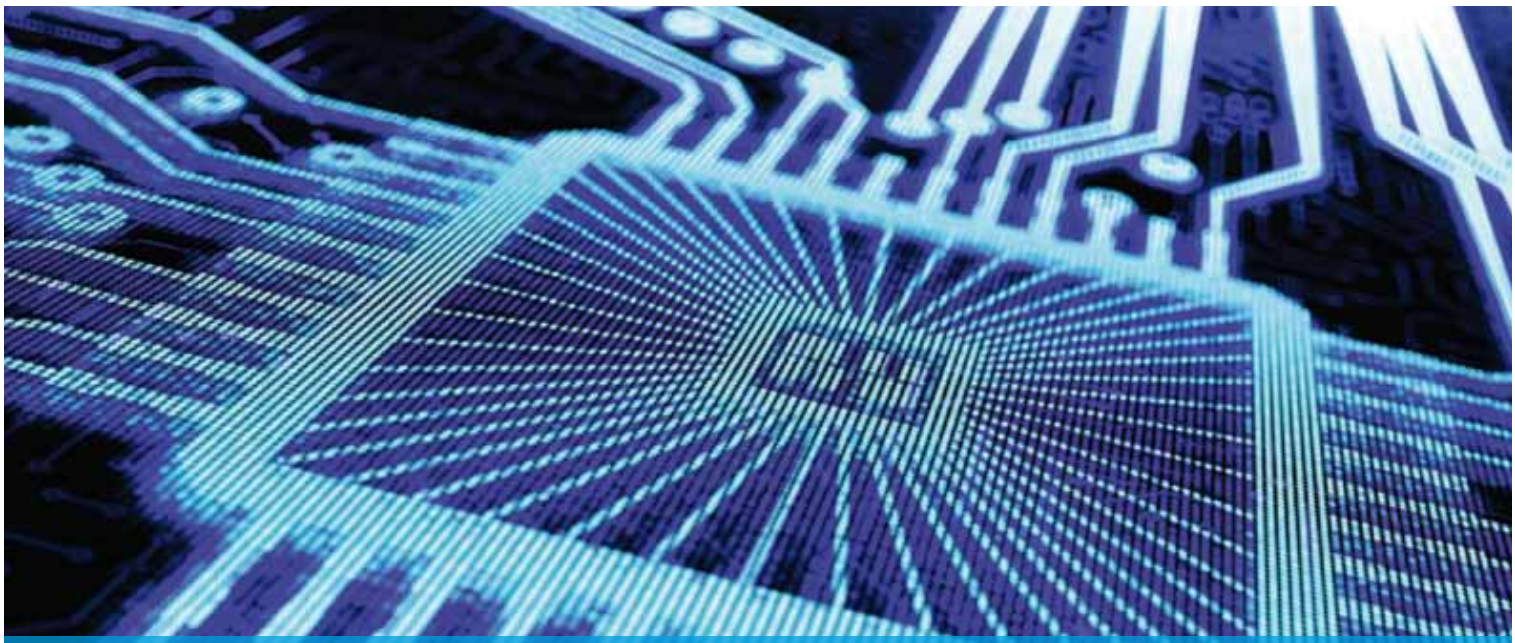

Aanpak toenemende digitale dreiging

Defensie geeft vorm aan cybercapaciteit

Digitale spionage en cybercriminaliteit vormt volgens veel deskundigen en inlichtingendiensten momenteel de grootste dreiging voor overheid en bedrijfsleven. Recente cyber incidenten, waaronder de DDOS-aanvallen op Nederlandse banken, tonen aan dat er ook in ons land cyberinstrumenten worden gebruikt voor malafide cyber-activiteiten.

KLTZ Peter Kwant, plv commandant Taskforce Cyber.

Bij Defensie is sinds begin 2012 de Taskforce Cyber (TFC) actief. Deze taakgroep is opgericht om nieuwe Cybercapaciteiten binnen defensie te initiëren en de ontwikkeling van reeds bestaande cybercapaciteiten te coördineren. Het Marineblad sprak met KLTZ Peter Kwant, plaatsvervangend commandant Taskforce Cyber.

Bekend is dat statelijke actoren, waaronder China, proberen gevoelige politieke, militaire, technisch-wetenschappelijke en economische informatie te krijgen. Zeer onlangs kwam dit weer in de aandacht bij de publicatie van het Mandiant-rapport. De conclusie van dit rapport was dat een groep *hackers* in Shanghai – naar Mandiant's overtuiging aantoonbaar in dienst van de Chinese krijgsmacht als Unit 61398 – zes jaar lang systematisch honderden terabytes aan data hebben gestolen van ten minste 141 bedrijven, organisaties en overheidsinstanties, in de Verenigde Staten en daarbuiten. Het is echter onmogelijk om dergelijke beschuldigingen hard te bewijzen.

