Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

33 321 Defensie Cyber Strategie

Nr. 5 **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 februari 2015

Inleiding

Een van de meest ingrijpende veranderingen sinds het begin van deze eeuw is de exponentiële ontwikkeling en de massale en mondiale verspreiding van digitale technologie. Defensie wordt op tal van manieren geconfronteerd met de gevolgen van deze «digitale revolutie». Deze «revolutie» biedt kansen om de doeltreffendheid en de doelmatigheid van het militaire optreden wezenlijk te bevorderen, maar levert tegelijkertijd niet te veronachtzamen risico's op voor het ongestoorde functioneren van de defensieorganisatie en de nationale veiligheid. Om in het digitale tijdperk voorop te blijven lopen en digitale dreigingen het hoofd te bieden, wil Defensie de komende jaren de krachten bundelen en de samenwerking met haar partners verdiepen. Defensie zal zich verder moeten ontwikkelen tot een slagvaardige en op innovatie gerichte organisatie, die erin slaagt *cyberprofessionals* te blijven boeien en binden. Daarop is deze actualisering van de Defensie Cyber Strategie gericht.

De Defensie Cyber Strategie (Kamerstuk 33 321, nr. 2) van juni 2012 heeft de afgelopen jaren richting, samenhang en focus gegeven aan de integrale aanpak van de ontwikkeling van het militaire vermogen in het digitale domein. Het gaat hierbij om defensieve, offensieve en inlichtingenmiddelen. Defensie erkende in deze strategie dat digitale middelen in toenemende mate integraal deel uitmaken van het militaire optreden. Sinds enkele jaren wordt het digitale domein (*cyberspace*) in bondgenootschappelijk verband beschouwd als het vijfde domein voor militair optreden, naast het land, de lucht, de zee en de ruimte. Defensie wil van dit domein optimaal gebruik maken om haar effectiviteit te vergroten. De Defensie Cyber Strategie onderstreepte bovendien dat de afhankelijkheid van digitale middelen op een breed terrein tot kwetsbaarheden leidt die urgente aandacht behoeven.

De afgelopen twee jaar heeft Defensie forse stappen gezet. De intensivering die is ingezet met de beleidsbrief *Defensie na de kredietcrisis* van

kst-33321-5
ISSN 0921 - 7371
's-Gravenhage 2015

8 april 2011 (Kamerstuk 32 733, nr. 1) en de versnelde voortzetting hiervan in het kader van de nota *In het belang van Nederland* (Kamerstuk 33 763 nr. 1), krijgen op dit ogenblik hun beslag. Met de uitbreiding van het Defensie *Computer Emergency Response Team* (DefCERT), de versterking van de inlichtingenpositie in het digitale domein van de MIVD, de oprichting van de Joint Sigint Cyber Unit (JSCU) samen met de AIVD (Kamerstuk 29 924, nr. 113) en de lancering van het Defensie Cyber Commando (DCC) in 2014, is de basis gelegd voor het functioneren en het optreden van Defensie in het digitale domein. De intensivering in de begroting van 2015 van structureel 100 miljoen euro (vanaf 2017) wordt voorts, zoals bekend, voor een deel aangewend om het optreden van Defensie in het digitale domein verder te versterken. Dit betreft een jaarlijkse investering oplopend tot 9 miljoen euro vanaf 2017.

Tegelijkertijd is duidelijk dat de aard, de snelheid en de intensiteit van de ontwikkelingen in het digitale domein nopen tot periodieke actualisering en zo nodig aanpassing van de strategie. Bovendien is sinds het verschijnen van de Defensie Cyber Strategie in 2012 de veiligheidscontext ingrijpend veranderd als gevolg van het destabiliserende optreden van Rusland op het Europese continent, de conflicten in het Midden-Oosten en Noord-Afrika en de daarmee gepaard gaande aanzienlijke terroristische dreiging. De beleidsbrief Internationale Veiligheid van het kabinet (Kamerstuk 33 694 nr. 6) onderstreept dat het kabinet cyberdreigingen juist ook in deze nieuwe veiligheidscontext als één van de belangrijkste aandachtsgebieden voor de toekomst beschouwt.

In het algemeen overleg over digitale oorlogsvoering van 26 maart 2014 heb ik toegezegd de Defensie Cyber Strategie te zullen actualiseren (Kamerstuk 33 321, nr. 4). Met deze brief doe ik deze toezegging gestand. Deze actualisering is bedoeld om de komende jaren richting te geven aan de verdere ontwikkeling van en investering in digitale middelen bij Defensie. De Nationale Cybersecurity Strategie 2 (NCSS 2) van oktober 2013 («Van bewust naar bekwaam») heeft hierbij als rijksbreed kader gediend.[1] Ook voor Defensie geldt dat zij haar bekwaamheid en slagvaardigheid in het digitale domein verder wil verhogen. Op basis van de actualisering zal Defensie in de komende maanden de nodige vervolgstappen nemen, onder andere op het gebied van personeel, verwerving en innovatie in het cyberdomein. Verdiepen en verbinden zijn daarbij kernwoorden.

