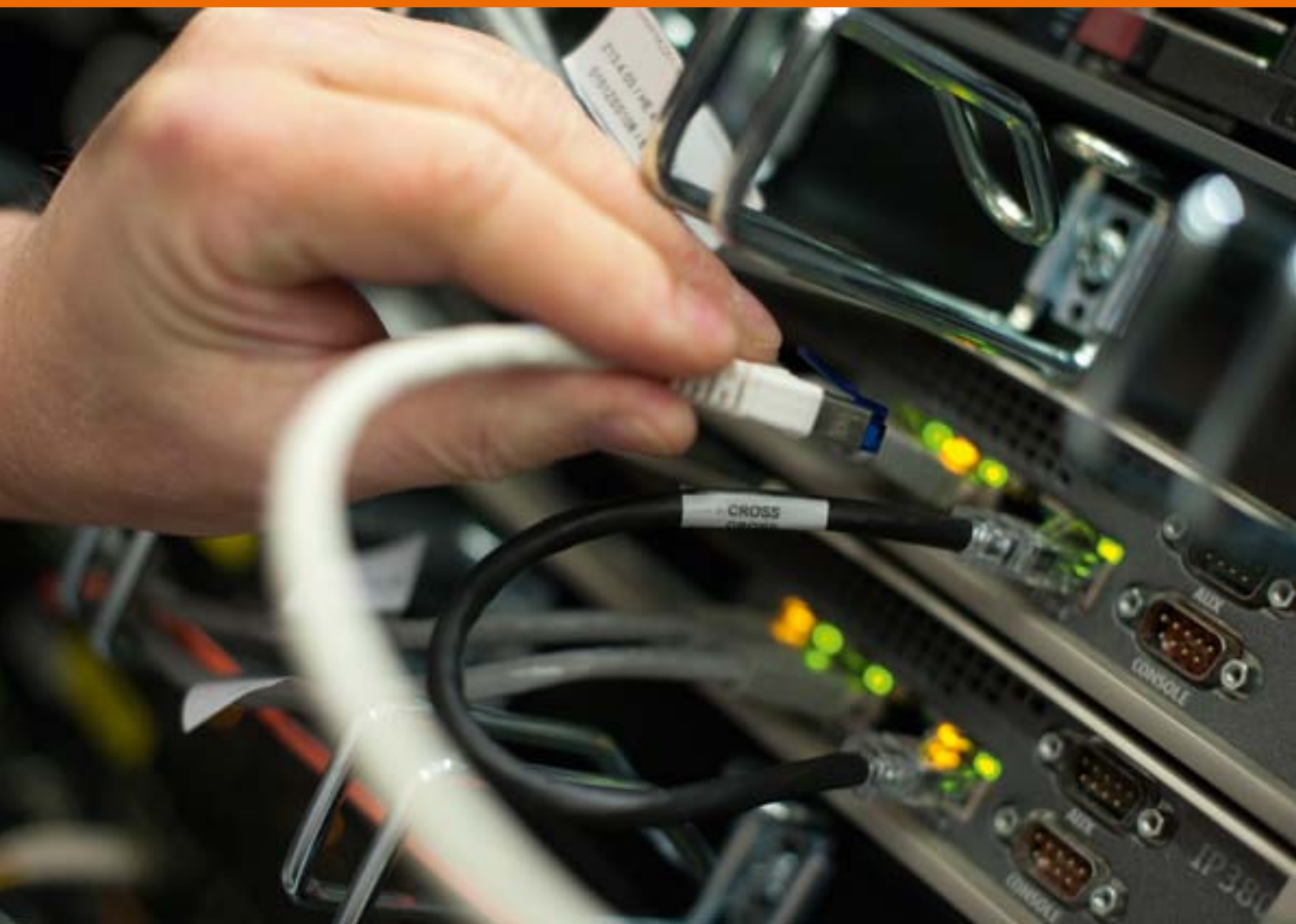
Ministerie van Defensie

DEFENSIE CYBER STRATEGIE



Ministerie van Defensie

> Retouradres Postbus 20701 2500 ES Den Haag

de Voorzitter van de Tweede Kamer
der Staten-Generaal
Plein 2
2511 CR Den Haag

Ministerie van Defensie

Plein 4
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

Onze referentie
BS2012021117

Afschrift aan
de Voorzitter van de Eerste Kamer der Staten-Generaal
Binnenhof 22
2513 AA Den Haag

Bij beantwoording datum, onze referentie en betreft vermelden.

Datum 27 juni 2012
Betreft Defensie strategie voor het opereren in het digitale domein

Het digitale domein is, naast het land, de lucht, de zee en de ruimte, inmiddels het vijfde domein voor militair optreden. Dit domein en de toepassing van digitale middelen als wapen of inlichtingenmiddel zijn onmiskenbaar sterk in ontwikkeling. Digitale middelen zullen in toenemende mate integraal deel uitmaken van het militaire optreden. De afhankelijkheid van digitale middelen leidt daarentegen ook tot kwetsbaarheden die urgente aandacht behoeven. De Nederlandse krijgsmacht trekt hier de noodzakelijke conclusies uit en wil in het digitale domein de vooraanstaande rol spelen die bij ons land past. Om de inzetbaarheid van de krijgsmacht te waarborgen en haar effectiviteit te verhogen, versterkt Defensie de komende jaren haar digitale weerbaarheid en ontwikkelt zij het vermogen om *cyber operations* uit te voeren.

