

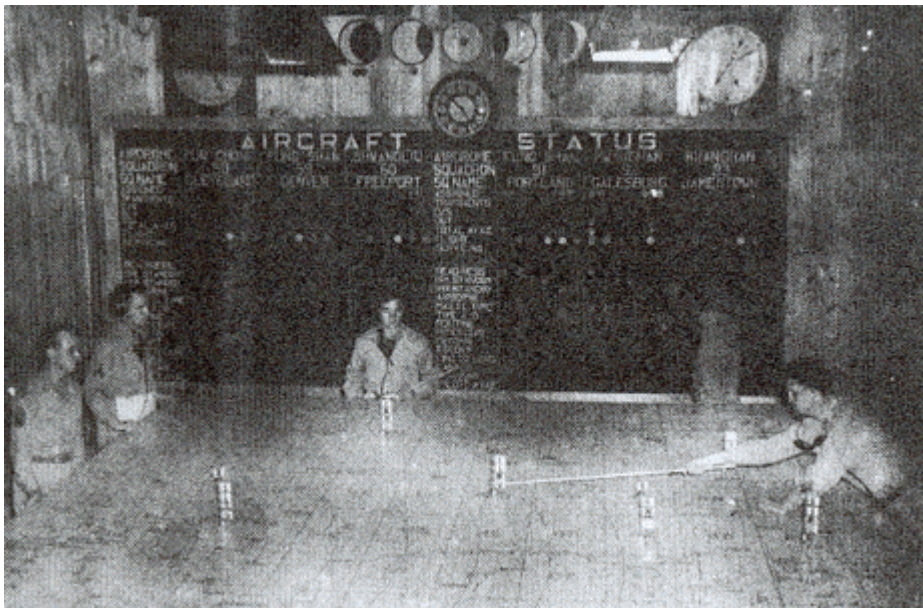
**Humboldt-Universität zu Berlin  
Institut für Sozialwissenschaften**

SE „Neuere Debatten zur Innovations- und Technikanalyse“  
WS 2001/2002

Dozenten: Dr. Daniel Bieber, Dr. Marc Bovenschulte, Dr. Susanne Giesecke

## **Cyberwar – Neue Technologie und Rüstungskontrolle**

Bearbeitet von: Thoralf Kamin (chimney@gmx.net),  
Philipp Mayr (mayr@informatik.hu-berlin.de), Martin Merl (martin.merl@gmx.de)



The brain of a human-machine weapon system. As the official description puts it China: Operations. Men plotting the course of 14<sup>th</sup> Air Force planes in the fighter control section of the 312<sup>th</sup> Fighter Wing, 14<sup>th</sup> Air force at a base somewhere in China. ... The control of information is crucial. USAAF files, NASM Library, photo 2188.

## Inhalt

1. CYBERWAR - BEGRIFFSTHEORETISCHE ÜBERLEGUNGEN.....	3
2. ERSCHEINUNGSFORMEN.....	6
3. CYBERWAR UND POLITIK .....	7
4. VOM KRIEGE .....	8
5. NEUERE DEBATTE ZUM THEMA CYBERWAR .....	12
6. VERLETZLICHKEIT KRITISCHER INFRASTRUKTUREN.....	13
7. KRITISCHE INFRASTRUKTUREN.....	15
8. MIßBRAUCH VON TECHNIKSYSTEMEN / VARIANTEN UND MOTIVE FÜR MIßBRAUCH.....	16
9. AUSPRÄGUNGEN EINES CYBERWAR.....	16
9.1 CYBERWAR .....	16
9.2 INFORMATION WARFARE.....	17
9.3 REALE ERSCHEINUNGSFORMEN VON CYBERWAR .....	19
9.4 SCENARIO „ELECTRONIC PEARL HARBOR“ .....	19
10. AKTEURE .....	20
11. SICHERHEITSSTRATEGIEN - DER DINOSAURIER STAAT LÄUFT UNSIHTBAREN ERREGERN HINTERHER .....	21
12. KONVENTIONELLE RÜSTUNGSKONTROLLE UND INFORMATION WARFARE .....	22
13. LITERATUR .....	27

## 1. Cyberwar - begriffstheoretische Überlegungen

Die Lufthoheit über dem Begriffsfeld "Cyberwar ist noch nicht ausgefochten. Je nach forschungslogischem Vorgehen oder ideologischer Selbstverortung variiert das gewählte Definitionsvokabular.

Wenn man mit R. Kipling annimmt, daß das erste Opfer des Krieges die Wahrheit sei, so befinden wir uns in einem Zustand des Krieges um die Definition des inkriminierten Begriffes.

Neuere kulturtheoretische Ansätze beschäftigen sich seit den 90-er Jahren und bis in die jüngste Zeit mit dem Phänomen eines technisierten militärischen Interventionismus. Die Vereinigten Staaten von Amerika mit ihrer als expansiv wahrgenommenen Außenpolitik, stehen im Fokus des kritischen Interesses.

Aus der Befassung mit Tagesaktualitäten wurde dadurch ein Debattenfeld gespeist, das den informationalen Aspekt dieser Entwicklung beleuchtet. Einer bestimmten theoretischen Annäherung kann dabei noch nicht der Vorzug gegeben werden. verschiedene Ansätze widmen sich dem mithin doch recht diffusen Begriffsfeld "Cyberwar", "Cyberkrieg". Sie sind bisher vor allem an der Schnittstelle zwischen Kultur- und Sozialwissenschaften auszumachen. Aus der Urbanistik kommend hat sich der französische Kulturtheoretiker Paul Virilio mit dem Phänomen der gesellschaftlichen Beschleunigung befaßt, welche er in der von ihm benannten Forschungsgattung der "Dromologie" [FN: "dromos"=( (griech.)Geschwindigkeit] behandelt.

Seine "Dromologie" versteht sich als transhistorischer Versuch, die nach-moderne Existenz analytisch zu erfassen. Er geht in seiner jahrzehntelangen Befassung mit seinem Gegenstand historisch vor unter häufigem Rückgriff auf militärische Phänomene, wodurch sich die Dromologie für die Frage nach dem "Cyberkrieg" von selbst empfiehlt [vgl. Virilio 1989].

Zentrale These im Virilioschen Oeuvre, ist die, daß die Geschwindigkeit die verborgene Seite des Reichtums und der Macht sei [vgl. Weiß 1998:34f.]. Geschwindigkeit ist nach Virilio das zentrale Agens der modernen Kommunikationsmedien [vgl. Virilio 1990] Dromologie gereicht zu einer Gesellschaftstheorie eigener Art, da sie versucht, in Einzeldisziplinen entwickelte Ansätze übergreifend zusammenzuführen. Daher finden sich in die Stichworte: Medien, Geschwindigkeit, Gesellschaft, Krieg mit und nebeneinander.

Für die jüngere militärische Entwicklung, die Virilio ebenso beleuchtet wie die Zeiten der Kriegsführung vor dem Epochenbruch der französischen Revolution, erlangen jedoch die Medien in seinem Konzept eine zentrale Stellung [vgl. Virilio 1993].

Durch Beschleunigung werden Medien, so der Autor, zu einer Trajektorie auf elektronischer Basis, womit man bereits bei der Synthese von Waffensystemen und medialer Perzeption wäre. Informationen werden im Virilioschen Begriffskosmos zu "lichtgeschwinden Geschossen", die nicht mehr physische sondern mediale Zerstörungskraft besitzen. Ein Gedanke, der später noch auszuführen ist. Mit dieser definitorischen Weitung verschwindet der herkömmliche Begriff des Projektils aus der Betrachtung. Nicht mehr auf dessen physische Konkretisierung käme es demnach mehr an, sondern auf die mit seiner Geschwindigkeit verbundene auch immaterielle Zerstörungskraft. Denn ein Geschöß das nur noch als ein imaginäres angenommen wird, ist nicht mehr aus realer Materie herzustellen, sondern wird abstrahiert zum bloßen Konzept. Prägendes Merkmal dieses Konzeptes von Projektil ist aus dem Dromologie-Ansatz folgend, seine Eindringgeschwindigkeit und diese muß für alle elektronischen Formen als sehr hoch angenommen werden.

Vermögen herkömmliche, stofflich gebundene Projektile im Extremfall die Grenze der Schallgeschwindigkeit gerade zu transzendieren, so reichen elektronische "Geschosse" mit lediglich Näherungsverlusten an die Lichtgeschwindigkeit an. Vereinfachend spricht Virilio bei einem solchen Übertragungsmodus von "Lichtgeschwinden Medien". Die Effizienz von Geschossen jeder Provenienz muß sich mit dieser Verschiebung an der Beschleunigungsfront auf die Kategorie von Echtzeit anwenden lassen, denn in Echtzeit liegen inzwischen alle kriegsrelevanten Informationen vor. Der Krieg selbst war lange Zeit ein Bestimmungsfaktor, wenn es darum ging, Transportzeiten von Menschen und Material oder Information zu vermindern. Am Ende dieser militärlogisch gerichteten Entwicklung steht die Information selbst und ihre ubiquitäre Verfügbarkeit fast jederzeit, fast überall. Jene unterliegt nicht länger der Defizienz stofflicher Waffen. Diese bedürfen relativ viel Energie, um von A nach B transportiert zu werden. Abstrahiert man von ihrer physischen Natur, so bleibt als militärlogisch "bester" Transportmodus nur die lichtgeschwinde Übertragung übrig. Ihre Bestimmung wird die einer Waffe mit unbestimmt hohem Potential.

