
ETH-Zürich, Abteilung für Militärwissenschaften
Militärische Führungsschule, Diplomstudium

**Information Warfare - Ein strategisches
Mittel der Zukunft. Darstellung der Mittel,
Möglichkeiten und Einsatzarten**

Diplomarbeit

Referent: Prof. Dr. Albert A. Stahel
Korreferent: Prof. Dr. Curt Gasteyger

1996

Christoph M. V. Abegglen
Mooswiesstrasse 7
8118 Pfaffhausen

Inhaltsverzeichnis

	Seite
Abkürzungsverzeichnis	3
1. Einführung	5
2. Was ist "Information Warfare"? Stand der Diskussion	8
2.1. Informationsrevolution und ihre Folgen	8
2.2. Information Warfare: Inhalt	13
2.3. Mittel und Einsatzarten	16
2.3.1. Command-and-Control Warfare	16
2.3.2. Intelligence Based Warfare.....	17
2.3.3. Electronic Warfare	18
2.3.4. Psychological Warfare	19
2.3.5. Hacker Warfare	21
2.3.6. Economic Information Warfare	24
2.3.7. Cyberwarfare	25
2.4. Möglichkeiten	26
3. Ein strategisches Modell	33
3.1. Definitionen.....	33
3.2. Ebenen des strategischen Denkens und "Information Warfare"	35
3.3. Phasen der Dialektik des Willens	41
4. Schlusswort	45

	Seite
5. Anhang	48
5.1. Ursachen unbeabsichtigter Computerausfälle	48
5.2. Ursachen beabsichtigter Computerausfälle	48
5.3. Das strategische Denken Beaufres im Überblick	51
6. Literaturverzeichnis	52

Abkürzungsverzeichnis

AWACS	Airborne Warning and Control System
BDA	Battle Damage Assessment
C ² W	Command-and-Control Warfare
C ⁴ I	Command, Control, Communication, Computer and Intelligence
CERT	Computer Emergency Response Team
CyberW	Cyberwarfare
DISA	Defense Information System Agency
DoD	Department of Defense
EIW	Economic Information Warfare
E-Mail	Electronic Mail
EW	Electronic Warfare
GPS	Global Positioning System
HARM	High-speed Anti-Radiation Missile
HIC	High Intensity Conflict
HPM	High Power Microwaves
HW	Hacker Warfare
IBW	Intelligence based Warfare
IR	Infrarot
IW	Information Warfare
JSTARS	Joint Surveillance Target Attack and Reconnaissance System
LIC	Low Intensity Conflict
NEMP	Nuklearer Elektromagnetischer Impuls
NGOs	Non-Governmental Organizations
PSYW	Psychological Warfare
RC-135 RJ	Flugzeug zur Aufklärung elektromagnetischer Sender
TCOs	Trans-National Criminal Organizations
TNCs	Trans-National Corporations
UAVs	Unmanned Aerial Vehicles

UNO	United Nations Organization
WWW	World Wide Web

1. Einführung

Summers (1995) beschreibt die künftige Militärpolitik der Weltmacht USA nach dem Wegfall der bipolaren Konfrontation wie folgt: Die USA sollen ihre Containment-Strategie, die sie im Spiegel einer mit Nuklearwaffen ausgerüsteten Sowjetunion sowie im Hintergrund eines drohenden Landkrieges mit China formulierten, abwerfen und wieder zur Strategie des "Rollback and Liberation" zurückkehren. Die politisch strategische Defensive des Kalten Krieges, die während dem Korea- und dem Vietnamkrieg militärische Operationen stark einschränkend beeinflusste und dadurch zu Pattsituationen status quo ante führte, soll nun durch die strategische Offensive ersetzt werden. Die nach der Aufarbeitung des Vietnamkrieges formulierte AirLand Battle Doktrin führte zwar die operative und taktische Initiative wieder in die Kriegskunst ein, die USA verharrte jedoch bis zum Zusammenbruch der UdSSR in der strategischen Defensive. Erst der Wegfall eines drohenden sowjetischen Überfalls auf Westeuropa machte es möglich, das VII. Korps im Golfkrieg 1990/91 aus Europa abzuziehen und in die arabische Wüste zu setzen: Die grössere Handlungsfreiheit der USA hat sich abgezeichnet.

Als Startpunkt dieser neuen Ära amerikanischer Militärpolitik und Militärstrategie wird denn auch im durchschlagenden Erfolg der Befreiung Kuwaits gesehen. Nicht nur die AirLand Battle Doktrin hat sich erfolgreich bewährt, sondern auch der Kampf der verbundenen Waffen zu Luft, zu Land, zur See sowie im All hat durch die Vernetzung von "Command, Control, Communication, Computer and Intelligence" (C⁴I) einen noch nie dagewesenen Grad und Wirkung erreicht. Das Operationstheater erhielt durch den Einsatz modernster Aufklärungsmittel wie AWACS, Joint STARS, RC-135 RJ und Drohnen für die Koalitionskräfte eine solche Transparenz, dass der irakischen Führung in der ersten Angriffswelle der

alliierten Luftoffensive die Kontrolle über deren Streitkräfte entzogen werden konnte:

Iraq's command and control structures (its command post, headquarters, electrical power and telephone centres) was the first target on January 17, 1991, and that hapless nation may have been the first in history to fall victim to what our defense department now aptly calls the *differential* in information warfare.

Iraq was left blind, deaf, dumb and deceived; its impressive military strength fatally weakened in the opening minutes of the war by precisely planned and skillfully executed campaign to destroy the means of force control (Campen, 1992, S. 172).

Demgegenüber etablierten die USA ein in der Kriegsgeschichte nie dagewesenes Kommunikationsnetz, welches mit 98 prozentiger Verfügbarkeit glänzte und in Spitzenzeiten täglich 700'000 Telephonate, 152'000 Mitteilungen sowie 600 Bilder auf Korpsstufe und 30-50 zusätzliche Bilder pro Division verarbeitete. Über 30'000 Radiofrequenzen wurden verwaltet, um die notwendige Verbindung unter minimalster Interferenz sicherzustellen (Toma, 1992, S. 1; Menoher, 1992, S. 73).

