CYBER – EEN NIEUWE DREIGING

Generaal-majoor Koen Gijsbers, Directeur HDIO

INLEIDING

Eén van de onderwerpen die in de toekomst zeker de nodige aandacht zal gaan krijgen is die van cyber security. Het grootschalig gebruik van ICT-applicaties stelt Defensie in staat om haar taken effectiever en efficiënter uit te voeren. Maar dit intensieve gebruik zorgt echter ook voor een steeds grotere afhankelijkheid en daardoor grotere kwetsbaarheid wanneer systemen uitvallen. Dit betreft niet alleen de ICT-systemen, ook onze wapensystemen en regelsystemen zijn potentieel kwetsbaar voor aanvallen uit het zogenaamde cyberdomein. Om te voorkomen dat deze kwetsbaarheden het voortzettingsvermogen van Defensie in gevaar brengen en dat we onze taken dus niet meer kunnen uitvoeren, zijn maatregelen in het cyberdomein noodzakelijk.

Het belang van het cyberdomein is al eerder onderkend in de Militair Strategische Visie van de CDS en in de het Eindrapport Verkenningen. In dit laatste document is *cyber defence* in alle beleidsopties één van de onderwerpen waar extra inspanningen noodzakelijk worden geacht. Recente gebeurtenissen zoals de uitbraak van de Stuxnetworm en het neerhalen van het Bredolab botnet tonen aan dat de cyberdreiging reëel is.

Ook binnen de EU en NAVO en een (groot) aantal landen wordt aan een visie op het gebied van *cyber security* gewerkt. Naast de VS beschikken onder andere Frankrijk, Engeland, Zweden en recentelijk ook Canada over een *cyber security* strategie. In de recente UK *National Security Strategy* wordt de cyberdreiging als één van de grootste bedreigingen voor de nationale veiligheid gezien en in de UK *Strategic Defense and Security Review* wordt er (dus) – ondanks de forse bezuinigingen - een substantieel bedrag voor vrij gemaakt. Ook in Nederland wordt momenteel in interdepartementaal verband een Nationale *Cyber Security* Strategie (NCSS) ontwikkeld, waarbij Defensie ook is betrokken. Bij het verder uitwerken van de NCSS zal ook duidelijk worden welke rol Defensie in nationaal verband kan vervullen. Hierbij kan worden gedacht aan het beschikbaar stellen van de robuuste defensie ICT-infra voorzieningen in het geval van uitval van de ICT van andere overheidsinstellingen. Dit is vergelijkbaar met afspraken die nu ook in het kader van de Intensivering Civiel Militaire Samenwerking (ICMS) zijn gemaakt.

DE DEFENSIEVISIE OP CYBER OPERATIONS

Binnen Defensie is in het afgelopen jaar gewerkt aan een eigen visie op het gebied van cyber operations. Deze visie is eind november goedgekeurd. In de visie wordt op basis van een analyse van de huidige en gewenste situatie een aanbeveling gedaan voor een aantal acties, die er tezamen voor zorgen dat Defensie voorbereid is op de toenemende uitdagingen in cyberspace. Hierbij wordt een aantal aandachtsgebieden onderkend: sturing (governance), defence (passief en actief) en inlichtingen. Binnen deze aandachtsgebieden moeten - op hoofdlijnen - de volgende activiteiten worden ontplooid:

Sturing.

De centrale sturing moet er zorg voor dragen dat de schaarse middelen, zowel binnen als buiten Defensie, optimaal kunnen worden ingezet. In dit kader heeft de Hoofddirecteur Informatie en Organisatie (HDIO) de coördinatie van het defensiebrede cyberbeleid, waarbij de overige beleidsverantwoordelijken zoals bijvoorbeeld D-MIVD, CDS en de BA uiteraard verantwoordelijk blijven voor hun eigen verantwoordelijkheidsgebieden. Daarnaast moeten de wettelijke bevoegdheden worden verkend en wordt deelgenomen aan cyberoefeningen.

Defence.

Hier bij kan onderscheid worden gemaakt in twee aspecten, passieve en actieve verdediging. Een goed ingerichte passieve verdediging zorgt er voor dat Defensie is voorbereid op cyberaanvallen en zich hiertegen kan verdedigen. Hierdoor blijft het voortzettingsvermogen van de krijgsmacht in stand. Eén van de aspecten die daarbij aan de orde komt is het verhogen van de kennis en van awareness van het personeel. Hier is een rol weggelegd voor de opleidingsinstituten. De oprichting van DefCERT (Defensie Computer Emergency Respeons Team), het verhogen van het veiligheidsbewustzijn bij alle medewerkers van Defensie en het uitvoeren van het accreditatiebeleid maken deel van uit van het inrichten van de goede passieve defence. Daarnaast moeten de kwetsbaarheden van IV-, wapen en regelsystemen nader worden vastgesteld en waar nodig worden weggenomen. Als onderdeel van defence moet ook de afhankelijk van tweeden en derden in kaart worden gebracht, denk hierbij bijvoorbeeld aan de ontwikkelingen op het gebied van sourcing, die in de ICT wereld zeer actueel is. Om een adequate actieve defensie tegen cyberaanvallen in te kunnen richten, zijn kennis en kunde nodig van het uitvoeren van offensieve activiteiten in het cyberdomein. Of en in hoeverre Defensie de ambitie moet hebben om commandovoerings systemen van tegenstanders aan te vallen is onderwerp van nadere studie.

Inlichtingen.

Ook in het cyberdomein moet Defensie een goede inlichtingen positie hebben, om de cyberdreigingen beter in kaart te kunnen brengen. Om hier invulling aan te kunnen geven moet de inlichtingbehoefte in het cyberdomein nader worden gespecificeerd. Hieruit zal ook moeten blijken of de bestaande wet- en regelgeving voldoende is om een antwoord te geven op de speciale eigenschappen van het cyberdomein.

HOE VERDER

Nu de visie is goedgekeurd is de volgende stap om die nader uit te werken: wat moet er nu concreet gebeuren? Dit zal op korte termijn moeten plaatsvinden, omdat de (financiële) consequenties moeten worden meegenomen in de heroverwegingen als gevolg van de bezuinigingen die met het regeerakkoord zijn opgelegd. En de beslissingen daarover moeten begin volgend jaar worden genomen! Hoewel het op dit moment te vroeg is om een voorschot te nemen op de uitkomst van deze discussie, lijkt het redelijk om aan te nemen dat cyber zeker een plaats zal krijgen in de toekomstige krijgsmacht en dat de opleidingsinstanties waar ICT professionals worden opgeleid hierbij ook een rol zullen krijgen.