Tegen deze achtergrond doe ik u hierbij de Defensie strategie voor het opereren in het digitale domein toekomen: de Defensie Cyber Strategie. Zij geeft op een voortvarende manier uitwerking aan de in de beleidsbrief 'Defensie na de kredietcrisis' van 8 april 2011 (Kamerstuk 32 733, nr. 1) opgenomen cyberintensivering en aan het defensiedeel in de Nationale Cyber Security Strategie (Kamerstuk 26643, nr. 174). De strategie is aangekondigd in de kabinetsreactie op het advies over 'digitale oorlogvoering' van de Adviesraad voor Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV) (Kamerstuk 33 000-X, nr. 79).

De Defensie Cyber Strategie geeft de komende jaren richting, samenhang en focus aan de integrale aanpak voor de ontwikkeling van het militaire vermogen in het digitale domein. Zij is daardoor van wezenlijk belang voor de toekomstige effectiviteit en relevantie van onze krijgsmacht.

DE MINISTER VAN DEFENSIE

drs. J.S.J. Hillen

Inleiding

Het digitale domein[1] is, naast het land, de lucht, de zee en de ruimte, het vijfde domein voor militair optreden. Dit domein en de toepassing van digitale middelen als wapen of inlichtingenmiddel zijn onmiskenbaar sterk in ontwikkeling. Digitale middelen zullen in toenemende mate integraal deel uitmaken van het militaire optreden en tot moderniseringen leiden. De afhankelijkheid van digitale middelen leidt echter ook tot kwetsbaarheden die urgente aandacht behoeven. De impact op de samenleving van een grootschalige cyberaanval kan enorm zijn. De effecten kunnen evenals bij een terreuraanval grote ontreddering en maatschappelijke ontwrichting teweegbrengen. In het militaire domein kunnen de infrastructuur en wapensystemen zodanig worden aangetast dat van een slagvaardige verdediging geen sprake meer is. De Nederlandse krijgsmacht trekt hier de noodzakelijke conclusies uit en wil ook in het digitale domein haar rol als "zwaardmacht" naar behoren vervullen.

De drie hoofdtaken van Defensie zijn ook in het digitale domein leidend voor de inspanningen van de krijgsmacht.[2] Zij moet derhalve handelend kunnen optreden tegen een digitale bedreiging van de samenleving of van de internationale rechtsorde. Daarbij is sprake van een toenemende overlap tussen de eerste en de derde hoofdtaak. Het onderscheid tussen de hoofdtaken blijft echter van belang omdat de grondslag en de procedures voor de inzet van de krijgsmacht per hoofdtaak verschillen. De staatsrechtelijke verhoudingen gelden onverkort in het digitale domein. De inzet van de krijgsmacht geschiedt derhalve bij internationale operaties op grond van een mandaat van de regering en voor nationale inzet in beginsel op grond van een verzoek tot bijstand aan civiele autoriteiten (over het algemeen de minister van Veiligheid en Justitie).

Om de inzetbaarheid van de Nederlandse krijgsmacht te waarborgen en haar effectiviteit te verhogen, versterkt Defensie haar digitale weerbaarheid en ontwikkelt zij het vermogen om *cyber operations* uit te voeren. De Defensie Cyber Strategie geeft de komende jaren richting, samenhang en focus aan de integrale aanpak voor de ontwikkeling van het militaire vermogen in het digitale domein. Zij geeft daarmee uitwerking aan de in de beleidsbrief 'Defensie na de kredietcrisis' (Kamerstuk 32 733, nr. 1) opgenomen cyberintensivering en aan het defensiedeel in de Nationale Cyber Security Strategie (Kamerstuk 26643, nr. 174).

De krijgsmacht wil optimaal gebruik maken van de mogelijkheden die de ontwikkeling van digitale technologie biedt. Deze technologie wordt al op grote schaal door Defensie gebruikt en stelt de krijgsmacht in staat haar taken doelmatiger en doeltreffender uit te voeren. Zo functioneren vrijwel alle wapensystemen dankzij het gebruik van ICT-componenten. Ook de commandovoering en de logistieke ondersteuning leunen zwaar op digitale systemen. Tevens worden de informatiepositie en de *situational awareness* van de krijgsmacht aanzienlijk versterkt met behulp van digitale middelen. Digitale netwerken en systemen, waaronder zowel wapensystemen als meet- en regelsystemen worden begrepen, en de daarop aanwezige informatie zijn daarmee voor de krijgsmacht van levensbelang geworden.

[1] Er bestaat op dit ogenblik geen internationaal geaccepteerde definitie van het begrip digitaal domein (*cyber space*). In deze strategie wordt het digitale domein beschouwd als alle entiteiten die digitaal verbonden (kunnen) zijn. Het domein omvat zowel permanente verbindingen als tijdelijke of plaatselijke verbindingen en betreft altijd op enigerlei wijze de gegevens (data, programmacode, informatie, etcetera) die zich in dit domein bevinden.