Nach Summers (1995) gilt es, diesen Informationsunterschied für den Kampf der verbundenen Waffen auszunützen, wobei Kommunikationsmittel und Sensoren im All den Schlüssel dafür darstellen:

The joint campaign should *exploit the information differential*. Space power is crucial to establishing superiority in command, control, communications, intelligence, navigation, and information processing (1995, S. 112).

So wird in den Operationen zur Befreiung Kuwaits 1990/91 der erste "Information War" gesehen: der erste Auftritt einer Kriegführung, welche das 21. Jahrhundert prägen soll:

By leveraging *information*, U.S. and allied forces brought to warfare a degree of flexibility, sychronization, speed and precision heretofore unknown. More to the point, Desert Storm shows that, by leveraging information, a much smaller and less expensive military force can continue to underpin U.S. foreign policy in an unpredictable and disorderly new world (Campen, 1992, S. ix).

Doch ist diese Militärstrategie wirklich etwas Neues? Ist diese Konzeption nicht vielmehr eine Version des 'Blitzkrieges' Ende des zwanzigsten Jahrhunderts?

Die Diskussion über das Konzept "Information Warfare" ist besonders in den Vereinigten Staaten von Amerika entflammt. Diese Arbeit will in einem ersten Teil den Stand dieser Auseinandersetzung darstellen, indem sie einerseits Klarheit in den Begriffsverwendungen zu schaffen versucht und andererseits Mittel, Möglichkeiten und die daraus resultierenden Konsequenzen beleuchtet.

In einem zweiten Teil soll das Konzept von "Information Warfare" in ein strategisches Gedankengebäude gefasst werden, um Chancen und Gefahren zu umreißen. Zum Schluss sollen mögliche Phasen einer künftigen Konfliktaustragung skizziert werden.

2. Was ist "Information Warfare"? Stand der Diskussion

Die Bedeutung, welche der "Information Warfare" in Zukunft beigemessen wird, zeigt sich an der ständig wachsenden Anzahl von Institutionen, die sich alleine in den USA mit diesem Themenbereich auseinandersetzen: Sämtliche Teilstreitkräfte sind daran, ihre aus dem Golfkrieg, der als erster Informationskrieg betrachtet wird, sowie aus Übungen gewonnenen Erkenntnisse in Doktrin, Taktik, Ausbildung und Erziehung umzusetzen. Organisationsstrukturen und Logistik werden den Anforderungen des Informationszeitalters angepasst. So wird zum Beispiel im Februar 1997 eine digitalisierte Brigade der 4th Infantry Division Mechanized (Niefong, 1996, S. 62) und zum zweitenmal ein digitalisiertes Bataillon der 2nd Armoured Division gegen das konventionell ausgerüstete Übungsbataillon am National Training Centre in Fort Irwin, Kalifornien, antreten, um weitere Lehren im Hinblick auf die Armeereform Force XXI ziehen zu können (Economist, 1995, S. 9; Calvo, 1996, S. 68). Während sich die Defense Information System Agency (DISA) und die Advanced Research Projects Agency vor allem mit der Sicherheit von der Informationsinfrastruktur auseinandersetzen, werden militärische Führungspersonen aller Teilstreitkräfte an der National Defense University in der School of Information Warfare and Strategy weiter ausgebildet (Magsig, 1995, S. 1).

In diesem Kapitel soll der Stand der Diskussion betreffend dem Konzept "Information Warfare" umrissen werden. Dabei werden zunächst bewusst Unklarheiten in Begriffsbestimmung beibehalten, um den Prozess dieser intellektuellen Durchleuchtung wiederzugeben.

2.1. Informationsrevolution und ihre Folgen

Die der "Information Warfare" zugrunde liegende These formuliert Toffler (1993) wie folgt:

...the way we make war reflects the way we make wealth — and the way we make anti-war must reflect the way we make war (S. 3).

A new revolutionary economy is arising based on knowledge, rather than conventional raw materials and physical labor. This remarkable change in the world economy is bringing with it a parallel revolution in the nature of warfare (S. 4-5).

Doch die hervorragende Bedeutung des Wissens im zwischenmenschlichen Handeln stellt wohl keine neue Erkenntnis dar. So rät schon Sun Tzu (ca. 400-320 v. Chr.): "...Know the enemy and know yourself; in a hundred battles you will never be in peril" (Griffith, 1971, S. 84). Ebenso betont Jomini (1994):

...il faut tenter tous les moyens de se bien instruire (S. 290).

...en multipliant des renseignements, quelque imparfaits et contradictoires qu'ils soient, on parvient souvent à démêler la vérité du sein même de leurs contradiction (S. 290).

Nicht die Bedeutung des Wissens oder die der Informationsbeschaffung stellt also den Kern von "Information Warfare" dar, sondern die Geschwindigkeit, mit welcher Information und Wissen dank der technologischen Revolution gesammelt, verarbeitet, gespeichert, verbreitet und dargestellt werden können.

Der Einzug der Digitalisierung, die Einführung des Glasfaserkabels und die Leistungssteigerung von Schaltungen haben nicht nur zur gewaltigen Kapazitätssteigerung in der Telekommunikation geführt, sondern im Zuge des Deregulierungsprozesses fallen auch die Preise (Cairncross, 1996). Zudem ist die Anzahl der Medien zur Informationsverbreitung gestiegen: Neben Presse, Radio und öffentliches Fernsehen sind Privatsender, E-Mail, Natel, Satellitenfernsehen und -telephon, Fax, Global Positioning System (GPS), Internet sowie Videokonferenzen getreten. Um nicht in der Datensintflut zu versinken, schreitet die Datenverarbeitungstechnologie, welche Datenfusion und -analyse automatisiert sowie die Entscheidungsfindung mit Expertensystemen unterstützt, gleichzeitig voran. So ist es heute jedem jederzeit und über-

all möglich, eine grosse Menge von nahezu Echtzeitinformation zu erhalten oder zu verbreiten (Alberts, 1996).