Speerpunten voor de komende jaren

De uitgangspunten die ten grondslag lagen aan de Defensie Cyber Strategie van 2012 blijven onverminderd van belang. Nu de fundamenten voor defensieve, offensieve en inlichtingenmiddelen zijn gelegd, gaat het in deze actualisering om het verschuiven van accenten, het stellen van nieuwe doelen en het herformuleren van speerpunten.

Met het oog op de benodigde verdere versterking van haar digitale middelen wil Defensie zich de komende jaren richten op het scheppen van de juiste voorwaarden voor succes in het digitale tijdperk. Speerpunten daarbij zijn:

[1] De Minister van Veiligheid en Justitie is verantwoordelijk voor de coördinatie van cyber security in Nederland en de uitvoering van de Nationale Cybersecurity Strategie (NCSC). De NCSS 2 beziet de maatregelen voor *cyber security* als een dynamische balans tussen (nationale en internationale) digitale veiligheid, maatschappelijke groei (de economische en sociale voordelen die digitalisering biedt) en vrijheid (het waarborgen van fundamentele rechten en waarden). De Defensie Cyber Strategie maakt deel uit van deze samenhang door bij te dragen aan de digitale veiligheid van Defensie en de cybercapaciteiten van de krijgsmacht.

1. het boeien, binden en ontwikkelen van cyberprofessionals;
2. het verruimen van de mogelijkheden binnen Defensie om in het digitale domein snel te innoveren;
3. het bundelen van de krachten bij Defensie en het intensiveren van de samenwerking met partners;
4. het verbreden en verdiepen van de kennis over het digitale domein binnen Defensie (inclusief de versterking van de cyber awareness van de gehele organisatie).

Door de komende jaren actief aan deze speerpunten te werken, wil Defensie de verdere versterking van haar digitale middelen maximaal ondersteunen. De speerpunten voor de verdere versterking van de digitale middelen van Defensie betreffen:
5. de digitale weerbaarheid van Defensie;
6. het inlichtingenvermogen van Defensie in het digitale domein;
7. de ontwikkeling en de inzet van cybercapaciteiten als integraal onderdeel van het militaire optreden (defensief, offensief en inlichtingen).

Deze zeven speerpunten worden hieronder toegelicht. Zij komen in de plaats van de speerpunten zoals deze in de Defensie Cyber Strategie waren verwoord.[2]

VOORWAARDEN SCHEPPEN VOOR SUCCES IN HET DIGITALE TIJDPERK

1. Boeien, binden en ontwikkelen van cyberprofessionals

Slimme, kundige en gemotiveerde *cyberprofessionals* zijn de belangrijkste «capaciteiten» waarover Defensie in het digitale domein moet beschikken. Om in het digitale domein succesvol te zijn, is diepgaande kennis van dit domein immers onontbeerlijk en deze kennis schuilt hoofdzakelijk in mensen. Defensie zal de komende jaren veel moeite moeten doen om voldoende mensen met specifieke kennis te boeien en te binden. Vanwege de schaarste op de arbeidsmarkt zijn concurrerende werving en flexibele omgang met aanstellingseisen noodzakelijk. Ook is afstemming van het Defensiepersoneelsbeleid voor *cyberprofessionals* met publieke en private partners van belang. Defensie zal het voorts moeten hebben van de unieke betekenis van haar werk en de zingeving die medewerkers daaraan kunnen ontlenen.
Om aantrekkelijk te zijn voor *cyberprofessionals* en om rekening te kunnen houden met de specifieke kenmerken van dit vakgebied, zal Defensie flexibel met het personeelsbeleid omgaan.
De *Agenda voor de toekomst van het personeelsbeleid bij Defensie* (Kamerstuk 34 000 X, nr. 32) en de maatregelen die voortvloeien uit het eindrapport van de tijdelijke commissie ICT-projecten bij de overheid dienen hierbij zoveel mogelijk als uitgangspunt. Omdat in het cyberdomein specifieke kennis en competenties van belang zijn, moeten beperkingen die voortkomen uit het plaatsingsbeleid van militairen (zoals beperkte plaatsingsduur, functietoewijzingen en het systeem van rangen) zoveel mogelijk worden vermeden. Tevens zal Defensie flexibel moeten

[2] De speerpunten van de Defensie Cyber Strategie van juni 2012 zijn:
- de totstandkoming van een integrale aanpak;
- de versterking van de digitale weerbaarheid van Defensie;
- de ontwikkeling van militair vermogen om cyber operations uit te voeren;
- de versterking van de inlichtingenpositie in het digitale domein;
- 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;
- de intensivering van de samenwerking in nationaal en internationaal verband.

omgaan met salarisschalen om *cyberprofessionals* aan te kunnen trekken en te behouden.