Als Definitionsversuch sei aus diesen Überlegungen folgend angeboten:

- unter "Cyberwar" soll eine kriegerische Auseinandersetzung verstanden werden, die vermittels elektronischer Informationssysteme erfolgt.

Hinsichtlich des stofflichen Destruktionspotentials muss spezifiziert werden:

- im "Cyberwar" sollen militärische Aktionen verstanden werden, jede Form eines Angriffes auf Kommunikations- und Informationsinfrastrukturen.

Unter solche fallen:

alle Formen der Aufnahme, Verarbeitung und Speicherung von Informationen. Dem medienanalytischen Ansatz von Weischenberg und Schmitt folgend [vgl. Merten, Weischenberg, Schmitt 1998], sind die Fülle dieser Formen als Informations- und Kommunikationstechnologien zu fassen. Ihre Merkmale im Sinne sozialwissenschaftlicher Items sind:

- Multifunktionalität,
- Vernetzung,
- Diffusionsgeschwindigkeit sowie
- Diffusionsbreite.

Diese prägen die technologische Infrastruktur einer Gesellschaft und ihrer militärischen Einrichtungen. Nimmt in einer Gesellschaft Information und Kommunikation auf den genannten Items hohe Ausprägungen an, so spricht die Literatur von "Informationsgesellschaft" [vgl. Merten 1994].

Militärische Auseinandersetzungen in der Informationsgesellschaft tragen deren veränderten Produktions- und Reproduktionsbedingungen Rechnung. Im Vergleich stellen die sogenannten "kritischen Infrastrukturen" nicht die Stätten der Produktion und Distribution physischer Güter, sondern die Einrichtungen der Kommunikation dar. Dabei nehmen elektronische Datenverarbeitungssysteme eine Schlüsselstellung innerhalb dieser kommunikativen Infrastrukturen ein.

Die rasante technische Entwicklung innerhalb der vergangenen drei Jahrzehnte leistete den zentralen Beitrag zur Entwicklung komplexer Informationsnetzwerke.

Militärische Auseinandersetzungen werden sich, so die These, zunehmend gegen diese Strukturen nachindustrieller Gesellschaften richten [vgl. Weiß 1998]. Zugleich ermöglicht die technisch induzierte Fortentwicklung der Kriegsführung selbst, einen weitgehenden Verzicht auf Kriegstechniken, wie sie in der fortgeschrittenen Industriegesellschaft entwickelt wurden. Die Militärtechnik nimmt in diesem Rahmen die Position des Erzeugers neuer Waffensysteme und Methoden der Kriegsführung ein. Sie ist darin sowohl Nutznießer als auch Impulsgeber technischer Innovationen im zivilen Bereich.

Entgegen der Ansicht, daß der Krieg der Vater aller Dinge sei, muß man von einem mindestens zweidimensionalen Prozeß wechselseitiger Interaktion zwischen

militärischem und zivilem Bereich ausgehen. Damit wäre dem älteren Postulat eines militärisch-industriellen Komplexes, wie es aus marxistischer Provenienz klang, eine Absage zu erteilen. Für den interessierenden Bereich der IuK-(Informations- und Kommunikations-)Technologie muß vielmehr von interdependenten Systemen Militär und ziviler Forschung ausgegangen werden.

## **2. Erscheinungsformen**

Anknüpfend an den Objektbereich "Informationssysteme" gilt es festzuhalten, was unter einem kriegerischen Akt unter den Bedingungen des "Cyberwar" zu verstehen ist. Informationssysteme verstanden als "kritische Infrastrukturen", soll sich ein Akt des "Cyberwar" auf die Beschädigung oder Beseitigung dieser Informationseinrichtungen richten.

Dieser Akt soll definitorisch jedoch nicht primär die physische Beseitigung dieser Strukturen beinhalten, seien sie gleich militärischer oder ziviler Nutzung. Dieses Ziel ist mit herkömmlichen bis hin zu Massenvernichtungswaffen gleichfalls zu erreichen. Eine informationale Beeinträchtigung kommunikativer Strukturen ist auch strukturimmanent möglich.

Wesentlicher Bestandteil elektronischer Kommunikationssysteme, ist die ihnen eingeschriebene Verarbeitungslogik, welche in Programmiersprachen, der sogenannten "software", festgehalten wird. Diese Logiken werden in Informationssystemen bereitgehalten und als elektromagnetische Impulse auf geeigneten Speichermedien konkretisiert, um personenunabhängige Verarbeitungsvorgänge möglich zu machen.

Die darin enthaltenen symbolisch generalisierten Konnotate stellen die Information im weiteren Sinne dar.

Vermittels entsprechender Logiken verarbeitete Vorgänge, werden nur durch die Verarbeitung und Speicherung in den dafür ausgelegten Systemen zur "Information" im engeren Sinne. Informationen in alltagssprachliche Bedeutung des Begriffes, stellen dabei die Summe der symbolisch spezifizierten Konnotate, die aus logik-gebundener Verarbeitung hervorgehen, dar. Informationen die nicht verknüpft mit einer oder mehreren Arbeitsanweisungen ist, ist nicht mehr intersubjektiv reorganisierbar. Die Informationstheorie spricht im Falle der Abwesenheit von hinreichend niedrig konnotierenden Verarbeitungslogiken, im Hinblick auf den dann gegen null gehenden Informationsgehalt, von "Rauschen".

In Anlehnung an C.E.Shannon, kann Information auch vereinfachend als Summe aller Unterschiede gefasst werden [vgl. Shannon/Weaver 1963]. "Rauschen" in diesem Sinne, wäre die Abwesenheit eines nachweisbaren Unterschiedes.

### **3. Cyberwar und Politik**

Die vorangegangenen Überlegungen speisen die Frage, ob "Cyberwar" überhaupt noch als politisches Handeln zu bewerten ist.

Zwar wird cybermilitärisches Handeln noch länger mitbestimmt werden von kollektiven Akteuren wie dem Staat. Diesen Gedanken trägt noch die Hinführung zum Begriff vom Beispiel des globalen, militärischen Interventionismus ausgehend. Doch die Überlegungen zum Informationsbegriff und zu den Infrastrukturen der nachindustriellen Gesellschaft, lassen eine Verschiebung der Zuständigkeiten vermuten. Verkürzend wäre es heute mehr noch als zuvor, den Krieg als die Fortsetzung der Politik mit anderen Mitteln zu betrachten, doch soll die politische Dimension des Begriffes nicht ausgeblendet werden. Die Viriliosche Perspektive macht die Veränderungen auf der Ebene der Geschwindigkeit relevant für die Sphäre des Politischen, wie die Überlegungen zum „dromologischen Zeitalter“ zeigen [vgl. Virilio 1990].

"Cyberwar" erscheint auf der Begriffsagenda in Zeiten, in denen ein Wandel staatlichen Kriegshandelns auszumachen ist. Politische Erwägungen lassen den Einsatz von Massenheeren zunehmend unzweckmäßig erscheinen, womit von überkommenen Formen der Kriegsführung Abschied genommen wird. Das Beispiel des zweiten Golfkrieges aus dem Jahr 1990 hat gezeigt, daß das Bestreben der Kriegsparteien dahin geht, Distanzwaffen den personengebundenen Streitkräften vorzuziehen. Distanzwaffen unterliegen ihren anderen Perzeptionsbedingungen. Optische Apparaturen und vernetzte Information treten an die Stelle menschlicher Kombattanten [vgl. Virilio 1989]. Mit dieser Entwicklung rückt plötzlich der Krieg als völlige Distanzkategorie in den Blick: als Krieg in virtuellen Räumen: denen der elektronischen Datenbanken.