[2] De drie hoofdtaken van Defensie zijn:
- Bescherming van het eigen en bondgenootschappelijk grondgebied, met inbegrip van het Caribische deel van het Koninkrijk;
- Bevordering van de internationale rechtsorde en stabiliteit;
- Ondersteuning van civiele autoriteiten bij rechtshandhaving, rampenbestrijding en humanitaire hulp, zowel nationaal als internationaal.

De afhankelijkheid van de krijgsmacht van digitale technologie maakt haar echter ook kwetsbaar. Het is van wezenlijk belang dat Defensie de betrouwbaarheid[3] van de eigen netwerken, systemen en informatie waarborgt en ontvreemding van informatie voorkomt. Defensie moet waakzaam blijven en in hoogwaardige middelen en kennis investeren om de verdediging tegen digitale aanvallen op het vereiste niveau te houden. Zij moet ook meer zicht krijgen op de dreigingen waaraan zij in het digitale domein wordt blootgesteld om zich daartegen effectief te kunnen wapenen.

Aangezien niet alleen onze eigen digitale systemen kwetsbaar zijn maar ook die van (potentiële) tegenstanders kan het digitale domein ook worden gebruikt voor (militair) optreden tegen een tegenstander of om de eigen inlichtingenpositie te versterken. Defensie beschouwt digitale middelen daarom nadrukkelijk ook als operationele capaciteiten – als wapen of inlichtingenmiddel – die integraal deel moeten gaan uitmaken van het operationele vermogen van de krijgsmacht. Het gaat daarbij om de bescherming van de eigen netwerken, systemen en informatie tijdens inzet, de inzet van offensieve capaciteiten en het vergaren langs digitale weg van aan de inzet gerelateerde inlichtingen. Omdat alle defensieonderdelen intensief gebruik maken van ICT-middelen is vergaande *joint* samenwerking daarbij noodzakelijk.

Wegens het wijdvertakte en veelvormige karakter van het digitale domein en om de schaarse middelen van Defensie optimaal in te zetten, zijn centrale sturing en coördinatie nodig van alle activiteiten die aan het militaire optreden in het digitale domein zijn verbonden. De snelheid waarmee ontwikkelingen in het digitale domein zich voltrekken, stelt voorts hoge eisen aan het aanpassingsvermogen en de innovatieve kracht van Defensie. Zij moet in het digitale domein in staat zijn snel nieuwe technologie in te voeren en korte innovatiecycli te doorlopen. De dynamiek en de complexiteit van het digitale domein vergen voortdurende aanpassing van (initiële) behoeften aan kennis, kunde, vaardigheden en technieken, en wijze van optreden.

Door de grote onderlinge verbondenheid in het digitale domein en de afhankelijkheid van soortgelijke technologie is ook nationaal en internationaal een integrale aanpak noodzakelijk. De klassieke scheiding van militaire en civiele, publieke en private en nationale en internationale actoren is in het digitale domein minder helder. Zo kan de nationale veiligheid in gevaar worden gebracht door een grootschalige aanval op een private organisatie. Bij de verdediging tegen een dergelijke aanval is samenwerking tussen verschillende partijen noodzakelijk, waaronder de getroffen organisatie zelf, het Nationaal Cyber Security Centrum (NCSC), de inlichtingendiensten, de opsporingsdiensten en mogelijk ook de krijgsmacht.

[3] Onder betrouwbaarheid wordt verstaan beschikbaarheid, integriteit en exclusiviteit.

Speerpunten

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

1 de totstandkoming van een integrale aanpak;

2 de versterking van de digitale weerbaarheid van Defensie (“defensief”);

3 de ontwikkeling van het militaire vermogen om cyber operations uit te voeren (“offensief”);

4 de versterking van de inlichtingenpositie in het digitale domein (“inlichtingen”);

5 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”);

6 de intensivering van de samenwerking in nationaal en internationaal verband (“samenwerking”).

De ontwikkeling van de digitale dreiging voor Defensie

De Nederlandse defensieorganisatie is als gevolg van haar intensieve gebruik van hoogwaardige (satelliet)communicatie-, informatie-, sensor-, navigatie-, logistieke en wapensystemen afhankelijk van betrouwbare interne en externe netwerken en van digitale technologie. Zij is daardoor kwetsbaar voor digitale aanvallen.

Verschillende landen beschikken inmiddels over offensieve cybercapaciteiten voor militaire doeleinden of zijn bezig deze te ontwikkelen. Ook niet-statelijke actoren kunnen een bedreiging vormen voor de krijgsmacht door systemen en de informatievoorziening te ontregelen. In moderne conflicten vervaagt bovendien het onderscheid tussen combattanten en non-combattanten en is steeds minder sprake van een duidelijk afgebakend operatiegebied. Het optreden van “tegenstanders” zal steeds vaker ook digitale vormen aannemen en zich daarbij waarschijnlijk ook vaker uitstrekken tot het “thuisfront”.

De grootste dreiging voor Defensie in het digitale domein gaat op de middellange termijn uit van hoogwaardige en complexe digitale offensieve capaciteiten die tegen een specifiek (militair) doel gericht zijn en die de handelingsvrijheid van de krijgsmacht ernstig kunnen beperken. Een gebrek aan kennis over en inzicht in de digitale mogelijkheden om aanvallen uit te voeren, vormt daarbij een reëel risico voor de krijgsmacht.