Ook wil Defensie *cyber* als defensiebreed vakgebied nadrukkelijk op de kaart zetten, door de ontwikkeling van loopbaanpatronen en de uitwisseling van personeel tussen defensieonderdelen te bevorderen. Ook de samenwerking en de uitwisseling met publieke partners, zoals het Nationale Cyber Security Centrum (NCSC), en met private partners zijn hierbij van belang. De cyberleerstoel aan de Nederlandse Defensieacademie (NLDA), de Aanwijzing Cyberopleidingen van de Commandant der Strijdkrachten (CDS) en de ontwikkeling van cyberopleidingen door het Defensie Cyber Expertise Centrum (DCEC) zullen bijdragen tot een op *cyberprofessionals* toegesneden opleidings- en trainingsbeleid bij Defensie. Samenwerking met internationale partners, zoals het *NATO Cooperative Cyber Defence Centre of Excellence* (CCD COE) te Tallinn, neemt in dat verband eveneens een belangrijke plaats in. Defensie zoekt tevens samenwerking met externe partners zoals universiteiten, gerenommeerde opleidingsinstituten en het bedrijfsleven. Tot slot zal Defensie in de komende jaren het aantal cyberreservisten verder uitbreiden.

2. Slagvaardig innoveren en verwerven

Om in het digitale domein slagvaardig te kunnen innoveren en verwerven, zal Defensie de reguliere processen waar nodig aanpassen aan de specifieke kenmerken van dit dynamische domein. De ontwikkeling en de productie van wapensystemen vergen doorgaans jaren. In het digitale domein gaan ontwikkelingen echter razendsnel en is vaak sprake van een innovatiecyclus van maanden in plaats van jaren. De ontwikkeling van digitale technologie laat zich bovendien vaak moeilijk voorspellen. Om snel in een operationele behoefte te kunnen voorzien, is het noodzakelijk dat Defensie zelf snel digitale middelen kan ontwikkelen met behulp van op de markt verkregen digitale technologie («*rapid tool development*»). Ook de gerichte ontwikkeling van digitale middelen voor offensieve inzet vraagt om zelfontwikkelend vermogen (ondersteund door *Concept Development & Experimentation*). Daarnaast zal Defensie snellere en eenvoudige verwervings- en innovatieprocedures invoeren voor het digitale domein.

3. Bundelen en samenwerken

De cyberstrategie van Defensie berust op een geïntegreerde, defensiebrede aanpak, in het kader waarvan de schaarse cyberkennis, middelen, personeel en capaciteiten zoveel mogelijk zullen worden gebundeld. Voorts is nauwe samenwerking met nationale en internationale partners van wezenlijk belang om de defensiedoeleinden in het digitale domein te bereiken.

Binnen Defensie

Voor de bescherming van onze defensienetwerken, de inzet van cybermiddelen in militaire operaties of het vergaren van inlichtingen worden veelal dezelfde kennis, vaardigheden, technieken en materieel gebruikt. Daarom is het van belang dat de verschillende geledingen van Defensie zo geïntegreerd mogelijk werken. Dit leidt tot synergie, noodzakelijke kennisdeling en een doelmatig en doeltreffend gebruik van schaarse middelen en expertise.

De manier waarop en de mate waarin verschillende organisatieonderdelen samenwerken in het digitale domein, hangt samen met de taken die Defensie op dit terrein uitoefent. Dit kan variëren van de uitwisseling van

medewerkers en de aanleg van hoog gerubriceerde verbindingen tot het gebruik van gemeenschappelijke sensoren en ondersteunende IV-systemen. De wijze waarop binnen Defensie kennis en middelen worden gebundeld, wordt mede beïnvloed door wettelijke kaders en verplichtingen. Zo verschaft de Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv 2002) bijzondere bevoegdheden aan de MIVD en kaders voor (inter)nationale samenwerking en vertrouwelijke gegevensuitwisseling. De Koninklijke Marechaussee (KMar) oefent haar politietaken uit op grond van de Politiewet 2012. Met inachtneming van de wettelijke kaders kan binnen Defensie niettemin nog intensiever worden samengewerkt op het terrein van kennis en innovatie, het personeelsbeleid en opleiding en training. De synergie tussen de verschillende delen van de organisatie op deze gebieden zal daarom actief worden bevorderd. In dat verband zal Defensie tevens de colocatie van cyberdeskundigen waar mogelijk bevorderen.

Samen met andere geledingen van de overheid

Vanwege de grote onderlinge verbondenheid in het digitale domein is de slagkracht en veiligheid van Defensie op dit terrein sterk verbonden met de digitale weerbaarheid van partners. Het klassieke onderscheid tussen militaire en civiele, publieke en private en nationale en internationale dimensies is in het digitale domein minder scherp. Zo kan de nationale veiligheid in gevaar komen door een grootschalige digitale aanval op een of meer publieke of private organisaties. Om de nationale digitale weerbaarheid te versterken, is structurele samenwerking tussen publieke en private partners daarom wezenlijk. Met het Nationale Cyber Security Centrum (NCSC), dat als nationale coördinator optreedt, bestaan al afspraken over wederzijdse ondersteuning en militaire bijstand in het cyberdomein. Defensie en het NCSC zullen nauw blijven samenwerken in het belang van een gezamenlijk beeld van digitale dreigingen en de optimale coördinatie van operationele activiteiten. Zo worden er gezamenlijke oefeningen gehouden om de crisisbeheersingsstructuur verder te verbeteren en de civiel-militaire samenwerking te verdiepen.

