Naam:	Nick Ungerer
Studentnummer:	3175693
Blok/Studiejaar:	1, 2010
Begeleider:	M.T. Schäfer
Onderdeel:	Nieuwe media en cultuurconstituerende aspecten Cyberwarfare

Zeventien Jaar Cyberwarfare: Een exploratieve discourseanalyse naar de verbeelding van het begrip cyberwarfare in de literatuur van 1993 tot het heden.

Inhoudsopgave

Inleiding

Het fenomeen dat ik in mijn paper ter discussie wil stellen is op welke manier het concept 'cyberwarfare' de laatste jaren is uitgegroeid tot een beladen kwestie in zowel de massamedia, het academisch debat en in de politieke besluitvorming van naties. Daarbij staat centraal *hoe* dit begrip is getransformeerd in verschillende vooraanstaande militair-academische bronnen.

Een veelvoorkomende beschrijving aan het begin van de jaren '90 waaronder nu de verschillende vormen van cyberintrusies worden gecategoriseerd, is de algemene noemer InfoWar. Het groeiende aantal voorbeelden van cyber agressie, zorgt er voor dat *cybersecurity* een prioriteit wordt voor zowel overheid (en leger) en bedrijfsleven.

Gedurende de 21e eeuw kwamen verschillende naties en afzonderlijke bedrijven in toenemende mate in aanraking met verschillende cyberaanvallen. Er zijn echte grote meningsverschillen over de definitie van die aanvallen en hun ernst. Velen argumenteren dat er (tot voor kort) nog geen voorvallen van *cyberwarfare* zijn geweest, maar dat deze verschillende vormen van spionage en criminaliteit beter onder de noemer van *cybercrime* kunnen worden gecategoriseerd.

We hebben een grote toename gezien in de berichtgeving van zowel tekstuele als visuele digitale en traditionele media, waarin er sprake is van een te fantasierijke verbeelding van de gevaren die cyberwarfare met zich meebrengt, het is verworden tot een soort van *buzzword*. Het is om meerdere reden belangrijk om een goede definitie van cyberwar te hebben, die niet alle lichtere vormen van online criminaliteit omvat. Een reden is dat conflicten die vrij weinig blijvende economische schade aan hebben gericht worden, toch aangemerkt als daden van cyberwar.[1] Het lijkt me dus van belang dat de media ook een zo objectief mogelijke benadering van het begrip nastreven om een onderscheid te maken tussen de lichtere vergrijpen en de meer verregaande vorm van cyberagressie.

Een andere reden is van juridisch-militaire aard. Als een natiestaat wordt aangevallen, hetzij door een andere natiestaat of een kleinere organisatie, is het belangrijk om het incident in te kunnen delen, omdat de classificatie daarvan bepaalt met welke middelen en onder welke voorwaarden de slachtofferstaat terug kan slaan.[2]

Verder is het de vraag of aanvallen op private bedrijven ook aan kunnen worden gemerkt als daden van cyberwarfare. Er dient dan te worden gekeken in hoeverre het bedrijf essentieel is voor de nationale infrastructuur van een land, en welke gevaren er in geval van een aanval zijn voor haar burgers.

---

[1] http://www.newsweek.com/2009/04/17/the-fog-of-cyberwar.html Het conflict tussen Estland en Rusland heeft geleid tot de oprichting van het Cooperative Cyber Defense Centre of Excellence (CCDCoE), dat zich bezighoudt met onderzoek naar de versterking van de digitale Europese infrastructuur.

[2] Sklerov M.J., *Responding to International Cyber Attacks As Acts of War*

Er gaat een uitgebreide historie schuil achter retoriek rondom de term ‘oorlog’. Vanuit de literatuur zal ik analyseren hoe de principes van traditionele oorlogsvoering opgaan voor oorlog en andere conflicten binnen het cyberdomein. In hoeverre is het metafoor ‘cyberwarfare’ geschikt om die conflicten te beschrijven? Welke overeenkomsten zijn er met echte oorlogsvoering? Leent cyberwar zich wel goed als definitie van wat in historische context altijd vrij bloedige conflicten zijn geweest? De vraag die ik hier centraal zal stellen is:

Hoe is de verbeelding van het begrip cyberwarfare in het militair-academisch discours van de VS van 1993 tot aan het heden getransformeerd?

In de literatuur die ik behandel, ligt de nadruk op het perspectief van de VS, die voorop lopen in de ontwikkeling van een cyberstrategie. De literatuur die ik behandel begint in 1993, met een stuk dat kan worden gezien als het fundament voor de discussie rondom de verbeelding van het begrip van cyberwarfare. We zullen zien dat de verbeelding van het begrip in de loop van het nieuwe millennium verandert, onder invloed van verschillende voorbeelden van cyberagressie. Analyse daarvan maakt het mogelijk een duidelijker beeld te scheppen van consequenties, en in dit essay zal ik kijken hoe de literatuur deze transformatie van het begrip en haar context weergeeft.

Dit beeld zal samenhangen met een aantal korte, concrete gedocumenteerde vormen van cyberaanvallen, om te illustreren wanneer er wel of geen sprake is van cyberwarfare. Ik zal een analyse van het militair-academisch discours inzetten om tot een zo duidelijke mogelijke beschrijving te komen van welke daden in het cyberdomein gecategoriseerd kunnen worden als cyberwarfare.

Hoofdstuk 1: Theorie en vertrekpunt

1.1 *Begrippen*

Zoals ik hierboven duidelijk heb gemaakt zal ik een beeld schetsen van hoe de verbeelding van de term 'cyberwarfare' in de militair-academische literatuur tot uiting komt gedurende het tijdsframe 1993 tot het heden. We zullen zien dat het begrip op een instrumentele manier gebruikt wordt, maar in verschillende contexten toch diverse betekenissen lijkt te hebben. Bij het beschrijven van cyberwarfare is het noodzakelijk om te kijken naar de afzonderlijke categorieën die binnen het bereik van de term vallen, zoals kleinere vormen van cyber intrusies als spionage en andere vormen van criminaliteit.

In het volgende hoofdstuk zal ik beginnen met het analyseren van de verbeelding van het begrip cyberwarfare aan de hand van de literatuur van de RAND Corporation, een denktank van het Pentagon die onderzoek doet naar alles wat er in de maatschappij leeft. Dit is de tekst *Cyberwar is Coming!* (Arquilla en Ronfeldt, 1993). Deze zal ik samen gebruiken met literatuur van *Battlefield of*

the Future (Schneider, 1995) en een werk dat is opgesteld naar aanleiding van het festival Ars Electronica, met als thema InfoWar. (Stocker, 1998).

