DEFENSIE ONTWIKKELT EEN NIEUW WAPEN

Cyber **Operations**

'One hacker and one modem cause an enemy damage and losses almost equal to those of a war.'

Qiao Liang and Wang Xiangsui, Unrestricted Warfare (1999)

Dagelijks worden we in kranten en websites geïnformeerd over cybernieuws. Of het nu gaat over het hacken van websites, het ontvreemden van creditcardnummers of de invasie van ongewenste e-mails. Iedereen heeft er tegenwoordig mee te maken. Enerzijds omdat we allemaal internet gebruiken en niet meer zonder kunnen en anderzijds omdat we ons leven digitaal hebben ingericht. Wat velen zich echter niet realiseren, is dat deze voorbeelden nog maar 'kruimeldiefstallen' zijn in vergelijking tot de gewapende overvallen die ons te wachten staan, of mogelijk al plaatsvinden! De dreiging die komt vanuit het cyberdomein is namelijk niet in te schatten.

HANS FOLMER

Recentelijk is in de buurt van Utrecht een signaalkabel van Rijkswaterstaat kapot gegaan. Resultaat was dat op alle wegen rondom Utrecht boven alle rijbanen een rood kruis verscheen. Een verkeersinfarct was het gevolg. Een grote bank had recentelijk grote problemen met internetbankieren en de mobiele applicaties. Duizenden webshops konden de aankopen van klanten niet afrekenen. Een grote telecommaatschappij moest de e-mail van haar klanten blokkeren omdat onduidelijk was of bij een inbraak in het computersysteem gegevens waren ontvreemd. Kunt u zich voorstellen wat er gebeurt als al deze zaken tegelijk plaatsvinden en daarnaast in grote delen van het land de stroom uitvalt, er geen water meer uit de kraan komt, enkele gemalen niet meer functioneren en de luchtverkeersleiding foute positie- en hoogtegegevens aan vliegtuigen doorgeeft? Helaas is dit scenario niet ondenkbaar. Dus moet er iets gedaan worden om dit te voorkomen.

Na een kort overzicht van de algemene dreiging en de Nationale Cyber Security Strategie zal ik aangeven wat de specifieke cyberdreiging is voor Defensie. Daarna ga ik in op de kansen die dit voor Defensie biedt en hoe militairen in operaties van cyberspace gebruik zullen maken. Ik geef aan hoe de toekomstige cyberorganisatie van de krijgsmacht er in grote lijnen uitziet en zal ingaan op uitdagingen en juridisch kader.

NATIONALE STRATEGIE

Nationaal zijn er in het afgelopen jaar veel stappen gezet op weg naar een veiliger digitaal domein. Nadat onderkend was dat er in Nederland duidelijke afspraken over verantwoordelijkheden en taken op het gebied van cyber security (zie definitie in kader) nodig zijn, is in maart 2012 door de regering de Nationale Cyber Security Strategie (NCSS) gepresenteerd. In de NCSS wordt gesteld dat digitale weerbaarheid van fundamenteel belang is voor de samenleving en de economie. Diezelfde samenleving is echter wel kwetsbaar en dient beschermd te worden. Dat is niet primair een taak van de overheid, maar van de eigenaren en beheerders van ICT-middelen. De minister van Veiligheid en Justitie heeft een coördinerende rol. Het doel van de NCSS is het realiseren van veiligheid en vertrouwen in een open en vrije digitale samenleving.

'Cyber security is het vrij zijn van gevaar of schade, veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.'

NCSS, maart 2012

In de NCSS is een viertal mijlpalen gesteld om dit doel te bereiken.

Ten eerste de oprichting per 1 juli 2011 van een Cyber Security Raad (CSR). De CSR is een adviesorgaan van de regering bestaande uit vertegenwoordigers van publieke en private partijen en wetenschappers. De CSR wordt voorgezeten door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en door de Bestuursvoorzitter van KPN.