#### 4. Vom Kriege<sup>1</sup>

Ein mit einer Vielzahl von Definitionen und Beschreibungen besetztes Feld ist die Frage, was denn Krieg sei. Historische Entwicklungslinien, einmal in techniziden Kategorien von Mannes- und Feuerkraft, ein andermal unter dem Focus der strategischen Genialität eines Feldherren usw. Das bekannteste Diktum ist wohl das des preußischen Generals Carl von Clausewitz: „So sehen wir also, daß der Krieg nicht bloß ein politischer Akt, sondern ein wahres politisches Instrument ist, eine Fortsetzung des politischen Verkehrs, ein Durchführen desselben mit anderen Mitteln.“<sup>2</sup> Er war der Theoretiker der begrenzten kriegerischen Auseinandersetzung zwischen Staaten zwecks Erlangung eines politisch definierten Zieles. Zwar sei das Geschehen an sich gekennzeichnet von zahlreichen Friktionen, die die Beherrschung des Kriegsgeschehens an der Kriegswirklichkeit scheitern lassen können, aber die Wägung und Gewichtung von Wahrscheinlichkeiten kann helfen, die *Nebel des Krieges*<sup>3</sup> zu lichten.

Kriege zu Clausewitz' Zeit waren Zermürbungskriege, in denen sich teure Söldnerheere gegenüberstanden, um nach Vernichtung der jeweils feindlichen Armee ihr erkämpftes Ziel durchzusetzen. Clausewitz betont die Staatlichkeit der Akteure; die Zeit der Warlords des Dreissigjährigen Krieges war lange vorbei. Krieg war von Frieden klar geschieden durch die Institute der Kriegserklärung und des Friedensschlusses, durch Trennung Kämpfender und Unbeteiligter. Die Bezwingung des Gegners erfolgt mittels physischer Gewalt, die, nach der Logik des Krieges bis zum Äußersten angewandt werden muss, um dem Gegner nicht durch zuviel Milde die Möglichkeit zu geben, das Blut der eigenen Seite zu vergießen.

Napoleon weitete den Kreis der Beteiligten aus, indem er zwar nicht als erster, aber doch am umfassendsten eine Verpflichtung der Bevölkerung zum Kampf proklamierte, Frauen und Alte eingeschlossen, ein(e) jede(r) nach seinen oder ihren Möglichkeiten. Ein Prinzip, das sich bald als allgemeine Wehrpflicht durchzusetzen begann.

Man mag den *Feldherrenhügel* als Versuch auffassen, dem Kriegsherren die größtmögliche Kontrolle über das Kriegsgeschehen zu geben, allein wurde durch größere Truppenstärken und stärkere Feuerkraft die hergebrachte Ordnung der

---

<sup>1</sup> Clausewitz (1957)

<sup>2</sup> ebd. (zit. nach Die Zeit. 2001, H. 43, S. 94)

<sup>3</sup> ebd.

offenen Feldschlacht aufgelöst<sup>4</sup>. Was sich herauszubilden begann war eine Form des Krieges, die Ludendorff später den *totalen Krieg* nannte, und der nicht etwa einen Hobbes'schen bellus omnia contram omnes, sondern die völlige Ausrichtung der Wirtschaft, der Wissenschaft, der gesamten Bevölkerung eines Landes auf den zu führenden Krieg, auf den zu besiegenden Gegner meint. Auch die Politik hat sich den kriegsbedingten Erfordernissen unterzuordnen; der Krieg als ultima ratio aller Dinge. Im ersten Weltkrieg wurde diese Strategie benutzt, an der Front in der Form des Zermürbungskrieges, der Feldschlacht, in einem bis dato ungeheuren, unbekanntem Ausmaß. Doch der totale erste Weltkrieg wurde totaler noch im zweiten. War die gezielte Tötung von Zivilisten zwischen 1914 und 1918 noch die Ausnahme, so wurde sie im zur Regel im zweiten Weltkrieg. Die Unterscheidung von Kombattanten und Nichtkombattanten existierte zwar noch, fand aber zumindest im Luftkrieg sowohl von der deutschen als auch der alliierten Seite keine Beachtung. Man war bestrebt, nicht nur die feindliche Armee zu vernichten, sondern das gesamte militärische Potential des Gegners zu zerstören, wobei eine Unterscheidung von zivilen und militärischen Infrastrukturen im *totalen Krieg* schlechterdings unmöglich ist. Dieser mechanisierte Krieg spiegelte die Produktionsform des Fließbandes wieder, er war *koordiniert und geordnet, aber starr und rigide*<sup>5</sup>.

Die rasante technische Entwicklung von Zerstörungsmaschinerien und ihre Integration in Millionenheere war nur möglich durch die Herstellung eines medial konstituierten und kontrollierten Verbundes von Mensch und Maschine. Ein Kommandomedium, das schneller war als die Geschwindigkeit der motorisierten Truppen, ermöglichte die Wiedererlangung einer Perspektive, wie sie der Feldherrenhügel geboten hatte. Man sieht: je größer die Truppen, desto wichtiger die freie, vom Gegner uneingesehene Fluidation von Information. Schon früh spielte das Erkennen der gegnerischen Absichten eine Rolle in, vor und nach Kriegen - als Mittel der Kriegführung. Dies reichte von Spionen, Kundschaftern, Geheimboten und Militärattachés in potentiell als gefährlich erkannten Hauptstädten bis zum Einsatz neuartiger Übertragungsmedien - so entschied Napoleon den Feldzug gegen Österreich 1809 durch den Einsatz optischer Telegraphie für sich<sup>6</sup>. Beschleunigung des Krieges mittels Technikgenese: von der optischen zur elektrischen Telegraphie zum Funk zur satellitenvermittelten oder netzgestützten Verbindung neuerer Zeit. Das Hinarbeiten auf

---

<sup>4</sup> Bernhardt/ Ruhmann (1998), S. 2 f.

<sup>5</sup> Weiguang (1998), S. 74

<sup>6</sup> Kittler (1998), S. 303

Informationsaustausch in Echtzeit. Und dies mit einschneidenden Folgen im zivilen Bereich: *Radio ist nur der um seine Wechselsprechmöglichkeit amputierte Heeresfunk des Ersten Weltkriegs, Fernsehen nur der zivile Zwilling der Radarschirme des Zweiten. Ganz zu schweigen von der Computertechnik, deren kryptoanalytische und damit militärische Herkunft [...] kein britisches Staatsgeheimnis mehr ist*<sup>7</sup>. Die Entschlüsselung des ENIGMA-Codes der deutschen Wehrmacht kann durchaus als ein kriegsentscheidender Faktor angesehen werden.

Dennoch: der Konflikt um die Vorherrschaft auf dem Feld der Information war nur ein Mittel in der Auseinandersetzung zur Erreichung des Zieles, den Gegner zu vernichten. Das Militär wurde mehr und mehr zu einer großen Institution, die vielfältige Arbeitsabläufe und Funktionslogiken vernetzt. In der Entscheidungen, trotz (und wegen) steigender Geschwindigkeit des Informationsflusses, immer länger dauerten. Eine Tatsache, die das Konzept des *Blitzkrieges*<sup>8</sup> auszunutzen versucht.

Aber nicht immer muss der Vorsprung auf dem informationellen Sektor zwangsläufig zum Erfolg führen. In Vietnam stand eine militärische Supermacht, streng hierarchisch organisiert mit dem Präsidenten am oberen Ende des pyramidalen Aufbaus, einer kleineren und weniger durchorganisierten Guerillastreitmacht von Vietnam und Vietcong gegenüber. Die Institution im Widerstreit gegen ein Netzwerk. Den die dynamischere, d.h. die Netzwerkseite für sich entschied. Ein anderes Beispiel hierfür wäre der Krieg in Afghanistan in den 80er Jahren. Diese Auseinandersetzungen sind jedoch keine Informationskriege gewesen, da das Hauptaugenmerk der USA ganz traditionell darauf gerichtet war, die feindliche Effektivstärke zu vernichten, nicht etwa, wie sie es im Golfkrieg praktizierten, die Entscheidungsabläufe des Gegners soweit zu unterminieren, dass er seine Aktivitäten nicht mehr wirksam koordinieren kann.

Shen Weiguang spricht von einer *fünften Dimension*, auf der es im Krieg die Vorherrschaft zu erlangen gilt: neben der Luft-, Land-, See- und Weltraumherrschaft diejenige der Information. Es gilt nunmehr die Wissens- und Glaubenssysteme des Gegners zu beherrschen, Bombardements nicht mehr flächendeckend, sondern punktgenau auszuführen und die eigenen Kräfte „intelligenter“ zu organisieren, d.h. rigide command/ control - Abläufe in ein networking zu überführen<sup>9</sup>. *Informationen und Kontrolle sind nicht mehr bloß notwendige Mittel, sondern der Zweck des Krieges. Dies entspricht dem Wandel des innerstaatlichen Gewaltmonopols, den Michel Foucault*

---

<sup>7</sup> ebd.

<sup>8</sup> Arquilla/ Ronfeldt (1992), S. 6

<sup>9</sup> Weiguang (1998), S. 73

*beobachtet hat: Nicht mehr der Körper des Verbrechers ist heute das Objekt des Strafvollzugs, sondern sein Willen*<sup>10</sup>

Es wäre allerdings verkürzend, die gestiegene Bedeutung von Information nur innerhalb des militärischen Funktionsapparates zu betrachten, denn es kann nicht nur um militärische Effizienz gehen.