Daarnaast zal ik kijken naar de strategische implicaties die cyberwarfare heeft binnen het beleid van de VS en hoe deze zich verhouden in de context van traditionele oorlogsvoering. Ik zal aantonen dat de definitie van cyberwar veranderd is van InfoWar, een algemene term waarin de nadruk ligt op psychologische kant van manipulatie van informatie (propaganda), tot de meer technische kant van cyberwarfare, waarbij aanvallen zich concreter op de toegang tot internetsites richten. Deze verschuiving komt vooral naar voren in de modernere literatuur van na 2003. Stukken van Lonsdale (2004), Carr (2009) en Libicki (2009) vormen de hoofdlijn binnen mijn argumentatie van deze recente periode.

Terwijl ik de theoretische kant van het onderwerp belicht, heb ik vooral oog voor de strategische overwegingen die in de literatuur worden gemaakt. De technische voorwaarden van het uitvoeren van zowel offensieve als defensieve methoden van cyberwarfare, alsmede een aantal juridische vraagstukken zullen wel kort behandeld worden maar vallen verder buiten het bereik van dit onderzoek. Wel ga ik analyseren hoe de nieuwe middelen van oorlogsvoering leiden tot nieuwe mogelijkheden voor zowel het militaire bestel als individuen of groepen die zich bedienen van hun cybercapabiliteit. Cumulatief gezien hebben deze aanvallen vooral een grote impact op het bedrijfsleven.

1.2 *Clausewitz en de aard van oorlog*

Om na te kunnen denken over cyberwarfare is het eerst noodzakelijk om een definitie van traditionele oorlogsvoering als beginpunt te gebruiken, om de implicaties van het nieuwe digitale slagveld te kunnen contextualiseren. Hier komt de Pruisische soldaat en oorlogsfilosoof Carl von Clausewitz van pas. Hij stelt:

War is nothing but a duel on a larger scale. Countless duels go to make up war, but a picture of it as a whole can be formed by imagining a pair of wrestlers. Each tries through physical force to compel the other to do his will; his immediate aim is to throw his opponent in order to make him incapable of further resistance. War is thus an act of force to compel our enemy to do our will.[3]

Waarbij fysieke kracht wordt gebruikt als middel om de vijand machteloos te maken. Dit, zegt hij, is het werkelijke doel. Verder geeft hij aan dat ‘war is merely the continuation of policy by other means’, oftewel dat oorlog een extensie van het beleid is, alleen met gebruik van andere middelen. In dit nieuwe domein lijkt fysiek geweld naar de achtergrond te zijn verschoven (Clausewitz, 2007).

[3]Clausewitz, Carl, von. *On War* p. 44

We zullen in de volgende hoofdstukken zien hoe dit het begrip van het slagveld beïnvloedt.

Zoals we verder ook nog zullen zien als we de literatuur van vooral na 2003 gaan bekijken, is dat er vraagtekens bij deze stelling worden gezet, als er ook steeds meer sprake is van *nonstate actors* (onafhankelijk opererende groeperingen, waaronder terroristische cellen en anderszins religieuze of fanatieke groepering), in andersoortige conflicten van lagere intensiteit. Is hier dan wel sprake van cyberwar? Of is cyberwar dan een te algemene term?

Hoofdstuk 2: De verbeelding van het begrip cyberwarfare in literatuur tot 2000

In dit hoofdstuk zal ik definities van het concept *cyberwarfare* bespreken uit de literatuur van de jaren ’90. In deze vroege literatuur wordt vooral veel aandacht besteed aan de manier waarop er als het ware sprake is van een transformatie van traditionele oorlogsvoering, onder invloed van de informatierevolutie. De nieuwe ‘informatiewapens’ ontregelen, manipuleren en vernietigen de vormen van communicatie en informatie van de vijand. (Hables Gray, 2009)

2.1 *Nieuwe technologie vanuit historisch perspectief*

Technologische innovatie wordt vaak geleid door militaire motieven. Er worden technologieën gecreëerd, die dan onvoorziene applicaties hebben in de 'gewone' maatschappij. Zo was het ook met het internet, de oorsprong van de capabiliteit tot cyberwarfare. Onder andere dit medium ontstond vanuit de militaire noodzaak om middels innovatieve informatietechnologie een zogenaamde *force multiplier*, een strategisch fysiek voordeel op het slagveld te behalen.

Thus, infowar is not solely a matter for the military in cyberspace, but to a much greater extent a phenomenon inherent in our society whose driving forces are technologies that have been developed from out of a military context. Infowar is a question of the increasing emancipation of the civilian domain—”vote with your modem …”—a question of knowledge and perception of the world. (Stocker, 1998)

Stocker (1998) argumenteert dat dit leidt tot een ‘permanente mobilisatie’ van de maatschappij:

With three key technologies developed in the interest of war and from its logic – electricity, telecommunications and the computer – having made a permanent mark on civil society, these technologies of simultaneity and coherence are now putting this society onto a footing of permanent mobilization. A struggle for markets, resources and spheres of influence is being waged to attain supremacy in processes of economic concentration, in which the fronts are no longer formed by the borders of states or the jurisdictional limits of legal systems, but rather by technical

standards; a battle in which the power of knowledge is managed as a lucrative monopoly over its distribution and dissemination. (Stocker, 1998)

De implicaties van die nieuwe technologie zijn echter niet meteen volledig duidelijk. De nadruk op de mogelijkheden van cyberwar, of 'information warfare', de term die in de literatuur van voor 2000 vooral gebruikt werd, lag dan ook op het manipuleren van informatie. De beoogde effecten van deze strategie moesten vooral op psychologisch gebied de publiek opinie van de bevolking van de vijand beïnvloeden.

Om dit argument te illustreren halen Arquilla en Ronfeldt (1993), Schneider et. al. (1995) en Stocker et. al. (1998) verscheidene conflictsituaties uit het verleden aan. Zo worden er parallellen getrokken met bijvoorbeeld de kruistocht van de Mongolen onder leiding van Genghis Khan, de Blitzkrieg van de Duitse pantserdivisies in de Tweede Wereldoorlog en de eerste Golfoorlog. De voorbeelden illustreren krijgsmachten die via optimale communicatie, snelheid en logistieke efficiëntie hun tegenstanders kansloos laten. De auteurs geven aan dat informatie belangrijk is, maar dat het in de informatiesamenleving op een andere manier in wordt gezet.

