CYBER ONTWIKKELINGEN BIJ DEFENSIE

Generaal-majoor Sander Schnitger, Directeur DOBBP en Defensielid Cybersecurity Raad
Kolonel ir. Hans Folmer, Commandant Taskforce Cyber

Dagelijks worden we als burger geconfronteerd met berichten over gehackte websites en verlies van privacy gevoelige gegevens. Meestal gaat het om cyber criminaliteit met geldelijk gewin als doel, zoals bij het sturen van *spam mails* om medicijnen te verkopen of *phishing emails* om uw wachtwoorden te achterhalen, soms om (h) activisten die willen protesteren door het wijzigen van websites of door websites onbereikbaar te maken door *denial of service* aanvallen. Ook als militair hebben we te maken met deze en met potentieel gevaarlijkere vormen van cyber aanvallen.

In dit artikel zal beknopt de huidige situatie, bedreigingen en kansen voor defensie in cyberspace worden geschetst. Aansluitend zal worden ingaan op de rol van de krijgsmacht in cyberspace en zal worden aangeven welke activiteiten Defensie de komende periode op dit gebied zal ontplooien. Ten slotte zal worden aangegeven hoe defensie aansluiting zoekt bij nationale en internationale ontwikkelingen.

BEDREIGINGEN EN KANSEN

Alle middelen die we tegenwoordig gebruiken als "wired" wereldburger, zoals computers, *tablets*, internet en *smart phones*, gebruiken we ook als militair. Daarnaast zien we dat al onze wapensystemen, al onze communicatie en informatiesystemen, radars en sensoren, gebruik maken van *cyberspace*. We zijn afhankelijk en dat maakt ons kwetsbaar. Tegen deze kwetsbaarheid moeten we ons wapenen. Aan de andere kant biedt deze situatie ook ruimte voor initiatief, voor nieuwe acties en reacties, nieuwe technieken en modi operandi in aanvulling op het bestaande operationele vermogen.

Om te beginnen onze eigen kwetsbaarheid. Een relevant voorbeeld is StuxNet. StuxNet is een softwareprogramma (malware) dat specifiek is ontworpen om de besturing van ultracentrifuges in een Iraanse nucleaire opwerkingsfabriek aan te vallen en een deel van het nucleaire verrijkingsproces te verstoren. Een proces dat – voor zover we nu weten – *stand alone*, dus niet verbonden met internet, wordt aangestuurd. De in StuxNet verpakte software wijzigde de aansturing van de ultracentrifuges en veroorzaakte daarmee een afwijking in het vereiste toerental van die centrifuges. Als gevolg hiervan verliep de nucleaire opwerking niet optimaal.

StuxNet heeft gebruik gemaakt van minimaal 4 *zero-day exploits*, unieke kwetsbaarheden in software die nog niet eerder waren ontdekt. De conclusie ligt dan ook voor de hand dat StuxNet door een grote groep ontwikkelaars (*hackers*) gedurende een langere periode is ontwikkeld en uitgewerkt. Interessant voor Defensie is de constatering dat er succesvol *malware* met een specifiek doel is ontworpen en vervolgens als wapen is ingezet.
StuxNet leert ons vier lessen:

- geautomatiseerde systemen kunnen zeer specifiek worden aangevallen en malware kan dus als wapen worden ingezet;
- de airgaps kunnen worden overbrugd en geïsoleerde *stand alone* systemen zijn niet zo veilig als we altijd dachten;
- de ontwikkeling van dergelijke wapens kost (nu nog) erg veel geld;
- ook geïsoleerde en specifieke systemen zijn kwetsbaar.