Die oben angedeuteten innermilitärischen Tendenzen spiegeln gesamtgesellschaftliche Entwicklungen. Zwar ist der technologische Ursprung des Computers ebenso wie seine Vernetzung militärisch zu verorten, jedoch sind Netzstrukturen - ob intern oder über das Internet organisiert - zu einem bedeutenden Medium des Informationsaustauschs geworden. Die eher schlechten - nebulösen - als rechten Stichworte hierzu lauten Globalisierung, Informations- und Wissensgesellschaft. Nachrichtentechnik, Spionage und strategisches Kriegsspiel fallen in einem weltweiten offenen Datennetz zusammen. Die Zahl der möglichen Akteure hat sich potenziert; jeder mit einem Computer versehene Schreibtisch kann zum Schauplatz einer kriegerischen Auseinandersetzung werden<sup>11</sup>. Was bedeutet das Wort *Krieg* überhaupt noch? Noch in der Zeit des Kalten Krieges konnte man mit einiger Sicherheit Zuständigkeiten für Angriffe auf Staat oder Gesellschaft festlegen. Kamen Attacken aus dem eigenen Land, so war die Polizei zuständig; für das Äußere verantwortlich waren Regierung und Geheimdienste und als letzte Möglichkeit das Militär. Das eine war Kriminalität zu nennen, das andere Angriff, kriegerische Attacke, die Reaktion darauf Verhandlung und/oder Verteidigung. Dieses Bild ist ein wesentlich vereinfachtes; es wird der Akteurskonstellation des Kalten Krieges kaum gerecht. Dennoch: die *fünfte Dimension* hat eine Eigenschaft, die so segensreich wie fatal wirkt - sie ist grenzenlos. Das territoriale Prinzip, das es ermöglicht ein *Inneres* und ein *Äußeres* zu definieren funktioniert nicht mehr. Da es nur schwer und keinesfalls in Echtzeit zu leisten ist, den Urheber einer Attacke im Netz mit Sicherheit festzustellen, werden die Grenzen zwischen z.B. Wirtschaftsvergehen, kriminellen Handlungen, terroristischen oder gar kriegerischen Akten fließend. Und unklar ist noch immer, welches Recht anzuwenden sei. Nur von einem kann man sich mit Sicherheit verabschieden: von der mühsam eingeführten und völkerrechtlich anerkannten Verregelung und Verrechtlichung des Krieges. Die Genfer Konvention beruht auf der Unterscheidung von legitimen staatlichen Kriegen und illegitimen nichtstaatlichen Kriegen: der Soldat darf sich selbst verbergen, nur nicht die Tatsache,

---

<sup>10</sup> Bendrath (1999), S. 158

<sup>11</sup> Kittler (1998), S. 301

dass er Soldat ist. *Im Cyberkrieg sind Militär und Polizei, staatliche und nichtstaatliche Akteure gleich*<sup>12</sup>.

Und es verschwindet der Unterschied von Krieg und Frieden. Denn um in einer im Datennetz geführten Auseinandersetzung erfolgreich zu sein, müssen die Sicherheitslücken des Gegners schon frühzeitig entdeckt werden. Das heißt, das staatliche Einheiten fast gezwungen sind, in einer Weise, die weit über frühere Spionagetätigkeit hinausgeht, Daten zu sammeln, um diese im Kriegsfall verwerten zu können. Nur so kann sich der Wissensvorsprung des Militärs erhalten, denn viel Wissen, das früher der Geheimhaltung unterzogen werden konnte, ist inzwischen frei zugänglich, zumindest käuflich (wie z.B. Satellitenbilder in einer Auflösung, wie sie bis vor wenigen Jahren nur dem Militär zur Verfügung stand). Wenn der Unterschied zwischen Krieg und Frieden schwindet, so wird zum Beispiel das Recht des Parlaments, einen Krieg zu erklären, ausgehebelt. Auf diese politischen Implikationen werden wir späterhin noch eingehen, nachdem die Möglichkeiten des Technischen ausgeleuchtet sind.

## **5. Neuere Debatte zum Thema Cyberwar**

Die Debatte, wie sie sich etwa Mitte der neunziger Jahre darstellte, basierte auf drei grundlegende Annahmen<sup>13</sup>:

- Erstens einer wachsenden sicherheitspolitischen Ungewißheit über mögliche Gegner, verbunden mit der unkontrollierbaren Diffusion von Software und Know-How über Cyber-Angriffstechniken;
- zweitens einer wachsenden militärischen Angst vor der elektronischen Verwundbarkeit der US-Streitkräfte, basierend auf einer möglichen asymmetrischen Cyberkriegführung durch konventionell unterlegene Gegner;
- drittens auf der anarchischen Struktur des Internet als sozialem Raum, der sich staatlichen Kontrollversuchen und damit auch dem staatlichem Sicherheitsbedürfnis zu widersetzen schien.

Es war also nicht die neue Technologie allein, von der die Risiken ausgingen, sondern erst ihre Einbettung in ein System von sicherheitspolitischen Normen und Ideen in

---

<sup>12</sup> ebd. S.10

<sup>13</sup> Vgl. Bendrath, Ralf: Elektronisches Pearl Harbor oder Computerkriminalität?“

einer spezifischen historischen Situation, die das Internet ins Bewußtsein des sicherheitspolitischen Establishments der USA rückte.

„War die Diskussion über Computer in den Streitkräften zunächst von großer Euphorie über digitalisierte und vernetzte C<sup>3</sup>I- Systeme geprägt, so ist seit Mitte der neunziger Jahre eine stärkere Beachtung der Risiken zu beobachten.“<sup>14</sup>

Ein weniger häufig genannter Hintergrund für die besondere Leidenschaft der Amerikaner bezüglich des Themas Cyberwar, ist die Urangst der Amerikaner auf Ihrem eigenen Territorium angegriffen zu werden.

## **6. Verletzlichkeit kritischer Infrastrukturen**

Die Verletzlichkeit der Gesellschaft wird im folgenden als Kriterium zur Betrachtung und Bewertung von künftigen Technikfolgen herangezogen. Das durch den Einsatz neuer Techniken die Verletzlichkeit der Gesellschaft nicht erhöht sondern viel eher gesenkt werden soll, wird als breiter Konsens angenommen. Das vorrangige Problem stellt die zunehmende Verlagerung von gesellschaftlichen Funktionen vom Menschen auf vernetzte Techniksysteme (wie z.B. der Informations- und Kommunikationstechniken) dar. Diese angesprochene Verlagerung birgt auf der einen Seite große Leistungssteigerungen aber auf der anderen Seite auch ein erhöhtes Schadenspotenzial beim Ausfall oder dem Mißbrauch von Technik. „Das inhärente Schadenspotenzial eines Techniksystems ist die Kehrseite der Abhängigkeit einer Gesellschaft von dieser Technik.“<sup>15</sup>

Es wird angenommen, dass das Schadensspektrum von technischen Infrastrukturen außerordentlich breit und vielfältig ist.

Aufgrund der Komplexität von heutiger Technik fällt eine Einordnung eines entstandenen Schadens zunehmend schwer.

Wichtige für eine Verletzlichkeitsuntersuchung zu prüfende Variablen sind nach PORDESCH und ROßNAGEL (1997) folgende:

- die erwartende Abhängigkeit einzelner oder der Gesellschaft von bestimmten Techniksystemen,

---

<sup>14</sup> Bendrath, Ralf: Elektronisches Pearl Harbor oder Computerkriminalität?“

<sup>15</sup> Pordesch, Ulrich; Roßnagel, Alexander: Untersuchungen zur Verletzlichkeit einer vernetzten Gesellschaft S. 189

- das mögliche Schadensausmaß eines Versagens der Technik, oder eines gelungenen Mißbrauchs,
- die Möglichkeiten, das potentielle Schadensausmaß zu vermindern oder Mißbrauchsmöglichkeiten auszuschliessen,
- aber auch die sozial begründete Verlässlichkeit solcher Sicherungsmaßnahmen und ihre sozialen Auswirkungen.

Bedeutsam für die spätere Betrachtung eines Szenarios „Cyberwar“ sind die zunehmende Abhängigkeit immer größerer gesellschaftlicher Bereiche von technischen Infrastrukturen (Telekommunikation) und die für diese Technologie typischen Schadensverläufe.