Het belangrijkste aspect van deze vroege literatuur is het bieden van handvaten om de implicaties van de informatierevolutie te beschrijven. De uitkomsten van de verschillende mogelijkheden van cyberwar beschrijven is niet het hoofddoel. De teksten zijn provocerend bedoeld om een constructieve dialoog over het fenomeen te houden, dat niet alleen het militaire bestel treft, maar vooral ook de maatschappij als geheel verandert:

It is not technology per se, but rather the organization of technology, broadly defined, that is important. (…) *In our view, the technological shift that matches this broad view is the information revolution. This is what will bring the next major shift in the nature of conflict and warfare.*(Arquilla & Ronfeldt, 1993: 25)

We zien in *Battlefield of the Future* dat er nog veel aandacht wordt besteed aan de invloed van de nucleaire dreiging van de 'weapons of mass destruction', zoals de atoombom. Als het gaat om information warfare, ligt er heel veel nadruk op de strategische zwaartepunten die de geboorte van cyberwarfare met zich mee zou brengen. Zo wordt er in de literatuur ook de koppeling gemaakt tussen de computer vooruitgang en de atoombom.

This correspondence climaxes in the historic connection between the development of the atomic bomb and the computer, whereby the fateful synergy of destructive energy and information laid the foundation for the strategic power of information as a new type of weapon. (Stocker, 1998)

Het *cyber*-domein wordt wel gezien als het vijfde domein in de oorlogsvoering, naast land, zee,

lucht, en ruimte. In de militaire theorie was de verwachting dat cyberwarfare altijd ingezet zou worden ter ondersteuning van de fysieke troepenmacht. Doelstellingen op het gebied van deze online oorlogsvoering zijn in grote lijnen het verstoren van de logistiek van vijandelijke troepen. Hierbij kan gedacht worden aan het beperken van de logistieke toevoer van gemobiliseerde troepen, of het aantasten van de administratieve efficiëntie. (Schneider et. al.: 1995) De disruptieve werking van cyberwarfare lijkt dus het belangrijkste instrument te zijn. Verderop zal ik echter terugkomen op andere benaderingen, waarbij de rol van informatie en infrastructuur verandert.

2.2 *De definitie van InfoWar en het belang van informatie en infrastructuur*

De term 'informatie' neemt een centrale rol in wanneer we spreken over de verbeelding van het begrip cyberwarfare. Het is een essentieel onderdeel uit bij het opstellen van zowel sociaal-maatschappelijk als militair beleid. De consensus in de jaren '90 was dat informatie en de systemen die het verwerken, behandeld dienden te worden als een *strategic asset*:

A strategic information warfare attack on America's communication systems, including our military communication systems, air traffic control system, financial net, fuel pipeline pumping software,and computer-based clock/timing systems, could result in societal paralysis.

(…)Information Warfare is publicly identified as "actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems and computer-based networks while defending one's own…" (Stein, 1998)

De kritieke infrastructuur is een onderdeel dat beschermd en gekoesterd moest worden. Het wordt hierbij gelijk gesteld aan productiefactoren als kapitaal en arbeid. Het belang van de infrastructuur is duidelijk op alle niveau's van de maatschappij. Zoals Stocker aangeeft:

[T]oday's modern information infrastructure as the most essential pillar of transnational economic systems is not only the highest-priority target of potential aggression, but has also become—due to the computer's inherent capability of automating intelligence and to be Medium and Message simultaneously—the weapon and the battlefield all in one. (Stocker, 1998)

De juiste organisatie van de eigen informatie, en de controle van die van de vijand, zou leiden tot een strategisch voordeel, dat uitmondt in *information dominance*. (Arquilla en Ronfeldt: 1993: 25) De (discutabele) mogelijkheid van bloedeloze conflicten is de belofte van cyberwarfare. Het is voor een overwinning niet nodig de vijandelijke troepen te vernietigen. Ook via geweldloze middelen is het mogelijk om de vijand voorafgaand aan de fysieke strijd te doen geloven dat het ingaan van een gewapend conflict zinloos is. Dit is ook een adagium van Sun Tzu, die stelt: "For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without

fighting is the acme of skill"(Sun Tzu, 2003). Gewapende conflicten lijken vooralsnog onafwendbaar en volledig bloedeloze conflicten een utopische situatie. (Schöfbanker: 1998)

Een paradoxaal aspect in de literatuur van Arquilla en Ronfeldt, is dat ze aannemen dat cyberwar en netwar goede methodes zijn voor naties om tegen kleinere vijanden te vechten. Het recente verleden heeft echter aangeduid dat deze kleine mogendheden juist moeilijk te bestrijden zijn in het cyberdomein en zij juist makkelijkere middelen hebben met een globaal platform om schade aan te richten.

2.3 *Het gedecentraliseerde karakter van netwerken*

Hier krijgen we ook te maken met de mogelijkheid tot conflicten van lage intensiteit, met *non-state* actoren, waartoe bijvoorbeeld terroristische of anderszins fanatieke groeperingen kunnen worden gerekend.

Arquilla en Ronfeldt argumenteren dat het de strategische inzet is van de middelen die een partij voorhanden heeft die zorgen voor het effect op een tegenstander, en niet per se de kwantiteit van de middelen. Dit is evident wanneer we kijken naar hoe kleine groepen hackers toch relatief veel schade kunnen aanrichten, in zowel bedrijfsleven als bij overheid, door het stelen van gevoelige overheidsinformatie of informatie waar intellectueel eigendomsrecht op rust. In principe kan iedereen met een computer zich zonder al te veel moeite engageren in cyberaanvallen. Hier zien we het asymmetrische, gedecentraliseerde karakter van deze nieuwe bedreiging, die guerilla-oorlogsvoering in het cyberdomein mogelijk maakt, een paradigma verandering:

We anticipate that cyberwar, like war in Clausewitz's view, may be a "chameleon." It will be adaptable to varying contexts; it will not represent or impose a single, structured approach. Cyberwar may be fought offensively and defensively, at the strategic or tactical levels. It will span the gamut of intensity. (Arquilla & Ronfeldt, 1993)

Cyberaanvallen zijn bij uitstek geschikt voor laaggefinancierde non-state actors, die daarnaast niet eens veel kennis van zaken hoeven te hebben. Het is voor naties juist lastig om adequaat te reageren op cyberaanvallen van deze actoren. Als we kijken naar de *low-intensity* vijanden, bijvoorbeeld terroristische cellen die politieke vijanden worden genoemd, is de grootste dreiging voor de nationale veiligheid hun mogelijkheid *'to specialize in a specific military capability that appears to have high leverage against US forces'* (McKitrick, 1995). Vijanden exploiteren het meest kwetsbare gedeelte van de infrastructuur, waarbij ze weinig risico lopen om gevonden en vervolgd te worden, en toch een wijd bereik hebben via de cybermiddelen.