We weten dat potentiële opponenten – van *hackers* tot vijandelijke strijdkrachten – ook actief zijn in *cyberspace* en daarin net zo kwetsbaar zijn als wij. Soms gebruikt onze tegenstander een eenvoudige mobiele telefoon voor communicatie of het laten exploderen van een *Improvised Explosive Device*, soms alleen een internetcafé, maar in veel gevallen gebruikt hij dezelfde geavanceerde middelen die wij hebben. Van deze kwetsbaarheid moeten we – uiteraard binnen de grenzen van de juridische kaders – gebruik maken. Allereerst door inlichtingen te verzamelen over zijn kwetsbaarheden: Wat voor soort systemen – hardware en software - gebruikt hij? Ten tweede door in zijn systemen op zoek te gaan naar vitale informatie. Ten derde door zo nodig informatie te wijzigen of te vernietigen en, ten vierde, door de tegenstander – in ruimere zin – via *cyberspace* aan te pakken. Bijvoorbeeld door zijn toegang naar internet tijdelijk te blokkeren, door zijn *Command & Control* systemen te verstoren of door de radar van de luchtverdedigingssystemen onklaar te maken. Cyber Ops komt daarmee overigens vaak in de buurt van Elektronische Oorlogsvoering.

Natuurlijk is het moeilijk om een cyber aanval te lanceren op een Taliban strijder met een Kalasjnikov, maar als we ons concentreren op het te bereiken effect wordt het al weer wat overzichtelijker. Zijn berichtenverkeer kunnen we onderscheppen, en bovenal: zijn commandant maakt wél gebruik van telefoons en internet. En de commandanten daarboven voeren een mediastrategie via internet en Youtube en ga zo maar door. Bedreigingen dus, maar er zijn ook contouren van kansen zichtbaar. En er is een rol weggelegd voor de krijgsmacht.

DE ROL VAN DE KRIJGSMACHT

De bijdrage van Defensie vloeit 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.

De krijgsmacht heeft dus niet alleen de ruimte en het mandaat om op nieuwe dreigingen als in het cyberdomein bedacht te zijn, maar moet zich ook voorbereiden op passende antwoorden. Aangezien cyber overal is en we in toenemende mate de generaal direct verbinden met de korporaal, moeten cyberoperaties op elk niveau worden uitgevoerd. Defensie moet in de toekomst niet alleen in cyberspace kunnen verdedigen, maar ook inlichtingen kunnen verzamelen en– *last but not least* – in staat zijn het initiatief te grijpen, door aanvallen te lanceren.

Cyber is dus een dreiging en een kans. Cyber is een wapen, maar ook het terrein, het is de infrastructuur, maar ook de *modus operandi*. Het kan naast zee, land, lucht en ruimte gezien worden als het vijfde domein. Het is een domein, omdat je erin kunt opereren *zonder* de andere domeinen te gebruiken. Wat we ons vooral moeten realiseren, is dat we niet meer kunnen functioneren zonder gebruik te maken van *cyberspace*. Cyber is, totdat we de coördinatie en synchronisatie met de andere domeinen tot stand hebben gebracht, vooral ondersteunend aan die domeinen, een *enabler* zonder dat afbreuk wordt gedaan aan het joint optreden. Cyber is daarmee nu al een operationeel vermogen met een werkelijk onbegrensd potentieel. Maar dit potentieel waarmaken vereist wel een andere manier van denken en nieuwe paradigma's.

Met het voorgaande in gedachte 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 in het kader van ICMS. Defensie is een betrouwbare en innovatieve kennispartner ten aanzien van Cyber.

Zoals gemeld in de beleidsbrief *Defensie na de kredietcrisis* zal Defensie daarom 50 miljoen euro investeren om de bestaande capaciteiten aanzienlijk te versterken en nieuwe te ontwikkelen. Defensie moet daartoe fors investeren in kennis, inlichtingen, defensieve *en* offensieve capaciteiten. De operationele cybercapaciteit gaat daarmee het totale operationele vermogen van de krijgsmacht vergroten en het geïntegreerd optreden van de krijgsmacht in alle dimensies versterken. Zo ontstaat niet alleen de noodzakelijke Cybercapaciteit. Ook wordt het reguliere optreden van de krijgsmacht ondersteund. En, zoals in de visie aangegeven, ondersteunt Defensie hiermee ook de ambities van het Kabinet zoals verwoord in de *Nationale Cyber Security Strategie*. Bij de uitvoering daarvan staan wij voor meerdere uitdagingen. Op een aantal daarvan gaat dit artikel nader in.