Ten tweede de oprichting per 1 januari 2012 van het Nationale Cyber Security Centrum (NCSC). Het NCSC is een platform waar overheid en bedrijfsleven kennis over cyber security(incidenten) delen. Het voormalige Govcert.nl maakt deel uit van het NCSC en geeft op basis van verzamelde informatie cyber securityadviezen aan de verschillende partijen. Het NCSC is onderdeel van de organisatie van de NCTV. Diverse departementen, waaronder Defensie, hebben liaisonofficieren in het NCSC.

Ten derde is in de NCSS een nationale cyberdreigingsanalyse aangekondigd. Afgelopen december is het Cyber Security Beeld Nederland voor het eerst verschenen.

Ten vierde zal onderzoek en onderwijs op cybergebied worden gestimuleerd en gecoördineerd. Op dit moment wordt door alle betrokken departementen een inventarisatie gemaakt van lopende onderzoeksprogramma's om doublures te voorkomen.

DEFENSIE

Voor Defensie is in de NCSS een aantal specifieke taken opgenomen. Defensie heeft de opdracht gekregen om kennis en capaciteiten te ontwikkelen om in het digitale domein effectief te kunnen opereren. Daarbij staat in de NCSS de duidelijke aanwijzing dat maximaal moet worden ingezet op de mogelijkheden om kennis en expertise uit te wisselen met civiele en internationale partners. Tevens zal Defensie kennis en capaciteiten voor haar (derde) hoofdtaak, het ondersteunen van civiele autoriteiten in geval van crisis, beschikbaar stellen binnen de daarvoor gemaakte afspraken.

DREIGING VOOR DEFENSIE

Defensie is net als elk ander departement en groot bedrijf afhankelijk van interne en externe netwerken. Niet alleen de netwerken die in verbinding staan met internet, maar ook netwerken die verbinding onderhouden met de operatiegebieden en hoog geclassificeerde netwerken. Daarnaast is defensie voor alle communicatie afhankelijk van digitale verbindingsmiddelen. Maar heden ten dage zijn ook alle wapensystemen en sensorsystemen afhankelijk van ICT. Geen enkel wapen of sensorsysteem kan nog functioneren zonder de digitale middelen. Of het nu gaat om de radar van een fregat, de hoogtemeter in een F16 of het *battlefield* managementsysteem in een pantserrupsvoertuig. Tot voor kort was de algemene opvatting dat dit soort gespecialiseerde, geïsoleerde en onafhankelijke systemen niet gevoelig zouden zijn voor cyberaanvallen. Helaas is dat niet zo. De Stuxnet-aanval op een ultracentrifuge fabriek in Iran heeft laten zien dat het met veel inspanning, kennis en geld mogelijk is om ook zeer specifieke systemen aan te vallen. Het voert te ver daar in dit kader op in te gaan, maar het heeft wel de ogen geopend. De conclusie kan niet anders zijn dan dat Defensie kwetsbaar is voor cyberaanvallen en zich daartegen moet verdedigen.

KANSEN VOOR DEFENSIE

Maar er zijn ook kansen! De opponent is net zo kwetsbaar als wij zijn. Ook de tegenstander is afhankelijk van ICT. Daarbij maakt het niet uit of deze tegenstander technologisch ontwikkeld is of dat het een guerrillastrijder is die gebruikmaakt van een internetcafé en zijn mobiele telefoon. Deze kwetsbaarheid moeten we uitbuiten. Defensie moet in staat zijn om in het digitale domein inlichtingen te verzamelen. Dus door in te breken in vijandelijke systemen om informatie uit die systemen te halen. Maar Defensie moet ook offensief op kunnen treden. Dat kan eenvoudig, bijvoorbeeld door een propagandawebsite te hacken en van andere informatie te voorzien, maar het kan ook verder gaan. Van het hacken van vijandelijke commandovoeringsystemen en de informatie veranderen of verwijderen, tot het met behulp van een cyberwapen uitschakelen van vijandelijke radarsystemen.