Nu al worden krijgsmachten en bedrijven die zijn betrokken bij de ontwikkeling en de productie van hoogwaardige militaire technologie doorlopend geconfronteerd met – pogingen tot – digitale aanvallen en spionageactiviteiten. De strategische en economische waarde van de informatie in deze sector is groot. Voorts zal Defensie in een vroeg stadium alert moeten zijn op de heimelijke introductie van kwetsbaarheden (“achterdeurtjes”) in informatie- en communicatiesystemen. De complexiteit van en hoeveelheid componenten in systemen maakt dit in toenemende mate een risico. Inlichtingendiensten zullen het vooraf manipuleren van aan potentiële opponenten te leveren apparatuur zeer waarschijnlijk niet schuwen.

Speerpunt 1: een integrale aanpak

Uitgangspunt is dat cybercapaciteiten van Defensie een belangrijke en reële aanvulling vormen op de bestaande militaire capaciteiten. De kracht van digitale middelen ligt in de mogelijkheden die deze bieden het optreden langs alle lijnen en in alle domeinen te ondersteunen en te versterken. Digitale middelen versterken het optreden van de krijgsmacht in alle functies van het militaire optreden: logistiek, commandovoering, inlichtingen, bescherming, manoeuvre en slagkracht. Deze strategie gaat dan ook uit van een integrale aanpak, zowel wat de ondersteunende processen betreft (gereedstelling, operationele ondersteuning, instandhouding) als de operationele inzet (zelfstandig en als onderdeel van het optreden van andere eenheden, eventueel onder civiel gezag).

In het kader van militaire operaties zal steeds vaker van operationele cybercapaciteiten gebruik worden gemaakt, voornamelijk ter ondersteuning van het reguliere optreden van de krijgsmachten maar ook als zelfstandig wapen. Het is noodzakelijk dat operationele cybercapaciteiten onderdeel worden van het totale militaire vermogen van de Nederlandse krijgsmacht. Defensie moet daartoe fors investeren in het versterken van de cybercapaciteiten. Defensie zal geen afzonderlijk krijgsmachtdeel oprichten voor het optreden in het digitale domein. De daarvoor in aanmerking komende cybercapaciteiten zullen in 2014 als *joint* eenheid worden ondergebracht in het Defensie Cyber Commando (DCC) dat onder *single service management* bij het Commando landstrijdkrachten (CLAS) wordt ondergebracht.

Een operationele cybercapaciteit omvat alle kennis en middelen die nodig zijn om gedurende operationele inzet langs digitale weg het handelen van tegenstanders te voorspellen, te beïnvloeden of onmogelijk te maken, en zich te verdedigen tegen vergelijkbaar handelen door de tegenstander. Dit gebeurt door infiltratie van computers, computernetwerken, wapen- en sensorsystemen en software om informatie en inlichtingen te vergaren en systemen te beïnvloeden. Een operationele cybercapaciteit omvat dus inzetbare defensieve, inlichtingen- en offensieve elementen.

Bij de planning van en de voorbereiding op operaties worden ook voor het digitale domein relevante aspecten meegenomen. Het digitale domein vormt daarmee een integraal deel van het *joint* operationeel planningsproces. Hierbij wordt zowel gekeken naar de potentiële invloed van het digitale domein op de opgedragen taak als naar de effecten die door inzet van cybercapaciteiten kunnen worden bereikt. Een operationele commandant beschikt daarom over eigen capaciteiten en kan een beroep doen op de inlichtingencapaciteit om cyber informatie te vergaren, te verwerken en tijdig beschikbaar te stellen voor het besluitvormingsproces. Dit betreft zowel de dreiging tegen eigen netwerken en systemen als de mogelijkheden om kwetsbaarheden bij de tegenstander uit te buiten. Een goede *situational awareness* in het digitale domein maakt deel uit van de totale *situational awareness* van de commandant.

Voor operaties in het digitale domein is het noodzakelijk dat het mandaat hier ruimte voor biedt en moet in de *Rules of Engagement* opgenomen worden hoe offensieve cybercapaciteiten ingezet mogen worden.

Speerpunt 2: Defensief

Netwerken en systemen zijn kwetsbaar voor aanvallen en verstoringen, zowel van buitenaf als van binnenuit. De verdediging hiertegen behelst de bescherming van netwerken, het monitoren en het analyseren van dataverkeer, het onderkennen van digitale aanvallen en de reactie hierop.

Defensie is vanzelfsprekend verantwoordelijk voor de beveiliging van de eigen netwerken en systemen. Zij moet zijn voorbereid op cyberdreigingen en zich hiertegen kunnen beschermen om de inzetbaarheid van de krijgsmacht te garanderen. Defensie moet daartoe bekend zijn met de mogelijke dreigingen in het digitale domein en de kwetsbaarheden van haar eigen netwerken en systemen. Defensie zal daarom een risico-analyse uitvoeren op grond waarvan wordt vastgesteld welke minimale beveiligingsmaatregelen nodig zijn. Hierbij zullen de te nemen maatregelen en de werkbaarheid in evenwicht moeten zijn en zal worden gestreefd naar een samenhangend pakket van personele, fysieke en informatiebeveiligingsmaatregelen. Voor netwerken en systemen waarin hooggerubriceerde informatie wordt verwerkt en opgeslagen zal een strenger beveiligingsregime gelden. Ongeautoriseerde toegang tot die gegevens zou immers kunnen leiden tot (zeer) ernstige schade voor Defensie, voor de overheid of voor onze bondgenoten. Voor netwerken en systemen met ongerubriceerde of laaggerubriceerde informatie kan worden volstaan met een beperktere set aan beveiligingsmaatregelen.