Bei der Analyse von Schäden im Umfeld von Informations- und Kommunikationssystemen kann man nach PORDESCH und ROßNAGEL (1997) zwischen folgenden Schadensverläufen unterscheiden :

- Schadensmultiplikation: Schäden können multipliziert werden, wenn fehlerhafte oder manipulierte Systeme in verschiedenen Bereichen verwendet oder wenn Netze zu ihrer Verbreitung genutzt werden,
- Kumulationsschäden: Schäden können vervielfacht werden, weil Schwachstellen der eingesetzten Systeme zu vielfachen voneinander unabhängigen Handlungen verleiten,
- hoher Einzelschaden: Schäden können besonders hoch werden, weil die neuen technischen Möglichkeiten bisherige Grenzen von Raum, Zeit, Energie oder Informationsdichte zu durchbrechen vermögen,
- Komplexschäden: Schäden in Netzknoten und anderen Komponenten vernetzter Systeme können sich in verschiedenen Systemen und den darauf aufbauenden Anwendungsstrukturen auswirken und die Schäden vervielfachen und
- Kopplungsschäden: Schäden können trotz räumlich und zeitlich vollständiger Entkopplung trotzdem gleichzeitig auftreten, wenn sie dieselben Programme nutzen oder mit denselben manipulierten Werkzeugen entwickelt wurden, eine bei anderen Techniksystemen unbekannte Gefährdung besonderer Tragweite.

## 7. Kritische Infrastrukturen

Kritische Infrastrukturen spielen die entscheidende Rolle in der Diskussion um das Thema Cyberwar.

Der Ausdruck „kritische Infrastrukturen“ stammt aus dem 1997 veröffentlichten PCCIP-Report<sup>16</sup>, dessen Ergebnis die Identifikation der in den USA als „kritisch“ zu bewertenden Infrastrukturen und deren mögliche Bedrohungen war.

Hintergrund der Diskussion ist die offene Struktur der amerikanischen Datennetze und den daraus folgenden Angriffsmöglichkeiten.

Folgende Infrastruktursektoren sind demnach als kritisch zu bewerten.

- Telekommunikation
- Energieversorgung
- Finanzwirtschaft
- Transport
- Rettungsdienste
- Öffentliche Verwaltung

Das Gefährdungspotenzial dieser kritischen Infrastrukturen wird deutlich wenn man die Vielzahl möglicher Bedrohungen ausführt. Von Naturkatastrophen über physische Attacken bis zu den Cyber-Attacken reichen mögliche Bedrohungen.

Im Fall einer Cyber-Attacke kann verkürzt ausgesagt werden, dass von „Insidern“ die größten Gefahren für kritische Infrastrukturen ausgehen. Insider sind Personen mit besonderem technischen Wissen wie z.B. Systementwickler, -verwalter, Netzwerktechniker, usw.

Statt einer zentralen staatlichen Koordination tendieren Firmen, die in vielen Fällen Betreiber kritischer Infrastrukturen sind häufig zu einer privaten, lokalen Sicherheitspolitik, die jeweils nur ihre eigenen Systeme sicherer macht. Der Grad an erreichbarer Sicherheit wird deshalb wesentlich von den Selbstschutzmaßnahmen der Anwender und lokaler Anbieter abhängen.

---

<sup>16</sup> Report of the „President’s Commission on Critical Infrastructure Protection (PCCIP)

## **8. Mißbrauch von Techniksystemen / Varianten und Motive für Mißbrauch**

Insgesamt kann im Vergleich zum fortschreitenden Technikeinsatz angenommen werden, daß Mißbrauchsanreize tendenziell steigen. Typische Motive eines Mißbrauch von Techniksystemen sind:

- persönliche Motive (Ärger, Stress, Neugier),
- Bereicherungsmotive,
- politische Motive (Terrorismus, Wirtschaftsspionage,
- kriminelle Motive und
- neue Formen sozialen Widerstands.

## **9. Ausprägungen eines Cyberwar**

Eine besondere Schwierigkeit bei der Strukturierung dieses Themas war es die Vielzahl der bestehenden Ansätze und Definitionen zu ordnen und wenn möglich voneinander abzugrenzen.

### **9.1 Cyberwar**

Der Begriff Cyberwar wurde von JOHN ARQUILLA (Naval Postgraduate School) und DAVID RONFELD (RAND Corporation) erstmalig veröffentlicht. „Sie und andere begannen Anfang der 1990er Jahre, über gesellschaftliche - und damit auch militärische – Veränderungen durch neue Informationstechnologien nachzudenken. ... Mit der Ausbreitung des Internet und der entstehenden Diskussion um die "Informationsgesellschaft" geriet dann das Konzept von Information als Ressource ins Zentrum der Aufmerksamkeit. Wenn postindustrielle Gesellschaften und ihre Streitkräfte nicht mehr vor allem auf Menschen und Maschinen als Mittel von Produktion oder Destruktion angewiesen sind, so die Überlegungen, dann sind die Angriffsziele militärischer Operationen nicht mehr die Kräfte des Gegners, sondern seine Informationsverarbeitungssysteme.“<sup>17</sup>

Zusammenfassend wird Cyberwar demnach militärisch als digitale/elektronische Kriegführung bzw. als Krieg gegen die kritische Infrastruktur eines Gegners beschrieben. Es besteht die Annahme, daß jede militärische Einheit nutzlos ist, wenn

---

<sup>17</sup> Bendrat, Ralf: Krieger in Datennetzen

sie nicht kommunizieren kann. Die Manipulation aller Teile des C<sup>3</sup>I-Systems<sup>18</sup> des Gegners ist eines der vorrangigsten Ziele. Cyberwar wurde demnach zu den sogenannten High-Intensity-Conflicts (HIC) oder Major Regional Conflicts (MRC) gezählt.

Davon abgegrenzt wird Netwar als Medienbeeinflussung im Sinne der psychologischen Kriegführung bezeichnet. Ebenso werden gesellschaftliche Konflikte im Cyberspace unter Netwar subsumiert. Netwar wird in der militärischen Verortung zu den Low-Intensity-Conflicts (LIC), Operations-Other-Than-War (OOTW) bzw. nichtmilitärischen Konflikten gezählt.

John Arquilla hat sich Anfang dieses Jahres in einem Interview zur Karriere und der deflationären Benutzung des von ihm geschaffenen Begriffs „Cyberwar“ geäußert. Er verdeutlichte nochmals die ursprüngliche Intension des Begriffs. „So, our notion of cyberwar was intended to refer basically to military interaction. Hacking today, that is conflated with cyber-war, is a small part of it. But it can be the part that strikes directly at a country's infrastructures.“<sup>19</sup>

## 9.2 Information Warfare<sup>20</sup>

Kennzeichnend für den Information Warfare ist sein Ansatz bereits deutlich unterhalb der Schwelle klassischer militärischer Auseinandersetzungen. SZAFRANSKI (1996) unterscheidet in seiner "Theory of Information Warfare" explizit zwischen "War" und "Warfare", wobei Warfare nicht unbedingt Krieg voraussetzt und nicht auf eine zwischenstaatliche Auseinandersetzung beschränkt ist.

Die Mittel dafür können neben Cyberattacken auch psychologische Kriegführung, Störsender oder auch konventionelle Angriffe auf Kommunikationseinrichtungen sein.

---

<sup>18</sup> C<sup>3</sup>I steht für Command Control Communication Intelligence und meint den ganzheitlichen Einsatz von IuK-Technologien in modernen Streitkräften

<sup>19</sup> Krempf, Stefan: Be Prepared: Cyberwar is Coming – or maybe not

<sup>20</sup> Information Warfare: ab 1993 offiziell erwähnt von der US-Regierung (Das US-Verteidigungsministerium definiert „Information Warfare“ als „actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks“, DoD Dictionary

Martin Libicki strukturiert den Information Warfare in sieben Arten:

- Command and Control Warfare: der Versuch die Kommando- und Kontrollstruktur des Gegners durch Ausschalten der Kommandozentrale oder Verhinderung des Informationsfluss zu (zer-)stören
- Intelligence Based Warfare: elektronische Aufklärung als Dreh- und Angelpunkt moderner Kriegführung. Sowohl auf Kommandoebene als auch auf konkreten Operationsebenen (einzelne Soldaten bis zu autonomen Waffensystemen) stehen allen Beteiligten kontinuierliche Aufklärungsinformationen zur Verfügung.
- Elektronik Warfare: Hier spielen Methoden der physischen Störung als auch kryptografische Verfahren eine zentrale Rolle und sind Voraussetzung für einen Intelligence Based Warfare.
- Psychological Warfare: Durch moderne Informationstechnik läßt sich auch die Wirksamkeit der psychologischen Kriegführung steigern. Beispiele sind hier die Propaganda über die verschiedenen Kanäle der Massenmedien auf Bevölkerung sowie Militär.
- Hacker Warfare: Als Bedrohung werden hier die geringen Voraussetzungen für Hacker-Angriffe angegeben.
- Economic Information Warfare: Hierunter sind die Handlungen zu subsumieren, die in die Informationsflüsse eines Wirtschaftssystems (z.B. elektronische Handels- und Zahlungssysteme) eingreifen. Libicki bringt hier erneut den zivilen Informationsaustausch als Element von Information Warfare ins Spiel.
- Cyber Warfare: Cyber Warfare umfaßt nach Libicki Informationsterrorismus, semantische Attacken sowie "Gibson Warfare"<sup>21</sup>. Der Informationsterrorismus macht sich zunutze, daß Datenbestände heute einen so großen Wert darstellen, daß ihre Zerstörung eine erhebliche Bedrohung für Personen oder Institutionen bedeutet. Ebenso läßt sich mit der Veröffentlichung sensibler Daten drohen. Semantische Attacken zielen darauf ab, informationstechnische Systeme so zu manipulieren, daß sie als korrekt funktionierend erscheinen, aber trotzdem falsche Ergebnisse liefern. Im „Gibson Warfare“ werden Menschen zu Bestandteilen informationstechnischer Systeme.