Wat de KMar betreft, werkt Defensie als korpsbeheerder nauw samen met het Ministerie van Veiligheid en Justitie en het Openbaar Ministerie. De KMar voert haar politietaken immers uit op grond van de Politiewet 2012 en onder gezag van onder andere het Openbaar Ministerie en de Minister van Veiligheid en Justitie. Digitale technologie speelt ook hierbij een steeds grotere rol, onder andere in het kader van informatiegestuurd optreden. Voor Defensie zijn de politietaken van de KMar binnen de krijgsmacht voorts belangrijk om een verantwoord militair gebruik van het digitale domein te garanderen. Zo moet de KMar de rechtmatigheid van cyberinzet in nationale en internationale militaire operaties kunnen toetsen en mogelijke strafbare feiten in het cyberdomein tegen de krijgsmacht kunnen onderzoeken. Ook moet de KMar mogelijke strafbare feiten in het digitale domein door defensiepersoneel en op defensielocaties kunnen opsporen en onderzoeken. Voor alle wettelijke taken van de KMar zal het belang van het digitale domein verder toenemen. Daarom zal Defensie samen met Veiligheid en Justitie en het Openbaar Ministerie onderzoeken welke vervolgstappen nodig zijn om de KMar hiervoor voldoende toe te rusten.

Samen met het bedrijfsleven

Het bedrijfsleven is een belangrijke aanjager van kennisontwikkeling en innovatie in het digitale domein. Ook de Defensie Industrie Strategie (DIS)

geeft hiervan blijk.[3] Actieve samenwerking met het bedrijfsleven is daarom van groot belang. Gezamenlijke onderzoeksprogramma's, ontwikkeling van capaciteiten en samenwerking bij opleidingen en trainingen staan hierbij centraal. Deze kunnen de ontwikkeling van de verschillende digitale middelen bij Defensie belangrijke impulsen geven.

Samen met internationale partners

In internationaal verband zoekt Defensie nadrukkelijk de samenwerking met gelijkgestemde landen. Hierbij ziet Nederland een belangrijke ondersteunende rol voor de Navo, onder andere door het opstellen van beveiligingsstandaarden voor lidstaten, het bevorderen van de interoperabiliteit en een betere informatie- en kennisuitwisseling. Ook de samenwerking tussen de Navo en het bedrijfsleven in het kader van het *NATO Industry Cyber Partnership* (NICP) is voor Defensie relevant. In EU-verband is de samenwerking in het Europese defensieagentschap (EDA) van belang, waarbij het accent ligt op het gezamenlijke onderzoek naar methoden en technieken.

4. Kennis en cyber awareness: verbreding en verdieping

De snelheid van technologische ontwikkelingen en de veranderlijkheid en onvoorspelbaarheid van het digitale domein onderstrepen de noodzaak om te blijven investeren in het kennisniveau bij Defensie. Hierbij staan samenwerking en kennismanagement centraal. De Nederlandse Defensie Academie (NLDA), het Defensie Cyber Expertise Centrum (DCEC) en de Defensiestaf zullen een innovatief en experimenteel werkklimaat bij Defensie bevorderen. Ook de JSCU zal hieraan actief bijdragen. Tot slot zorgen opleidingen en trainingen ervoor dat cyberkennis wordt ingebed in de gehele defensieorganisatie. Het DCC zal opleidingen en trainingen initiëren en faciliteren die van belang zijn voor alle lagen van de organisatie. De thema's zullen variëren van *cyber awareness* tot hoogwaardige deskundigheid, afhankelijk van de doelgroep. Hierbij werkt het DCC intensief samen met de *warfare centres* van de krijgsmachtdelen, de kenniselementen van de MIVD, het JIVC (inclusief DefCERT), de *Chief Information Officer* (CIO) en de Beveiligingsautoriteit.