Er moet van uit worden gegaan dat een vasthoudende en technologisch hoogontwikkelde tegenstander niettemin in staat zal zijn (delen van) netwerken en systemen te compromitteren. Het inrichten van een allesomvattende digitale verdediging is vrijwel onmogelijk en bovendien onbetaalbaar. Bij de bescherming van de eigen digitale infrastructuur moet om die reden zoveel mogelijk flexibiliteit worden ingebouwd, zowel ten aanzien van de (passieve) beveiliging van netwerken als van de actieve respons op een aanval. Prioriteit moet liggen bij de bescherming van informatie en informatie-uitwisseling. Daarnaast moeten systemen weerbaar zijn door snel te kunnen reageren op een aanval en in staat te zijn zich aan te passen om te blijven functioneren.

De belangrijkste kwetsbaarheid die kan leiden tot het verlies of het compromitteren van informatie komt doorgaans voort uit onopzettelijk handelen door medewerkers, zoals ondeskundig of onzorgvuldig gebruik van ICT-middelen. Daarom is het noodzakelijk dat elke defensiemedewerker zich bewust is van de risico's die aan het gebruik van digitale middelen zijn verbonden. Digitaal beveiligingsbewustzijn zal daarom integraal onderdeel uitmaken van alle defensieopleidingen. Ook moeten defensiemedewerkers worden geoefend in het werken onder omstandigheden waarbij ze tijdelijk niet kunnen beschikken over de (volledige) functionaliteit van netwerken en systemen.

Defensie zal de bescherming van haar netwerken en systemen (continu) versterken. De uitvoering hiervan ligt bij het Joint Informatievoorzieningscommando (JIVC) in oprichting, dat naar verwachting begin 2013 operationeel zal zijn. Het JIVC realiseert toereikende en hoogwaardige beveiliging en bewaakt daarbij alle netwerken en systemen. Onrechtmatig

en afwijkend gebruik wordt gesignaleerd. Het Defensie *Computer Emergency Response Team* (DefCERT) waakt over de beveiliging van systemen en netwerken, rekening houdend met actuele dreigingsniveaus. DefCERT, dat onderdeel zal worden van het JIVC, moet 24 uur per dag, zeven dagen per week risico's voor en kwetsbaarheden van de belangrijkste defensienetwerken identificeren en analyseren en de defensieorganisatie adviseren over de te nemen beveiligingsmaatregelen. Ook DefCERT moet beschikken over een goede cyber *situational awareness*. DefCERT werkt hiertoe binnen Defensie nauw samen met de overige onderdelen van het JIVC en met de MIVD. Buiten Defensie wordt samengewerkt met het NCSC, de NAVO, andere CERT's en met bedrijven die over specifieke kennis of middelen beschikken. Dit kan zowel informatie-uitwisseling betreffen als (personele) ondersteuning bij calamiteiten.

Met de beschikbare defensieve cybercapaciteit moet zowel de ICT-infrastructuur van Defensie worden beschermd, als de door Defensie gebruikte unieke wapen- en sensorsystemen. Het betreft hier capaciteiten ter bescherming van zowel de generieke netwerken en systemen van Defensie door het JIVC als de operationele netwerken en systemen tijdens inzet door het DCC. Ook zal Defensie de betrouwbaarheid van wapen- en sensorsystemen verbeteren door het inzicht in digitale kwetsbaarheden te vergroten en de controle over de ontwikkeling, de *supply chain* en het gebruik van ICT-componenten te versterken. Bijzondere aandacht is er bij aanschaf van zowel software als hardware voor de digitale weerbaarheid. Bij de aanschaf of ontwikkeling van nieuwe systemen moet van meet af aan rekening worden gehouden met mogelijke risico's voor de betrouwbaarheid van die systemen. Deze risico's moeten zo mogelijk vooraf worden beperkt door beveiligingseisen of beveiligingsmaatregelen.

Speerpunt 3: Offensief

Offensieve cybercapaciteiten zijn die capaciteiten die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Defensie moet over de kennis en capaciteiten te beschikken om offensief op te treden in het digitale domein, zowel om een effectieve verdediging te kunnen voeren als ter ondersteuning van operaties.

Het gaat hier om het ontwikkelen van (kennis over) complexe en hoogtechnologische middelen en technieken die er specifiek op zijn gericht het eigen militaire vermogen te vergroten. Zo kan een cyberaanval op een luchtverdedigingssysteem de effectiviteit van een eigen luchtaanval vergroten terwijl het risico op nevenschade wordt beperkt.

Een offensieve cybercapaciteit kan fungeren als een *force multiplier* en daarmee de effectiviteit van de krijgsmacht vergroten. Door de ontwikkeling van een robuuste cybercapaciteit kan Nederland op dit vlak binnen de NAVO een belangrijke rol gaan spelen.