De taken van Defensie vloeien voort uit de bepalingen over de krijgsmacht in de Grondwet. Artikel 97 van de Grondwet stelt dat er een krijgsmacht is 'ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde.' Deze doelen zijn bewust abstract beschreven om zo het hoofd te kunnen bieden aan nieuwe bedreigingen als terrorisme, aan nieuw materieel en nieuwe inzetmethoden, aan gecombineerde trainingsmissies of aan de beveiliging van de koopvaardij voor de kusten van verre, warme landen. Defensie heeft dus de ruimte en het mandaat om op nieuwe dreigingen als in het cyberdomein te reageren en moet zich ook voorbereiden op passende antwoorden.

> 'We must learn to defend, delay, attack and manoeuvre in cyberspace, just as we might on the land, sea or air and all together at the same time.'
>
> *Sir General David Richards*

CYBER OPERATIONS

Defensie moet capaciteiten ontwikkelen om in het cyberdomein op dezelfde manier op te kunnen treden als in de andere domeinen, land, lucht, zee en ruimte. Daarmee wordt cyber een volwaardige operationele capaciteit. Dat wil overigens niet zeggen dat het te verwachten is dat een toekomstig conflict volledig in cyber zal worden uitgevochten. Cybercapaciteiten zullen altijd ingezet worden als onderdeel van operaties in één van de andere domeinen. De reden is dat het vrijwel onmogelijk is om in cyberspace voortzettingsvermogen te genereren. Voortzettingsvermogen is de capaciteit om een behaald succes uit te buiten en een beslissende actie in te zetten. In cyberspace wordt gebruikgemaakt van de kwetsbaarheid van de ICT-systemen van de tegenstander. Deze kwetsbaarheid bestaat zolang de tegenstander dezelfde software gebruikt. Verandert deze, zal de aanvaller ook zijn 'wapen' opnieuw moeten ontwikkelen. Verder kan een 'cyberwapen' maar eenmaal worden ingezet en bestaat de kans dat het na de inzet tegen jezelf wordt gebruikt. Anderzijds moeten we ons ook realiseren dat we niet meer kunnen functioneren zonder gebruik te maken van cyberspace. Cyber is vooral ondersteunend aan de andere domeinen.

> 'Cyber operations zijn operaties, of de verdediging daartegen, waarbij bewust wordt gestreefd om door infiltratie van computers, computernetwerken, software en het internet, informatie en inlichtingen te vergaren en systemen te beïnvloeden of uit te schakelen om daarmee het handelen van opponenten te voorspellen, beïnvloeden of onmogelijk te maken.'
>
> *Ministerie van Defensie*

VISIE

Met het voorgaande in gedachten heeft Defensie de volgende, weliswaar ambitieuze, visie gedefinieerd:

Defensie heeft in 2015 een robuuste cybercapaciteit. Deze capaciteit is in staat de ICT-middelen van Defensie te verdedigen tegen aanvallen en verstoringen van buitenaf. De cybercapaciteit draagt met behulp van inlichtingen en offensieve operaties in cyberspace bij aan het totale operationele vermogen van de krijgsmacht en versterkt het geïntegreerd optreden van de krijgsmacht in alle dimensies. Deze robuuste capaciteit is bovendien relevant voor civiele autoriteiten en ondersteunt deze indien nodig. Defensie is een betrouwbare en innovatieve kennispartner ten aanzien van Cyber.

De invulling van deze visie wordt gerealiseerd met het cyber operationsprogramma.

Om de schaarse middelen binnen Defensie optimaal te kunnen inzetten, is centrale sturing en coördinatie nodig van de activiteiten die aan cyber operations zijn verbonden. Daartoe is in januari 2012 de Taskforce Cyber opgericht. De commandant Taskforce Cyber is verantwoordelijk voor de coördinatie van alle cybertaken binnen Defensie en treedt op als cyberaanspreekpunt voor Defensie. Het uitgangspunt is daarbij dat de betrokken Defensieonderdelen hun eigen uitvoerende taken blijven behouden.