Structurele aanpak van cyber awareness

Het is noodzakelijk dat defensiepersoneel in alle lagen van de organisatie zich bewust is van de mogelijkheden en de gevaren van het digitale domein. Medewerkers kunnen onbedoeld een risico vormen voor de digitale veiligheid van Defensie door ondeskundig of onzorgvuldig gebruik van IT-middelen. Om dit tegen te gaan, zal Defensie hieraan structureel aandacht besteden in alle opleidingen en trainingen van de organisatie. Zo heeft de Beveiligingsautoriteit van Defensie inmiddels cursusmateriaal en een «digitaal rijbewijs»[4] ontwikkeld voor het defensiepersoneel. Ook zullen opleidingen en trainingen in toenemende mate worden gericht op de mogelijkheden die digitale middelen bieden voor de uitvoering van defensietaken. Cyberoperaties zullen bij het ontwerp, de planning en de uitvoering van oefeningen een steeds grotere rol gaan spelen. Ook zal Defensie medewerkers en militaire eenheden trainen om te werken onder omstandigheden waarbij zij tijdelijk niet over de

[3] Op pagina 13 van de Defensie Industrie Strategie wordt elektronische en informatiebescherming en bewapening aangemerkt als één van de gebieden waar het instrumentarium van de DIS zich op richt: «dit betreft defensieve (cyber)capaciteiten voor informatiebescherming en integriteitsbewaking en capaciteiten voor offensieve (cyber)activiteiten inclusief psyops en strategisch informatiegebruik, als tegenaanval of als onderdeel van actieve verdediging».

[4] Het digitaal rijbewijs is een *cyber awareness* training voor Defensiemedewerkers.

(volledige) functionaliteit van netwerken en systemen kunnen beschikken. Ten slotte zal Defensie investeren in de opleiding van alle IT en CIS-medewerkers, zodat zij cyberaanvallen nog sneller kunnen detecteren en de juiste maatregelen kunnen nemen.

Niet alleen voor Defensie is *cyber awareness* van groot belang. Voor nationale en internationale partners geldt hetzelfde. Daarom werkt Defensie op dit gebied zoveel mogelijk samen met (veiligheids)partners, bijvoorbeeld in de *Alert Online* campagnes (gericht op burgers, de overheid en het bedrijfsleven) die worden gecoördineerd door het NCSC.

VERDERE VERSTERKING VAN DIGITALE MIDDELEN

5. Versterking van de digitale weerbaarheid

De krijgsmacht is in toenemende mate afhankelijk van de betrouwbaarheid van informatie. Ook leunt zij sterk op hoogwaardige communicatie- en informatiesystemen, genetwerkte wapensystemen en logistieke systemen. Zowel in militaire operaties als in de algehele bedrijfsvoering, is Defensie sterk afhankelijk van deze systemen om de inzetbaarheid van de krijgsmacht te garanderen. De hoeveelheid data die ligt besloten in bijvoorbeeld sensoren, wapensystemen en commandosystemen (SEWACO-systemen) en netwerken neemt bovendien exponentieel toe. Defensienetwerken en -systemen zijn voorts gevoelig voor manipulatie tijdens de ontwikkeling, de productie, het transport en het onderhoud. Niet alleen de beveiliging van systemen en netwerken, maar ook de beveiliging van de informatie zelf is derhalve van wezenlijk belang. Hierbij staan de exclusiviteit (alleen gemachtigde en geautoriseerde toegang), de integriteit (geen ongeautoriseerde wijzigingen) en de beschikbaarheid (toegang) van informatie voorop.

Het Cyber Security Beeld Nederland 4 (CSBN-4) maakt duidelijk dat de digitale dreigingen toenemen en ook complexer en geavanceerder worden (Kamerstuk 26 643, nr. 322). Defensie en samenwerkingspartners hebben te maken met steeds agressievere vormen van spionage, criminaliteit en andere activiteiten zoals cybersabotage. Het gaat daarbij niet alleen om bekende en gangbare *malware*. Een urgenter probleem zijn de gerichte, geavanceerde en heimelijke digitale inbreuken van veelal statelijke actoren die onvoldoende kunnen worden bestreden met reguliere beveiligingsmaatregelen. Deze dreiging is aanzienlijk. Ook niet-statelijke actoren vormen een steeds groter risico. De kennis, middelen en technieken om geavanceerde digitale aanvallen te plegen zijn immers in toenemende mate voor iedereen beschikbaar.

Ook de toepassing van digitale middelen in militaire operaties heeft een enorme vlucht genomen en is sterk in ontwikkeling. Een cyberaanval op IT-, sensor-, wapen- en commandosystemen of op de logistiek van een operatie vormt een ernstige bedreiging voor de inzetbaarheid en de doeltreffendheid van de krijgsmacht. Deze dreiging beperkt zich niet tot het inzetgebied, maar strekt zich ook uit tot de defensienetwerken en -systemen op locaties elders in de wereld en kan zich tevens richten op de Nederlandse vitale infrastructuur of op bondgenoten.

Een volledig «waterdichte» digitale verdediging is onhaalbaar. Door afwijkingen in de (vitale) systemen snel waar te nemen en extra maatregelen te nemen, kan de schade in het geval van digitale spionage of sabotage zoveel mogelijk worden gemitigeerd. Inlichtingen zijn onmisbaar om actief te kunnen optreden tegen kwetsbaarheden van, en dreigingen tegen, netwerken en systemen.