---

<sup>21</sup> Gibson Warfare ist orientiert an Gibson's „Neuromancer“ 1992

### 9.3 Reale Erscheinungsformen von Cyberwar

Die nachfolgend aufgezählten im World Wide Web beobachtbaren gesellschaftlichen Bewegungen, die häufig im Zusammenhang mit Cyberwar genannt werden, sind größtenteils dem zuvor definierten Netwar zuzurechnen.

- Hacktivism: Hacker<sup>22</sup> sind zunehmend zu politischen Aktivisten geworden (Hacker – Activism), das ursprüngliche Aufdecken von IT-Sicherheitslücken (Hackerethik<sup>23</sup>) ist in den Hintergrund getreten. Koalitionen von politischen Hackern wie „Russian Hackers Union“ oder „Kosovo Hackers Group“ belegen diese zunehmende Politisierung dieser Bewegung.
- Web-Defacements und Hijacking: Die Entstellung von Websites durch Veränderungen von Website-Inhalten stellt eine der häufigsten Erscheinungsformen von Cyber-Attacken dar. So hat inzwischen jeder klassische Konflikt seine Entsprechung in der virtuellen Welt.
- Web Sit-ins: Der Massenbesuch einzelner Websites und das zeitweise Besetzen dieser Seite gilt als vergleichbar harmloser Protest von Aktivisten.
- Denial of Service Attacken: Hierunter sind Angriffe auf Webserver zu verstehen, die darauf zielen, den Server so weit auszulasten, dass ein Service nicht mehr möglich ist. Prominente Beispiele sind die DOS-Attacken auf Websites renommierter amerikanischer Anbieter von Internet-Dienstleistungen (Yahoo, Amazon, ect.).
- Datenzerstörung: Hierunter fallen sowohl die Programmierung und Aktivierung von aggressiven/zerstörerischen Viren/Trojanern/Würmern, als auch die manuelle Zerstörung von Daten.
- Manipulation und Ausforschung

### 9.4 Szenario „Electronic Pearl Harbor“

Das Bild des „Electronic Pearl Harbor“ beschreibt ein Szenario, das aus einem überraschenden elektronischen Angriff auf wichtige Teile der amerikanischen

---

<sup>22</sup> Hacker: „A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, ...“ aus The New Hacker’s Dictionary

<sup>23</sup> „1. The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing free software and facilitating access to information and to computing resources wherever possible. 2. The belief that system-cracking for fun and exploration is ethical OK as long as the cracker commits no theft, vandalism, or breach of confidentiality. ...“ aus The New Hacker’s Dictionary

Computersysteme und von ihr gesteuerter Anlagen besteht, etwa „kollabierende Stromnetze, eine Softwarebombe auf dem Aktienmarkt, ein elektromagnetischer Impuls, der das Telefonnetz zusammenbrechen läßt.“

In einem solchen Fall wird die Entscheidung zwischen Krieg und Kriminalität plötzlich eine Frage, bei der das Militär quasi „blind“ ist und sich auf das Urteil von Strafverfolgungsbehörden oder sogar privaten Infrastrukturbetreibern verlassen muß. Über die möglichen Folgen eines „Electronic Pearl Harbor“ ist in der öffentlichen Diskussion sehr viel gesprochen und phantasiert worden, die Wahrscheinlichkeit des Eintritts solch eines Szenarios kann allerdings nach Einschätzungen der realen Gefahren momentan als sehr gering angenommen werden.

## 10. Akteure

- „Rogue states<sup>24</sup>“,
- „Cyberterroristen“,
- Sekten,
- Terroristen,
- Extremisten,
- ethnische und religiöse Fanatiker

In der Diskussion um Cyberwar wird immer wieder die wachsende Bedrohung von Seiten der „neuen“ Akteure erwähnt und deren Verflechtung in verschiedenste unkontrollierbare Konflikte. Amerikanische Sicherheitsberater identifizieren vor allen die oben aufgeführten Gruppen als offensive Akteure in einem möglichen Cyberwar. Die Studie „Cyberterror: Prospects and Implications.“ des Center for the Study of Terrorism and Irregular Warfare der Naval Postgraduate School in Monterey erarbeitete 1999 drei Level möglicher Cyberterror-Szenarien.

- Einfach-unstrukturiert: Vorausgesetzt sind die Fähigkeit der Durchführung einfacher Hacks<sup>25</sup> individueller Systeme unter Verwendung bestehender verfügbarer Hackertools.
- Fortgeschritten-strukturiert: Vorausgesetzt sind ausgefeiltere Angriffstechniken gegen vielfältige Systeme oder Netzwerke und die Fähigkeit Hackertools zu erstellen oder anzupassen.

---

<sup>24</sup> Englisch für „Schurkenstaaten“

<sup>25</sup> umgangssprachlich für das Eindringen in fremde Computersysteme

- **Komplex-koordiniert:** In diesem Level wird vorausgesetzt koordinierte Attacken zur Störung integrierter, heterogener Sicherheitsmaßnahmen (einschließlich Kryptografie) durchzuführen sowie die Fähigkeit ausgeklügelte Hackersoftware zu erstellen.

„The Monterey team estimated that it would take a group starting from scratch 2-4 years to reach the advanced-structured level and 6-10 years to reach the complex-coordinated level, although some groups might get there in just a few years or turn to outsourcing or sponsorship to extend their capability.“<sup>26</sup>

## **11. Sicherheitsstrategien - Der Dinosaurier Staat läuft unsichtbaren Erregern hinterher<sup>27</sup>**

Die Diskussion um Sicherheitsstrategien begann in den USA nach dem Zusammenbruch der UdSSR. Ralf Bendrath extrahiert drei Diskurslinien<sup>28</sup>: die erstere impliziert eine Art Arbeitsbeschaffungsmaßnahme für die US-Streitkräfte nach dem Wegfall der Patt-Situation mit der SU. Hier geht es um die *Neuetablierung* einer Bedrohung und um die *Stiftung von Legitimität* für die Streitkräfte. Dies ging einher mit einer verstärkten Unsicherheitswahrnehmung für das Militär selbst, das zunehmend vernetzt wurde und damit anfälliger für Angriffe auf seine Kommando- und Kommunikationsstrukturen als Streitkräfte anderer Staaten. Dieser Diskursstrang *war eher militärstrategisch ausgerichtet und orientierte sich an Ideen der asymmetrischen und unkonventionellen Kriegführung.*

Der dritte schließlich ist geprägt von der Struktur des Internet selbst, das sich in einer Art Wildwest-Manier entwickelte und einen nahezu unkontrollierten Raum (aus staatlicher Sicht) darstellt. *Es war also nicht die neue Technologie allein, von der die Risiken ausgingen, sondern erst ihre Einbettung in ein System von sicherheitsspezifischen Normen und Ideen in einer spezifisch historischen Situation<sup>29</sup>.* In den USA ist bis heute keine einheitliche Sicherheitsstrategie feststellbar. Vielmehr hat sich eine Arbeitsteilung zwischen FBI, Militär, NSA und Verteidigungsministerium ergeben - wer welches Problem behandelt ist eher eine Frage von Eigenaquis und abhängig von der Art und Natur des jeweiligen Cyber-Problems, als dass eine klare

---

<sup>26</sup> Denning, Dorothy: Cyberterrorism

<sup>27</sup> Palm (2001a), S. 6

<sup>28</sup> i.f.: Bendrath (2000), S. 2 ff.

<sup>29</sup> Bendrath (2000), S. 4.

Zuständigkeit geregelt wurde. Durchgesetzt haben sich vor allem FBI aufgrund institutioneller und die NSA aufgrund technischer Vorleistungen, während das Militär eher eine marginalisierte Rolle spielt<sup>30</sup>. Die USA konzeptionalisieren weiterhin eine Strategie der nationalen Sicherheit gegen die Bedrohung der amerikanischen Gesellschaft, während die wahrscheinlich bedeutendsten Leistungen zur Sicherheit der Infrastrukturen von privaten Betreibern ausgehen, die an lokalen Sicherheitsmaßnahmen arbeiten ohne jedweden politischen Anspruch. Zwar hatte die amerikanische Regierung versucht, Institutionen ins Leben zu rufen, die eine Zusammenarbeit privater Infrastrukturbetreiber mit offiziellen Stellen garantieren sollten (ISACs: Information Sharing and Analysis Centers), was aber bislang am Misstrauen der Unternehmen scheiterte, da diese Details über eigene Sicherheitslücken nicht an Behörden oder Konkurrenten weitergeben wollten.