De ontwikkeling van offensieve operationele capaciteiten staat internationaal nog in de kinderschoenen. Er is nog veel onduidelijk over de aard van deze capaciteiten, de mogelijkheden die ze kunnen bieden en de effecten die ermee kunnen worden gesorteerd. Offensieve cybercapaciteiten onderscheiden zich van conventionele militaire capaciteiten doordat ze vaak slechts eenmalig inzetbaar zijn en veelal een beperkte levensduur hebben. Hoogwaardige cybercapaciteiten zijn nauwelijks vergelijkbaar met algemeen bekende, relatief laagdrempelige en wijdverbreide aanvalsmethoden. Het gaat hier om complexe middelen waarvan de ontwikkeling zeer kennisintensief is en daardoor kostbaar en tijdrovend. Een uitdaging is dat de gewenste effecten moeilijk gegarandeerd kunnen worden doordat de tegenstander op elk moment zijn eigen kwetsbaarheid kan ontdekken en beperken.

Bij het ontwikkelen van offensieve operationele capaciteiten zal zoveel mogelijk gebruik worden gemaakt van kennis en middelen die bij de MIVD aanwezig zijn. Gezien de schaarste aan gekwalificeerd personeel moeten deze kennis en middelen zo doelmatig mogelijk worden ingezet en moet worden voorkomen dat binnen Defensie middelen dubbel worden ontwikkeld. De kennis, middelen, samenwerkingsrelaties van de MIVD worden daarom optimaal benut bij de ontwikkeling en de inzet van offensieve middelen door de Commandant der Strijdkrachten (CDS). De CDS kan deze offensieve middelen op grond van een mandaat van de regering in een militaire operatie inzetten, waarbij de wettelijk vereiste scheiding tussen de taken en de verantwoordelijkheden van de CDS en de MIVD onaangetast blijft. Tevens kunnen offensieve middelen worden ingezet om een cyber aanval te voorkomen of af te slaan en de vrijheid van het eigen militair optreden in het digitale domein te waarborgen (‘actieve verdediging’). Het DCC draagt zorg voor de gereedstelling van offensieve cybercapaciteiten voor inzet. De Taskforce Cyber zal een doctrine voor het optreden in het digitale domein opstellen, inzetscenario’s ontwikkelen en de effecten en gevolgen van offensieve middelen nader beschrijven. Dit gebeurt onder meer door het houden van testen, trainingen en oefeningen.

Speerpunt 4: Inlichtingen

De opkomst van het digitale domein en de toenemende onderlinge verbondenheid van systemen, hebben de mogelijkheid tot het vergaren van informatie enorm doen toenemen. Het bezitten van een hoogwaardige inlichtingenpositie in het digitale domein is een voorwaarde voor zowel de bescherming van de eigen infrastructuur als voor de uitvoering van operaties. Defensie moet zicht hebben op de dreigingen in het digitale domein waaraan zij kan worden blootgesteld om zich daar effectief tegen te kunnen wapenen. Dit vereist inzicht in zowel de technische dreiging als de mogelijkheden en intenties van (potentiële) tegenstanders en aanvallers. De MIVD moet daarom beschikken over inlichtingencapaciteiten om deze informatie te verwerven, te analyseren en daarover tijdig te rapporteren. Voorts zal de dienst over het vermogen moeten beschikken inlichtingenactiviteiten van anderen te verstoren en een halt toe te roepen. De inlichtingenactiviteiten van de MIVD in het digitale domein worden vanzelfsprekend binnen de wettelijke kaders uitgevoerd.

De MIVD zal de komende jaren de capaciteit uitbreiden voor het op heimelijke wijze verwerven van informatie binnen het digitale domein. De activiteiten omvatten onder meer het infiltreren in computers en netwerken om gegevens te verkrijgen, het in kaart brengen van relevante delen van het digitale domein, het monitoren van vitale netwerken en het doorgronden van de werking van en de techniek achter aanvalsmiddelen. De vergaarde informatie wordt gebruikt voor *early warning* inlichtingenproducten, het opstellen van een cyber dreigingsbeeld, het versterken van de inlichtingenproductie in brede zin en het uitvoeren van contra-inlichtingenactiviteiten. Het digitale inlichtingenvermogen kan niet los worden gezien van inlichtingencapaciteiten als *signals intelligence* (SIGINT) en *human intelligence* (HUMINT) en het bestaande contra-inlichtingenvermogen van de MIVD. Doorslaggevend voor de doeltreffendheid van het optreden is de gecombineerde inzet van schaarse expertise en middelen. De MIVD en AIVD intensiveren daartoe de samenwerking op het gebied van cyber en SIGINT door de oprichting van een gemeenschappelijke SIGINT-Cybereenheid. De oprichting van deze eenheid moet de effectiviteit van het nationale cyber inlichtingenvermogen verder versterken. De MIVD zal tevens bijdragen aan het verder ontwikkelen van het Cyber Security Beeld Nederland (CSBN) dat onder verantwoordelijkheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid van het ministerie van Veiligheid en Justitie wordt opgesteld.