Zoals beschreven in hoofdstuk 4, zal digitale weerbaarheid een prominent onderdeel worden van alle defensieopleidingen. Ook richt Defensie één Security Operations Centre (SOC) op, waarin alle beheerorganisaties samenwerken om alle netwerken, IT-diensten en SEWACO-systemen van Defensie in Nederland en in operatiegebieden, dag en nacht te monitoren en te beschermen. Dit SOC krijgt extra personeel tot zijn beschikking en zal tevens nauw samenwerken met het DefCERT. Bij incidenten coördineert DefCERT de contacten met andere CERT's, verzamelt informatie over digitale kwetsbaarheden en geeft advies over maatregelen. Een onafhankelijke positie van DefCERT ten opzichte van het SOC is hierbij van groot belang. Defensie zal voorts blijven investeren in een hoogwaardige inlichtingenpositie in het digitale domein. Voor de digitale weerbaarheid van Defensie is samenwerking tussen de inlichtingenketen en de beheerorganisaties essentieel. Om dit te ondersteunen, richt Defensie met voorrang faciliteiten in die de betrokken organisatieonderdelen in staat stellen hoog gerubriceerde informatie uit te wisselen. Het spreekt verder voor zich dat Defensie de beveiliging van haar systemen doorlopend zal vernieuwen door de ontwikkeling van innovatieve beschermings-, detectie- en mitigatiemaatregelen. Ook verplicht Defensie leveranciers om soortgelijke maatregelen te nemen. Om de beveiliging van de IT-voorzieningen en de *supply chain* van toeleveranciers ook in de toekomst te kunnen blijven waarborgen, past Defensie de zogenaamde ABDO-regeling[5] aan. Deze beschrijft hoe externe dienstverleners moeten omgaan met vertrouwelijke informatie van Defensie.

De beveiliging, de continuïteit en het innovatieve vermogen van de IT-voorzieningen van Defensie en de verbetering daarvan zoals beschreven in de visie op IT (Kamerstuk 31 125 nr.45), zijn uiteraard van belang voor de verdere verbetering van de digitale weerbaarheid.

6. Versterking van het inlichtingenvermogen in het digitale domein

De mondiale digitalisering van de samenleving heeft vergaande gevolgen voor het inlichtingenwerk. De instabiele internationale veiligheidssituatie vraagt om een flexibele inlichtingencapaciteit om vroegtijdig informatie te kunnen vergaren, noodzakelijk voor politieke en militaire besluitvorming. Defensie ziet zich in Nederland, in bondgenootschappelijk verband en in (potentiële) inzetgebieden geconfronteerd met technisch geavanceerde actoren die via het digitale domein een bedreiging vormen voor Nederlandse veiligheidsbelangen en de veilige en effectieve uitvoering van militaire operaties.

Defensie heeft inzicht nodig in de middelen, intenties en activiteiten van opponenten om zichzelf, de regering en bijvoorbeeld bondgenoten handelingsperspectief te bieden. Ter versterking van de defensieve cybervermogens van Defensie is vooruitziend vermogen voor de bescherming van eigen systemen noodzakelijk. Daarnaast zal Defensie dreigingen zoals spionage tijdig moeten kunnen onderkennen, afweren en beïnvloeden. Ook voor offensief optreden in het cyberdomein zijn inlichtingen en voorbereidende inlichtingenactiviteiten noodzakelijk, bijvoorbeeld om toegang te krijgen tot systemen en mogelijke aangrijpingspunten in kaart te brengen. Deze activiteiten, voorafgaand aan en tijdens de inzet, beperken zich niet tot het digitale domein, maar vergen ook andere bijzondere middelen, zoals *human* en *signals intelligence*. Ook plaatselijk verworven gegevens kunnen een belangrijk onderdeel zijn van de inlichtingenondersteuning voor en tijdens de inzet.

---

[5] De huidige Algemene Beveiligingseisen voor Defensieopdrachten dateert uit 2006. De regeling zal worden aangevuld op grond van actuele inzichten in de digitale dreiging.

Bij Defensie is de inlichtingentaak primair belegd bij de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), onder verantwoordelijkheid van de Minister van Defensie. Het wettelijke kader voor het optreden van de MIVD wordt gevormd door de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). De MIVD kan op basis van de in deze wet genoemde bevoegdheden de noodzakelijke handelingen verrichten om inlichtingen te vergaren over het digitale domein en contra-inlichtingenactiviteiten uit te voeren in binnen- en buitenland. Zo is het, met inachtneming van de wettelijke vereisten, toegestaan computersystemen binnen te dringen. Gelet op de wettelijke plicht tot bescherming van bronnen en modus operandi, is de wet ook het fundament voor vertrouwelijke (inter)nationale samenwerking.

Om voldoende armslag in het digitale domein te krijgen en te houden is modernisering van de Wiv 2002 noodzakelijk. Het standpunt van het kabinet over de herziening van het interceptiestelsel in het kader van de Wiv (Kamerstuk 33 820, nr. 4) is van wezenlijk belang voor de doelstellingen van Defensie in het digitale domein. Toegang tot kabelgebonden telecommunicatie is een voorwaarde om cyberdreiging vroegtijdig te kunnen onderkennen en inlichtingen te kunnen verzamelen over de aard van de dreiging. Het kunnen verkennen van het digitale domein is bovendien van wezenlijk belang voor inlichtingenoperaties en de ondersteuning van cyberoperaties.

