Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

33 321 Defensie Cyber Strategie

Nr. 2 **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 augustus 2013

Inleiding

De vaste commissie voor Defensie heeft mij op 13 juni 2013 verzocht haar te informeren over de stand van zaken van de Defensie Cyber Strategie, inclusief een geactualiseerde reactie op het advies van de Adviesraad Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV) over digitale oorlogsvoering. Met deze brief voldoe ik aan dit verzoek.

Achtergrond

Mede naar aanleiding van de in de beleidsbrief 2011 aangekondigde cyberintensivering en de Nationale Cyber Security Strategie (Kamerstuk 26 643, nr. 174), brachten de AIV en de CAVV in december 2011 een advies uit over digitale oorlogsvoering. Dit advies onderschrijft het belang van de digitale weerbaarheid van Defensie en de ontwikkeling van operationele cybercapaciteiten. Het advies belicht tevens het volkenrechtelijke kader voor geweldgebruik in het digitale domein. Daarnaast adviseren de AIV en de CAVV de *signals intelligence* en cybercapaciteiten van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen en Veiligheidsdienst (AIVD) te bundelen in een gezamenlijke eenheid. Tevens doen zij de aanbeveling om te onderzoeken of, gezien de technologische ontwikkelingen, het onderscheid in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) tussen kabelgebonden en niet-kabelgebonden interceptie van telecommunicatie gehandhaafd moet blijven.

Het advies van de AIV en de CAVV en de kabinetsreactie daarop (Kamerstuk 33 000 X, nrs. 68 en 79) zijn onverminderd actueel en vormen de uitgangspunten voor de Defensie Cyber Strategie die mijn ambtsvoorganger in juni 2012 heeft aangeboden aan uw Kamer (Kamerstuk 33 321, nr. 1). Daarnaast onderzoeken de Ministeries van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie momenteel de mogelijkheden voor een wijziging van de Wiv 2002 in overeenstemming met het advies van de

kst-33321-2
ISSN 0921 - 7371
's-Gravenhage 2013

AIV en de CAVV. Ook wordt de Wiv2002 geëvalueerd door de commissie-Dessens. Naar verwachting zal de commissie in september a.s. over haar bevindingen rapporteren. Uw Kamer wordt hierover geïnformeerd.

Defensie Cyber Strategie

De Defensie Cyber Strategie omvat zes speerpunten aan de hand waarvan Defensie de komende jaren haar doelstellingen in het digitale domein zal verwezenlijken:

- de totstandkoming van een integrale aanpak;
- de versterking van de digitale weerbaarheid van Defensie («defensief»);
- de ontwikkeling van militair vermogen om *cyber operations* uit te voeren («offensief»);
- de versterking van de inlichtingenpositie in het digitale domein («inlichtingen»);
- de versterking van de kennispositie en het innovatieve vermogen van Defensie in het digitale domein, met inbegrip van de werving en het behoud van gekwalificeerd personeel («adaptief en innovatief»);
- de intensivering van de samenwerking in nationaal en internationaal verband («samenwerking»).

Voor de periode van 2011 tot 2015 bedraagt de totale intensivering voor de ontwikkeling van cybercapaciteiten bij Defensie € 45 miljoen, inclusief de personele exploitatie. Het zwaartepunt ligt initieel bij de bescherming van netwerken, systemen en informatie en de uitbreiding van de inlichtingencapaciteit in het digitale domein. Defensie zal tevens voldoende capaciteit moeten opbouwen om op de langere termijn operationele cybercapaciteiten te kunnen inzetten in militaire operaties. De geplande cybercapaciteit zal naar verwachting in 2016 gereed zijn. Daarna bedraagt de exploitatie structureel € 21 miljoen per jaar.

Integrale aanpak

Om een integrale aanpak in het digitale domein te verwezenlijken, is intensieve samenwerking tussen de verschillende betrokken defensieonderdelen essentieel. De uitvoering van de Defensie Cyber Strategie is belegd bij verschillende onderdelen van Defensie: de Commandant der Strijdkrachten (CDS), het Commando Landstrijdkrachten (CLAS) als *single service manager* voor alle operationele commando's, de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en het Joint Informatievoorzieningscommando (JIVC) van de Defensie Materieel Organisatie (DMO). Zij maken alle deel uit van de Stuurgroep Cyber, die verantwoordelijk is voor de aansturing van het cyberintensiveringprogramma van Defensie. Namens het Ministerie van Veiligheid en Justitie heeft de directeur Cybersecurity van de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) zitting in de stuurgroep. Ook TNO neemt deel aan de stuurgroep. De in 2012 opgerichte Taskforce Cyber (TFC) is verantwoordelijk voor de coördinatie van de aan de intensivering verbonden activiteiten binnen Defensie. Hiermee is de basis gelegd voor een integrale aanpak, die de komende jaren bij de verdere ontwikkeling van cybercapaciteiten nader vorm zal krijgen.

