Zes noties over digitale oorlogvoering

Binnen het thema cyber security valt de term "cyber warfare" met enige regelmaat. Dat geldt ook voor aanvallen en aanvallers (en de Engelse varianten). Soms bedoelt men daar criminaliteit mee, soms spionage of activisme via internet. Dit losse taalgebruik draagt niet bij aan een goed begrip van digitale oorlogvoering (cyber warfare) zoals dit binnen het ministerie van Defensie leeft. Met zes stappen – noties – valt te duiden wat cyber warfare is, waar het zich afspeelt, wat het doel zou zijn, hoe het wordt uitgevoerd, en wie daarover beslist. Maar eerst moet de plaats van cyber warfare binnen het bredere spectrum van cyber security worden bepaald.

Brigade-generaal prof. mr. Paul Ducheine
Hoogleraar Cyber Operaties & Cyber Security (NLDA)

1. OVERKOEPELEND: "CYBER SECURITY"

Digitale veiligheid is in de *National Cyber Security Strategy-2* gedefinieerd als: "het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan".
In relatie tot de diversiteit aan dreigingen (afkomstig van statelijke en niet-statelijk actoren, uit binnen- en buitenland, met gevarieerde motieven, dan wel ongelukken, falen en pech) en de overheidsreactie om die dreigingen te pareren, zijn 6 Cyber Security paradigma's te onderkennen. Het betreft: bescherming, rechtshandhaving, inlichtingen, diplomatie, conflict en (overkoepelend) coördinatie. Deze paradigma's zijn gekoppeld aan beleidsterreinen en departementen.
Coördinatie vanuit VenJ (NCTV) is het eerste en wellicht belangrijkste paradigma om veiligheid te borgen. Het gaat om een gesynchroniseerde en gecoördineerde publiek en private aanpak. Bescherming regardeert primair eenieder: burgers, bedrijven en organisaties. Maar uit de aard van de klassieke veiligheidstaak, ligt ook een verantwoordelijkheid bij de overheid. Bescherming als paradigma in het digitale domein heeft de aandacht van meerdere departementen (o.a. VenJ, BZK, EZ, I&M, OCW) en betreft verschillende aspecten in het digitale domein: fysieke beveiliging, technische standaarden, weerbaarheid, bewustzijn, kennis, ICT-(beveiligings)normen en -standaarden. Specifiek is de rol van VenJ vanwege het Nationaal Cyber Security Centrum en de directie Cyber Security van de NCTV. Maar ook het ministerie van EZ speelt hier een rol vanwege telecommunicatie. Het rechtshandhavingsparadigma is een zaak van onder andere het ministerie van VenJ (politie, Openbaar Ministerie) en andere opsporingsdiensten (bijvoorbeeld FIOD). Het inlichtingenparadigma is het domein van BZK (AIVD) en Defensie (MIVD).
Diplomatie is een verantwoordelijkheid van BZ waarbij bijdragen uit andere departementen belangrijk zijn. Het conflict paradigma is belegd bij BZ en Defensie. Dit is het domein voor *cyber warfare*.

2. WAT? DIGITALE OORLOGVOERING ("CYBER WARFARE")

Binnen dit grotere geheel past de *Defensie Cyber Strategie* uit 2012. Daarin staan, naast een aantal randvoorwaardelijk thema's, drie speerpunten centraal:

- de versterking van de digitale weerbaarheid van Defensie;
- de versterking van de inlichtingenpositie in het digitale domein;
- de ontwikkeling van militair vermogen om cyber operations uit te voeren.

Dit laatste speerpunt wordt ook wel aangeduid met "offensief" of "operationeel vermogen" wat gebruikt wordt bij cyber warfare.

Cyber warfare is strikt omschreven als "het uitvoeren van militaire operaties die erop zijn gericht om:

a. met digitale middelen
b. computersystemen of netwerken van een
c. tegenstander te
d. verstoren, misleiden, veranderen of vernietigen".[1]

Daaraan kan worden toegevoegd:

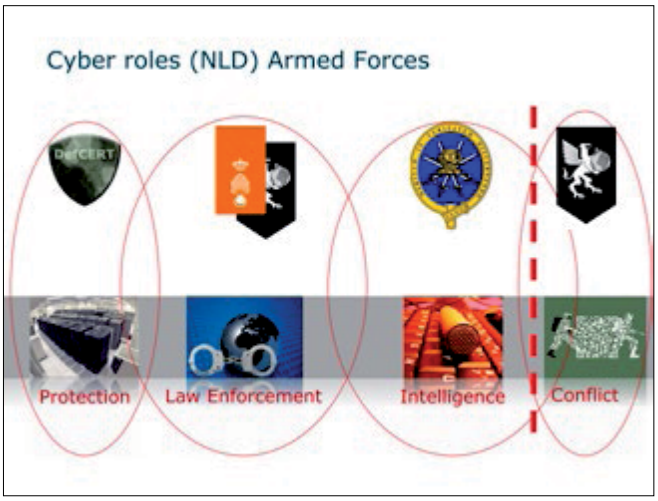
e. voor het realiseren van doelstellingen
f. door strijdkrachten.