ONTWIKKELINGEN BINNEN DEFENSIE

Om de schaarse middelen binnen Defensie optimaal te kunnen inzetten, is centrale sturing en coördinatie nodig van de activiteiten die aan *cyberoperations* zijn verbonden. Daarvoor wordt een *Taskforce Cyber* opgericht. De coördinatie van de beleidsontwikkeling komt bij de Hoofddirectie Beleid te liggen. Uitgangspunt blijft dat de betrokken organisatieonderdelen de eigen verantwoordelijkheden behouden. Op de middellange termijn (tot 2015) ligt de prioriteit voor Defensie bij het oprichten van een *Defensie Cyber Commando*, een *Defensie Cyber Expertise Centrum* en het versterken van de nationale en internationale samenwerking.

Het *Defensie Cyber Commando* (DCC) wordt verantwoordelijk voor *cyberoperations* 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 Defensie netwerken 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 waarschijnlijk een belangrijke, uitvoerende rol weggelegd voor het Commando Landstrijdkrachten.

Defensie is zelf verantwoordelijk voor de beschikbaarheid van de eigen communicatie systemen 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 – zowel de bedrijfsvoeringnetwerken zoals MULAN, als de operationele netwerken zoals TITAAN - wordt uitgevoerd door het *Defensie Computer Emergency Response Team* (DefCERT) dat onderdeel is van de Bedrijfsgroep IVENT. DefCERT heeft afgelopen jaar *Initial Operational Capability* bereikt en moet eind volgend jaar volledig operationeel zijn, dat wil zeggen 24 uur per dag en zeven dagen per week alle defensienetwerken beschermen. DefCERT zal binnenkort een convenant afsluiten met GovCERT.NL, waarin de intensieve samenwerking tussen beiden wordt afgesproken. Deze betreft zowel informatie-uitwisseling als (personele) ondersteuning bij calamiteiten. Ook de bescherming van wapen- en sensorsystemen vraagt specifieke aandacht. Alhoewel het aanvallen van geïsoleerde systemen erg complex is en veel geld kost, moet Defensie de bescherming van wapen-, regel- en IV-systemen en haar netwerken verder versterken.

Defensie moet ook in het digitale domein beschikken over een goede inlichtingenpositie en zorgen een goede *situational awareness* over dreigingen in het digitale domein. Het inlichtingenvermogen wordt door de MIVD gerealiseerd. Binnen de MIVD is daarom een taakgroep opgericht om de cyber inlichtingencapaciteit te vergroten. Daarnaast werkt de MIVD samen met de AIVD en draagt bij aan het opstellen van het Cybersecuritybeeld Nederland.

De krijgsmacht moet 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. In 2012 zal een *Defensie Cyber Doctrine* worden 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.

We onderscheiden drie mogelijkheden:
- een offensieve reactie na een aanval door de tegenstander (juridische gezien is dat overigens een defensieve actie);
- een proactieve actie om een onmiddellijke dreiging van een vijandelijke aanval te voorkomen;
- een offensieve actie die op zichzelf staat, en waarbij wij het initiatief nemen. Bij deze laatste kun je nog onderscheid maken tussen een actie in het kader van een lopende operatie of een actie voorafgaande aan een operatie.