Volgens de New York Times worden er ook door de VS forse investeringen gedaan in het cyberdomein. De krant publiceerde op basis van anonieme bronnen binnen het Amerikaanse leger en de inlichtingendiensten dat de VS betrokken waren bij de ontwikkeling en de inzet van de Stuxnet-worm waarmee in 2011centrifuges in de Iranese nucleaire faciliteit in Natanz werden uitgeschakeld.

Door de geavanceerde ICT-infrastructuur en de aard van de Nederlandse economie is het waarschijnlijk dat malafide cyberactiviteiten zullen toenemen, die daardoor in potentie een aanzienlijke bedreiging vormen voor de Nederlandse economie en de nationale veiligheid. Cyber incidenten, zoals DigiNotar en Pobelka, bewijzen dat dit in ons land ook al daadwerkelijk gebeurt.

Civiele (AIVD) en militaire (MIVD) diensten bundelen daarom sinds oktober 2011 hun krachten in de gezamenlijke sigint-cyber eenheid met het project 'Symbolon'. Hierbij wordt geïnvesteerd in digitale onderzoekscapaciteit en –expertise. Het betreft hier ondermeer uitbreiding van de detectiecapaciteit om het zicht op cyberspionage in Nederland te vergroten.

Daarnaast investeert Defensie in cybercapaciteiten. Bij al deze activiteiten wordt nauw samengewerkt met het Nationale Cyber Security Centrum (NCSC). Het NCSC heeft onder meer de taak om publieke en private instellingen, waaronder dus ook Defensie, actief te waarschuwen voor kwetsbaarheden en te adviseren over te nemen maatregelen.

Wat is cyber, welke definitie houdt Defensie aan?

'Er bestaat op dit ogenblik geen internationaal geaccepteerde definitie van het begrip digitaal domein, of *cyberspace*. In de Defensie cyberstrategie 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 enige wijze de gegevens, zoals data, programmacode en informatie, die zich in dit domein bevinden.'

Aan welke Nederlandse belangen moeten we denken bij cyberveiligheid?

'De nationale cyber veiligheidsstrategie is gebaseerd op drie kernwaarden: de economische belangen in het digitale domein, de privacy van de burgers en de veiligheid van de staat. Defensie speelt bij het beschermen van al deze waarden een relevante rol. Maar de primaire verantwoordelijkheid voor de cyberveiligheid van civiele partijen ligt nadrukkelijk bij de belanghebbenden zelf. Enigszins gechargeerd gesteld is Defensie niet de digitale brandweer van de samenleving. Ook in het cyberdomein kan Defensie alleen optreden binnen grondwettelijke en internationaal rechtelijke kaders die ook in het fysieke domein gelden.'

Defensie moet over de kennis en capaciteiten beschikken om offensief op te treden in het digitale domein, zowel om een effectieve verdediging te kunnen voeren als ter ondersteuning van operaties.

Is de cyberstrategie puur defensief georiënteerd?

'Het onderscheid tussen defensief en offensief is in elk domein lastig te maken. Veelal wordt aangenomen dat het onderscheid niet zozeer zit in de technologie als wel in de intentie van de operator. Volgens de cyberstrategie zijn offensieve cybercapaciteiten die capaciteiten die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Defensie moet over de kennis en capaciteiten beschikken om offensief op te treden in het digitale domein, zowel om een effectieve verdediging te kunnen voeren als ter ondersteuning van operaties.

Oprichting cybercapaciteit Defensie

In de beleidsbrief van 2011 wordt de oprichting van een nieuwe Defensie cybercapaciteit aangekondigd. In de nota "Maatregelen beleidsbrief" wordt het voornemen met een financiële reeks en aanvullende aanwijzingen aangevuld:

'De cybercapaciteit van Defensie zal gefaseerd worden ingevoerd. Het zwaartepunt ligt de komende jaren bij het verbeteren van de bescherming van de netwerken, systemen en informatie van Defensie en de uitbreiding van de inlichtingencapaciteit in het digitale domein.
Een programmamanager wordt belast met de ontwikkeling van een initiële operationele cybercapaciteit. In het operationele domein is een belangrijke, uitvoerende rol weggelegd voor het CLAS. Voor de periode 2011 tot 2015 bedraagt de totale intensivering € 45 miljoen, inclusief de personele exploitatie. De thans geplande cybercapaciteit zal in 2016 gereed zijn. Daarna bedraagt de intensivering structureel € 21 miljoen.'

