Het vijfde domein voor de krijgsmacht

Naar een integrale strategie voor digitale defensie

Conflicten worden in deze tijd ook op het digitale slagveld uitgevochten. Eind jaren negentig zijn militaire grootmachten als de Verenigde Staten begonnen met het beschrijven van het fundament van *cyber defence*. Ook de NAVO en de Europese Unie hebben initiatieven genomen. Nederland dient op dit gebied een achterstand in te halen en heeft een integrale militaire cyberstrategie nodig. Niet militair deelnemen aan *cyber space* is in deze tijd geen optie meer.

*M.A.D. Tettero en P. de Graaf**

Bedreigingen voor westerse samenlevingen komen steeds vaker ook uit *cyber space*. In het recente verleden waren er diverse spraakmakende voorbeelden. In 2007 zetten Russische *hackers* met een *Denial of Service* (DoS)[1] Estse websites van financiële instellingen, de media en de overheid op zwart. Dit als vergelding voor het weghalen van een Russisch standbeeld in Estland. Het voorbeeld is niet uniek. In hetzelfde jaar legde een aanval van Chinese hackers een deel van het Pentagon-netwerk plat. Vlak voorafgaand aan de Russische inval in Georgië in 2008 werden vele Georgische websites onbereikbaar en werd de president op zijn eigen site afgebeeld als een nazi. De (*unclassified*) mailbox van de Amerikaanse minister van Defensie werd gekraakt in 2007. Onder *cyber warfare* valt ook de – niet officieel bevestigde – sabotage van een Sovjet-pijpleiding in 1982 door het in omloop brengen van opzettelijk foutief functionerende computerchips en programmatuur.[2] De daardoor veroorzaakte drie kiloton zware ontploffing van de pijpleiding was tot in de ruimte te zien.

Westerse landen ondervinden elk jaar tienduizenden kleine en grotere cyberaanvallen, met name gericht op het verzamelen van inlichtingen over het militaire apparaat, energievoorziening, luchtverkeersleiding en financiële markten. Van een grootschalige cyberoorlog is echter nog geen sprake, hooguit van digitale schermutselingen, gezien de voorbeelden. In een enkel geval ondersteunde de digitale aanval werkelijk een fysieke aanval (zoals in Georgië), maar het is niet vast komen te staan dat die door het Russische leger is gecoördineerd. Er kan namelijk ook een (niet al te toevallig) samenspel van activiteiten geweest zijn, gestuurd door sympathisanten van Rusland.

* De auteurs zijn beiden consultants bij Capgemini. Mike Tettero is gespecialiseerd in defensievraagstukken als *Network Enabled Capabilities* (NEC), commandovoering, cyber warfare en Information Operations. Patrick de Graaf richt zich op strategie en innovatie van IT-organisaties in en voor de publieke sector.

1 Een DoS aanval werkt als volgt: een groot aantal computers spreekt tegelijkertijd een bepaalde server, het doel, aan. Deze server bezwijkt vervolgens onder het hoge aantal bevragingen. Voor dit soort aanvallen worden vaak *botnets* ingeschakeld, een groep met een virus of met een *trojan horse* geïnfecteerde computers.

2 Voorbeeld aangehaald in het zeer lezenswaardige artikel van W.K. Clark en P.L. Levin, 'Securing the Information Highway. How To Enhance the United States' Electronic Defenses' in: *Foreign Affairs*, Vol. 88, No. 6 (November/December 2009) blz. 2-10.

Er is geen consensus over de definities van cyber space en cyber warfare of cyber defence. Wij gaan hier uit van de volgende omschrijvingen:

- Cyber space: het World Wide Web, maar ook andere vormen van digitale activiteiten in netwerken met anderen. De digitale communicatie van elektronische regel- en meetsystemen van bijvoorbeeld energievoorziening of chemische installaties valt er ook onder, evenals de hardware en software waaruit die systemen bestaan;
- Cyber warfare of cyber defence: conflictbeslechting in cyber space met middelen als hacken en afluisteren van informatiestromen, saboteren van elektronische systemen en uitschakelen van vijandelijke websites, dan wel de bescherming tegen dergelijke aanvallen. Cyber warfare en cyber defence worden hier in de praktijk beide voor gebruikt. We hanteren verder de term cyber defence.