De typering van dit *cyber warfare* paradigma is restrictief.
Naast deze rol kent Defensie intern ook nog *drie* andere rollen die aansluiten bij de eerder genemde paradigma's:

- "bescherming" (van de eigen cyberspace);
- "rechtshandhaving" (onder andere KMar en militaire bijstand aan de politie);
- "(counter-)intelligence" (MIVD).

Deze vier paradigma's maken samen weer deel uit van het integrale thema "cyber security" (zie figuur 1).

[1] AIV & CAVV, *Digitale oorlogvoering*, Den Haag 2011, 8.



Figuur 1 Vier cyber rollen binnen Defensie

3. WAAR? DIGITALE DOMEIN ("CYBERSPACE")

Cyberspace wordt omschreven als "het conglomeraat van ICT-middelen en -diensten en bevat alle entiteiten die digitaal verbonden (kunnen) zijn".[2] Het omvat permanente verbindingen én tijdelijke of plaatselijke verbindingen evenals data, software en operating systems.

Het betreft een gelaagd domein met fysieke én virtuele lagen:

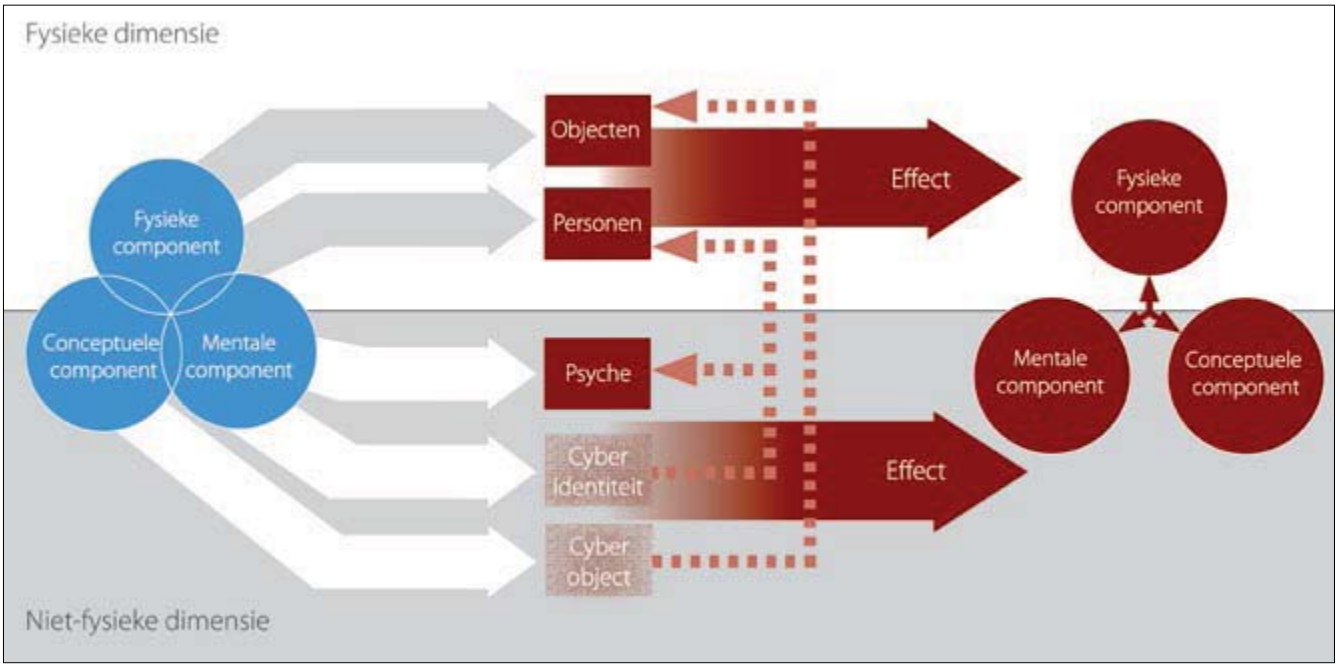
- sociale laag, met fysieke personen en hun cyber-identiteiten (onder andere e-accounts);
- logische laag (cyber-objecten zoals software, MAC- en IP-adres);
- fysieke laag, met fysieke ICT-infrastructuur (hardware) en geografische locaties.

Communicatie en informatie loopt door deze lagen heen, en daarom is Defensie – net als andere moderne organisaties – bijzonder afhankelijk van dit domein. Dat komt onder meer omdat daarin cruciale informatie ligt opgeslagen en communicatie- en informatiesystemen, sensoren, wapen- en commandosystemen hierin hun plaats hebben. Denk bijvoorbeeld aan het GPS-signaal of mobiele en draadloze verbindingen. Dat geldt uiteraard ook voor andere actoren om ons heen, waar ook ter wereld, eenieder gebruikt dit domein.