Taken Taskforce Cyber

Voor de uitvoering van het voornemen is begin 2012 een Taskforce Cyber (TFC) aangesteld. Sindsdien heeft de TFC zich geconcentreerd op urgente prioriteiten, zoals het versterken van het Defensie Computer Emergency Response Team (DefCERT) en de Militaire Inlichtingen en Veiligheidsdienst (MIVD), het bijdragen aan de Defensie cyberstrategie, het initiëren van cyber *awareness* trainingen en het opbouwen van een netwerk voor samenwerking en samenhang met cyber-gerelateerde organisaties, zowel intern als extern Defensie en in binnen- en buitenland.

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 CDS kan deze offensieve middelen op grond van een mandaat van de regering in een militaire operatie inzetten. Tevens kunnen offensieve middelen worden ingezet om een cyberaanval te voorkomen of af te slaan en de vrijheid van het eigen militair optreden in het digitale domein te waarborgen, ook wel "actieve verdediging" genoemd.'

Met welke civiele instanties werkt Defensie samen?

'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 komen de technieken die door aanvallers worden gebruikt grotendeels overeen 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.

Defensie is door de Directeur Operationeel Beleid, Behoeften en Plannen (DOBBP) vertegenwoordigd in de publiek-private Cyber Security Raad (CSR) onder het duo voorzitterschap van de CEO KPN en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV). Verder is Defensie via de commandant TFC actief in het Nationale Cyber Security Centrum (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. De capaciteiten van Defensie zullen op die manier een bijdrage leveren aan het vergroten van de veiligheid en de betrouwbaarheid van het gehele Nederlandse digitale domein.

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 worden ook voortdurend onderzocht.

Defensie draagt bij aan de Nationale Cyber Security Research Agenda waarin de R&D programma's van de verschillende departementen worden gecoördineerd.

Maar ook wordt er door het bedrijfslevenbeleid van het kabinet, in de topsector High Tech specifieke aandacht geschonken aan *cyber security*. Ook in dit verband zal Defensie nauw met andere departementen, de kennisinstellingen en het bedrijfsleven optrekken.'

Wat doet DefCERT, richt het zich enkel op het beschermen van de eigen systemen?

'Het Defensie Computer Emergency Response Team (DefCERT) waakt over de beveiliging van systemen en netwerken, rekening houdend met actuele dreigingsniveaus. DefCERT, dat onderdeel is van DMO/ 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.

Onlangs is er een convenant afgesloten tussen het NCSC en DefCERT waardoor deze partijen nu ook direct informatie kunnen uitwisselen. Bij het DigiNotar-incident heeft Defensie al aangetoond een wezenlijke en zeer gewaardeerde technische ondersteuning te kunnen bieden aan de civiele autoriteiten. Maar andersom is het ook mogelijk dat het NCSC op haar beurt ondersteuning geeft als er bij Defensie een cyberincident mocht plaatsvinden.'

Zijn we niet rijkelijk laat met het opzetten van DefCERT?

'Nee, zeker niet. Defensie had al in 2004 als één van de eerste organisaties in Nederland een CSIRT-capaciteit (Computer Security incident Response team) de voorloper van de capaciteit die we nu CERT (Computer Emergency Response Team) noemen. De kwaliteit en het volume van ons DefCERT is sindsdien enorm gegroeid en zal aan het eind van 2013 meer dan 30 VTE-en omvatten.'

In welke mate krijgt Defensie mogelijkheden om zelf binnen Nederland netwerken aan te vallen om beveiligingsrisico's te inventariseren?

'Onze defensienetwerken worden door de IVENT-organisatie ((Informatievoorziening en -Technologie), als onderdeel van de Defensie Materieel Organisatie /JIVC, beheerd. Bij die beheertaak hoort ook het verzorgen van de veiligheid van die netwerken. DefCERT heeft onder meer als taak om toezicht te houden op de uitvoering van die beveiligingstaak. Daarnaast monitort DefCERT, in nauwe samenwerking met nationale en internationale partners de omgeving van onze defensienetwerken, waardoor er een actueel beeld is van de mogelijke dreigingen die op onze netwerken af komen. Maar DefCERT is dus niet een soort Cyber geheime dienst binnen Defensie.