Defensief

Het Defensie Computer Emergency Response Team (DefCERT) maakt deel uit van het JIVC en waakt over de beveiliging van de netwerken en systemen. DefCERT monitort en analyseert digitale kwetsbaarheden en adviseert en ondersteunt bij cyberincidenten door het aandragen van mogelijke oplossingen. DefCERT werkt binnen Defensie nauw samen met

de MIVD en de operationele commando's en daarbuiten met het Nationaal Cyber Security Centrum (NCSC) van de NCTV, de Navo, andere CERT's en met bedrijven die over specifieke kennis of middelen beschikken.

DefCERT is inmiddels operationeel en ondersteunt de beveiliging van de meest kritieke defensienetwerken. Tijdens de recente door het *Cooperative Cyber Defence Centre of Excellence* (CCD COE) georganiseerde internationale oefening *Locked Shields* heeft DefCERT een internationaal aansprekend resultaat neergezet. De aanschaf van een aantal materiële voorzieningen voor het detecteren van mogelijke bedreigingen en anomalieën, heeft enige vertraging vanwege de reorganisatie. De betrokken defensieonderdelen zetten zich in om dit proces te versnellen. Naar verwachting zal DefCERT eind 2014 op volle sterkte zijn.

Offensief

Defensie zal geen afzonderlijk krijgsmachtdeel oprichten voor het optreden in het digitale domein. Bij de ontwikkeling en de inzet van offensieve operationele cybercapaciteiten door de CDS zal daarom zoveel mogelijk gebruik worden gemaakt van kennis en middelen die bij de MIVD aanwezig zijn. Gezien de schaarste aan gekwalificeerd personeel moeten kennis en middelen zo doelmatig mogelijk worden ingezet en moet worden voorkomen dat binnen Defensie capaciteiten dubbel worden ontwikkeld. De TFC zal in de tweede helft van 2013, in overleg met betrokken departementen, een doctrine opstellen voor het militair optreden in het digitale domein, inzetscenario's ontwikkelen en de gevolgen van de militaire inzet van offensieve middelen nader beschrijven. De daarvoor in aanmerking komende cybercapaciteiten zoals het Defensie Cyber Expertise Centrum (DCEC) en het militaire vermogen om *cyber operations* («offensief») uit te voeren worden als joint eenheid ondergebracht bij het op te richten Defensie Cyber Commando (DCC) dat onder *single service management* van het CLAS wordt opgezet. De TFC zal opgaan in het DCC dat eind 2015 operationeel zal zijn.

Inlichtingen

Een hoogwaardige inlichtingenpositie in het digitale domein is een voorwaarde voor zowel de bescherming van de eigen infrastructuur als voor de goede uitvoering van (militaire) operaties. De MIVD doet onderzoek naar alle actoren die een cyberdreiging vormen voor de Nederlandse krijgsmacht en de defensie-industrie. De MIVD detecteert, analyseert en duidt digitale aanvallen en digitale spionage en beschikt over het vermogen om inlichtingenactiviteiten van anderen te verstoren en een halt toe te roepen. In 2012 is de cybercapaciteit van de MIVD versterkt en in de periode van 2013 tot en met 2015 wordt deze verder uitgebreid.

Een deel van de cyberintensivering bij de MIVD wordt ondergebracht bij een gezamenlijke *signals intelligence* (SIGINT)-cybereenheid van de MIVD en de AIVD (project Symbolon). Ook de Nationale Sigint Organisatie (NSO) zal opgaan in deze eenheid, die in de loop van 2014 van start gaat. Vooruitlopend hierop is eind 2012 een kwartiermakerorganisatie ingesteld, bestaande uit delen van de MIVD en de AIVD die tot de gezamenlijke eenheid zullen gaan behoren.

Adaptief en innovatief

De snelheid waarmee ontwikkelingen in het digitale domein zich voltrekken, stelt hoge eisen aan het adaptieve en innovatieve vermogen van Defensie. Defensie moet daarom over de kennis beschikken om

relevante ontwikkelingen te volgen en snel en doeltreffend hierop in spelen. Begin 2014 wordt het Defensie Cyber Expertise Centrum (DCEC) opgericht dat zal fungeren als centraal punt voor kennisontwikkeling, -verankering en -verspreiding op het gebied van cyber, en onder meer intensief samenwerken met het NCSC en TNO. Naar verwachting zal het DCEC eind 2015 op volle sterkte zijn. Het DCEC zal deel uitmaken van het DCC.