Die Auswirkungen dieser Informationsrevolution sind wirtschaftlicher, sozialer, politischer und nicht zuletzt militärischer Art.

Wegen der Partikularisierung der Kundenbedürfnisse, wegen rascher werdenden Innovationszyklen sowie wegen dem steigenden Konkurrenzdruck im offenen Weltmarkt und wegen der zunehmenden Arbeitsteilung haben sich in der Wirtschaft Organisationen von Einlinien- hin zu Mehrliniensystemen sowie Matrixsystemen bewegt. Da der Informationsfluss nicht mehr ausschliesslich vertikal verläuft, sondern vermehrt horizontal und durch die zunehmende Interoperabilität vernetzt, ist eine Verflachung von Organisationen und eine zunehmende Dezentralisierung hin zu Organisationsnetzwerken absehbar:

[The information revolution] disrupts and erodes the hierarchies around which institutions are normally designed. It diffuses and redistributes power, often to the benefit of what may be considered weaker, smaller actors. It crosses borders, and redraws the boundaries of offices and responsibilities. It expands the spatial and temporal horizon that actors should take into account. Thus, it generally compels closed systems to open up (Arquilla und Ronfeldt, 1993, S. 143).

Many [institutions] will evolve from traditional hierarchical forms to new, flexible, network-like models of organization (Arquilla et al., 1993, S. 144).

Dabei erhalten Vorgesetzte immer mehr die Rolle des Beraters mit dem nötigen Überblick (Arquilla et al., 1993; Wenger und Köppel, 1995; Toffler, 1993).

Im Zuge des Individualisierungsprozesses und der Tendenz zur Vereinigung kommt der Wunsch nach Kommunität auf (Altermatt, 1996). Auf Mausklick öffnet sich im World Wide Web ein weltumspannendes Netzwerk, in dem Partikulärinteressen eine gemeinsame Plattform finden. So kann die nationale Souveränität durch transnationale Informationsflüsse unterminiert werden:

Der Fluss elektronischer Information ist schlecht kontrollierbar; Finanzinformation, Fernsehen oder elektronische Post halten sich nicht an politische Grenzen.

Die Folge sind Steuerausfälle, Umgehungsgeschäfte und ein Verlust des Informationsvorsprungs der Regierungen (Wenger et al., 1995, S. 4).

Analoge Auswirkungen wird die Informationsrevolution in der Organisation Militär nach sich tragen. Man wird vom traditionellen, an die Hierarchiestruktur untrennbar gebundenen Informationsfluss von Befehl, Nachrichten und Doktrin wegschreiten. Denn in Zukunft wird durch alle Führungsstufen hinweg dieselbe Information allen gleichzeitig zur Verfügung stehen (Alberts, 1996). Das führt schliesslich dazu, dass in den Streitkräften wie in der Wirtschaft die Bedeutung des mittleren Managements, d.h. Stufe Regiment, deutlich abnehmen wird. Damit die Führung wegen der verbesserten Schlachtfeldtransparenz nicht in die Falle des Mikromanagements tappt, gilt es besonders die Unterstellten im Rahmen der Auftragstaktik zu einer einheitlichen Denkweise zu erziehen. Es muss eine klare Trennung von Aufgaben und Kompetenzen zwischen den Führungsebenen erfolgen. In Mao Tse-tungs Worten:

...the command must be centralized for strategical purposes and decentralized for tactical purposes. Centralized strategical command takes care of the general management of all guerrilla units, their coordination within war zones, and the general policy regarding guerrilla base areas. Beyond this, centralization of command will result in interference with subordinated units, as, naturally, the tactics to apply to concrete situations can be determined only as these various situations arise. ... In a word, proper guerrilla policy will provide for unified strategy and independent activity (Griffith, 1978, S. 101).

Zudem wird mit der Verfügbarkeit von zeitverzugslosen Information der Hang zum Konsultieren anderer Ansichten und Meinungen vor einer Entschlussfassung und somit das Fassen von Kollektivbeschlüssen zunehmen. Im Entscheidungsprozess darf aber die Kreativität dem Konsensentschluss nie untergeordnet sein. Weiter besteht die Gefahr, dass die Führung mit der Erwartung auf perfekte Information Entschlüsse verzögert (Isbell, 1993). Doch gerade in einem modernen Schlachtfeld, wo sich die Lage rasch ändert und die Zeitspanne von Zielerkennung,

Zielerfassung, Waffenwahl, Waffenauslösung sowie Kontrolle der Waffenwirkung im Ziel durch Automation ständig abnimmt, rächt sich Zögern und Inaktivität mit ebenso unverzüglichen, letalen Konsequenzen (Alberts, 1996, /.../concerns.html).

Eine weitere Folge der Informationstechnologierevolution wird wohl das Verschwinden komplexer Waffenplattformen sein (Waller, 1995; Stix, 1995; Libicki, 1996, //.../a003ch04.html). Die Fortschritte in der Übermittlungstechnik machen es möglich, die bis anhin auf einer Waffenplattform vereinten Elemente wie Sensoren, Waffen, Entscheidungsträger und Ausführende physisch voneinander zu trennen. So wird eine teure Waffenplattform, die oftmals durch eine einzige kostengünstige Abwehrwaffe vernichtet werden kann, in ihre Einzelteile physisch zerstreut, welche einzig durch Kommunikation miteinander verbunden bleiben, um so die gegnerischen Mitteleinsatz ebenfalls zu verzetteln. Aus einem grossen Angriffsziel werden viele kleine, die in ihren Einzelteilen günstig sind und somit entbehrlich werden (Stix, 1995).

Schrumpfende Budgets bei erweitertem Aufgabenspektrum verursachen zudem wachsenden Kostendruck auf die verkleinerten Streitkräfte. Dies wird den Einzug von Informationstechnologie aus Überlegungen der Kosteneffizienz und Produktivitätssteigerung beschleunigen. Auch der Simulation eröffnet sich dank der gesteigerten Rechenleistung von Computern mit der "Virtual Reality" eine neue Dimension. Eine Panzermannschaft kann heute z.B. nicht nur von den USA aus gegen eine von Grossbritannien über die Datenautobahn in einem virtuellen Schlachtfeld antreten, sondern Echteinsätze können für einsatzbezogene Ausbildung in der virtuellen Welt eingeübt werden (Economist, 1995, S. 10).