Een complexe uitdaging vormt de attributie van gedetecteerde aanvallen of pogingen hiertoe. Als niet kan worden vastgesteld waar een dreiging of aanval vandaan komt, wie deze uitvoert en met welk doel, zijn de mogelijkheden tot een effectieve respons beperkt. De MIVD zal door middel van de inzet van alle mogelijke inlichtingenbronnen en forensisch onderzoek de mogelijkheden tot attributie vergroten en hierbij nauw samenwerken met onder andere het JIVC , de AIVD, het Nederlands Forensisch Instituut (NFI) en de opsporingsdiensten (het Korps Landelijke Politiediensten en de Koninklijke marechaussee). Voorts is intensieve vertrouwelijke internationale samenwerking vaak essentieel bij het uiteindelijk kunnen vaststellen van de identiteit van de aanvaller en het kunnen treffen van effectieve beschermingsmaatregelen.

Speerpunt 5: Adaptief en innovatief

De snelheid waarmee ontwikkelingen in het digitale domein zich voltrekken, stelt hoge eisen aan het aanpassingsvermogen en de innovatieve kracht van Defensie. Zij moet in het digitale domein in staat zijn snel nieuwe technologie in te voeren en korte innovatiecycli te doorlopen. De dynamiek en de complexiteit van het digitale domein vergen voortdurende aanpassing van (initiële) behoeften aan kennis, kunde, vaardigheden en technieken, en wijze van optreden.

Defensie moet over de kennis beschikken om relevante ontwikkelingen te volgen en hierop snel en doeltreffend in te spelen. Zij investeert in mensen, technologie, onderzoek en ontwikkeling om de noodzakelijke cybercapaciteiten tijdig te kunnen verwerven of ontwikkelen en in te kunnen voeren. Het Defensie Cyber Expertise Centrum (DCEC) wordt de centrale entiteit ter versterking van kennisontwikkeling, -borging en -verspreiding. Het DCEC moet de kennis van Defensie op het gebied van *cyber operations* op een hoog niveau brengen en houden. Het is zowel gericht op kennisontwikkeling (onder andere *research & development* en *concept development and experimentation*) als op kennisoverdracht (oefening, training en opleiding) binnen Defensie. Het DCEC zal intensief samenwerken met kennisinstellingen, zoals TNO.

Om de veiligheid van netwerken en systemen duurzaam te verbeteren moet Defensie snel en effectief kunnen reageren op nieuwe ontwikkelingen, nieuwe technieken in een vroeg stadium testen en toepassen en nauw samenwerken met het bedrijfsleven en de wetenschap. Aanbestedingen en verwerving in het digitale domein worden zo ingericht dat goed ingespeeld kan worden op het veranderlijke karakter van dit domein en tegelijkertijd de betrouwbaarheid van middelen en bedrijfsprocessen wordt gewaarborgd. In het digitale domein is het bedrijfsleven de motor van innovatie, ook met betrekking tot het beveiligen en beschermen van ICT-infrastructuur. Defensie moet dan ook optimaal gebruik maken van deze innovatiekracht. Het sourcingbeleid van Defensie kan hier een bijdrage aan leveren.

Voor onderzoek en ontwikkeling, maar ook voor opleiding, training en oefening zal Defensie beschikken over een ‘cyber laboratorium’ en een testomgeving. Dit cyberlab zal door de diverse onderdelen kunnen worden gebruikt en ook beschikbaar zijn voor partners. Onderdelen kunnen zich op verschillende fysieke locaties bevinden en op afstand worden gekoppeld.

Een bijzondere uitdaging voor Defensie vormt het aantrekken en het behouden van gekwalificeerd personeel dat ook kan functioneren in een militaire omgeving. De benodigde militaire personele capaciteit zal voor een deel worden gerealiseerd door de inzet van cyberreservisten. Om de noodzakelijke kennis, kunde en vaardigheden in huis te halen en binnen te houden wordt specifiek aandacht besteed aan personeelsbeleid en opleidingen. Zo zullen onder andere specifieke loopbaanpatronen worden ontwikkeld om de kennis en ervaringsopbouw van defensiemedewerkers op het gebied van cyber te verankeren en verder te ontwikkelen. Door samenwerking met het NCSC, opsporingsdiensten en het bedrijfsleven kan uitwisseling van personeel worden bevorderd. Hierdoor wordt een goede ervaringsopbouw gewaarborgd en kan medewerkers een interessant loopbaanperspectief worden geboden.

Nader onderzoek naar de impact van digitale middelen als operationele capaciteit en de dreiging die hiervan uitgaat tegen de krijgsmacht, zowel op technisch en procesmatig als op juridisch vlak, is noodzakelijk. Defensie zal hierbij aansluiting zoeken bij onderzoek dat elders in Nederland en internationaal wordt uitgevoerd. Ook voert Defensie zelfstandig onderzoek uit. Zo wordt in 2014 een leerstoel digitale weerbaarheid en *cyber operations* aan de Nederlandse defensieacademie (NLDA) ingesteld.

Speerpunt 6: Samenwerking

De digitale veiligheid is afhankelijk van het vermogen van landen en organisaties om het digitale domein te beschermen, individueel en gezamenlijk. Het digitale domein is van nature een domein waarin publieke en private, civiele en militaire en nationale en internationale actoren tegelijkertijd opereren en onderling afhankelijk zijn. Tevens zijn de technieken die door aanvallers worden gebruikt grotendeels overeenkomstig en maken deze gebruik van generieke kwetsbaarheden van netwerken en systemen. Een gezamenlijke aanpak van de digitale onveiligheid is daarom noodzakelijk om de digitale veiligheid duurzaam te versterken.