Initieel ligt de prioriteit van Defensie bij het beschermen van de eigen netwerken en het versterken van de inlichtingencapaciteit. Op de middellange termijn (tot 2015) zal Defensie zich richten op het oprichten van een Defensie Cyber Commando, een Defensie Cyber Expertise Centrum en het versterken van de nationale en internationale samenwerking.

DEFENSIE CYBER COMMANDO

Het Defensie Cyber Commando (DCC) wordt verantwoordelijk voor cyber operations binnen Defensie. Op dit niveau vindt ook de verbinding tussen de verschillende cybervermogens en de betrokken defensieonderdelen plaats, nationaal en internationaal. Het DCC draagt zo bij aan de betrouwbare werking van Defensienetwerken en -systemen, uitvoering van militaire (cyber)operaties, en het verzekeren van de vrijheid van handelen in cyberspace voor Nederland en haar bondgenoten. In het operationele domein is een belangrijke, uitvoerende rol weggelegd voor het Commando Landstrijdkrachten.

Defensie is zelf verantwoordelijk voor de beschikbaarheid van de eigen communicatiesystemen en netwerken. Het is essentieel dat we erop kunnen vertrouwen dat informatie in onze systemen betrouwbaar is en dat onze systemen betrouwbaar zijn. De beveiliging van onze netwerken wordt mede uitgevoerd door het Defensie Computer Emergency Response Team (DefCERT). Het DefCERT zal in 2012 verder worden uitgebreid, zodat de organisatie begin volgend jaar 24 uur per dag en zeven dagen per week alle defensienetwerken kan beschermen. Daarnaast zal Defensie de bescherming van wapen-, regel- en informatievoorzieningssystemen en de daarbij behorende netwerken verder versterken.

Defensie moet ook in het digitale domein beschikken over een goede inlichtingenpositie en zorgen voor goede informatie over dreigingen in het digitale domein. Het inlichtingenvermogen wordt door de Militaire Inlichtingen en Veiligheidsdienst gerealiseerd. Binnen de MIVD is daarom een taakgroep opgericht om de cyberinlichtingencapaciteit te vergroten. Daarnaast werkt de MIVD samen met de AIVD en draagt die bij aan het opstellen van het Cyber Security Beeld Nederland.

Zoals eerder aangegeven, moet de krijgsmacht ook in het digitale domein tegenstanders uit kunnen schakelen door hun middelen onschadelijk te maken. Het is daartoe noodzakelijk dat Defensie beschikt over de kennis en capaciteiten om offensieve handelingen in het digitale domein te verrichten, zowel op strategisch, operationeel als tactisch niveau. Momenteel vindt gedachtevorming plaats over een offensieve capaciteit. Dit jaar wordt een Defensie Cyber Doctrine opgesteld. In deze doctrine zal worden beschreven hoe we met gebruik van cyberspace en in cyberspace zullen optreden en hoe dit in de planningsprocessen moet worden verwerkt. Onder offensief wordt verstaan:

- Een offensieve reactie na een aanval.
- Een proactieve actie ter voorkoming van een onmiddellijke dreiging.
- Een op zich zelf staande aanval (al dan niet binnen een grotere operatie).

Natuurlijk is een nieuwe organisatie alleen niet genoeg, er is ook een aanpassing in denken en opereren nodig. Tijdens toekomstige operaties zal de commandant worden bijgestaan door een cyberadviseur die hem helpt te bepalen waar de tegenstander kwetsbaar is, hoe de tegenstander gebruikmaakt van het cyberdomein en welke effecten hij kan bereiken door inzet van een cyberwapen. Maar ook wat zijn eigen kwetsbaarheden zijn en hoe hij die kan beschermen. De commandant kan op basis van dit advies een afgewogen keuze maken welk middel hij inzet om zijn doel te bereiken.