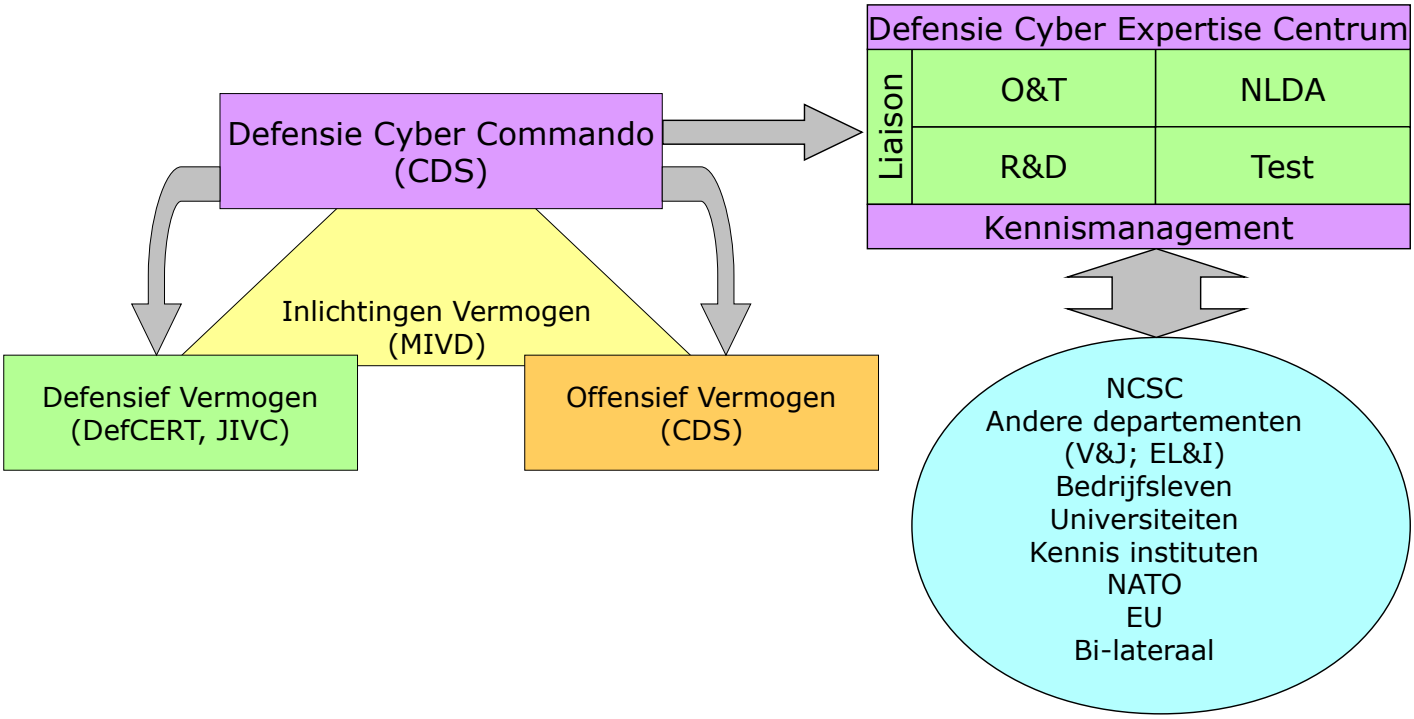
Ook wordt onderzocht welke mogelijkheden er zijn om een pool van cyberreservisten te creëren. Daartoe vindt overleg plaats met het bedrijfsleven en universiteiten. Een dergelijk systeem functioneert al in Estland.

Het *Defensie Cyber Expertise Centrum* (DCEC) is een zogeheten *shared service center* voor *cyberoperations* dat het strategische, tactische en operationele kennis- en vaardighedenpeil van Defensie voor militaire cyberoperations op het gewenste niveau moet brengen. Dit gebeurt enerzijds door het ontwikkelen en samenbrengen van (strategische, beleidsmatige en technologische) kennis (kennisontwikkeling) en anderzijds door opleiding, training en oefening, zowel met als zonder 'live' cybercomponent (kennisverspreiding).

SAMENWERKEN

Defensie staat niet alleen aan het Cyberfront. Ook op nationaal niveau en in interdepartementaal verband wordt hard aan de weg getimmerd. Cyber is een *gezamenlijke* verantwoordelijkheid. Ik heb al aangegeven dat het Defensie cyberprogramma bijdraagt aan de ambitie van het kabinet zoals verwoord in de in maart gepubliceerde *Nationale Cyber Security Strategie*. Samenwerking staat hierin centraal. De minister van Veiligheid en Justitie heeft een coördinerende taak, maar alle ministeries houden hun eigen verantwoordelijkheden. Defensie heeft daarbij vanuit artikel 97 Grondwet een taak die zich niet alleen beperkt tot expeditionaire missies, maar ook nationale operaties bestrijkt.