Die wachsende Abhängigkeit von Informationstechnologie aber bietet neben Chancen auch Gefahren. So warnt Van Creveld (1991) vor der beschränkten Einsatztauglichkeit technischer Mittel in einem stark strukturierten Gelände:

...targets are detected by radar and appear as blips on fluorescent screens. They are acquired, tracked, and engaged with the aid of technical, read "electronic", instruments.

Thus, modern aircraft, helicopters, ships, tanks, antitank weapons, artillery, and missiles of every kind are all becoming dependent on electronics to the point where this dependence is itself the best possible index of their modernity. Now electronic sensing devices and the computers to which they are coupled are very sensitive to environmental interference. They work fairly well in simple media such as air, sea, even open plains and deserts. However, the more complicated the surroundings the greater the problems. (...)

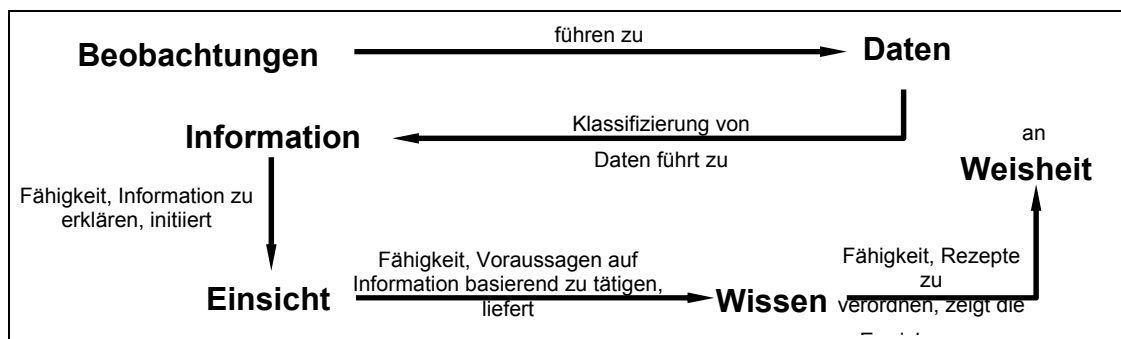
What is more, once the principles on which these gadgets operate are understood they are easy to spoof, overload, or jam (S. 30-31).

2.2. Information Warfare: Inhalt

Voraussetzung für eine klare Definition des Begriffes und der Mittel der "Information Warfare" sind einige grundlegende Gedanken betreffend Information, Entscheidungszyklus und möglicher Ansatzpunkte von "Information Warfare".

Unter Information versteht man im allgemeinen den Inhalt oder die Bedeutung einer Mitteilung. Information kann aber ebenfalls aus einer Veränderung des Mitteilungsflusses resp. aus einer Nichtmitteilung geschöpft werden. Abbildung 1 soll den Zusammenhang zwischen Information im engeren Sinne und Information in ihrer umfassenden Betrachtungsweise darstellen:

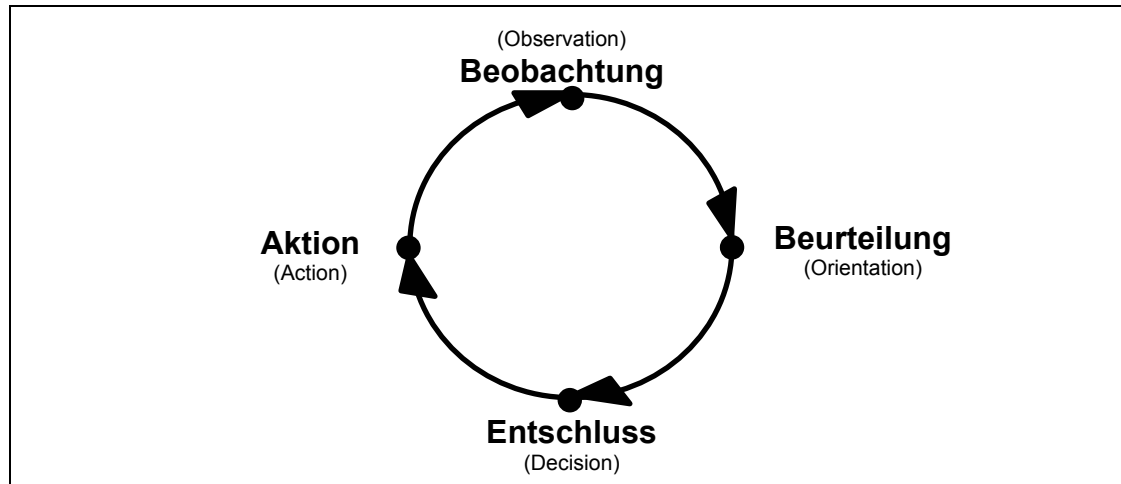
Abbildung 1: Umfassende Betrachtung von Information



Quelle: Magsig, 1995, S. 2.

Wie vorgängig bemerkt, ermöglicht die Informationsrevolution ein immer schnelleres Durchlaufen des Entscheidungszyklus. Abbildung 2 zeigt die Elemente dieser OODA-Zyklus (Observation, Orientation, Decision and Action Loop):

Abbildung 2: OODA-Zyklus



Quelle: *Economist*, 1995, S. 5.

Ganz allgemein formuliert versucht "Information Warfare", den OODA-Zyklus des Gegners zu beeinträchtigen, währenddem der eigene vor fremder Beeinflussung geschützt werden soll. Mit anderen Worten besteht das Ziel von "Information Warfare" darin, in einem Interessenskonflikt den gegnerischen Willen zum Widerstand zu brechen oder zumindest den Gegner in seiner Entscheidungsprozess so zu hemmen, dass er Aktionen nicht rechtzeitig auslösen kann. Zudem sollen einmal ausgelöste Aktionen des Gegners ins Leere schlagen, weil der Gegner seine Beurteilung sowie seinen Entschluss auf irrelevante Informationen von getäuschten Beobachtungssensoren abstützt.