In *CyberWar is Coming* (1993) proberen Arquilla en Ronfeldt al een onderscheid te maken tussen

cyberwarfare als operationeel onderdeel van een strategisch fysiek militair conflict en 'netwar' aan de andere kant, als sociaal-ideationeel conflict, dat gevoerd wordt via zowel de traditionele mediakanalen als radio, televisie en print, als ook het internet:

We offer a distinction between what we call "netwar"—societal-level ideational conflicts waged in part through internetted modes of communication—and "cyberwar" at the military level. (Arquilla en Ronfeldt, 1993)

De inclusie van de verschillende meer propagandistische vormen van media manipulatie lijken echter in belang hebben ingeboet als we kijken naar de huidige kwesties rondom cyberwarfare, die niet zozeer te maken hebben met de manipulatie of kleuring van informatie als wel het afsluiten van de toegang daartoe. Er wordt dus wel rekening gehouden met de mogelijkheid dat door vijandelijke aanvallen de functionering van datastructuren wordt aangetast. De term InfoWar heeft wel weerslag op het informatiebestel, maar de nadruk ligt vooral op de manipulatie van informatie en psychologische oorlogsvoering.

In het hoofdstuk hierna zal ik analyseren dat er in de moderne literatuur de focus verschuift naar het blokkeren van de toegang tot informatie en andere potentiële gevaren van cyberagressie voor de infrastructuur.

Hoofdstuk 3: De verbeelding van het begrip cyberwarfare in literatuur van 2000-heden

3.1 *Cybersecurity als prioriteit*

Het is van essentieel belang voor zowel overheden, bedrijven als burgers dat de werking van de digitale infrastructuur te allen tijde kan worden gegarandeerd. Het gevaar van externe aanvallen wordt ook in steeds grotere mate erkend, dat onder meer naar voren komt in een speech met betrekking tot cybersecurity van de Amerikaanse president, Barack Obama, die stelde dat:

From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.[4]

Cyberwarfare krijgt steeds meer aandacht in media en beleidsvorming. Beleidsbepalers in de Verenigde Staten staan daarom nu voor het probleem om gestandaardiseerde wetgeving in en

[4] http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ Speech van de president Obama over Cybersecurity in de VS (transcript).

door te voeren, waarbij de duidelijkheid richting de burger gewaarborgd blijft, terwijl tegelijkertijd een gestructureerd apparaat van overheidsinstellingen bezig is de veiligheid van datanetwerken te garanderen. Er is een speciale organisatie aan het Pentagon toegevoegd, te weten het CyberCommand, dat zich zal bezighouden met cybersecurity.[5] Deze afdeling moet ervoor zorgen dat de overheid niet alleen reactionair te werk gaat, maar vooral preventief een solide, veilige infrastructuur opbrengt, waarbij technologische superioriteit het streven is.

We hebben recentelijk ook voorbeelden gezien van cyber aanvallen die in de buurt komen van de definitie van cyberwarfare zoals het voorbeeld van Rusland en Estland.[6] Cyberwarfare als operationele cyberwar bestempelen legt een blinde vlek neer bij het daadwerkelijke probleem, aldus Carr in *Inside Cyber Warfare* (2009). Er bestaat namelijk veel overlap tussen cybercrime, terreur, spionage en andersoortige cyberaanvallen. Nonstate actoren vallen ook de privésector aan. Deze cyberaanvallen brengen de natie als geheel wel in gevaar. De distinctie die incorrect gemaakt wordt tussen cyberwar en andere vormen van cybercriminaliteit, is dat de ene te maken heeft met militaire zaken en de andere juridisch aangepakt moet worden. *Cybercrime* gebruikt namelijk tools die potentieel collectief ingezet kunnen worden binnen een cyberoorlogsconflict.

Een andere opmerkelijke constatering is dat de houdbaarheid van het begrip InfoWar intact blijft. Carr geeft aan dat bij de aanslagen in Mumbai er bijvoorbeeld sprake is van een grote hoeveelheid van desinformatie, die we terugzien op *microbloggingsite* Twitter.com. Dit voegt alleen maar toe aan de chaos.[7]

Hoewel we dus theoretiseren over wat cyberwarfare nu precies inhoudt, moeten we ook aandacht besteden aan de precieze cases die we in voorbijgaande jaren hebben gezien. Wat hierbij opvalt is dat de impact van de cyberwar tot dusverre alleszins meevalt op militair gebied. De schade in de

---

[5] http://www.defense.gov/releases/release.aspx?releaseid=14030 Het was eerst het idée om het CyberCommand onder te brengen onder het gezag van de U.S. Air Force. Uiteindelijk is echter besloten dat er een apart onderdeel zou worden opgezet, dat het United States Cyber Command (USCYBERCOM) heet en onder de bevoegdheid van het United States Strategic Command valt. Het bereikte *full operational capability* op 31 oktober 2010

[6] http://www.newsweek.com/2009/04/17/the-fog-of-cyberwar.html Estland was in 2007 in conflict met Rusland om het weghalen van een standbeeld van een Russisch standbeeld uit de Tweede Wereldoorlog uit de hoofdstad Talinn. Dit leidde tot woede vanuit Rusland, waardoor er een beweging tot stand kwam die de internetverbinding naar een aantal overheidssites en banken platlegde, middels datavloeden vanuit een botnet, computers die over zijn genomen door hackers. Estland staat bekend als een natie die sterk afhankelijk is van haar moderne infrastructuur, waaronder voor een belangrijk deel het internet.

Vanuit de NAVO is toen een nieuw orgaan opgezet, het Cooperative Cyber Defense Centre of Excellence (CCDCoE), dat zich bezighoudt met het onderzoek van manieren om een robuustere infrastructuur op te stellen. Daarnaast houdt legt de overheid van Estland de nadruk op educatie op het gebied van cyber veiligheid.