Ook Nederland is kwetsbaar voor cyberaanvallen, gezien onze open economie en hoogwaardige communicatievoorzieningen, zichtbaarheid in de internationale gemeenschap en een hoge afhankelijkheid van ICT voor het reilen en zeilen van de samenleving. Uitval of verstoring van of verlies aan vertrouwen in digitale voorzieningen is desastreus voor onze economie en maatschappij als geheel. De vraag rijst wat de rol van de krijgsmacht is bij het beschermen van Nederland tegen deze dreigingen. Eind 2009 verschenen er daarom berichten in de pers over het ontbreken van een cyberstrategie bij het ministerie van Defensie.[3] De teneur was dat Nederland een cyberstrategie en een cyberleger nodig heeft. We lopen anders te veel achter bij landen als de Verenigde Staten, Groot-Brittannië, China, Frankrijk, Duitsland en Rusland en vermoedelijk ook Iran en Noord-Korea. Deze landen investeren al enige tijd in hun vermogen om langs digitale weg de vitale voorzieningen van andere staten en groeperingen te kunnen treffen.

De uitbreiding van de strategie van Defensie met een cybercomponent is primair een politiek onderwerp. De politiek bepaalt immers het speelveld van de krijgsmacht. De Tweede Kamer heeft de minister van Defensie verzocht aan te geven wat diens aanpak voor digitale verdediging is.[4] De minister heeft daarop in maart 2010 bij brief aan de Tweede Kamer aangegeven welke maatregelen hij momenteel heeft genomen.[5] Deze passeren later in dit artikel de revue. Een (integrale) beleidsvisie is momenteel nog in wording. We bieden hier een *sneak preview* van wat zo'n cyberstrategie zou kunnen inhouden.

FOTO AVDD, A. VERMEULEN

Volgens berichten in de media loopt Nederland zonder een eigen cyberstrategie en cyberleger achter bij andere landen

Cyber wat?

In de praktijk worden veel termen voor kwaadaardig gedrag in cyber space door elkaar heen gebruikt en met wisselende definities: cyber warfare, cyberterrorisme, cyber defence, cyber crime, hacktivisme, et cetera. Achter deze termen gaan verschillende verschijnselen schuil, die met elkaar gemeen hebben dat ze internet

3 Zie bijvoorbeeld een artikel in *De Pers*: (http://depersnew.republisher.modernmedia.nl/238726/De_Pers_dinsdag_10_november_2009.pdf).

4 Motie van het lid Knops c.s., Kamerstuk 2009-2010, 32123 X, nr. 66, Tweede Kamer: '(…) *verzoekt de regering in interdepartementaal verband een cyber security strategie te ontwikkelen, actief bij te dragen aan de gedachtevorming over cyberwarfare binnen de NAVO en de Kamer hierover uiterlijk 1 maart 2010 te informeren* (…)'.

5 Kamerstuk 2009-2010, 26643, nr. 149, Tweede Kamer.

en andere digitale wegen gebruiken om eigen (politieke) belangen te dienen en die van anderen te schaden. Doelwit, actor, motief, organisatiegraad en potentiële schade verschillen echter aanzienlijk, wat cruciaal is voor de wijze van bestrijding en wie daarvoor de eerst aangewezen verantwoordelijke is. In de praktijk is dat een ingewikkeld probleem, aangezien er vaak gebruik wordt gemaakt van dezelfde kwetsbaarheden in hard- en software. De 'wapens' zijn ook identiek: virussen, *botnets*, Denial of Service-aanvallen, et cetera. De beschikbare responstijd is in de praktijk echter zeer kort, te kort om de reactie tijdig te routeren naar de juridisch eerst aangewezen instantie. Strategische en operationele samenwerking, inclusief actieve kennisuitwisseling tussen bestrijders, is daarom noodzakelijk. Tabel 1 geeft een overzicht van verschillende vormen van cyberaanvallen, oplopend in het geweldsspectrum.

Cyber defence, gericht op fysieke en omvangrijke financiële schade, beschouwen we als de zwaarste in het digitale geweldsspectrum. Bij dergelijke cyber attacks gaat het om (militaire) spionage, zoeken naar zwakke plekken, vingeroefeningen voor echte aanvallen, kleinschalige schermutselingen in cyber space of de ondersteuning van daadwerkelijke fysieke conflicten, dan wel de complete substitutie van fysieke operaties door digitale.