Per 1 januari 2012 wordt het *Nationaal Cyber Security Centrum* (NCSC) opgericht. Defensie participeert bij de totstandkoming van dit centrum, een defensievertegenwoordiger (MIVD) heeft zitting in de kwartiermakergroep. Vanaf 1 januari 2012 zal er een permanente liaison door de *Taskforce Cyber* worden uitgebracht. DefCERT heeft een convenant met GovCERT over de uitwisseling van informatie en het versterken van elkaar in geval van een incident of crisis. Dit zijn geen loze woorden, maar absolute noodzaak en al in de praktijk gebracht. Tijdens de DigiNotar crisis heeft personeel van DefCERT gewerkt op de locatie van GovCERT.



Positionering Defensie Cyber organisatie

Defensie draagt ook bij aan het tot stand komen van het *Cybersecuritybeeld Nederland*. Dit rapport geeft een beeld van de actuele cyberdreiging in Nederland en zal voor het kerstreces aan de Tweede Kamer worden aangeboden. Het zal informatie bevatten over actoren en mogelijke dreigingen en biedt private en publieke partijen de mogelijkheid tijdig te reageren.

Ook zullen ministeries samenwerken op het gebied van onderzoek. Onderzoeksvragen worden afgestemd teneinde duplicatie te voorkomen en resultaten zijn voor allen beschikbaar. Hierbij wordt ook samengewerkt met universiteiten, kenniscentra en het bedrijfsleven.

Natuurlijk zal ook aansluiting worden gezocht bij de ontwikkelingen binnen NATO en EU. In NATO verband wordt momenteel gewerkt aan een actieplan om de bescherming van eigen netwerken te verbeteren en met NC3A wordt samengewerkt in de ontwikkeling van cyber instrumenten. Ook bilateraal zijn er contacten met diverse partners. Doel van de samenwerking is in alle gevallen het efficiënt gebruik maken van de beperkte beschikbare middelen en het voorkomen van doublures.

AFSLUITING

Cyberoperaties zijn geen *science fiction* meer. Via Cyber kunnen en moeten wij ons beschermen. Cyber biedt mogelijkheden om tegenstanders in hun bewegingen te belemmeren (contra-mobiliteit) en is een operationeel vermogen waarmee we eigen mobiliteit genereren. Ik zie daarin een interessante analogie met de drieledige taak die het Wapen der Genie typeert bij de Landmacht:

- bescherming bieden;
- mobiliteit ten eigen faveure genereren;
- contra-mobiliteit (hindernissen) ten nadelen van de tegenstander creëren.

De samenleving en ook Defensie zijn afhankelijk van Cyber en ICT en dus kwetsbaar voor cyberaanvallen. De mogelijkheden die cyber biedt aan een tegenstander zijn enerzijds een bedreiging voor ons operationeel vermogen. Anderzijds is cyber een kans. Defensie ontwikkelt daarom een operationele cybercapaciteit. Het digitale domein vormt daarmee naast Land, Zee, Lucht en Ruimte, een nieuw operationeel domein voor de krijgsmacht. Defensie kan in de toekomst operaties in andere domeinen ondersteunen en versterken door inlichtingenvergaring en offensieve operaties in *cyberspace*. Ook buiten Defensie, in binnen- en buitenland, zowel in het publieke als in het private domein, wordt gewerkt aan het ontwikkelen en verstevigen van cybercapaciteit. Defensie zet daarom in op nationale en internationale samenwerking op dit terrein. Indien nodig zal Defensie in de toekomst zijn cybercapaciteiten in het kader van de civiel-militaire samenwerking beschikbaar stellen.