[7] http://www.forbes.com/2008/11/28/mumbai-twitter-sms-tech-internet-cx_bc_kn_1128mumbai.html Tijdens de terroristische aanvallen op Mumbai, werd er veel desinformatie verspreid via Twitter, wat leidde tot nog meer onduidelijk in de reeds chaotische situatie.

privé sector wordt echter gegist op enkele tientallen tot honderden miljarden.[8]

3.2 *Strategie in Cyberspace*

Kunnen we het domein van de cyberspace binnen de militaire traditie als vijfde domein zien, naast land, zee, lucht en ruimte? Uit militaire overwegingen kan dit gesteld worden, om de veiligheid van netwerken en de bescherming tegen vijanden te garanderen. Het is echter wel duidelijk dat het probleem ook grotendeels buiten het militaire spectrum valt, omdat er sprake is van een maatschappelijk probleem. Een groot gedeelte van de netwerken is in privé handen van het bedrijfsleven (Carr, 2009).

Zoals Libicki (2009) stelt, is er sprake van cyberspace als een menselijk construct. Als we deze ruimte dan zien als virtueel slagveld, moet er rekening gehouden worden met de menselijke factor, omdat burgers zich er direct binnen navigeren.

Libicki redeneert dat cyberspace uit drie lagen bestaat. De fysieke laag, waar sprake is van de systemen, de hardware en de bedrading; de syntactische laag, dit is de kwetsbare laag die hackers kunnen manipuleren; de semantische laag, hier gaat het om de laag van de informatie, het te controleren doel bij cyberaanvallen. (Libicki 2009: 37)

Libicki (2009) geeft aan dat het debat is verschoven uit het academisch domein naar dat van beleidsbepalers binnen overheid en leger. Hij weegt in *Cyberwar and Cyberdeterrence* (2009) af hoe zinvol het is om een beleid van *deterrence*, oftewel afschrikking, te voeren. *Deterrence* bestaat uit twee componenten. Er is de intentie om een zeker belang te verdedigen en daarnaast een getoonde capabiliteit om de verdediging van dat belang na te streven, of de potentiële vijand een zo hoge prijs te laten betalen, dat het hem niet de moeite waard is om een aanval te ondernemen. (Libicki: 2009: 7)

Libicki maakt daarnaast een onderscheid tussen een strategische en een operationele cyberwar. Strategische cyberwar vindt plaats als er alleen sprake is van het inzetten van digitale methoden om tot strijd te komen. Er komen dus geen fysieke troepen aan te pas en geweld wordt vermeden. Daarnaast stelt de auteur dat een strategisch cyberconflict plausibel is zonder escalatie tot fysiek geweld. Het beeld dat door Libicki is gesteld is dat we ons gematigd zorgen moeten maken over de implicaties van strategische cyberwar. Hier zien we weer de mogelijkheid van de amateuristische *cyberwarrior*, die met zijn daden effect kan bereiken, zonder een gewelddadig conflict te ontlokken.

Van een operationele cyberwar wordt gesproken, als cyberwapens worden ingezet in de context van een traditioneel fysiek strijdtoneel. Het fenomeen kent in dit scenario dus een ondersteunende functie die, mits juist toegepast, wel kan leiden tot een expliciet voordeel in het

[8] http://www.sciencedaily.com/releases/2009/10/091008113339.htm Er wordt gegist naar schade van cyberaanvallen op de privésector: enkele tientallen tot honderden miljarden dollars.

conflict aan de hand van het verrassingselement, mits goed gepland en gedoseerd.

In de literatuur van Libicki (2009) blijven er ook parallellen getrokken worden met het verleden. De Koude Oorlog is een metafoor dat in verschillende contexten wordt aangehaald. Libicki geeft aan dat er sprake is van een bepaalde vorm van *deterrence*, afschrikking, zoals dat ook bestond bij de twee grootmachten die toentertijd over kernwapens beschikten. Dit was een punt dat Stein (1998) ook aanhaalde. Hij vroeg zich af of twee grootmachten zich zouden laten verleiden tot een totale informatie oorlog, die gevolgen zou hebben die niet in verhouding staan tot het gewin dat behaald kon worden.

Just as the mutually destructive effects of nuclear war were disproportionate to the goals of almost any imaginable conflict, so may be the mutually destructive effects of a "total" information war exchange on the publics exposed and subsequent rational communication between the sides. And as the techniques of "cyberstrike" proliferate throughout the world, enabling small powers, nonstate actors, or even terrorist hackers to do massive damage to the United States, "mutually assured cyberdestruction" may result in a kind of infowar deterrence. As Sun-Tzu advised, "without advantage, do not act; without gain, do not utilize; without crises, do not battle. (Stein, 1998)

Libicki zet echter terecht zijn vraagtekens bij de kracht van die wederzijdse afschrikking, omdat in het geval van cyberwar, het nooit duidelijk is waar de *second strike* op gericht moet worden en de vijand wel bewezen dient te worden. Is het echter wel duidelijk wie de vijand is, dan kan het conflict zich lang voortslepen, terwijl het bijvoorbeeld bij de aantasting van fragiele economische markten tot enorme schade kan leiden onder de burgerbevolking, die indirect kan leiden fysieke schade en verdere onrust.

De vraag die in meerdere werken rijst is dan ook: "Wat is belangrijker, offensieve capabiliteit, of een solide, veilig netwerk; dus verdediging?" Het tweede lijkt belangrijker, vooral omdat het moeilijk aan te tonen is wie de aanvaller is. Natiestaten zullen geen *high profile* cyberwar aanknopen, en de kleinere facties zijn vaak moeilijk te lokaliseren. De offensieve capabiliteit moet echter niet worden onderschat. Potentiële aanvallers zijn zo gedwongen om rekening te houden met de consequenties van hun daden.

3.3 *Het belang van een duidelijk afgebakende definitie van cyberwarfare*

Als term zijn zowel *cyberwarfare* als *information warfare* de laatste tijd onderwerp van discussie geworden. Het feit dat er zich steeds meer voorbeelden van cyberconflicten voor hebben gedaan in de recente geschiedenis, betekent dat er een steeds duidelijker beeld gevormd kan worden van wat er mogelijk is binnen een cyberconflict. De technische mogelijkheden, alsmede verschillende politieke motieven zijn duidelijker geworden, waardoor er een noodzaak komt tot een nog

scherpere definitie.

Carr (2009) omschrijft de volgende definitie van cyberwarfare, gebaseerd op Sun Tzu: “Cyberwarfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood”. Volgens deze definitie komen we bij een problematisch punt als we naar de realiteit kijken. Veel verhalen die worden aangemerkt in de media, vallen helemaal niet binnen deze definitie van cyberwar, aangezien het niet gaat om het 'verslaan' van een vijand, maar puur om geldelijk gewin, het stelen van informatie (bijvoorbeeld intellectueel eigendom), of andere gevoelige documenten.