Defensie neemt tevens deel aan de Nationale Cyber Security Research Agenda, aan verschillende Navo en EU-programma's en aan CCD COE in Tallinn. Ter voorbereiding op de inrichting van een leerstoel in 2014 is in 2012 een Universitair Hoofddocent Cyber Operations aangesteld bij de Nederlandse Defensie Academie. Daarnaast ontwikkelt de Taskforce Cyber een opleidingsplan om de cyberkennis binnen Defensie te vergroten.

Voor de algemene cyber bewustwording is voor alle defensiemedewerkers ondertussen een elektronische leeromgeving beschikbaar en worden simulatietrainingen georganiseerd. Onlangs heeft de departementale leiding daaraan deelgenomen.

Samenwerking

Defensie werkt intensief samen met andere partijen in Nederland om de nationale digitale weerbaarheid te vergroten en levert een bijdrage aan het Nationale Cyber Security Beeld. Defensie levert bijdragen aan de tweede Nationale Cyber Security Strategie die zich richt op een integrale aanpak van digitale weerbaarheid en digitale dreigingen. Tevens heeft Defensie een liaison bij het NCSC en hebben zowel DefCERT als de MIVD samenwerkingsafspraken met het NCSC over wederzijdse ondersteuning en samenwerking.

De (operationele) cybercapaciteiten (zowel defensief als offensief) van de krijgsmacht kunnen net als de overige defensiecapaciteiten op verzoek van en onder gezag van civiele autoriteiten worden ingezet. Wederzijds kunnen ook civiele cybercapaciteiten worden ingezet ter ondersteuning van Defensie in het geval van ernstige cyberincidenten of dreigingen tegen militaire doelen in Nederland. De mogelijkheden hiertoe worden onderzocht door een gezamenlijke werkgroep van de Ministeries van Defensie en Veiligheid en Justitie.

In internationaal verband werkt Defensie onder andere samen binnen de Navo.
In 2011 is een nieuw Navo Cyber Defence Beleid en bijbehorend Actieplan vastgesteld, waarbij het zwaartepunt ligt bij de bescherming van de eigen netwerken en systemen van Navo. Defensie ondersteunt de verdere ontwikkeling en uitvoering van dit beleid. Nederland is een van de tien *sponsoring nations* van het CCD COE in Tallinn. Op uitnodiging van het CCD COE heeft een internationale groep van experts de *Tallinn Manual on the International Law Applicable to Cyber Warfare* geschreven, een weergave van het toepasselijk recht tijdens digitale oorlogvoering. Dit handboek is begin 2013 gepubliceerd. De regering is van mening dat het een waardevolle bijdrage levert aan de discussie over de juridische kaders van digitale oorlogvoering. Ook neemt Defensie deel aan het *Multinational Cyber Defence Capability Development*[1] programma en de

[1] Het *Multinational Cyber Defence Capability Development* dat onder leiding van Canada door het *NATO Communication and Information systems Agency* (NCIA) wordt uitgevoerd, richt zich voornamelijk op kennisdeling en het verhogen van het gemeenschappelijk omgevingsbeeld op het gebied van *cyber.*

Multinational Capability Development Campaign[2] van de Navo. Daarnaast neemt Defensie deel aan diverse internationale oefeningen, workshops en andere initiatieven die samenwerking en onderling begrip bevorderen. Nederland is ook nauw betrokken bij de ontwikkeling van de cyberstrategie van de EU. Deze strategie behelst onder andere de ambitie een gemeenschappelijk veiligheids- en defensiebeleid te ontwikkelen (GVDB) op het gebied van cyber. Hierbij staan het delen van informatie, gezamenlijke oefeningen, civiel-militaire samenwerking en nauwe samenwerking en afstemming met de NAVO centraal.

Vervolg

Het cyberdomein is voor Defensie van toenemend belang. Op 10 december a.s. heeft de vaste commissie voor Defensie mij uitgenodigd voor een algemeen overleg over de Defensie Cyber Strategie en het advies van de AIV en de CAVV over digitale oorlogsvoering. Dit biedt de gelegenheid nader in te gaan op de stand van zaken van de ontwikkeling van cybercapaciteiten bij Defensie.

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

[2] Het *Multinational Capability Development Campaign* is een programma van *Allied Command Transformation* (ACT) en wordt gezamenlijk geleid door Italië en Noorwegen. Dit programma heeft als doel *cyber* te integreren in het operationele planningsproces van de Navo.