Digitale defensie komt internationaal op stoom

Eind jaren negentig zijn militaire grootmachten als de VS begonnen met het beschrijven van het fundament van cyber defence. De VS kwamen in 1998 met hun *Joint Publication* 3-13 over

Soort cyberaanval	**Cyber vandalisme**	**Misdaad via internet**	**Cyber crime**	**Cyber terrorisme**	**Cyber warfare / defence**
Actor	Potentieel iedereen op internet	Criminelen	Criminelen	Politieke / ideologische groeperingen	Nationale staten
Doelwit (domein)	Digitaal	Fysiek	Digitaal	Fysiek en digitaal	Fysiek en digitaal
Motief	Genot, afreageren	Gewin, genot	Gewin	Ideologisch, politiek	Politiek
Schade	Beperkt en gericht	Wisselend, kan aanzienlijk zijn	Wisselend, kan aanzienlijk zijn	Doorgaans gericht	Gericht tot omvangrijk
Benodigde kennis en organisatiegraad actors	Laag	Laag-Middel	Laag-Middel	Laag-Middel	Middel-Hoog
Voorbeelden	*Defacing* van websites, beledigende *tweets* of *comments*	Kinderporno, stalking, piraterij, racisme	*Phishing*, DoS, digitale inbraak, industriële spionage	Sabotage vitale voorzieningen	Spionage, sabotage vitale voorzieningen, censuur via DoS
Primaire bestrijders	Providers, webmasters	Politie, OM	Politie, OM, eigen bescherming	NCTb, AIVD, MIVD, eigen bescherming	Diplomatie, politiek, Defensie

Tabel 1 Soorten cyberaanvallen

Information Operations. Deze doctrine zet cyber defence in een breder perspectief van niet-fysieke oorlogvoering. Datzelfde deden Qiao Liang en Wang Xiangsui, beiden kolonel in het Chinese leger, in hun strategie die vertaald is onder de titel *Unrestricted Warfare*.[6] Hierin beschrijven zij hoe een land als China een technologisch superieur land als de VS met een combinatie van middelen kan verslaan. Opvallend aan dit document is dat geen enkel domein (economisch, crimineel, informatie, psychologisch en dergelijke) als strijdtoneel wordt uitgesloten.
De VS en andere landen ontwikkelen nu hun integrale cyberveiligheidsstrategieën en operationele vaardigheden voor cyber defence. Het Pentagon installeerde in 2009 als voorlopig hoogtepunt een volwaardig *Cyber Command* (USCYBERCOM), te leiden door een viersterrengeneraal of een vice-admiraal.[7] Hetzelfde jaar stelde president Obama ook een *Cyber Security Chief* aan in de persoon van Howard Schmidt, die als opdracht heeft het formuleren en (doen) uitvoeren van een integrale (civiele) cyberstrategie voor de VS. De diverse recente berichten over de aanval op Google en gecompromitteerde USB-sticks voor Britse diplomaten laten zien dat men ook in China zijn cyberoperaties serieus neemt en daadwerkelijk inzet. Ook hier blijft het lastig om er echt de vinger op te leggen: zijn het staatsactiviteiten of zijn het acties van sympathisanten? Niet alleen naties, ook georganiseerde groepen (zogeheten *non-state actors*) gebruiken namelijk het digitale wapen voor psychologische of fysieke oorlogvoering. Het digitale wapen is immers erg aantrekkelijk: het is goedkoop, snel, anoniem en het gebruik kent lage risico's voor de dader. Schadelijke *scripts* zijn al voor een paar dollar te koop, je moet alleen weten waar. De schade is echter groot en redelijk precies toe te brengen. Soms acteren dergelijke groepen in het verlengde van een landsbelang, soms ook uit eigen ideologische motivatie, aanzien bij de eigen groep of financieel gewin.

De NAVO heeft na de digitale aanval op Estland rond het thema cyber defence drie concrete initiatieven genomen:

In 'Unrestricted Warfare' beschrijven Chinese militairen hoe hun land de technologisch superieure VS met een combinatie van middelen kan verslaan

1. Op operationeel niveau de vorming van een nieuwe *Cyber Defence Management Authority* (CMDA, gevestigd in Brussel) om operationele cyber defence activiteiten van alle lidstaten te bundelen. De CMDA zal naar verwachting uitgroeien tot een *war room* voor de cyber defence van de NAVO, waarbij de daadwerkelijke tactische respons op aanvallen wordt uitgevoerd door lidstaten (in een *coalition of the willing*);
2. Oprichting van het *Cooperative Cyber Defence (CCD) Centre of Excellence* (CoE), gevestigd in Tallinn, Estland. Dit Centre of Excellence heeft als doel de vorming van doctrine en strategie te bevorderen ten aanzien van cyber

6 http://www.c4i.org/unrestricted.pdf. Zie ook: http://defensetech.org/2009/03/03/confronting-unrestricted-warfare/.