De MIVD zal op de afnemers toegesneden rapportagemechanismen ontwikkelen. Het kan gaan om geïntegreerde analyses (zogenoemde *all source* producten), een verkenning van cyberspace in relatie tot een potentieel operatiegebied of een *signature* van een geavanceerde cyberdreiging. Cybergerelateerde onderzoeksvragen zullen worden opgenomen in de jaarlijkse Inlichtingen- en Veiligheidsbehoefte Defensie (IVD) om nadere richting te geven aan de inspanningen van de MIVD. Ook beoogt Defensie een verdere integratie van de inzet van bijzondere middelen zoals *human* en *signals intelligence* en de uitbreiding van de analysecapaciteit ter versterking van de informatiepositie in het digitale domein. Geavanceerde dreigingen, bijvoorbeeld tegen de defensiegerelateerde industrie en Navo-instituten, beperken zich zelden tot Nederland. Internationale samenwerking is daarom bij uitstek een voorwaarde voor het tegengaan van dergelijke bedreigingen. Gelet op het gerubriceerde karakter geschiedt dit in veel gevallen tussen inlichtingen- en veiligheidsdiensten.

Een van de kerncapaciteiten voor Defensie en Binnenlandse Zaken in de komende jaren is de JSCU, die de MIVD en de AIVD in 2014 hebben opgericht (zie Kamerstuk 29 294, nr. 113). Defensie streeft naar versterking van deze eenheid en de samenwerking met de AIVD. In deze gezamenlijke eenheid van en voor de MIVD en de AIVD zijn de technische kennis en deskundigheid op het gebied van sigint en cyber gebundeld. De JSCU verwerft en ontsluit gegevens uit technische bronnen, doet data-analyse en technisch onderzoek naar cyberdreigingen en richt zich op innovatie en kennisontwikkeling.

7. Versterking van de cyberinzet in missies

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 alsmede het vermogen eigen eenheden tegen vergelijkbaar handelen door een tegenstander te beschermen. Operationele digitale middelen bevatten dus defensieve, offensieve en inlichtingenelementen. Zij maken onlosmakelijk deel uit van het moderne militaire optreden.

Offensief

Onder offensieve cybercapaciteiten verstaat Defensie digitale middelen die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Dit gebeurt door infiltratie van computers, computernetwerken en wapen- en sensorsystemen om informatie en systemen te beïnvloeden. Defensie zet offensieve digitale middelen uitsluitend in tegen militaire doelen.

Als gevolg van het intensieve gebruik van hoogwaardige communicatie-, informatie- en wapensystemen zijn ook steeds meer opponenten afhankelijk van de betrouwbaarheid en beschikbaarheid van digitale middelen. Offensieve cybercapaciteiten kunnen daarom, als deel van het totale militaire vermogen, een wezenlijk bijdrage leveren aan het bereiken van beoogde effecten. Zij vormen daardoor een belangrijke toevoeging aan de bestaande middelen.

Defensief

In een militaire operatie zijn defensieve maatregelen tegen cyberdreigingen van belang om de effectiviteit en de inzetbaarheid van de krijgsmacht te waarborgen. Dit begint al bij de integrale voorbereiding op een missie, onder andere door de belangrijkste kwetsbaarheden van de netwerken en systemen in het inzetgebied en mogelijke defensieve scenario's in kaart te brengen. In het operatiegebied moeten de netwerken en systemen doorlopend worden gemonitord, om te kunnen ingrijpen bij inbreuken. Bij een cyberaanval tijdens een militaire operatie kan een snelle reactie nodig zijn. Hierbij is een sluitende attributie (door inlichtingen over de wijze waarop en door wie de aanval is uitgevoerd en met welke intentie dit is gedaan) essentieel. Dit onderstreept de behoefte aan geëvalueerde en gevalideerde inlichtingen, die tijdig ter beschikking worden gesteld aan de verantwoordelijke commandant. De verantwoordelijke commandant zal operationele en inlichtingenbelangen moeten afwegen, de legitimiteit van het eigen optreden moeten zekerstellen en vaak onder tijdsdruk moeten besluiten. Het mandaat voor de inzet van digitale middelen zal per militaire operatie worden vastgesteld, mede op grond van het politieke risico, de potentiële nevenschade, het juridische kader en de noodzaak tot geheimhouding.

Inlichtingen

Een hoogwaardige inlichtingenpositie op elk niveau is een voorwaarde voor de uitvoering van militaire missies. Juist in het digitale domein is daarbij sprake van een vervlechting van strategische en operationele inlichtingen, die doorgaans met hoogwaardige en soms kostbare middelen gedurende een langere periode moeten worden verworven. Deze kunnen worden aangevuld met veelal plaatselijk verworven inlichtingen. Een integrale inlichtingenpositie brengt Defensie in de positie om kansen, bedreigingen en risico's goed te schatten en te beïnvloeden.