DEFENSIE CYBER EXPERTISE CENTRUM

Het op te richten Defensie Cyber Expertise Centrum (DCEC) is de cyberkennisomgeving voor Defensie. Het DCEC is gericht op het vergaren en ter beschikking stellen van kennis voor strategisch, tactisch en operationeel niveau. Het vergaren van kennis gebeurt door onderzoek, experimenteren en testen, zowel in het DCEC zelf als in samenwerking met anderen. Ook zal een leerstoel bij de Nederlandse Defensie Academie worden ingericht voor specifiek cyberonderzoek in een militaire context. Het beschikbaar stellen van kennis gebeurt door opleiding, training en oefening. Het DCEC zal cyberopleidingen voor alle medewerkers van Defensie initieren. Juist in het cyberdomein, waar iedereen dagelijks mee te maken heeft, is het van belang de bewustwording voor de gevaren bij iedereen te vergroten. Daarnaast zal het DCEC trainingen voor cyberspecialisten opzetten en oefeningen voor eenheden begeleiden.

SAMENWERKING

Het DCEC zal zich ook ontwikkelen tot het centrum voor samenwerking met vele partijen. Cyber is complex en specialisten op dit gebied zijn ▸

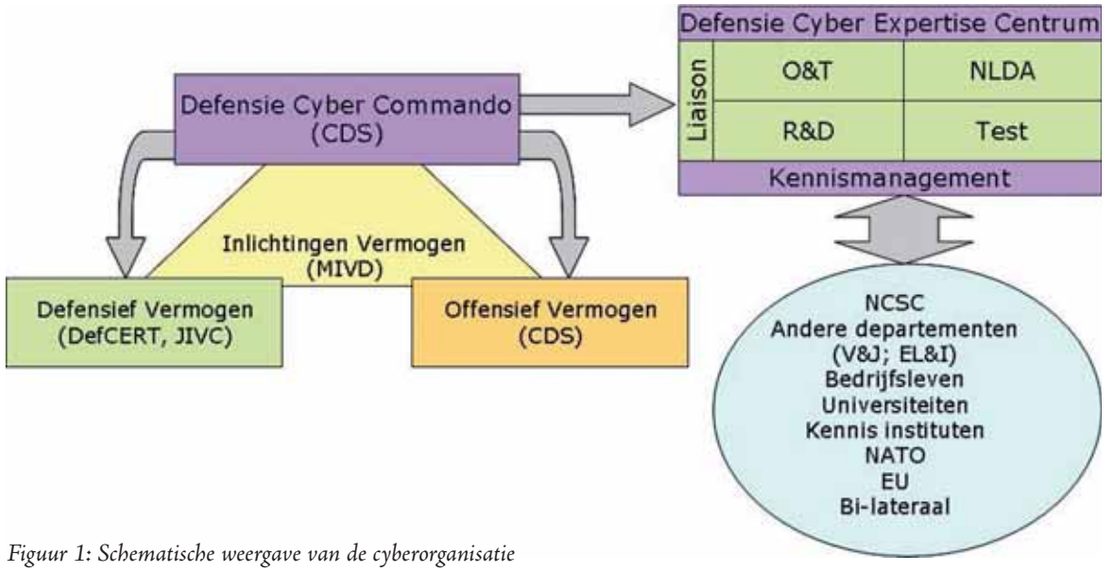
schaars. De schaarse capaciteit in Nederland kan alleen effectief worden ingezet door samen te werken. Defensie heeft zich al aangesloten bij het NCSC en werkt nauw samen met andere departementen. Ook zal gezocht worden naar samenwerkingsverbanden met het bedrijfsleven. Hierbij wordt bijvoorbeeld gedacht aan de inzet van cyberreservisten. Medewerkers van bedrijven die tijdelijk als militair functioneren en daar ervaring opdoen in een andere omgeving dan de dagelijkse. Die ervaring nemen ze weer mee naar hun burgerwerkgever. Voor onderzoek wordt gekeken naar kennisinstituten zoals TNO en het Nationaal Lucht- en Ruimtevaartlaboratorium en naar Nederlandse universiteiten. Er wordt heel veel onderzoek op cybergebied gedaan en we moeten voorkomen dat hetzelfde onderzoek op meerdere plaatsen wordt uitgevoerd.