7 http://online.wsj.com/public/resources/documents/OSD05914.pdf.

defence. Nederland is hier op dit moment nog geen actief sponsorland van;
3. Versneld versterken van de beveiliging van de eigen netwerken.

Zowel operationeel als intellectueel neemt de NAVO dus de handschoen op het digitale slagveld op.

De Europese Unie heeft inmiddels ook beleid en regelgeving ontwikkeld, ingegeven door het belang van de informatie-infrastructuur voor Europa en het grensoverschrijdend karakter van cyberaanvallen. Reeds in 2005 werd ENISA operationeel, het *European Network and Information Security Agency*.[8] Het doel van ENISA is een hoge en effectieve beveiliging van netwerken en informatie in de EU. ENISA heeft taken op het gebied van bewustwording, opleiding,

Niet militair deelnemen aan *cyber space* is in deze tijd geen optie meer

bijstand en advies voor lidstaten. De communautaire digitale defensie kreeg in april 2009 een nieuwe duw in de rug door de EU-top in Tallinn. Daar werd een cyber-actieplan van de Europese Commissie overgenomen.[9] Kortweg volgt dit actieplan vijf lijnen:

1. Paraatheid en preventie, via nationale *Computer Emergency Response Teams* (CERT), inrichting van een Europees publiek-privaat partnership voor meer veerkracht en een Europees Forum voor informatiedeling tussen lidstaten. ENISA ondersteunt bij deze acties;
2. Detectie en respons op aanvallen door een Europees Informatiedelings- en alarmeringssysteem (EISAS);
3. Mitigatie en herstel via nationale en pan-Europese digitale rampenoefeningen en een verhoogde samenwerking tussen nationale CERT's;
4. Internationale samenwerking leidend tot Europese prioriteiten voor veerkracht en stabiliteit, beginselen en richtsnoeren voor lidstaten voor veerkracht en stabiliteit van het internet. Tevens streeft de EU naar mondiale oefeningen voor herstel en mitigatie bij grootschalige internetincidenten;
5. Vaststellen criteria voor de Europese kritieke informatie-infrastructuur (specifiek de ICT-sector).

De meeste actielijnen moeten eind 2010 hun eerste vruchten af gaan werpen. Daarbij rijst wel de vraag of meer coördinatie door de EU tot een intrinsiek betere verdediging leidt. De EU richt zich vooral op het smeden van samenwerkingsverbanden en het door (laten) geven van kennis en informatie. De verantwoordelijkheid voor de uitvoering van cyber defence blijft bij de nationale instanties liggen. De EU levert dus een paraplu, die deels die van de NAVO overlapt.

Nederland: achterstand inhalen

De digitale defensie is niet los te zien van het bredere vraagstuk van de digitale veiligheid van Nederland. Vanuit de Nationale Veiligheidsstrategie zijn belangrijke publieke en publiek-private initiatieven tot stand gebracht ter bescherming van de vitale infrastructuur. Daarbij valt te denken aan GOVCERT[10] en het publiek-private Nationale Infrastructuur Cyber Crime (NICC).[11] Vitale bedrijven zoals energiemaatschappijen en nucleaire instituten zijn er zelf verantwoordelijk voor om hun informatiebeveiliging op een hoger plan te brengen. Het NICC faciliteert wel actief kennisuitwisseling via sectorale informatieknooppunten. De Algemene Inlichtingen en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen en Veiligheids-

