gericht op het versterken van de JSCU en van de samenwerking van de MIVD met de AIVD. De beide diensten overleggen altijd over investeringsvoorstellen ten behoeve van de JSCU en er zijn inmiddels onderwerpen in het cyberdomein opgenomen in het Geïntegreerde Aanwijsbesluit. Hierdoor worden de financiële middelen en inlichtingencapaciteit zo effectief mogelijk ingezet.

7. Cybercapaciteiten als integraal onderdeel van het militaire optreden

Sinds 2012 heeft Defensie door middel van de *Taskforce* Cyber gewerkt aan de opbouw van cybercapaciteiten. Met de formele oprichting van het DCC in juni 2015 heeft Defensie een belangrijke mijlpaal bereikt in de opbouw van operationele cybercapaciteiten. De komende periode werkt Defensie aan het volledig operationaliseren van het DCC. Wanneer het DCC aan alle voorwaarden voldoet om operationele cybercapaciteit te ontwikkelen, is het volledig operationeel. Dat betekent onder meer dat al het benodigde personeel opgeleid op functie is, de infrastructuur aan de eisen voldoet, het cyberlaboratorium operationeel is en de cyberdoctrine gereed en getest is. Het DCC en de andere betrokken defensieonderdelen werken met prioriteit aan het vervullen van de voorwaarden en verwachten het DCC eind 2016 operationeel te hebben.

De huidige cybersecurity-aanpak kenmerkt zich door de nadruk op de dreigingen en de weerbaarheid, ofwel de verdediging. Bij de verdediging tegen cyberaanvallen is het van belang deze te kunnen herkennen, erop te kunnen reageren en ervan te kunnen herstellen. Uitsluitend aandacht besteden aan verdedigen vergt een grote financiële en personele investering, terwijl de aanvaller zich niet geremd voelt door een potentiële offensieve tegenactie. De aanvaller kan dus ongestoord aanvallen en loopt daarbij weinig risico. Offensieve cybercapaciteiten hebben tot doel het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Met de combinatie van detecterende en offensieve cybercapaciteiten kunnen niet alleen effectieve tegenmaatregelen worden genomen, maar worden aanvallers ook afgeschrikt. Een offensieve cybercapaciteit is een *force multiplier* die de effectiviteit van de krijgsmacht vergroot.

Het DCC is opgericht om operationele cybercapaciteiten voor de ondersteuning van militaire missies te creëren en de inzet ervan te coördineren. Operationele digitale middelen bestaan uit het geheel van de kennis, de middelen en het conceptuele kader om in een militaire operatie het handelen van tegenstanders te voorspellen, te beïnvloeden of onmogelijk te maken. Ook het vermogen eigen eenheden tegen vergelijkbaar handelen door een tegenstander te beschermen is onderdeel van de operationele cybercapaciteit. Operationele digitale middelen bevatten dus defensieve, offensieve en inlichtingenelementen. DMO/JIVC ondersteunt

de operationele commandant primair bij de uitvoering van de defensieve taken. Op inlichtingengebied wordt hoofdzakelijk gebruikgemaakt van de MIVD. De KMar heeft de taak om de rechtmatigheid van de inzet van offensieve elementen te toetsen. Al deze elementen maken onlosmakelijk deel uit van operationele cybercapaciteiten en daarmee van het moderne militaire optreden.

De komende periode besteedt Defensie nadrukkelijk aandacht aan het inzichtelijk maken van de mogelijkheden die het cyberdomein biedt voor operaties. Bewust nadenken over de kansen en bedreigingen in het cyberdomein, als onderdeel van het planningsproces en in militaire oefeningen, vergroot dit inzicht. Het DCC zal bijvoorbeeld samen met de directie Operaties en andere onderdelen van de Defensiestaf regelmatig *table top exercises* doorlopen. Reeds in 2015 heeft het DCC een bijdrage geleverd aan oefeningen van het Duits-Nederlands Legerkorps en de *Netherlands Maritime Force* (NLMARFOR). Al deze activiteiten leiden er uiteindelijk toe dat Defensie goed is voorbereid op het moment dat cybercapaciteiten in werkelijke operaties moeten worden ingezet.

Conclusie

Het afgelopen jaar heeft Defensie op een aantal speerpunten concrete voortgang geboekt. Zo is de samenwerking met publieke en private partners geïntensiveerd en zijn waardevolle stappen gezet in het bundelen van de krachten binnen Defensie. Ook is de digitale weerbaarheid van Defensie verhoogd en zijn cybercapaciteiten verder geïntegreerd in het militaire optreden en de voorbereiding daarop.

Op andere terreinen verwacht Defensie op korte termijn de vruchten te kunnen plukken van lopende activiteiten. De huidige onderzoeken naar het boeien en binden van *cyberprofessionals*, het innovatievermogen van Defensie en de doorlooptijden in het verwervingsproces worden binnenkort voltooid. De resultaten en aanbevelingen leiden tot maatregelen die succesvol opereren in het cyberdomein verder bevorderen. Voorts zal Defensie op de ingeslagen weg voortgaan en de defensieve, operationele en inlichtingencapaciteiten verder ontwikkelen.

Sinds de actualisering van de Defensie Cyber Strategie in 2015 heeft Defensie op verschillende terreinen vorderingen gemaakt. De rapportage laat zien dat Defensie binnen de mogelijkheden goed op weg is met de opbouw van cybercapaciteiten, maar ook dat de snelheid van de ontwikkelingen in het cyberdomein een onafgebroken inspanning vereisen.