Voor samenwerking zal niet alleen nationaal gezocht worden, maar moeten zeker ook internationale partners gevonden worden. Zowel EU als NATO hebben cyberprogramma's geïnitieerd. Defensie zoekt daarbij aansluiting. Daarnaast zijn er vele landen die dezelfde stappen nemen als wij. Met deze bondgenoten kunnen we ervaringen delen. Daarnaast biedt deze samenwerking de mogelijkheid om ook operationeel vooruitgang te boeken. In april 2012 is Nederland toegetreden tot het Cooperative Cyber Defense Centre of Excellence (CCD COE) in Tallinn, Estland. Nederland is het elfde lid dat deelneemt in het CCD COE. De andere partners zijn: Duitsland, Estland, Hongarije, Italië, Letland, Litouwen, Polen, Spanje, Slowakije en de Verenigde Staten. Het militaire kenniscentrum doet sinds 2008 onderzoek naar onder meer cyber dreiging en techniek en beleid en juridische aspecten rondom cyber operations. Daarnaast verzorgt het centrum opleidingen en symposia en organiseert het oefeningen.
Samenvattend is het doel van het DCEC om het kennis- en vaardighedenpeil van Defensie voor militaire cyber operations op het gewenste hoge niveau te brengen.

UITDAGINGEN

Cyber operations kennen helaas niet alleen oplossingen zoals hiervoor beschreven, het cyberdomein wordt juist gekenmerkt door uitdagingen. Twee belangrijke uitdagingen die van grote invloed zijn op cyber operations zijn *attributie* en *collateral damage*. Bij conventioneel optreden is het over het algemeen duidelijk wie de aanvaller is en wat zijn intentie is (attributie). Als je dan tegen die aanvaller wilt optreden, is het ook goed in te schatten wat de effecten van het ingezette wapen zijn en welke schade daarmee aangericht zal worden. In het cyberdomein is dit niet evident. De aanvaller kan een vijandelijke natie, staat, een terrorist, een activist of een zestienjarige *script kiddie* zijn. Het verschil zal pas blijken als de aanval wordt opgeëist of met andere middelen wordt bekrachtigd. Ook is het niet direct duidelijk waar de aanval vandaan komt, in cyberspace zijn er geen grenzen. Het is meestal niet wat het lijkt. Bij het oprollen van een groot botnet bleek dat Nederland vanuit Frankrijk werd aangevallen, terwijl de aanvaller zelf in Armenië zat. Een andere uitdaging is om te identificeren wat de intentie van de aanvaller is. Is het doel van een aanval op een Nederlandse bank het ontvreemden van geld of het ontwrichten van de staat?

Op al deze vragen zijn antwoorden nodig, voordat tot een tegenaanval kan worden overgegaan. Maar wat zijn dan de effecten van de inzet van een cyberwapen, welke ongewenste neveneffecten treden er op? (collateral damage) Als je een worm zou kunnen ontwikkelen om de radarsystemen van land X uit te schakelen, wat



Figuur 1: Schematische weergave van de cyberorganisatie

gebeurt er dan met de radarsystemen van land Y dat het systeem geleverd heeft? Misschien heeft land Z, onze bondgenoot, wel dezelfde systemen, essentieel voor de gevechtsleiding van onze vliegtuigen.