Een advies dat Farivar (2009) geeft is dat de retoriek omtrent cyberwarfare niet overdreven moet worden. Oorlog is gebaseerd op twee facties die ongeveer op gelijke voet staan, qua capabiliteit. (Farivar, 2009) Zoals ik in het hoofdstuk hierna zal beargumenteren, is een vernauwing van de definitie nodig, omdat lang niet alle vormen van cyberaanvallen per se oorlogen zijn. Veel vaker zijn dit gevallen van georganiseerde criminaliteit, of van spionage van het bedrijfsleven dan wel overheden.

De noodzaak voor een scherpe definitie van het begrip is om meerdere redenen belangrijk. Ten eerste is het belangrijk om het publiek van accurate informatie te voorzien. Het heeft dus een educatieve functie, zodat er een goed begrip bestaat van wat er nu wel en niet als daad van cyberwar geldt, om zo verwarring te voorkomen.

De tweede, belangrijkere reden is dat een heldere definitie bijdraagt aan betere wetgeving. Zo kan het probleem gerichter aan worden gepakt. Het gevaar is concreet en het is duidelijk dat verschillende landen bezig zijn zich te oefenen in de verschillende concepten en technologieën, om zo een technologisch voordeel te putten uit het virtuele domein. In dit licht is er dus zeker sprake van een proliferatie van cyberwapens en technologie, alleen proberen naties er alles aan te doen om *low key*, zo geheim mogelijk, te regelen om zo juridische obstakels en internationale vervolging te vermijden.

Er zijn meer dan 120 naties die het internet gebruiken voor *leverage,* als een hefboom om doelen te bereiken. Ze hebben een vrij anonieme manier om op illegale wijze aan informatie te komen (Carr, 2009). Het probleem in deze situatie is dat het moeilijk voor de slachtofferstaat is om te komen tot *attribution*, het met zekerheid aanwijzen van de dader, om vervolgens adequaat te reageren. Zelfs als er al een dader kan worden aangewezen, onder welke voorwaarden mag het slachtoffer dan terugslaan. En mag dit met fysieke middelen? Daarnaast moeten naties met vooral kleinere vijandelijke groeperingen rekening houden. Deze laatstgenoemden onderhouden in sommige gevallen banden met de overheden van de landen waarbinnen ze opereren.

Een voorbeeld hiervan is het conflict tussen Rusland en Georgië, dat ging om de provincie Zuid- Ossetië, die onafhankelijk wil worden van Georgië. Het moest lijken alsof er sprake was van een spontane hackersbeweging die zich inzette voor het Russische doel, maar betrokkenen

plaatsen hun vraagtekens daar bij. Zij stellen dat het de Russische overheid is die een flinke druk uitoefent op deze bewegingen en dat het de overheid is die de organisatie in het geheim in handen had. Opmerkelijk is verder dat deze cyberaanval hand in hand ging met de mobilisatie van een fysieke troepenmacht. In die zin kan er in deze context worden gesproken van een operationele cyberwar op kleine schaal. (Carr, 2009: 3, 17)
Tekenend is daarnaast dat er in dit conflict ook sprake is van het publiceren van veel informatie en desinformatie. Beide betrokken partijen noemen elkaars 'feiten' propaganda. De Russen beschuldigen Georgië ervan dat zij de eerste cyberaanval hebben gelanceerd, terwijl op hun beurt de Georgiër aangeven dat het slechts een aanval was op de Russische agressie. Ook proberen ze de Amerikanen, die pro-Georgisch waren, ervan te beschuldigen dat zij de agressor waren. Het Kremlin wil de discussie rondom cyberwar richten op de militaire capabiliteit, terwijl hun eigen betrokkenheid bij de cyberincidenten onbesproken blijft. Er was echter niet genoeg bewijslast om betrokkenheid aan te tonen. Dat neemt echter niet weg dat in de opinie van betrokken partijen er een duidelijke connectie is tussen de hackers en het Kremlin (Carr, 2009: 17,18).

Er is een bewijslast nodig om de connectie met de overheid aan te tonen. Is er geen duidelijke connectie, dan kan het land zich nog verschuilen achter 'plausible deniability', het ontkennen van enige betrokkenheid. Dit betekent vervolgens dat er geen juridische consequenties aan het conflict zijn verbonden (Sklerov, 2009).

3.4 *Cyberwar als zwaarste vergrijp*

Vele vormen van disruptie middels informatietechnologie lijken onder de noemer *cyberwarfare* te vallen. Zo omschrijft Myriam Dunn Cavelty in de *Parliamentary Brief* cybercriminaliteit als een breed scala aan activiteiten die niet allen op politiek niveau geadresseerd dienen te worden. Ze onderscheidt verschillende categorieën, gerangschikt naar mate van ernst. Er is de noodzaak cyberwarfare te scheiden van andere vormen van cyber aanvallen zoals cybercrime en spionage, die wel chaos zaaien of info stelen, maar niet van permanente aard zijn.[9] Alleen de vijfde rang, valt onder haar definitie van cyberwarfare, een digitale vorm van oorlogsvoering waarbij het doel is gehele communicatiesystemen lam te leggen:

Rung five: cyberwar. Refers to the use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems. In military terms, such activities are known as Computer Network Attack (CNA), a concept which is part of the official information operations doctrine. Two types need to be distinguished: CNA as a tactical- operational means in

[9] Dunn-Cavelty, M. The Reality and Future of Cyberwarfare, http://www.parliamentarybrief.com/2010/03/the-reality-and-future-of-cyberwar

the context of an overall operation or CNA as a strategic, stand-alone tool.[10]

Er is steeds meer inzicht gekomen in de technische aspecten van cyberaanvallen. De verschillende gradaties van cyberaanvallen, van criminaliteit tot aan spionage, tonen aan dat we met een reële bedreiging te maken hebben. Westerse informatiemaatschappijen lopen risico's als het aankomt op bijvoorbeeld toegang tot overheidssites, maar ook meer ingrijpende kwetsbaarheden ten opzichte van de elektriciteits*grid* zijn niet ondenkbaar. Vooral in de literatuur van de laatste jaren is steeds meer oog voor het cyberdomein in relatie tot de burgermaatschappij, dus niet alleen vanuit militair oogpunt. Dit betekent ook dat we niet blijven steken in het klassieke paradigma van traditionele oorlogsvoering (Carr, 2009) (Janczewski, 2007).