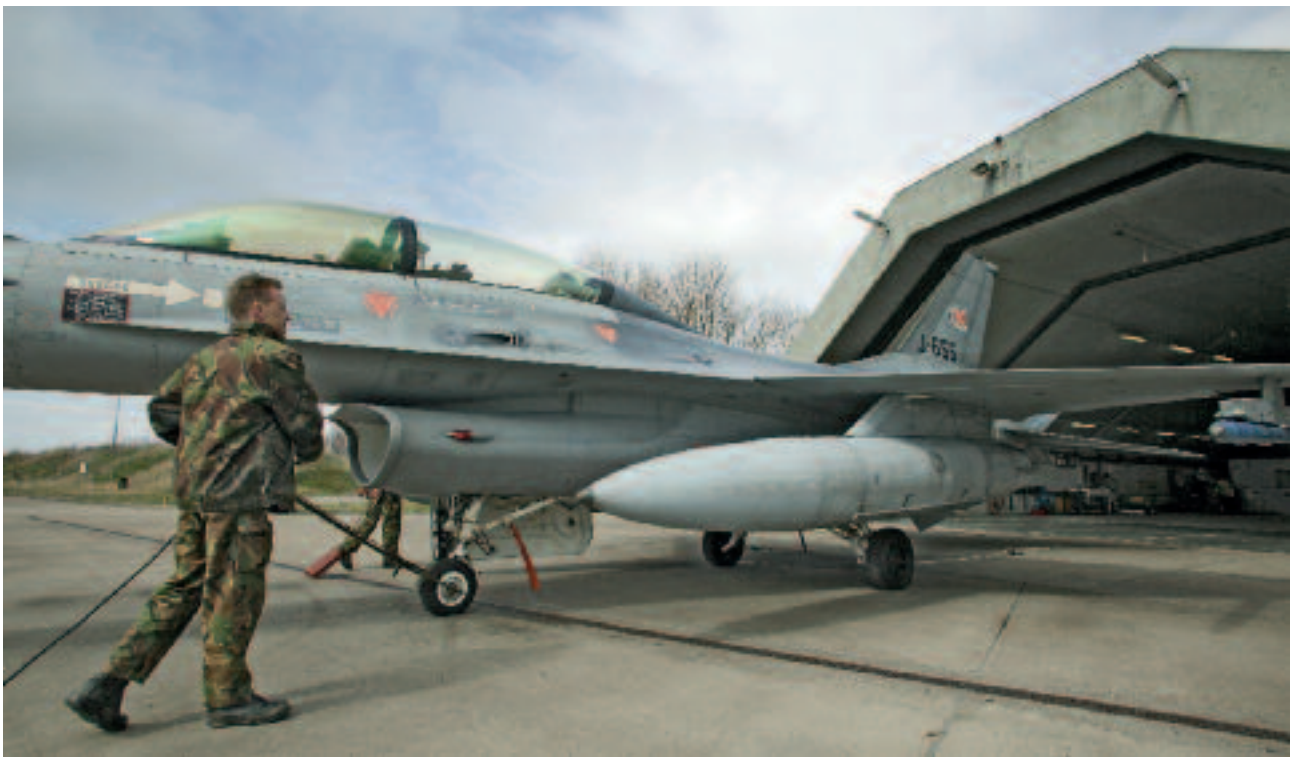
8 Ingesteld bij Verordening (EG)460/2004. Het mandaat van ENISA is in 2008 verlengd tot 2012 (Verordening (EG) 1007/2008).

9 Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende de bescherming van kritieke informatie-infrastructuur: 'Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht', Brussel, 30 maart 2009 COM(2009) blz. 149.

10 GOVCERT.NL is het Computer Emergency Response Team van de Nederlandse overheid. GOVCERT verricht activiteiten op het gebied van preventie, signalering, kennisdeling, monitoring en begeleiding bij incidenten. Veel overheden zijn deelnemer van GOVCERT. Zie verder: www.govcert.nl.

11 Het doel van het programma NICC is één publiekprivate, geïntegreerde aanpak van veilig digitaal werken, ofwel één sluitende Nationale Infrastructuur ter bestrijding van Cyber crime. Zie: www.samentegencybercrime.nl.

FOTO AVDD, H. KEERIS



Strategische documenten van Defensie richtten zich tot voor kort alleen maar op het fysieke domein

dienst (MIVD) waarschuwen ons ten slotte voor digitale spionage.[12]
Het ministerie van Defensie zit ook niet stil. Het neemt deel aan GOVCERT en heeft DEFCERT (Defensiebreed Computer Emergency Response Team) opgericht. DEFCERT richt zich op adviesverstrekking over beveiliging van IT-systemen van Defensie en neemt maatregelen bij incidenten. Ook wordt er een hoogwaardig *Intrusion Detection System* ontwikkeld. Het Defensienetwerk gold al als één van de best beveiligde in Nederland. Verder heeft het Hoofd van de Dienst Informatie en Organisatie van Defensie in de Interdepartementale Commissie van *Chief Information Officers* het onderwerp security in portefeuille.