Was bisher sowohl von politischer als auch von wissenschaftlicher Seite nur in sehr eingeschränktem Maß diskutiert wurde, ist die Frage der Möglichkeiten von Rüstungskontrolle. Es lässt sich aus dem bisher Gesagten ableiten, dass die Art der Kriegführung bzw. Aspekte derselben sich unter dem Focus des *Information Warfare* verändern werde. Es besteht die Möglichkeit, dass technologisch weniger entwickelte Staaten hiervon profitieren, woraus moderne Industrie- und Dienstleistungsstaaten, vor allem die USA, die Notwendigkeit ableiten, ihren Vorsprung auf diesem Sektor zu halten bzw. auszubauen. Dies geht einher mit dem nach Ende des Kalten Krieges erfolgten Strategiewechsel der Militärs weg von der Defensivtaktik hin zu einer Interventionspolitik. Der Golfkrieg 1991 und der Kosovokrieg 1999 können als Vorboten für eine solche Entwicklung angesehen werden. Sie beweisen außerdem ein augenfälliges Interesse an Formen der Auseinandersetzung, die eine reale Feindberührung vermeiden - die Abneigung demokratisch gewählter Regierungen gegen in Zinkbehältern nach Hause expedierte Soldaten mag hierbei eine Rolle spielen. Diese Interessenlage könnte einen *selbstverstärkenden Kreislauf in Richtung aller Aspekte von IW*[information warfare; d.V.] *in Bewegung setzen*<sup>31</sup>.

---

<sup>30</sup> ebd. S. 16

<sup>31</sup> Minkwitz/ Schöfbänker (2001), S. 4

## 12. Konventionelle Rüstungskontrolle und Information Warfare

Was waren die grundlegenden Mechanismen der Rüstungskontrolle, die zur Zeit des Kalten Krieges implementiert wurden und was lässt sich aus ihnen für ebensolche Maßnahmen in bezug auf Informationwar ableiten?

Konventionelle Rüstungskontrollmaßnahmen sind auf Waffensysteme ausgerichtet, deren, zerstörerisches Potential evident ist. Das Problem eines strategischen Wettrüstens und der damit verbundene Aufbau eines gigantischen Bedrohungspotentials wurde schon vor der ersten Zündung einer Atombombe im Kampfeinsatz diskutiert<sup>32</sup> - für ein Problembewusstsein war also schon hinreichend gesorgt. Zugang zum Know-how des Baus von Sprengköpfen, notwendigen Trägersystemen und Zielfindungstechnik hatten im wesentlichen nur militärische Eliten, sodass eine Proliferation der Technologie zumindest erschwert gewesen ist. Weiterhin war die Zahl der Akteure im Rüstungswettlauf begrenzt - das politische System und das Militär einiger weniger Staaten (im wesentlichen nur USA und UdSSR). Auf diesen Bedingungen fußend hatte Rüstungskontrolle das Ziel mittels Verhandlungen und „vertrauensbildenden Maßnahmen“ ein Klima der Berechenbarkeit zu schaffen und einen Verhaltens- und Tabukodex zu errichten und diesen durch bi- oder multilaterale Abkommen oder die Installation internationaler Regime zu verrechtlichen. *Allgemein hat sich dabei der Begriff einer ‚kooperativen Rüstungssteuerung‘ herausgebildet, der vor allem eines zum Ziel hat: Durch die Erzeugung von Transparenz der in Frage stehenden Waffensysteme und ihres Zerstörungspotential eine möglichst rationale Bewertung vornehmen und darüber möglichst intersubjektiv urteilen, verhandeln und rasonieren zu können. Das Ziel von Abrüstung ist die definitive quantitative (geringere Obergrenzen) oder qualitative (die gänzliche Bannung, etwa: Landminen, Massenvernichtungswaffen) Beseitigung von Waffensystemen.*<sup>33</sup>.

Die Technik vernetzter Computersysteme und auf ihr fußende Informationskriegs-szenarien schaffen wesentlich veränderte Voraussetzungen für einen künftigen Prozess der Rüstungskontrolle: die BetreiberInnen von IuK-Technologie sind im wesentlichen am kommerziellen Markt, mithin also im zivilen Bereich zu finden. Eine Regulation des freien Informationsflusses ist weder möglich noch wünschenswert in politischer, wirtschaftlicher und gesellschaftlicher Hinsicht. Diese Auflösung der Grenzen von militärischer und ziviler Technologie impliziert, dass ein Prozess der

---

<sup>32</sup> ebd. S. 2

<sup>33</sup> ebd.S. 7

Rüstungskontrolle wie er zur Zeit des Kalten Krieges stattfand - in Form der Reduktion von Waffensystemen - unmöglich ist. Minkwitz/ Schöfbänker formulieren dies wie folgt: *Rüstungskontrolle in Zeiten technologischer Diffusion muss sich deshalb an Intentionen und Perzeptionen anstatt an Fähigkeiten orientieren und gleichzeitig bestrebt sein, neue Normen im Umgang mit und der Applizierbarkeit von militärischen IW-Technologien und -Konzepten zu formulieren*<sup>34</sup>. Es bleibt also nur die zu nichts verpflichtende Verzichtserklärung einiger Staaten, keine Information-Warfare-Szenarien befördern zu wollen (woran die USA, nebenbei bemerkt überhaupt kein Interesse haben<sup>35</sup>)? Man muss sich noch einmal vor Augen führe, dass man sich international in einem völlig rechtsfreien Raum bewegt. Es ist noch nicht einmal klar, ob der Angriff auf Netzbereiche in einem Staat als Angriffe im Sinne der Charta der Vereinten Nationen gewertet werden können. Minkwitz und Schöfbänker leiten folgende Fragen, die in internationaler Debatte und nachfolgender Verrechtlichung zu lösen seien, aus der komplexen Problematik ab, die hier zur Gänze zitiert seien:

- *Definitionsfragen der Natur der Waffensysteme und damit eine politische Anmeldung des Problems auf der Ebene der Staatengemeinde, bei der Forschung und bei Nicht-Regierungsorganisationen. [...] Die entscheidende Frage ist: Was soll als eine Waffe "unter den IW-Bedingungen" angesehen werden?*
- *Definition der "Waffenwirkung". Diese reicht von der Form des zivilen elektronischen Widerstandes von nicht-staatlichen oder einzelnen Akteuren oder des wirtschaftlichen Schadens eines E-Commerce-Unternehmens über verschiedenste Zwischenstufen, bei denen nationale militärische Akteure in realen Kriegen involviert sind (taktischer C2-C3I IW), bis hin zu hyperalarmistischen Szenarien, die die Integrität der C2-Systeme der strategischen Kernwaffen durch unautorisierten Zugriff oder durch die Manipulation von Frühwarnsystemen gefährdet sehen. Ein Beispiel: "Fifth, it is important to recognize that soon both sides (US and Russia) will have the ability to use holograms and other IT manifestations that will offer the opportunity to completely fool one another both on the battlefield and through the airwaves ././ A hacker simulating an incoming ICBM nuclear attack on the radar screens of the military of either Russia or the United States is but one manifestation of this threat".*

---

<sup>34</sup> ebd. S. 12

<sup>35</sup> Krempf, Stefan (2001)

- *Fragen der Universalität. Der NV-Vertrag, der CTBT, die C- und B-Waffen-Konventionen sind als Abkommen einer erwünschten hohen Universalität anzusehen. Andere Rüstungskontrollabkommen sind lediglich bilateraler Art: SALT I, II, START I, II (III?), das Abkommen zur Verhütung von Atomkriegen.*
- *Fragen der Abgrenzung von genuin ‚zivilen‘ und ‚militärischen‘ Ursprüngen von Technologien, von den darüber verfügenden Akteuren und daraus abgeleiteten operativen Konzepten. Um wiederum ein Beispiel für die Schwierigkeit der Materie zu nennen: Im ‚klassischen Krieg‘ ist der Angriff des Militärs auf zivile Einrichtungen, auf Hospitäler, Kulturdenkmäler, auf die Zivilbevölkerung und auf Nichtkombattanten, sowie unzulässige Grausamkeit - selbst das Verbot des Einsatzes von Kernwaffen oder dessen Androhung wurde vom IGH in Haag festgestellt - in vielfältiger Weise rechtlich sanktioniert und reguliert, auch wenn wesentliche Akteure diese Rechtsmeinung nicht teilen sollten, ihnen keine Bedeutung beimessen oder ihr bewusst zuwider handeln. Anders ist dies im Bereich der offensiven IW-Führung. Hier stellt sich die Frage, ob informationstechnische Angriffe etwa auf zivile Einrichtung (Hospitäler), die zu Schaden an Leib und Leben führen, von den bisherigen Regelungen des Kriegsrechts überhaupt erfasst werden.*
- *Damit stellt sich das letzte und - neben der Definitionsfrage - schwierigste Problem: Was ist überhaupt ein kriegerischer IW-Akt?*
- *Frage der Verifizierbarkeit von Handlungen, Akteuren und I-Waffen: Ist schon in einer ‚normalen‘ kriegerischen Situation die Verschuldensfrage von nicht mit dem Kriegsrecht konformen Handlungen oft schwer zu klären, so trifft dies um so mehr im Bereich IW zu. Die Frage, ob dies ein IW-Angriff war, führt unmittelbar zur nächsten: Wer war der Akteur? Lässt sich ein solcher überhaupt eruieren?<sup>36</sup>*