Dat neemt niet weg dat terrorisme een belangrijke instrument is voor nonstate actors binnen de grotere context van cyberwarfare. Er bestaat zo ook een gemedieerd beeld van cyberwarfare, via propaganda en deceptie, onder het credo 'meer visibiliteit van aanslagen leidt tot een hogere impact en meer onderhandelingsruimte (Janczewski, 2007: 42).

Hoofdstuk 4: *De toekomst van Cyberwarfare: een realistische aanpak*

Op dit moment zien we dat er globaal veel aandacht wordt besteed aan het thema *cybersecurity*. Zo worden er op internationaal niveau samenwerkingsverbanden opgezet die het gevaar adequater aan kunnen pakken, omdat naties samen beter in kunnen spelen op de aard van het probleem, namelijk het gedecentraliseerde karakter van de bedreiging. Er is veel aandacht voor de het beschermen van de infrastructuur. Een voorbeeld van een van deze ondernemingen is het zeer recente *Cyber Europe*, waarin de Europese Unie een cyberaanval op haar eigen infrastructuur simuleert, om de kwetsbaarheden en aandachtspunten bloot te leggen.11

Situaties van totale oorlog, ondersteund door een cyberwar op volle schaal zijn natuurlijk niet uit te sluiten, maar lijken naar aanleiding van de literatuur niet erg realistisch, gezien de consequenties die dit voor natiestaten zou hebben.

In de literatuur worden echter wel potentiële bedreigingen geschetst, waaronder het metafoor van de wapenwedloop, alleen dan in de vorm van een *cyberarmsrace*. Zoals veel experts aangeven is er sprake van een revolutie op het gebied van cyberwarfare, een veld dat nu volwassen lijkt te worden. Aanleiding is de *StuxNet*-malware, die een andere aard heeft dan traditionele virussen.

---

[10] Ibid.
[11] http://www.bbc.co.uk/news/technology-11696249 *Europe Simulates Total Cyberwar* en http://www.bbc.co.uk/news/technology-11726671 *European Cyber Defenses 'Must Improve', Tests Show.* Deze nieuwsberichten tonen de stappen die gezet worden om de Europese infrastructuur collectief gezien weerbaarder te maken tegen aanvallen van buitenaf.

Ingewijden en experts binnen de wereld van cybersecurity hebben deze vorm van malware al bestempeld als een revolutie binnen de cyberwarfare, omdat het qua karakter verschilt van andere virussen en malware; het steelt geen informatie, gebruikt geen *botnets* om de toegang te beperken, maar kan de processen binnen de infrastructuur regelen.[12] Daarnaast hebben experts aangegeven dat dit project te gecompliceerd en kostbaar was om in een kort tijdsbestek door een willekeurig groepje programmeurs uit te zijn gevoerd. Het is een gecontroleerd virus, dat zichzelf alleen onder eigen voorwaarden verspreidt. De StuxNet malware zorgt ervoor dat het de *programmable logic controller* kan saboteren, om zo verschillende systeemprocessen te ontregelen, wat volgens een technisch rapport van internet veiligheidsspecialist Symantec ernstige gevolgen kan hebben.[13]

Dunn-Cavelty stelt dat het gevaar van cyberwar moet worden gerelativeerd. Ze stelt dat de hype moet worden vermeden, en er moet worden gesproken van criminaliteit en cyber veiligheid om beter samen te werken met de zakelijke sector, die de 'most crucial role in critical infrastructure protection' speelt, omdat het grootste gedeelte van de infrastructuur in privébezit is.[14]

Conclusie

De doelstelling van dit paper was het geven van een duidelijk beeld van hoe de (vooral militair georiënteerde) literatuur het begrip 'cyberwarfare' verbeeldde sinds het invloedrijke artikel 'Cyberwar is Coming!' van Arquilla en Ronfeldt. In de loop van dit eerste decennium van de 21e eeuw heeft de globale maatschappij kennis gemaakt met de invloed van verschillende vormen van conflicten in cyberspace. Dit heeft ertoe geleid dat er een steeds hogere prioriteit wordt verbonden aan de beveiliging van kwetsbaarheden binnen de datanetwerken van natiestaten en de zakelijke sector.

Een vraag die rijst is of we daadwerkelijk al de ware potentie van cyberwarfare hebben gezien. In de behandelde literatuur kwamen veel van de concrete bedreigingen aan bod. Zo proberen auteurs door middel van provocatie een discussie uit te lokken over de eventuele implicaties van cyberconflicten op het globale politieke landschap.

---

12 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf Er is geen sprake van zogenaamde *botnets*: zombiecomputers die in worden gezet om datavloeden in te zetten.

13 Ibid. Dit rapport van Symantec analyseert de technische aspecten van de StuxNet-malware. Daarnaast wordt er uiteengezet in hoeverre het progamma nieuwe implicaties zal hebben op het landschap van cybersecurity.

14 http://www.parliamentarybrief.com/2010/10/the-real-cyberwar-is-about-beating-the-crooks-and-the#page_2 Dunn-Cavelty geeft aan dat we het gevaar van cyberwarfare wel serieus moeten nemen, maar daarnaast dienen te relativeren. We zouden vooral moeten denken in termen van cybercriminaliteit, aangezien dit de meest voorkomende vormen va bedreigingen zijn, die ons ook het meeste geld kosten.

Het metafoor 'cyberwapen-wedloop' is echter wat vergezocht. Zoals Libicki aangaf is de impact van cyber-*deterrence* vergeleken met de dreiging van *weapons of mass destruction* veel kleiner. Elke natie zal daarnaast voorop willen lopen in technologische innovatie. De dominante positie verzorgt naast strategische voordelen ook economisch gewin en daarom zal dit een gebied blijven dat elke natie zal willen exploiteren. Op dit moment zitten we als globale samenleving middenin het proces van verandering; van het oprichten van nieuwe samenwerkingsverbanden, het aanpassen van wetgeving, zowel nationaal en internationaal en de verregaande activiteiten van beveiligers om de datanetwerken veilig te stellen.

Hoewel er in de literatuur veel gesproken wordt over de capabiliteit tot cyberwarfare, blijft het tot nu toe vooral bij aanvallen en conflicten op kleinere schaal, van lagere intensiteit. Er zijn nog geen echte grootschalige conflicten geweest die hebben geleid tot een wereldwijde escalatie. Wel is er veel aandacht voor het plannen van de toekomst, zorgen voor veiligere netwerken, omdat ook deze conflicten met een lage intensiteit bij elkaar opgeteld enorm veel (vooral financiële) schade aanrichten.