Het accent ligt op de bescherming van de (ICT) infrastructuur van Defensie, opdat cyberaanvallen de operatie zo min mogelijk hinderen. Een verbreding van de defensieve rol van het militaire apparaat naar andere vitale sectoren ligt niet voor de hand. Zowel in Nederland als in de ons omringende landen is de heersende opvatting dat bescherming van de vitale infrastructuur primair een eigen verantwoordelijkheid is van de bedrijven zelf. Het antwoord van bijvoorbeeld het Nederlandse XS4ALL op de vraag van het Britse *House of Lords*, '*Should the military be more involved in protecting the Internet?*' is duidelijk in zijn afgemetenheid: '*Absolutely not*'.[13] De private sector wil het zelf oplossen. Het is ook moeilijk voor te stellen dat militaire operators bij bedreigingen een commerciële *internet service provider* overnemen. Lichtere vormen van samenwerking, zoals uitwisseling van informatie, is voor zowel publieke als private partijen wel een aanvaardbare stap.

Verkenningen

Het blijft wel een dilemma of de bescherming van voorzieningen die voor de samenleving van

12 Zie: https://www.aivd.nl/@125345/drie-publicaties#616871.

13 *Memorandum by XS4ALL Internet*, bijlage bij House of Lords European Union Committee, Protecting Europe against large-scale cyber-attacks, 5th Report of Session 2009-10, maart 2010.

zo'n vitaal belang zijn, geheel aan private partijen moet worden gelaten. Continuïteit van de betreffende voorziening staat ongetwijfeld zeer hoog op de agenda van de leverancier, maar moet wedijveren met andere bedrijfsdoelen. De volgende stap voor Defensie is verbreding naar cyberactiviteiten die ook externe effecten hebben, zowel defensief als offensief. Immers, aanval is soms de beste verdediging. Zelf offensieve vaardigheden ontplooien stelt de krijgsmacht ook in staat de ontwikkelingen in de technieken voor *cyber attack* beter te doorgronden voor een betere verdediging van de nationale belangen van Nederland. We moeten echter beginnen bij het fundament. Tot de meest recente Defensie Verkenningen van 2010[14] richtten strategische documenten als de Defensie Doctrine zich louter op het fysieke domein. Alleen met een zeer ruime interpretatie waren de strategische overwegingen toe te passen op cyber defence. In de Verkenningen komen de ruimte als vierde[15] én cyber space als vijfde domein er voor de krijgsmacht bij, een noodzakelijke opfrisser in het denken over moderne oorlogvoering en bescherming van de nationale belangen. De Verkenningen schenken veel aandacht aan context, belang en oplossingsrichtingen voor cyber defence. Opvallend is dat cyber defence in alle vier de beleidsopties voor de toekomstige krijgsmacht tot de prioriteiten behoort. Ook in zogenoemde min-varianten, die van een lagere defensiebegroting uitgaan, blijft cyber defence staan als punt van intensivering. Defensie komt dus uit de startblokken en moet nu overgaan tot concrete uitwerking, te beginnen met een cyberstrategie of inhoudelijke beleidsvisie.

Cyber defence moet tot de kerncompetenties van onze krijgsmacht gaan behoren

Beginnen met een integrale cyberstrategie

De militaire cyberstrategie van Nederland geeft aan wat Defensie moet doen om cyberaanvallen succesvol af te weren en tegenstanders in cyber space te verslaan. De strategie moet aansluiten bij de drie hoofdtaken van Defensie, gericht op het hogere segment van het (digitale) geweldsspectrum. De taak van Defensie op het gebied van cyber defence zou net als de 'fysieke' taakstelling drieledig moeten zijn:

1. Het beveiligen en beschermen van het nationaal relevante deel van cyber space door continue surveillance en de inzet van cybermiddelen, een taak analoog aan de luchtverdedigingstaak van de Luchtmacht;[16]
2. Het militair optreden in cyber space ter verdediging/bescherming van nationale en internationale belangen onder de vlag van NAVO, EU en/of VN. Het optreden als *cyber peacekeeper* zou dus – in elk geval theoretisch – tot de mogelijkheden kunnen behoren;
3. Het ondersteunen en bijstaan van civiele instanties bij cyberaanvallen en -verdediging, onder meer met kennisdeling en bijdragen in mensen en middelen.