JURIDISCH KADER

Veel antwoorden zullen gevonden moeten worden in het juridisch kader. De vraag daarbij is of het bestaande juridische kader van toepassing is op het optreden in het cyberdomein. Voor expeditionaire operaties is het geweldsverbod in artikel 2 van het VN Handvest het startpunt. Dit verbiedt namelijk het gebruik van interstatelijk of transnationaal militair geweld. Vallen cyberactiviteiten onder militair geweld? Dat zal eerst bewezen moeten worden, hetgeen zoals beschreven niet eenvoudig is. Is dat het geval, dan is een operatie rechtmatig als een adequaat volkenrechtelijk mandaat beschikbaar is. Nederland zal alleen met toestemming van een andere staat, een mandaat van de VN Veiligheidsraad of door beroep te doen op zelfverdediging een eventuele cyberopponent mogen aanpakken.
Het beroep op zelfverdediging lijkt evident, maar is het niet. Het is bijvoorbeeld onduidelijk in welke gevallen zelfverdediging na een vijandelijke cyberaanval is toegestaan. Die cyberaanval moet dan namelijk als een 'gewapende aanval' in de zin van het VN Handvest worden aangemerkt. Volgens het advies van de Adviesraad Internationale Vraagstukken (2011) kan een cyberaanval als gewapende aanval worden beschouwd. Internationale voorbeelden en/of jurisprudentie bestaat echter nog niet.

Een ander deel van het juridische raamwerk bestaat uit rechtsregimes die voorschrijven hoe operaties op de lagere niveaus moeten worden ▶

De IT-auditor

De Carnegie Mellon University/CERT heeft richtlijnen opgesteld voor het inrichten van een Computer Security Incident Response Team (CSIRT). Hierbij worden 'services' onderscheiden die het CSIRT moeten bieden. Het gaat om:

- *reactieve services*;
- *proactieve service*; en
- *security quality management services.*

CSIRT en deze services zijn in een artikel op deze diverse aspecten al eens in het perspectief van de IT-audit geplaatst.[1]

Tot de proactieve services behoren Security Audits or Assessments. Er is een scala aan audits mogelijk:

- *Infrastructure review: manually reviewing the hardware and software configurations, routers, firewalls, servers, and desktop devices to ensure that they match the organizational or industry best practice security policies and standard configurations.*
- *Best practice review: interviewing employees and system and network administrators to determine if their security practices match the defined organizational security policy or some specific industry standards.*
- *Scanning: using vulnerability or virus scanners to determine which systems and networks are vulnerable.*
- *Penetration testing: testing the security of a site by purposefully attacking its systems and networks.*

Vooral voor *scanning* en *penetration testing* gelden de nodige (rand)voorwaarden. Deze zijn eerder in een tweetal artikelen in de IT-Auditor beschreven.[2]

Gezien de vereiste opleiding en ervaring kan een IT-auditor diverse werkzaamheden verrichten op het gebied van de *cyber defence*. Voorbeelden hiervan zijn:

- Adviseren over/beoordelen van cybervisie.
- Adviseren over/beoordelen opzet cyberorganisatie(delen).
- Beoordelen functioneren van de cyberorganisatie(delen).
- Uitvoeren/coördineren onderzoek naar kwetsbaarheden van de infrastructuur.

Visie/beleid

In het algemeen zal een organisatie beleid formuleren in relatie tot cyber defence. Dit beleid moet een duidelijke en uitvoerbare vertaling zijn van de aanwezige achterliggende visie op cyber defence. Deze visie moet dus eerst aanwezig zijn. Zowel visie als beleid zijn object van onderzoek voor de IT-auditor. Belangrijk is dat de visie duidelijk aangeeft wat het 'speelveld', problemen, risico's en kansen inhouden, en welke keuzes men maakt voor de langere termijn. De te bereiken doelen moeten helder zijn gedefinieerd. Vervolgens dient het beleid een juiste vertaling van deze visie te zijn. Kunnen de beoogde doelen worden bereikt met de uitvoering van het beleid? Wie ziet toe op naleving, zijn er evaluatie- en sanctiemogelijkheden?