Sucht man nach einer Definition von "Information Warfare", so stösst man auf eine Vielzahl von Varianten (vgl. Magsig, 1995; IASIW, 1996). Dies verdeutlicht den Prozess, den das Konzept "Information Warfare" durchläuft. Einige Definitionen wie diejenige des Verteidigungsministeriums (DoD) der USA sehen das operative Ziel von "Information Warfare" in der Erreichung der Informationsüberlegenheit:

Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based network, while defending ones own information, information based process, information systems and computer-based networks (Manthorpe, 1996, S. 9).

Doch das Konzept von Informationsüberlegenheit resp. Informationsherrschaft macht wenig Sinn, da die Quantifizierung des Erfolges nicht wie bei der Luftkriegführung möglich ist. In Analogie zur Luftüberlegenheit soll Informationsüberlegenheit dann erreicht sein, wenn "während einer bestimmten Zeit über einem begrenzten Gebiet...ohne Einschränkung" einer Partei lediglich diejenige Information zukommt, welche die Gegenseite beabsichtigt, ohne dass die eigenen Informationssysteme in irgendeiner Weise vom Gegner beeinträchtigt werden können (Stahel, 1993, S. 63). Ruft man sich die ganzheitliche Bedeutung von Information in Erinnerung, so leuchtet es ein, dass Informationsüberlegenheit ein Ding der Unmöglichkeit darstellt. Wie es "keine Nicht-Kommunikation" (Steiger, 1990, S. 145) gibt, gibt es keine Nicht-Information, da auch Ausbleiben von Daten, Befehlen, Aufklärungsergebnisse u.s.w. Information beinhaltet. Zudem kann Information von tradiertem Wissen kaum unterbunden werden.

Hier soll die Variante des Institute for the Advanced Study of "Information Warfare" (IASIW) als Definition dienen:

Information Warfare is the offensive and defensive use of information and information systems to exploit, corrupt, or destroy an adversary's information and information systems, while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries (IASIW, 1996, S. 1).

2.3. Mittel und Einsatzarten

Libicki (1996) unterscheidet sieben Formen von "Information Warfare":

Seven forms of information warfare — conflicts that involve the protection, manipulation, degradation, and denial of information — can be distinguished:

- (i) command-and-control warfare [C²W] (which strikes against the enemy's head and neck),
- (ii) intelligence-based warfare [IBW] (which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace),
- (iii) electronic warfare [EW] (radio-electronic or cryptographic techniques),
- (iv) psychological warfare [PSYW] (in which information is used to change the minds of friends, neutrals, and foes),
- (v) "hacker" warfare (in which computer systems are attacked),
- (vi) economic information warfare (blocking information or channelling it to pursue economic dominance),
- (vii) cyberwarfare (a grab bag of futuristic scenarios).

(Libicki, 1996, //.../a003ch00.html)

Im folgenden sollen Mittel und Einsatzarten von "Information Warfare" näher vorgestellt werden.

2.3.1. Command-and-Control Warfare

"Command-and-Control Warfare" (C²W) ist gegen die feindlich gesinnte Führung und deren Führungseinrichtungen gerichtet. Diese Form von "Information Warfare" verfolgt den Zweck, die gegnerische Führung auszuschalten. Dies erfolgt auf zwei Arten: Erstens, indem die Führungsperson als solche oder deren Kommandoposten vernichtet wird; zweitens, indem Kommunikationsverbindungen zwischen Führung und Unterstellten durch physische Zerstörung, elektronische Störung oder Täuschung unterbunden werden. Dieses Mittel von "Information Warfare" wurde im Golfkrieg erfolgreich eingesetzt. Die alliierte Luftoffensive konzentrierte sich in der ersten Phase des Luftkrieges auf diese zwei Ziele: Irakische Kommunikationsverbindungen und Energieversorgung wurden durch Luftangriffe auf Kraftwerke, Verteilerzentren, Pipelines zur Energieversorgung von Kraftwerken, Sendeanlagen und Radars nachhaltig gestört:

Some Tomahawk cruise missiles dispensed ribbons of carbon fibers over Iraqi electrical power switching systems, causing short circuits, temporary disruptions and massive shutdowns in the power systems (Campen, 1992, S. 173).

In der sich als erfolgreich erwiesenen "Command-and-Control Warfare" (C²W) wurde denn auch diejenige Militärstrategie gesehen, die "Information Warfare" auf dem Schlachtfeld umsetze. Dies ist aber eine zu eingeschränkte Sichtweise von "Information Warfare".

2.3.2. Intelligence Based Warfare

Unter "Intelligence Based Warfare" (IBW) wird das direkte Einfließen von Echtzeitnachrichten resp. Echtzeitaufklärungsergebnisse (wie z.B. Zielzuweisung und Battle Damage Assessment (BDA)) während einer Operation verstanden. Dies im Gegensatz zu Nachrichten, die als Input zur Gesamtführung dienen (Libicki, 1996, //.../a003ch04.html). Die Anzahl von Sensoren, die für diesen Zweck eingesetzt werden können, wächst ständig an. Solche Sensoren werden in vier Gruppen unterteilt:

- (i) far stand-off sensors (most space but also seismic and acoustic sensors);
- (ii) near stand-off sensors (e.g., unmanned aerial vehicles [UAVs] with multispectral, passive microwave, synthetic aperture radar [SAR], and electronic intelligence [elint] capabilities, as well as similarly equipped offshore buoys and surface-based radar);
- (iii) in-place sensors (e.g., acoustic, gravimetric, biochemical, ground-based optical);
- (iv) weapons sensors (e.g., IR, reflected radar, and light-detection and ranging [lidar]).

(Libicki, 1996, //.../a003ch04.html).