Erst nachdem diese Fragen international verbindlich geklärt sind - was angesichts der weiten Streuung der Problemlagen nahezu utopisch scheint - können daraus Verhaltenskodizes oder gar Verbote vereinbart werden. Denkbar wären etwa die weltweite Ächtung der Durchführung von Informationsoperationen oder die Etablierung von No-first-use und Code-of-Conduct Strategien.

Und eine weitere Problematik besteht. In diesem Kapitel sprachen wir bisher nur über Handlungsoptionen unter der Voraussetzung, dass an potentiellen Auseinandersetzungen Staaten beteiligt sind: Risikobereiche wie Cyberkriminalität, das

---

<sup>36</sup> Minkwitz/ Schöfbänker, S. 19 f.

kriegerische Handeln von Personen/Netzwerken, das nicht staatlich autorisiert ist, Spionage, Hactivism usw. sind von derartigen Abkommen nicht einmal betroffen. Insofern ist noch einmal zu fragen, ob Strategien, die auf ganzheitliches (staatliches) Handeln gerichtet sind überhaupt dazu geeignet sind, in einem offenen Netzwerk kriminelles oder kriegerisches Handeln zu verhindern. Und nicht vergessen werden sollte die Tatsache, dass man sich im Bereich der Risikoabschätzung noch immer im Feld der Spekulation bewegt, da wirklich gravierende Schäden aufgrund von Attacken noch nicht aufgetreten und die Hochrechnung von unsicheren Wahrscheinlichkeiten keine Grundlage für eine ernsthafte Umgrenzung möglicher Schäden sein kann. Zweifelsohne sind Möglichkeiten vielfältiger Gefährdungen erkennbar, doch in welchem Ausmaß ist theoretisch überzeugend nicht zu sagen.

Dennoch: welche Chancen bestehen abseits intergouvernementaler Absprachen kritische (d.h. wichtige) zivile und militärische Infrastrukturen vor unberechtigtem Zugriff zu schützen? Da das Internet ein offenes Netzwerk darstellt scheint es auch am sinnvollsten zu sein, die Verteidigung gegen Angriffe und damit die Sicherung der jeweiligen lokalen Strukturen in Form eines Netzwerks zu organisieren, d.h. bei den jeweiligen Betreibern zu belassen. Und ob Militär und Geheimdienste hierfür die richtigen Partner sind ist sehr in Frage zu stellen, da diese in der Logik des Information Warfare nicht an sicheren IuK-Techniken interessiert sind, sondern eben an der selektiven Nutzung von Sicherheitslücken. Notwendig ist eine möglichst hohe Redundanz und Varianz verfügbarer Techniken; weiterhin müssen für Funktionskerne in Wirtschaft und Verwaltung Rückfallsysteme zur Verfügung stehen. Maßnahmen in dieser Richtung - der Zivilisierung der Sicherheit - scheinen am realistischsten, um es den information warriors möglichst schwer zu machen, ihren Krieg auf dem Rücken der Informationsgesellschaft zu führen.

### 13. Literatur

Arquilla, John/ Ronfeldt, David: Cyberwar is coming. Santa Monica 1992.

Bendrath, Ralf: Elektronisches Pearl Harbour oder Computerkriminalität? Die Reformulierung der Sicherheitspolitik in Zeiten globaler Datennetze. In: S+F. Vierteljahresschrift für Sicherheit und Frieden, Nr 2/2000.

Bendrath, Ralf: Das Ende des Kämpfers? Postmoderne Kriegsstrategien in den USA. In: diskus, H. /, April 2001.

Bendrath, Ralf: Der Kosovo-Krieg im Cyberspace. Cracker, Infowar und Medienkrieg. In: telepolis 1999.

Bendrat, Ralf: Krieger in Datennetzen. In: telepolis 2001.

Bendrath, Ralf: Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges. In: Bittner, Peter/ Woinewski, Jens (Hg.): Mensch - Informatisierung - Gesellschaft. Münster 1999.

Bernhardt, Ute/ Ruhmann, Ingo: Krieg und Frieden im Internet./ Zur Prähistorie totaler Kontrolle: Medien im Krieg./ Internet: Zivile Nutzung oder militärischer Kampfraum?./ Armageddon des Internets: Information Warfare. In: telepolis 1998.

Clausewitz, Carl von: Vom Kriege. Berlin 1957.

Hables Gray, Chris: Postmodern War - The New Politics of Conflict, London 1997.

Kittler, Friedrich: Zur Theoriegeschichte von Information Warfare. In: Stocker, Gerfried/ Schöpf, Christine: Information. Macht. Krieg. Wien, New York 1998.

Krempf, Stefan: Be Prepared: Cyberwar is Coming – or maybe not. In: telepolis 2001

Krempf, Stefan: Im Trippelschritt zum Cyberpeace. Das Phänomen Cyberwar stellt Friedensforscher und Sicherheitspolitiker vor große Herausforderungen. In: telepolis 2001.

Libicki, Martin: What is Information Warfare. Institute for National Studies. ACIS-Paper 3, 1995.

Merten, Klaus; Schmid, Siegfried J.; Weischenberg, Siegfried: Die Wirklichkeit der Medien, Opladen 1994.

Minkwitz, Olivier/ Schöfbänker, Georg: Information Warfare: Die neue Herausforderung für die Rüstungskontrolle. In: telepolis 2000.

Palm, Goedart: Kapitulierte der Staat? Die wahre Front hinter Terrorkrieg, Jihad und Kreuzzug. In: telepolis 2001 (a).

Palm, Goedart: Zur Psychopathologie der amerikanischen Cyberangst. Wo bitte geht's zur Cyberfront? In: telepolis 2001 (b).

Pordesch, Ulrich; Roßnagel, Alexander: Untersuchungen zur Verletzlichkeit einer vernetzten Gesellschaft. In: Werle Raymond, Lang Christa: Modell Internet?. München 1997.

Report of the „President's Commission on Critical Infrastructure Protection (PCCIP).

URL: <http://www.ciao.gov/PCCIP/>

Stand: 08.02.02

Rötzer, Florian/ Weibel, Peter: Cyberspace. Zum medialen Gesamtkunstwerk. Wien, 1993.

Rüstungskontrolle im Cyberspace: Perspektiven der Friedenspolitik im Zeitalter von Computerattaken

URL: <http://www.boell.de/downloads/medien/cyberwarprog.pdf>

Stand: 08.02.02

Shannon, Claude; Weaver, Warren: Mathematical Theory of Communication, University of Illinois Press 1963.

Virilio, Paul: Die Sehmaschine, Berlin 1989.

Virilio, Paul: Die Eroberung des Körpers, Berlin 1986.

Virilio, Paul: Geschwindigkeit und Politik, Berlin 1990.

Virilio, Paul: Information und Apokalypse./ Die Strategie der Täuschung. München, Wien 2000.

Virilio, Paul: Krieg und Fernsehen, München 1993.

Weiguang, Shen: Der Informationskrieg - eine neue Herausforderung. In: Stocker, Gerfried/ Schöpf, Christine: Information. Macht. Krieg. Wien, New York 1998.

Weiß Johannes (Hrsg.): Mehrdeutigkeiten der Moderne, Kassel 1998.

## Links

Bendrath, Ralf: URL: <http://www.userpage.fu-berlin.de/~bendrath/>

Stand: 08.02.02

Telepolis: URL: <http://www.heise.de/tp>

Stand: 08.02.02

The New Hacker's Dictionary

URL: [http://www.instinct.org/texts/jargon-file/jargon\\_toc.html](http://www.instinct.org/texts/jargon-file/jargon_toc.html)

Stand: 08.02.02

Denning, Dorothy: Cyberterrorism. 2001

URL: <http://www.cs.georgetown.edu/~denning/publications.html>

Stand: 08.02.02