Medio 2015 wordt het Defensie Cyber Commando (DCC) opgericht en door dit commando zullen cybercapaciteiten worden ontwikkeld en gereedgesteld waarmee cyberinterventies uitgevoerd kunnen gaan worden. Het DCC wordt onder Single-Service Management

Het digitale domein wordt beschouwd als een vijfde operatiegebied – zij het met specifieke kenmerken – dat interacteert met de andere vier dimensies voor militaire operaties: land, zee, lucht en ruimte.

ondergebracht bij de CLAS. De operationele inzet zal, net als alle andere operationele capaciteiten van Defensie, worden aangestuurd door de CDS.

Om te controleren of onze defensienetwerken goed worden bewaakt worden deze bij voortduring getest. Dit vindt op vele niveaus plaats. Indien zo'n test een grootschalig en integraal karakter heeft, noemen we die dit ook wel een 'Red Team'-operatie. In dat geval weten slechts enkele defensiemedewerkers vooraf van de test af. Onlangs is er weer zo'n 'Red Team'-actie geweest, die is uitgevoerd door een zeer prominente gespecialiseerde firma. Defensie kwam daar heel behoorlijk uit, maar daaruit leerden we ook dat ondanks het hoge veiligheidsniveau er ook bij Defensie geen 100% veiligheid bestaat.'

Hoe staat de Taskforce Cyber in relatie tot het Defensie Cyber Commando en het DefCERT?

'De commandant TFC heeft de opdracht om als programmamanager namens de CDS de cyberintensivering gecoördineerd uit te voeren. Het intensiveringprogramma omvat versterkingen van capaciteiten die functioneel zijn ondergebracht bij verschillende defensieonderdelen: DefCERT bij DMO/JIVC; het Defensie Cyber Commando bij CDS en later bij CLAS; MIVD bij de Bestuursstaf en het NLDA bij het CDC. Als dit programma is afgerond zal de Taskforce waarschijnlijk opgaan in het DCC.'

Welke veiligheidsmaatregelen kan Defensie nemen als bedrijven niet meewerken?

'De MIVD beschikt over het vermogen om inlichtingenactiviteiten van anderen te verstoren en een halt toe te roepen. Bedrijven die omgaan met vertrouwelijke defensie-informatie zijn daarom gehouden aan het beleid van de MIVD voor de beveiliging van gerubriceerde en risicogevoelige informatie. Bedrijven zijn verplicht de opgelegde beveiligingseisen in te voeren. De MIVD controleert de naleving van deze beveiligingsmaatregelen. Deze eisen staan beschreven in de Algemene Beveiligingseisen voor Defensieopdrachten 2006, ook wel de ABDO 2006 genoemd.'

Satcom is een nauwe bundel en dus moeilijk af te luisteren/in te breken. In welke mate is extra cyberbeveiliging van toepassing op de netwerken aan boord van marineschepen?

'Cyber en wat we tegenwoordig noemen *Information Assurance* (IA) zijn niet hetzelfde. IA gaat voornamelijk over de beveiliging van de informatie zelf, cyber richt zich meer op de technologie waarmee informatie wordt verwerkt. Deze domeinen zijn wel complementair, hebben raakvlakken, net als het domein 'Elektronische Oorlogvoering' overigens.
Het afluisteren van transmissiekanalen is een passieve activiteit en niet altijd te voorkomen. Door onder meer cryptosystemen zorg je ervoor dat de afluisteraar alleen niets met de data kan doen. Cyberoperaties zijn

daarentegen meer actief, waarbij de *cyberoperators* – militaire *hackers* – proberen te interveniëren in een systeem. Het ontdekken en voorkomen van *hacken* is dus ook dynamisch, waarbij je actief monitort wat er op en bij je netwerken gebeurt en waarbij je dus snel moet reageren als blijkt dat er een onverwachte kwetsbaarheid optreedt.

Voor welk soort aanvallen zijn defensie-netwerken vatbaar?

'Zoals ik eerder aangaf bestaat 100% veiligheid niet. Ook Defensie kan dus last hebben van cyberaanvallen, maar Defensie is zich wel meer dan civiele partijen bewust van haar kwetsbaarheid en wij investeren dus ook aanzienlijk in de veiligheid. Een belangrijke kwetsbaarheid bij normale organisaties komt vaak voort uit directe koppelingen van de werkplek aan internet. Ons internet op de werkplek is een gescheiden functionaliteit en daarmee veel veiliger. Die scheiding kent overigens uit gebruikersoogpunt ook behoorlijke nadelen, maar dat moeten we accepteren.'