Die Entwicklung strebt nach Miniaturisierung, Interoperabilität, wachsende Präzision und Zuverlässigkeit. Die Sensoren sollen dank ihren sinkenden Kosten in grossen Mengen eingesetzt werden können. Der verfolgte Zweck dabei ist das Erlangen von Schlachtfeldtransparenz (battlespace visibility) und Lagebewusstsein (situational awareness). Die Sensoren sollten in der Lage sein, ihre Daten zeitverzugslos direkt an Zielzuweisungssysteme resp. an die geeignete Waffe zu übermitteln, ohne die Hierarchiestufen durchlaufen zu müssen (Libicki, 1996, //.../a003ch04.html). Angestrebt wird

die vollständige Interoperabilität sämtlicher Systeme aller Teilstreitkräfte.

2.3.3. Electronic Warfare

Unter "Electronic Warfare" (EW) versteht man "die Gesamtheit aller Massnahmen mit dem Ziel, einerseits fremde elektromagnetische Ausstrahlungen aufzuklären und zu beeinträchtigen, und andererseits sicherzustellen, dass eigene elektromagnetische Ausstrahlungen wirksam angewendet werden. Die Elektronische Kriegführung umfasst elektronische Gegenmassnahmen und elektronische Schutzmassnahmen" (Schweizerische Armee, 1994, Teil 9, S. 8).

Die Einsatzmittel dafür reichen vom einfachen Störsender (jammer) über Kryptographie und High-speed Anti-Radiation Missiles (HARM-Lenk Waffen) bis hin zu High Power Microwave (HPM)-Waffen und zum Nuklearen Elektromagnetischen Impuls (NEMP) (Gut, 1993; Libicki, //.../a003ch05.html).

2.3.4. Psychological Warfare

"Psychological Warfare" (PSYW) beinhaltet das Verwenden von Information gegen den menschlichen Geist. Dazu Mao Tse-tung:

The mind of the enemy and the will of his leaders are targets of far more importance than the bodies of his troops (Griffith, 1978, S. 20).

Grundsätzlich ist psychologische Kriegführung sowohl nach aussen gegen einen aussenstehenden Feind als auch nach innen gegen das eigene Volk gerichtet. Mit der Informationsrevolution haben die Möglichkeiten und Mittel psychologischer Kriegführung qualitativ neue Ausmasse erreicht. Satellitenfernsehen ermöglicht Live- Reportagen, die Bildausschnitte einer partiellen Wahrheit zeigen. So wird dem Fernsehen gerade in offenen Gesellschaften die Macht des politischen Agenda-Settings zugesprochen. Zudem eröffnet Satellitenempfang

den Führern von Konfliktparteien die Möglichkeit, direkt zum jeweiligen Zielpublikum zu sprechen (Libicki, 1996, //.../a003ch06.html). Was früher an die Masse einheitlich kommuniziert wurde, kann heute durch Aggregation persönlicher Daten und Marktforschung kundenspezifisch und individuell zugeschnitten via Fax, E-Mail, Privatsender, Internet oder Pager mitgeteilt werden. Neuste Hollywood-Techniken wie "morphing"¹, die dem Kinogänger in "Forrest Gump" und "Independence Day" als ausgereifte Illusion präsentiert worden sind, zeigen, dass fiktive, manipulierende Ereignisse künstlich geschaffen werden können.

Libicki unterscheidet vier Kategorien psychologischer Kriegführung:

- (i) operations against the national will,
- (ii) operations against opposing commanders,
- (iii) operations against troops, and...
- (iv) cultural conflict.

(Libicki, 1996, //.../a003ch06.html)

Unter die erste Kategorie fallen alle Unternehmen, die darauf abzielen, die öffentlich Meinung für den eigenen Zweck zu beeinflussen.

Als zweite Kategorie wird das Vorgehen gegen die Psyche der gegnerischen Führung genannt. Strategisches Ziel ist dabei die komplette Verwirrung derselben:

Hence *his* (stategist) *true aim is not so much to seek battle as to seek a strategic situation so advantageous that if it does not of itself produce the decision, its continuation by a battle is sure to achieve this*. In other words, dislocation is the aim of strategy ([Liddell Hart](#), 1991, S. 325).

Indirektes Vorgehen soll angewendet werden, damit Verwirrung erzielt werden kann ([Liddell Hart](#), 1991). Was darunter zu verstehen ist, wird im dritten Kapitel umrissen. Hier nur soviel: Der Täuschung

¹ "morphing" ist eine computerunterstützte Technik, die es dem Hauptdarsteller Tom Hanks in Filmsequenzen von "Forrest Gump" erlaubte, Seite an Seite von verschiedenen U.S. Präsidenten aufzutreten. Unter "morphing" versteht man auch das fließende Übergehen von einer Figur in eine andere. Im Film "Independence Day" war es dank Computeranimation möglich, ganze Luftschlachten zwischen UFOs und Abfangjäger darzustellen.

wird dabei grosse Bedeutung beigemessen. Denn nur durch Täuschung kann man Überraschung erzielen, die der gegnerischen Führung den Eindruck vermittelt, in der Falle zu sitzen. Im Gegensatz dazu vermittelt ein direktes Vorgehen, also eine vom Gegner erwartete Handlungsweise, diesem Sicherheit und somit psychische Stärkung.

In der dritten Kategorie der psychologischen Kriegführung geht es darum, das Vertrauen der Truppen in sich selbst, in ihre Vorgesetzten, in die Sache für die sie kämpfen, in die Unterstützung der Heimatfront sowie in ihre Ausrüstung und in die eigene Aussicht auf Erfolg zu beeinflussen.

In der letzten Kategorie wird der Kulturkampf genannt. Darunter wird die Assimilation fremder Werte und Normen im eigenen Kulturraum verstanden. Dabei fürchtet man den Verlust der eigenen Identität. Eine Andersartigkeit, die das Wir-Gefühl einer Nation durch Ausgrenzung des "Fremden" schüren soll. Die Dissemination solcher Wertvorstellungen erhält durch die Informationsrevolution neue Medien: Neben Presse treten Internet, Satellitenfernsehen, Video und Popmusik.