Nationaal
Voor Defensie is het van belang om in het kader van de Nationale Cyber Security Strategie (NCSS) nauw samen te werken met publieke en private partijen. Defensie is hiertoe onder meer vertegenwoordigd in de Cyber Security Raad (CSR) en neemt deel in het NCSC.

Als beheerder van hoogwaardige digitale netwerken en systemen is Defensie een belangrijke partner die beschikt over bijzondere kennis en capaciteiten. Op grond van de derde hoofdtaak kan Defensie op verzoek deze kennis en capaciteiten aan civiele autoriteiten beschikbaar stellen. Na formele aanvraag en toestemming conform de wettelijke basis voor bijstand of de regelgeving voor steunverlening kan, onder gezag van de aanvrager, worden opgetreden. De wijze waarop capaciteit in het kader van cyberoperaties beschikbaar kan worden gesteld, wordt nader uitgewerkt. Daarnaast is er reden te bezien of digitale middelen van Defensie kunnen worden betrokken bij de bestuurlijke afspraken over de specifieke gegarandeerde beschikbaarheid van de krijgsmacht in het kader van de Intensivering Civiel Militaire Samenwerking (ICMS). De capaciteiten van Defensie zullen een bijdrage moeten leveren aan het vergroten van de veiligheid en de betrouwbaarheid van het gehele Nederlandse digitale domein.

Bij het organiseren van een gezamenlijke aanpak is het van belang dat rollen, taken en verantwoordelijkheden duidelijk zijn. In dit kader zal, op initiatief van de NCTV, worden bezien of de huidige crisisbeheersingsstructuur toereikend is voor het snel en effectief beheersbaar maken van een grootschalige digitale verstoring. Defensie zal hier aan bijdragen.

Samenwerking met publieke partners, universiteiten en het bedrijfsleven is ook nodig op het gebied van onderzoek en ontwikkeling, opleiding en personeel. Partijen hebben te maken met dezelfde uitdagingen, zoals beperkte budgetten en schaarste aan gekwalificeerd personeel. Nieuwe mogelijkheden tot strategische samenwerking moeten worden onderzocht. Defensie draagt bij aan de Nationale Cyber Security Research Agenda en, in het kader van het bedrijfslevenbeleid van het kabinet, aan de specifieke aandacht die in de topsector *High Tech* wordt geschonken aan *cyber security*. Ook in dit verband zal Defensie nauw met andere departementen, de kennisinstellingen en het bedrijfsleven optrekken. Ten aanzien van het ontwikkelen van middelen zal worden gezocht naar mogelijkheden van allianties met het bedrijfsleven.

Internationaal
In internationaal verband zoekt Defensie samenwerking met landen die een vergelijkbare ambitie en aanpak als Nederland voorstaan en die op een vergelijkbaar niveau opereren. Doel van de samenwerking is in eerste aanleg gericht op het uitwisselen van kennis. Later zal ook worden bezien wat de mogelijkheden zijn tot het gezamenlijk ontwikkelen van middelen en technieken en het gezamenlijk inrichten van capaciteiten.

De NAVO is voor Defensie de primaire organisatie voor samenwerking ter vergroting van de weerbaarheid in het digitale domein. Defensie draagt daartoe onder meer actief bij aan de ontwikkeling en uitvoering van het beleid van de NAVO. Zoals onderstreept tijdens de top in Chicago in mei 2012 zal de NAVO de weerbaarheid versterken van de eigen netwerken en systemen en die van bondgenoten die essentieel zijn voor het functioneren van de NAVO. Nederland onderschrijft tevens de ambitie van de NAVO de gezamenlijke capaciteit voor inlichtingenanalyse te versterken. Het is niet aannemelijk dat in NAVO-verband gemeenschappelijke cybercapaciteiten worden ontwikkeld. Wel moet het bondgenootschap een visie ontwikkelen op de inzet van cybercapaciteiten in NAVO-operaties.

Defensie steunt ook de inzet van de EU om te komen tot een integrale internetveiligheidsstrategie. Voor Defensie is van belang dat de EU en de NAVO intensief samenwerken bij het vergroten van de weerbaarheid van lidstaten. Daartoe is het onder meer van belang dat de informatie-uitwisseling op dit terrein tussen beide organisaties wordt geïntensiveerd.

Tot slot

De in deze strategie opgenomen speerpunten moeten ervoor zorgen dat de krijgsmacht doeltreffend en doelmatig kan opereren in het digitale domein. Door te investeren in digitale weerbaarheid en operationele capaciteiten blijft Nederland beschikken over een hoogwaardige en technologisch vooraanstaande krijgsmacht die veelzijdig inzetbaar is en in alle domeinen haar taken kan uitvoeren. In de begroting en het jaarverslag zal de Tweede Kamer worden geïnformeerd over de voortgang van uitvoering van deze strategie. In 2016 zal voorts een beleidsdoorlichting worden uitgevoerd.

Deze brochure is een uitgave van:
Ministerie van Defensie
Bestuurstaf

juni 2012