Cyber Power is *core business*

Cyber defence moet gezien de eerder geschetste ontwikkelingen in cyber space en de bedreigingen die daaruit voortvloeien voor de Nederlandse samenleving tot de kerncompetenties van onze krijgsmacht gaan behoren. Cyber defence is niet exclusief het domein van ICT. De doctrinaire aanpassing, de ontwikkeling en implementatie van een cyber *Concept of Operations* en het ontwerpen en toepassen van processen, procedures, menskracht en technologie vormen de opmaat voor *Cyber Power*. Deze beschouwen we als kerncompetentie, op gelijke voet met *Air*, *Land* en *Sea Power*. Cyber Power kent een werkelijk *joint* en *combined* karakter.

14 *Eindrapport Verkenningen. Houvast voor de krijgsmacht van de toekomst* (Den Haag, ministerie van Defensie, maart 2010). Het twintigste rapport van de Brede Heroverweging is (mede) op deze Verkenningen gebaseerd. Overigens is het bevreemdend dat noch in de samenvatting van de Verkenningen, noch in de Brede Heroverweging cyber defence wordt genoemd.

15 Zie ook de toekomstvisie van de Koninklijke Luchtmacht, *Het Commando Luchtstrijdkrachten in 2020-2030: moderne militaire slagkracht in de 3e dimensie*, september 2009.

16 De luchtmacht observeert in NAVO-verband 24 uur per dag, zeven dagen per week het Nederlandse luchtruim met radars. Op deze wijze komt het *Recognized Air Picture* tot stand, een herkend luchtbeeld dat als basis dient voor verdere tactische beslissingen zoals de inzet van F-16's voor de onderschepping van een verdacht vliegtuig.

Wat zou een militaire cyberstrategie moeten bevatten?

- De nationale doelstelling ten aanzien van het gebruik en veiligheid van cyber space. De doelstelling zou in elk geval moeten onderstrepen dat de digitale infrastructuur een essentieel onderdeel is van de Nederlandse vitale infrastructuur. Nederland verklaart zich bereid om die infrastructuur met defensieve en offensieve middelen te verdedigen uit landsbelang;
- De rol die Nederland voor zichzelf ziet in cyberconflicten en de wijze van optreden, aansluitend op het geschetste ambitieniveau. Welk soort middelen zetten we in en waar in het geweldsspectrum? Die middelen zouden niet beperkt moeten blijven tot het beschermende 'harnas', maar voor een proactieve verdediging ook het 'zwaard' moeten omvatten;
- De wijze waarop onze militaire cybercapaciteiten georganiseerd zijn en hoe dit moet worden gerealiseerd met mensen, middelen en financiën;
- De zienswijze op de nationale en internationale samenwerking, zowel publiek als privaat: bijvoorbeeld NICC, de CMDA van de NAVO voor de operatie en de CCD CoE voor strategie en juridica. Intensieve samenwerking en wederzijdse ondersteuning met de andere *cyber warriors* in het publiek-private speelveld zijn onmisbaar, al is het maar voor de kennisuitwisseling en het verkrijgen van een digitale *Situational Awareness*;
- De definiëring en uitwerking van het juridisch kader. Belangrijke vragen die hier spelen zijn bijvoorbeeld de afbakening van het digitale gebied waarop Nederland mag opereren (stel bijvoorbeeld dat programmatuur van een Nederlandse organisatie draait op een server in India). Wanneer is een cyber attack een *casus belli*, zoals bedoeld in artikel 5 van het NAVO-verdrag en artikel 51 van het VN-Handvest?[17] En hoe moeten we omgaan met *collateral damage* (schade aan omliggende civiele infrastructuur bij een digitale aanval)? Dit zijn onderwerpen die in een internationale context beantwoord moeten worden, bijvoorbeeld met het CCD CoE van de NAVO en in EU-verband. Uiteindelijk zijn deze antwoorden nodig voor de *Rules of Engagement* voor 'onze jongens achter het beeldscherm';
- Normatief kader voor de robuustheid van de eigen informatievoorziening. Hier komen onderwerpen aan de orde als informatiebeveiliging, risicomanagement en gewenste diversiteit van het IT-landschap (hoe diverser, des te inefficiënter, maar met meer kans op overleven);
- Een *Road Map* voor de implementatie en evaluatie van deze strategie.