Organisatie

De auditor kan verder zonder twijfel een relevante bijdrage leveren aan de inrichting van een cyber defence organisatie. Achterliggende vraag is natuurlijk of het betreffende organisatiedeel in staat moet worden geacht om de gestelde doelen te verwezenlijken. Dit heeft te maken met de beschikbaarheid van betrouwbaar en goed opgeleid personeel, evenals effectieve en efficiënte hulpmiddelen. Buiten kijf staat de noodzaak van heldere taken en verantwoordelijkheden. Zijn er goede procedures om het hoofd te bieden aan bedreigingen en opgetreden incidenten? In het geval van defensie: is de organisatie toegerust om ook een proactieve, offensieve rol te spelen? Naast deze opzet beoordeling is het uiteraard goed mogelijk om het bestaan en werking van deze organisatorische maatregelen vast te stellen.

Kwetsbaarheden infrastructuur

IT-auditors voeren op diverse lagen in de infrastructuur onderzoek uit naar de beveiliging en betrouwbaarheid van de componenten. Voorbeelden zijn netwerken, besturingssystemen, database management systemen en *middleware*. Uiteraard maken de operationele en tactische beheerprocessen deel uit van mogelijke auditobjecten. De objecten worden vooral onderzocht op de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid, afhankelijk van de uitgevoerde risicoanalyse.

uitgevoerd. Hieronder valt het vaststellen van de Rules of Engagement, de begrenzing die aan een eventueel VN-mandaat wordt ontleend, maar ook zaken als mensenrechten en in een aantal gevallen ook het Humanitair Oorlogsrecht. Ook in dit geval gaat het om cruciale antwoorden. Welke schade moet je wel en niet laten meewegen in een *collateral damage estimate* van een voorgestane cyberaanval? Hoe is de positie van neutrale staten – op wiens grondgebied zich immers servers of ICT-verbindingen kunnen bevinden – in het oorlogsrecht geregeld?

CONCLUSIE

De afhankelijkheid van het digitale domein is heden ten dage zeer groot. De maatschappij kan niet meer zonder internet, mobiele telefoons en digitale besturingssystemen. Dit is in de krijgsmacht niet anders. Commandovoeringsystemen, wapens en sensoren zijn afhankelijk van ICT en militairen kunnen beperkt functioneren zonder deze systemen. Dat maakt militairen net zo kwetsbaar voor cyberdreigingen als de rest van de maatschappij. Nationaal zijn een aantal stappen genomen om de digitale weerbaarheid van Nederland te vergroten. Ook Defensie zet die stappen en neemt haar verantwoordelijkheid in de verdediging van de eigen infrastructuur, inclusief wapen- en sensorsystemen. Maar er is meer: cyber biedt voor Defensie ook kansen. De tegenstander is ook kwetsbaar en dat kan worden uitgebuit. Cyber is een operationele capaciteit die de krijgsmacht een voorsprong op een tegenstander kan geven. Met de oprichting van de Taskforce Cyber is een weg ingeslagen om de mogelijkheden van cyber operations te concretiseren en beschikbaar te stellen aan de operationele commandant. ■

Noten

1. Schaap, Rob en Erwin den Bak, CSIRT vanuit een IT-audit perspectief; *de EDP-Auditor,* jaargang 18, nr. 4, 2009.
2. Buijs, Maarten, Een methodiek voor preventieve, testgerichte beveiligingsaudits (penetratietesten) deel I; *de EDP-Auditor*, jaargang 16, nr. 2, 2007. En Veltman, Maarten, Een methodiek voor preventieve, testgerichte beveiligingsaudits (penetratietesten) deel II; *de EDP-auditor*, jaargang 7, nr. 3, 2008.

Kolonel ir. J.M. (Hans) Folmer MSS is commandant Taskforce Cyber bij de Defensiestaf. Hij is belast met de implementatie van het cyberprogramma binnen de krijgsmacht. Sinds zijn benoeming tot officier in 1986 heeft hij zowel operationele als technische functies in binnen- en buitenland vervuld. Zo was hij hoofd van het EU operatiecentrum en heeft hij een Nederlands-Duits Verbindingsbataljon gecommandeerd. Ook was hij senior projectmanager bij de Directie Materieel en hoofd logistiek bij 1e Divisie. In 2010 is Hans Folmer afgestudeerd aan het US Army War College.