2.3.5. Hacker Warfare

Unter "Hacker Warfare" versteht man das Ausnutzen von Sicherheitslücken ziviler Computernetzwerke, um Information zu beschaffen, zu verfälschen, anzupassen, zu vernichten oder ganze Netze lahmzulegen. Das militärische Pendant dazu fällt unter das zuvor beschriebene "Command-and-Control Warfare" (C2W) (Libicki, 1996, //.../a003ch07.html).

Die geringen Einstiegskosten für diese Art von Kriegführung ermöglicht eine breite Palette von Akteuren. Wegen der weltweiten Vernetzung lokaler Netzwerke über Internet reicht ein Notebook und ein Natel sowie Zugang zum Internet aus, um in diesem Bereich tätig zu werden. Der notwendige finanzielle Aufwand, um die Informationsin-

frastruktur der USA nachhaltig stören zu können, wird unterschiedlich geschätzt:

...the Naval Postgraduate School in August of 1993 claims that with 20 people and \$1 million the author can bring the U.S. to its knees (Steele, 1993 zit. nach Cohen, 1995, S. 68). Other expert claims range from \$100'000 and 10 people for large-scale disruption over a period of weeks, to \$30 million and 100 people for almost total information infrastructure disruption resulting in multi-year recovery time (Cohen, 1995, S. 68).

Weil grosse Wirkung verbunden mit solch niedrigen Kosten erzielt werden kann, wird dieses Mittel der "Information Warfare" an Bedeutung gewinnen. Denn das notwendige Know-how und die dazu nötige technische Ausrüstung ist überall erhältlich.

Da Institutionen der Landesverteidigung ihre Telekommunikation mit Schwergewicht über das öffentliche Netz betreiben, sind auch diese durch "Hacker Warfare" gefährdet. So haben sich drei Schweizer 1996 elektronischen Zugang zum Armee-Überwachungssystem verschafft, um dieses auszuforschen (Zeller, 1996). Die PTT-Telecom, Banken, Versicherungen und das EMD stellen ein natürliches Magnet für "Hacker Warfare" dar. So schätzt die Defense Information Systems Agency (DISA), dass alleine vergangenes Jahr der Verteidigungsbereich der USA Opfer von bis zu 250'000 Hackerattacken wurde (GAO, 1996, S. 3). Dabei sind rund 65% der Attacken erfolgreich und überwinden die etablierten Schutzmechanismen. Lediglich einer von 150 Hackervorfälle wird als solcher erkannt und rapportiert. Die daraus resultierenden Kosten werden im Verteidigungsbereich bis auf zu mehreren \$100 Millionen geschätzt (GAO, 1996, S. 4).

Die Motivation zu "Hacker Warfare" reicht vom "Computer-joy-riding" Jugendlicher über Gründe persönlicher Bereicherung, organisierte Kriminalität, Wettbewerb zwischen Geschäftskonkurrenten, persönliche Rachefeldzüge, Austesten von Sicherheitslücken im eigenen System zur Prävention, bis hin zur politischen Umwälzung. Das

Bedrohungsspektrum umfasst dabei wirtschaftliche Verluste durch Ausfall von Dienstleistungen sowie durch Diebstahl finanzieller Mittel, Dienstleistungen oder geistigen Eigentums, Spionage im wirtschaftlichen und politischen Bereich sowie Erpressung, Terrorismus und Chaos durch Zusammenbruch des öffentlichen Verkehrs, Stromversorgung und Telekommunikation.

Die Opportunitätskosten wegen Systemausfälle, sei dies durch gezielte Hackerattacken oder durch "Unfälle" (Softwarefehler, falsche Hardwarekonfiguration, Fehlmanipulationen u.v.a.) werden in den USA auf \$10 Mia. beziffert:

Tabelle 1: Bestätigte Verluste durch Systemausfälle in den USA

Item	Annual Cost Estimate
Denial of service attacks	\$4B
AT&T toll frauds	\$2B
Other toll frauds (est)	\$2B
FBI-reported computer crimes	\$2B
Total	\$10B

Quelle: Cohen, 1995, S. 78.

Cohen (1995) unterscheidet dabei zwischen rund 16 verschiedenen Arten unabsichtlich verursachter Systemunterbrüche sowie zwischen rund 20 Formen von Hackerattacken auf Computersysteme (siehe Anhang 5.1. und 5.2.).

Die USA reagierten auf diese Bedrohung auch mit der Bildung eines Interventionsteams CERT (Computer Emergency Response Team), das bei Systemausfällen in Aktion tritt.

Nachstehendes Beispiel soll verdeutlichen, dass auch die Schweiz von dieser Problematik betroffen ist: Im Mai dieses Jahres legte ein Systemunterbruch in der Payserv-Zentrale 3'300 Bancomaten der Schweiz lahm. Zudem wurde jegliche Transaktion aller 21'000 EC-Direct-Terminals in Ladengeschäften während 45 Minuten nicht zugelassen (Schoch, 1996). Weiter ist anzunehmen, dass Banken regelmässig Ziel von "Hacker Warfare"-Attacken sind. Die Vertuschung

solcher Ereignisse soll wahrscheinlich das Vertrauen der Kunden nicht beeinträchtigen (Cohen, 1995, S. 89). Dies verhindert jedoch, dass die Bedrohung, welche von "Hacker Warfare" ausgeht, in das öffentliche Bewusstsein eindringt, so dass der notwendige Prozess zur Sicherung von Computernetzwerken und von öffentlicher Informationsinfrastruktur nur schleppend eingeleitet wird.

Zwar existieren Meinungen, welche behaupten, mit der Zeit nehme die Gefährdung durch "Hacker Warfare" ab. Denn die Informationsinfrastruktur werde über die Dauer gegen Hackerattacken wie das Immunsystem eines Organismus gegen Viren ständig resistenter (Libicki, 1996, //.../niitemp.html). Gleichzeitig aber nimmt nicht nur die Gerissenheit solcher Attacken zu, sondern auch die dafür geeigneten Softwarehilfsmittel (GAO, 1996, S. 8). Mit dem exponentiellen Wachstum von Internet werden zudem die ca. 900 Mio. Einbruchversuche über das WWW pro Jahr sowie die nicht rapportierten und nicht aufgedeckten Vergehen um ein Vielfaches zunehmen (Cohen, 1995).