4. WAAROM? STRATEGISCHE DOELEN EN HET BEÏNVLOEDEN VAN ACTOREN

Nederland beschikt over meerdere machtsmiddelen (diplomatieke, economische, militaire en informatie) om (collectief) veiligheidsbeleid en andere strategische doelen te realiseren. Met deze machtsmiddelen wordt het gedrag van andere (statelijke of niet-statelijke) actoren – tegenstanders, medestanders en neutralen – beïnvloed. Het militaire instrument (de krijgsmacht) vervult daarbij via afschrikking, dwang en – ultimo – interventie met gebruik van geweld, strategische functies: anticiperen, voorkomen, afschrikken, beschermen, interveniëren, stabiliseren en normaliseren.
Cyber-capaciteiten bieden een uitbreiding van het militaire arsenaal, maar zullen – op zichzelf staand – niet voor alle functies even geschikt zijn.

[2] C. Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, Den Haag 2013, 85.



Figuur 2 *Militair vermogen - aangrijpingspunten - effecten (Ducheine & Van Haaster, 387)*

5. HOE? CYBEROPERATIES

Cyber warfare betreft – kort – het uitvoeren van militaire cyber-operaties.[3] De auteurs van de *Tallinn Manual* definiëren deze als het gebruik van cyber-middelen om beoogde effecten *in of via* cyberspace te realiseren.[4] Daarbij staan – net zoals bij andere militaire operaties – drie begrippen centraal: effecten, middelen en aangrijpingspunt (doelwit). Dit is schematisch weergeven in figuur 2.

De te realiseren effecten vormen het uitgangspunt in militaire operaties. Afhankelijk van het gewenste effect dat ìn (een van de drie lagen van) cyberspace, dan wel vìa cyberspace als medium/vector gerealiseerd moet worden, zal een keuze voor een cyber-middel en een aangrijpingspunt (doelwit) worden gemaakt. De effecten in cyberspace zijn doorgaans niet-fysiek, maar kunnen indirecte fysieke effecten op mensen en objecten hebben.

De aangrijpingspunten (doelwitten) bevinden zich ìn twee lagen van cyberspace: de cyber-identiteiten in de sociale laag en cyber-objecten in de logische laag. Cyber-middelen variëren van zeer geavanceerd (Stuxnet) tot betrekkelijk basaal (DDoS). Daarnaast bestaat de mogelijkheid vìa cyberspace effecten te realiseren. Bijvoorbeeld door informatie te delen (via social media).

6. WIE EN WANNEER? BESLUITVORMERS EN UITVOERDERS

In de besluitvorming over de inzet van militaire cyber-capaciteiten zijn het AIV&CAVV-advies en de *Tallinn Manual* belangrijke hulpmiddelen. Beide stukken bieden de regering houvast bij haar besluit of een adequate rechtsbasis voor een cyber-operatie bestaat.

Voor militairen die cyber-operaties plannen en uitvoeren (en daartoe opleiden en trainen) bieden beide documenten een goed inzicht in de rechtsregimes die tijdens de uitvoering van die operaties van toepassing zijn (onder andere oorlogsrecht). Adequate rechtsbasis en het respecteren van toepasselijke rechtsregimes dragen bij aan de legitimiteit van cyber-operaties en bieden houvast voor het afleggen van verantwoording daarover.[5] De Nederlandse regering zal slechts militaire cyber capaciteiten in het conflict paradigma in het buitenland inzetten, oftewel cyber warfare overwegen, als er overeenstemming over zo'n missie met het gastland, of met een mandaat van de VN-Veiligheidsraad, of in zelfverdediging na een gewapende aanval in de zin van het VN-Handvest.

TOT BESLUIT

Deze zes stappen beogen het begrip cyber warfare duidelijk(er) te maken. In de recente actualisering van de Defensie Cyber Strategie besteedt Minister Hennis-Plasschaert uitvoerig aandacht aan de "versterking van de cyberinzet bij missies". Deze operationele capaciteit voor "cyber warfare", eigenlijk voor het uitvoeren van militaire missies, kent zowel defensieve, inlichtingen gerichte als offensieve aspecten. Waarbij de laatste niet zonder de eerste twee kan: zonder inlichtingen en vrijheid van handelen, is elk initiatief kansloos.

[3] P. Ducheine & J. van Haaster, 'Cyber-operaties en militair vermogen', *Militaire Spectator* 182 (2013), 368-387, 369.

[4] M.N. Schmitt, (Ed.),*Tallinn manual on the international law applicable to cyber warfare.* New York: Cambridge University Press, 2013, 258.

[5] Zie uitgebreid: P. Ducheine & K. Arnold, 'Besluitvorming bij cyberoperaties', *Militaire Spectator* 184 (2015), 56-70.