In hoeverre is de beveiliging tegen cyber reactief dan wel pro-actief? Kan het overzee worden ingezet ter bescherming van troepen?

'Of een wapen reactief of proactief is, is een zaak van de *operator*, niet zozeer van het instrument. Het concept van preventieve interventies is zoals bekend, tamelijk omstreden.
Maar het internationaal recht en het humanitair oorlogsrecht vormen op zichzelf geen belemmering voor de inzet van cyberinstrumenten. Het besluit of het mag is daardoor een politieke keuze. En daaraan voorafgaand zal Defensie zelf moeten kunnen laten zien dat een dergelijk instrument ook op een effectieve manier kan worden ingezet.'

Bestaat er een specifieke maritieme cyber ruimte?

'*Cyberspace*, of het digitale domein, is geen losgekoppelde en zelfstandige 'ruimte'. Het is niet alleen het internet, maar ook alle niet met internet verbonden netwerken of andere digitale apparaten.

Wanneer we dit vertalen in termen van militaire activiteiten, dan wordt het digitale domein beschouwd als een vijfde operatiegebied – zij het met specifieke kenmerken – dat interacteert met de andere vier dimensies voor militaire operaties: land, zee, lucht en ruimte.
Dit betekent dat operaties in de vijfde dimensie ook kunnen fungeren als *force multiplier* van activiteiten in de overige dimensies. Het optreden in andere dimensies is overigens nauwelijks meer mogelijk zonder het gebruik van digitale middelen.

Oorlogen werden aanvankelijk alleen te land en ter zee uitgevochten. Aan het begin van de Eerste Wereldoorlog kwam hier, met de strijd in de lucht, een derde dimensie bij. Vanaf de jaren '80 kreeg de vierde dimensie, met de ontwikkeling van anti-satellietraketten en het *Space Defence Initiative*, operationele betekenis. De ontwikkeling en verspreiding van internet alsmede de algehele digitalisering van de samenleving maakt dat nu wordt gesproken over een vijfde dimensie.

Bij het uitvoeren van militaire operaties kan er voor worden gekozen ook gebruik te maken van digitale aanvallen. In essentie gaat het om de inzet van een middel – digitale capaciteit – uit de *toolbox* van militaire middelen die een bijdrage kunnen leveren aan het bereiken van een politiek doel. In een aantal van de meest bekende voorbeelden zijn digitale aanvallen gecombineerd met conventionele operaties. In het geval van de Stuxnet-worm was het noodzakelijk om het geïnfecteerde programma via een fysieke *human intelligence*operatie de Iraanse verrijkingscentrale in te smokkelen. Uiteraard is het mogelijk om een militaire operatie te beperken tot het uitvoeren van digitale aanvallen. Op deze wijze zou het technisch uitvoerbaar kunnen zijn om delen van de kritieke infrastructuur van een land – in ieder geval tijdelijk – te ontregelen.

Het is te verwachten dat het digitale domein in elk toekomstig conflict een belangrijke rol zal spelen. Een cyberoorlog, die uitsluitend in het digitale domein wordt uitgevochten, met verwoestende gevolgen, is echter niet aannemelijk. *Cyber warfare* kun je dus beschouwen als een onderdeel van een militaire operatie, die ook andere (niet digitale) dimensies kan omvatten.

Bij het *Maritime Warfare Centre* (MWC) en bij de NLMARFOR-staf worden analyses uitgevoerd over de integratie van cyber in het maritieme domein. Zo worden er met de andere OPCO's en TNO fictieve scenario's ontwikkeld waarin cyberelementen worden verwerkt. Het doel hiervan is om aan de hand van praktische en realistische gebeurtenissen inzicht te krijgen in de inhoud en consequenties van *cyber operations* in de context van de Nederlandse krijgsmacht.

Bij oefeningen, zoals bij Joint Warrior waaraan NLMARFOR onlangs deelnam, worden cyberincidenten in het oefenprogramma verwerkt. In geval van een cyberaanval moet de Taskgroup zorgen voor de continuïteit van Command en Control (C2) op het C2-netwerk. Deze ervaringen zijn enorm waardevol voor de opbouw van de cyberkennis van onze *operators*.' <

Lees verder op de KVMO-site!

Scan de QR-code, of ga naar kvmo.nl/2013, voor personele en opleidingsvragen met betrekking tot cyber.