In het geval van militaire operaties in het buitenland biedt het internationale juridische kader (het volkenrechtelijk mandaat) primair de grondslag en de kaders voor het optreden van de MIVD. De Wiv 2002 wordt dan analoog toegepast voor zover de omstandigheden in het operatiegebied dat toelaten.

Taken en bevoegdheden

Na een kabinetsbesluit tot inzet van de krijgsmacht, in het kader van de verdediging van het eigen of bondgenootschappelijke grondgebied of de

handhaving van de internationale rechtsorde, staan de digitale middelen van de krijgsmacht altijd onder bevel van de CDS. Het besluit tot Nederlandse deelneming aan een militaire operatie kan vergezeld gaan van nationale beperkingen (*caveats*) voor de inzet van Nederlandse eenheden, specifieke wapensystemen of de interpretatie van regels. Dit geldt ook voor eventuele inzet van cybereenheden of cyber(wapen)systemen. Bij de inzet van cybermiddelen in het kader van de derde hoofdtaak van Defensie – de ondersteuning van civiele autoriteiten bij rechtshandhaving, rampenbestrijding en humanitaire hulp, zowel nationaal als internationaal – staan cybereenheden onder civiel gezag.

Als Nederland een rechtsgrondslag heeft om op te treden, zullen voor cybereenheden van de krijgsmacht een duidelijke opdracht, een oogmerk en geweldsinstructies (*Rules of Engagement*) moeten worden geformuleerd. De juridische kaders zijn dus niet anders dan die voor de inzet van conventionele middelen. De inzet van strategische cybermiddelen wordt in beginsel op nationaal niveau bepaald. De bevoegdheid om tactische cybermiddelen in te zetten, zal per operatie in de geweldsinstructies worden vastgesteld.

Capaciteitsontwikkeling

Om de verantwoorde en doeltreffende inzet van digitale middelen in militaire operaties mogelijk te maken, zal Defensie de komende tijd in het bijzonder aandacht geven aan:
- de verdere ontwikkeling van een Defensie Cyber Doctrine;
- de ontwikkeling van offensieve cybermiddelen en van richtlijnen voor de gereedstelling van flexibel samen te stellen cybereenheden en cybermiddelen;
- de inrichting van defensieve digitale middelen bij missies;
- de ontwikkeling van cyber(inlichtingen)middelen voor tactische inzet;
- de integratie van cyberaspecten in het operationeel besluitvormingsproces, voorafgaand aan en tijdens operaties.

Offensieve cybermiddelen kunnen variëren van relatief eenvoudig en snel te ontwikkelen middelen met een tactische impact tot aan middelen met een hoge, strategische impact die een lange ontwikkelingstijd vergen. De complexiteit en de technologische hoogwaardigheid van die middelen hangen vooral af van de gewenste effecten. Deze middelen richten zich voornamelijk op het aangrijpen van informatie- en communicatienetwerken en sensor-, wapen- en commandovoeringssystemen van (potentiële) tegenstanders. Hoewel soms ook relatief eenvoudige offensieve cyberwapens gedurende kortere tijd effectief kunnen zijn, onderscheiden deze capaciteiten zich van conventionele militaire capaciteiten doordat ze vaak eenmalig inzetbaar zijn en specifiek voor één doel worden ontwikkeld. Het kan gaan om complexe middelen waarvan de ontwikkeling, instandhouding en toepassing kennisintensief en tijdrovend zijn. De voorbereiding, ontwikkeling en inzet zijn een samenspel van gespecialiseerd personeel, beschikbare techniek, goede inlichtingen en processen, mede om ongewenste neveneffecten bij de inzet van offensieve cybermiddelen te voorkomen. Het DCC zorgt voor de coördinatie tussen de verscheidene defensieonderdelen en hun digitale middelen en beschikt over specialisten om deze taak uit te voeren. Dit waarborgt de optimale benutting van cybermiddelen ten behoeve van de ondersteuning van militaire operaties en voorkomt dubbelingen binnen de defensieorganisatie.

TOT SLOT

Defensie heeft de afgelopen jaren forse stappen in het digitale domein gezet en forse investeringen gedaan. De Defensie Cyber Strategie legde daarvoor de basis. De nota *In het belang van Nederland* versnelde de tenuitvoerlegging. Deze actualisering bepaalt de richting waarin Defensie zich op dit vlak de komende jaren verder zal ontwikkelen, in het volle besef dat de digitale revolutie om flexibiliteit in de toepassing en de financiering van deze strategie kan vragen. Om gelijke tred te kunnen blijven houden met de stormachtige ontwikkelingen in het digitale domein zal Defensie daarom in 2016 en 2017 een beleidsdoorlichting uitvoeren, die de Tweede Kamer zal worden aangeboden.

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