Er zullen nieuwe militaire en politieke strategieën en tactieken nodig zijn. In hoeverre zijn concepten als *deterrence* en *flexible response*[18] toepasbaar? Komen we in een nieuwe wapenwedloop terecht, waarbij sprake kan zijn van *MAD* 2.0?[19] Maar ook praktische vragen zullen moeten worden ingevuld, zoals: hoe train je voor cyber defence? Bestaat er zoiets als een digitaal oefenterrein met dezelfde uitgestrektheid en complexiteit als het World Wide Web?[20] Het adagium *Train as you fight, fight as you train* kan dus nog een uitdaging worden. Zijn de lessen en voorbeelden uit het verleden van Von Clausewitz, Billy Mitchell en de Koude Oorlog toepasbaar? Voor de operaties van de krijgsmacht in cyber space is ten slotte meer dan elders *real time* inzicht nodig, oftewel: cyber space en de activiteiten die daar plaatsvinden zullen onderdeel moeten uitmaken van het *Common Operational Picture* en de Situational Awareness van de krijgsmacht. Hier ligt een geweldige technologische en cognitieve uitdaging. Hoe verkrijg je actueel inzicht in eventuele bedreigingen met vele miljoenen computersystemen en netwerken en potentieel miljarden gebruikers? Dreigingsanalyses en *intelligence* zijn essentieel. Cyber space voegt

17 De *NATO Policy on Cyber-Defence* gaat er vanuit dat dit niet het geval is. Het beleid staat geen *preemptive strikes* toe, maar wel een uitgebreide bescherming in geval van een digitale aanval, gecoördineerd door de CDMA.

18 *Flexible Response* is een concept binnen de NAVO, waarbij op proportionele wijze op een aanval wordt gereageerd, gebruikmakend van alle middelen in het geweldsspectrum. De tegenhanger hiervan was jarenlang de doctrine van *Massive Retaliation*.

19 *Mutually Assured Destruction* (MAD), een doctrine gebaseerd op het principe van afschrikking (deterrence), waarbij een aanval op de tegenstander resulteert in zelfvernietiging.

20 Het antwoord is vermoedelijk ja. De Verenigde Staten hebben in Maryland een militair cyber-oefencentrum ingericht.

al met al een geheel nieuwe dynamiek en complexiteit toe aan de krijgsmacht en vraagt om nieuwe ideeën over deze wijze van conflictvoering.

Gezocht: Cyber Warriors (m/v)

Door het multidisciplinaire karakter is het opstellen en operationaliseren van een cyberstrategie een complexe aangelegenheid. Politiek-bestuurlijke, juridische, militaire, organisatorische, psychologische en – *last but not least* – technologische factoren spelen een rol. Technologie is voor de meeste politieke en militaire leiders echter geen gemeengoed. Dit is waarschijnlijk de belangrijkste oorzaak waarom cyber defence tot dusverre slechts beperkt van de grond is gekomen. Het vergt ook schuiven met toch al schaarse middelen vanuit een duidelijke visie. Tastbaar, zichtbaar materieel zal het in de *mindset* van de gemiddelde (militaire) beslisser al snel winnen van de software van cyber warfare. Niet militair deelnemen aan cyber space is in deze tijd echter geen optie meer, gegeven de bedreigingen en de stappen die landen, verdragsorganisaties en groeperingen om ons heen nemen. In de internationale context is de nationale staat de eerst aangewezene om organisatorische, bestuurlijke en fysieke maatregelen te treffen. Primair moet de aandacht van Defensie uitgaan naar het op orde brengen van de beveiliging van 'het eigen huis' van de overheid en andere nationale belangen, in samenwerking met andere departementen met een veiligheidstaak (Justitie, Binnenlandse Zaken). Ook offensieve capaciteiten horen er echter bij: ter lering, als afschrikking of vergelding en ter bescherming van de eigen fysieke operaties in binnen- en buitenland.

FOTO AVDD, H. KEERIS

Het adagium 'Train as you fight, fight as you train' kan op het digitale oefenterrein nog een uitdaging worden

Cyber defence doet een beroep op relatief schaarse kennis, binnen en buiten de krijgsmacht. De diverse initiatieven voor kennisdeling op nationaal en internationaal niveau (EU, NAVO) zijn daarom ook belangrijker dan ze in eerste instantie misschien lijken. Ook samenwerking met private organisaties en de onderzoekswereld is nuttig bij het opzetten van cyberactiviteiten. Daar ligt immers veel kennis over netwerk- en informatiebeveiliging, hacking, et cetera. De recente Defensie Verkenningen hebben inmiddels de basis voor een cyberstrategie gelegd. Hier ligt een kans voor het uitwerken van een strategie van waaruit de krijgsmacht dit vijfde domein kan gaan bestrijken. Wie neemt de muis op? ■