Er is bovendien een duidelijke paradigmaverschuiving geweest van het propagandistisch psychologische karakter van 'InfoWar' naar een meer technocentrische benadering, waar ook de menselijke factor niet is weg te denken. Het gevaar van cyberwarfare wordt vooral gerepresenteerd als een manipulatie van de infrastructuur en het exploiteren van kwetsbaarheden. Het doel van die manipulatie is het beperken van de toegang.
Dat betekent niet dat het aandeel dat propaganda binnen een *infowar* speelt verdwijnt, maar puur dat die rol onder invloed van technologische ontwikkeling aan het transformeren is.

Er is geen pasklaar antwoord te vinden op wat de toekomst zal bieden, of de StuxNet-worm daadwerkelijk de Doos van Pandora heeft geopend qua cyberwarcapabiliteit. Geen enkele natie is namelijk op zoek naar een confrontatie, die onherroepelijk ook traditionele segmenten van het militaire bestel vereist. Zoals in *InfoWar* al aan werd gegeven:

> The actual danger of hacker attacks and cyberterrorists in the US does not lie in highly-improbable large-scale acts of destruction or sabotage, but rather in the effects of a small number of spectacular attacks on the American media public with the resulting consequences on the decision-making latitude of American politics.(Stocker, 1998)

De houdbaarheid van deze en veel andere theorieën uit de vroege cyberdoctrine blijven nog steeds opgaan. We moeten niet meegaan in de hype van het *buzzword*, maar realistisch blijven. Er is nog geen cyberescalatie op wereldniveau. Wel zijn er irritaties, bedreigingen en de noodzaak tot beveiliging. Waar veel van de militaire literatuur nog te weinig rekening mee houdt, is dat het

probleem van cyberdreiging meer is dan een puur militair probleem, vanwege de diepgewortelde connecties tussen internet en maatschappij. Wat we hebben gezien is dat er een belangrijke rol is weggelegd voor het militaire bestel in de huidige ordening voor cybertaken. Wat naar aanleiding van dit paper wel duidelijk is geworden is dat er, zolang er niet op grote schaal gebruik wordt gemaakt van een combinatie tussen traditionele fysieke factoren van oorlogsvoering in samenwerking met de door internet gemedieerde vormen van cyberwar, de cybertaken wellicht beter verzorgd kunnen worden door overheidsinstellingen die niet onder de directe autoriteit van het leger vallen, omdat het gaat om bijvoorbeeld netwerken die in het bezit zijn van bedrijven. Oplossingen zullen vooral in diplomatieke en juridische richting gevonden moeten worden. Het is de ambiguïteit van cyberwar als concept dat enerzijds een militaire onderneming is, maar nu actueel misschien nog wel relevanter, een economisch en politiek-maatschappelijk vraagstuk.

Bibliografie:

Carr, J. (red.) *Inside Cyberwarfare: Mapping the Cyber Underworld*, Sebastopol: O'Reilly Media 2009.

Clausewitz, C. von, *On War (Oxford World's Classics)*, Oxford: O.U.P., 2007.

Czosseck, C. en K. Geers (red.) *The Virtual Battlefield: Perspectives on Cyberwarfare*, Amsterdam: IOS Press, 2009.

Farivar, C. *A Brief Examination of Media Coverage of Cyberattacks (2007-Present).* In: *The Virtual Battlefield: Perspectives on Cyberwarfare,* Amsterdam: IOS Press, 2009

Janczewski L.J. en A.M. Colarik (red.) *Cyberwarfare and Cyber Terrorism*, IGI Global, 2007.

Libicki, M.C. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009.

Lonsdale, D.J. *The Nature of War in the Information Age: Clausewitzian Future*, New York: Frank Cass, 2004.

Sklerov M.J., *Responding to International Cyber Attacks As Acts of War* in: *Inside Cyberwarfare*

Sun Tzu, *The Art of War*, New York: Barnes & Noble Classics, 2003.

Internet

Arquilla, J. & D. Ronfeldt. *Cyberwar is Coming! Pp 23-54*

<http://www.rand.org/pubs/monograph_reports/MR880/MR880.ch2.pdf> 18-11-2010

BBC, *Europe Simulates Total Cyberwar*
<http://www.bbc.co.uk/news/technology-11696249> 18-11-2010

BBC, *European Cyber Defenses 'Must Improve', Tests Show*
<http://www.bbc.co.uk/news/technology-11726671> 18-11-2010

Dunn-Cavelty, M. The Reality and Future of Cyberwarfare,
<http://www.parliamentarybrief.com/2010/03/the-reality-and-future-of-cyberwar> 18-11-2010

Hables Gray, C. *The Crisis of InfoWar*
<http://90.146.8.18/en/archives/festival_archive/festival_catalogs/festival_artikel.asp?iProjectID=8449> 20-11-2010

Kittler, F. *Infowar. Notes On The Theory History*
<http://90.146.8.18/en/archives/festival_archive/festival_catalogs/festival_artikel.asp?iProjectID=8382> 18-11-2010

Nikolaewitsch Panarin, I. *InfoWar and Authority*
<http://90.146.8.18/en/archives/festival_archive/festival_catalogs/festival_artikel.asp?iProjectID=8445> 18-11-2010

Schneider, B.R. en L.E. Grinter. *Battlefield of the Future: 21st Century Warfare Issues*
<http://www.airpower.maxwell.af.mil/airchronicles/battle/bftoc.html > 18-11-2010

Stocker, G. en C. Schöpf. InfoWar (Ars Electronica)
<http://90.146.8.18/en/mainSearch/frame.asp?search=infowar&submit.x=0&submit.y=0> 18-11-2010

Schöfbänker, G. *From Cyberwar to INFOWAR - Computing and Telecommunications for "Real" and "Virtual" Warfare*
<http://90.146.8.18/en/archives/festival_archive/festival_catalogs/festival_artikel.asp?iProjectID=8383> 18-11-2010

Stein, G.J. *Information Warfare: Words Matter*
<http://90.146.8.18/en/archives/festival_archive/festival_catalogs/festival_artikel.asp?iProjectID=8446> 20-11-2010

Stocker, G. *InfoWar*
<http://90.146.8.18/en/archives/festival_archive/festival_catalogs/festival_artikel.asp?iProjectID=8442> 21-11-2010

Stocker, G. *InfoWar – The Re-ordering of Things*
<http://90.146.8.18/en/archives/festival_archive/festival_catalogs/festival_artikel.asp?iProjectID=8381> 20-11-2010