Die Schwierigkeit, und somit auch ein Teil ihrer Attraktivität, liegt im Erkennen von Hackerattacken. Denn die Symptome sind kaum von herkömmlichen, ungewollten Systemunterbrüchen zu unterscheiden. Zudem verschaffen sich die Täter Zutritt, indem sie sich gegenüber dem Zielcomputer als Benutzungsberechtigte ausgeben. Wird eine Attacke erkannt und gemeldet, ist die Identifizierung des Täters nicht einfach, weil dieser seine Spur unter Verwendung fremder Telephonanschlüsse sowie über Drittländern vermittelten Telephonverbindungen verwischen kann (GAO, 1996, S.11).

2.3.6. Economic Information Warfare

Unter "Economic Information Warfare" versteht man die Verbindung von "Information Warfare" mit "Economic Warfare". Dieses Konfliktaustragungsmittel kann dabei zwei Formen annehmen: Erstens kann "Economic Information Warfare" in Form von Informationsblok-

kade oder zweitens in Form von Informationsimperialismus geführt werden (Libicki, 1996, //.../a003ch08.html).

Eine Informationsblockade soll ähnlich wie Wirtschaftssanktionen oder Wirtschaftsblockaden, die den Güterverkehr mit einer Nation unterbinden, eine Nation durch Verwehren von Austausch elektronischer Daten zur Aufgabe des Widerstandes zwingen.

Unter Informationsimperialismus versteht man den Umstand, dass Staaten sich in gewissen Industriesektoren spezialisieren, um konkurrenzfähig zu bleiben. Dabei unterscheiden sich Industriezweige in ihrer Wissensintensität. So benötigen und fördern besonders Länder mit hohem Lohnniveau Branchen, Fertigkeiten und Know-how mit höherer Wissensintensität, als dies Billiglohnländer tun. Dieser Prozess wird durch das Festhalten an einer einmal erreichten Position in den wissensintensiven Industrien weiter verstärkt (Libicki, 1996, //.../a003ch08.html, S. 2).

2.3.7. Cyberwarfare

"Cyberwarfare" umfasst Informationsterrorismus, semantische Angriffe, Simulationskriegführung und "Gibson-warfare" (Libicki, 1996, //.../a003ch09.html).

Informationsterrorismus ist ein Ausleger von "Hacker Warfare" und versucht Lücken im Informationssystem auszunutzen, nicht um es zu stören oder lahmzulegen, sondern um Einzelpersonen anzugreifen. Sensitive Daten werden über eine Person aggregiert, so dass diese bedroh- oder erpressbar wird.

Semantische Angriffe versuchen im Anschein einwandfreiem Funktionieren eines Systems, dessen Antworten und Reaktionen auf eine nach eigenem Wunsch veränderte Realität zu provozieren. Dies kann z.B. über die Sensoren eines Systems geschehen: Kontrolliert ein Atomkraftwerk seismische Aktivitäten, könnten dessen Sensoren mit einem nichtexistenten Erdbeben so getäuscht werden, dass das Kraftwerk sich automatisch abschaltet.

Simulationskriegführung und "Gibson-warfare" fallen eher in den Bereich von Science Fiction. Es ist aber dennoch durchaus vorstellbar, dass Kriege in Zukunft nicht mehr auf einem Schlachtfeld mit mehr oder minder ausgefeilten Methoden des Totschlages ausgefochten werden. Kriege könnten zum Beispiel lediglich computersimuliert werden, wobei dessen Ausgang als rechtmässiges Ergebnis von allen Konfliktparteien akzeptiert würde. Ob sich diese blutlose Art des Kommentkampfes die archaischen Wurzeln des Tötens sowie des Krieges in der menschlichen Psyche (O'Connell, 1989; Burkert, 1972) überwinden wird, mutet doch sehr idealistisch an. "Gibson-warfare" ist eine gesteigerte Form der Simulationskriegführung. Die Namensgebung stammt von einem Schriftsteller, der in einem Science Fiction Roman die Antagonisten zu virtuellen Gestalten werden lässt, die sich dann in einer virtuellen Welt bekämpfen (Libicki, 1996, //.../a003ch09.html, S. 1).

Eher in den Bereich des Möglichen fällt die Substitution realer Waffen durch virtuelle in einem realen Operationsraum. So könnten Lasersimulationsausrüstungen, wie diese schon zu Ausbildungszwecken eingesetzt werden, echte Kugeln ersetzen (Libicki, 1996, //.../a003ch09.html).

2.4. Möglichkeiten

In der Anwendung von den im Kapitel 2.3. beschriebenen Mittel von "Information Warfare" wird zwischen zwei Einsatzmöglichkeiten unterschieden. So differenzieren Arquilla et al. (1993) zwischen "Netwar" und "Cyberwar". Während "Netwar" schwerwiegend gegen eine Gesellschaft und deren Informationsinfrastruktur geführt wird, zielt "Cyberwar" auf die gegnerischen Streitkräfte ab und betrifft militärische Operationen:

Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting, if not destroying, information and communication systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where

it is, what it can do when, why it is fighting, which threats to counter first, and so forth (Arquilla et al., 1993, S. 146).

The term 'netwar' denotes an emerging mode of conflict (and crime) at societal levels, involving measures short of war, in which the protagonists use — indeed, depend on using — network forms of organization, doctrine, strategy, and communication. These protagonists generally consist of dispersed, often small groups who agree to communicate, coordinate, and act in an internetted manner, often without a precise central leadership or headquarters. Decisionmaking may be deliberately decentralized and dispersed (Arquilla und Ronfeldt, 1996, S. 5).

"Netwar" unterscheidet sich demnach nicht nur in ihrer Zielgruppe von "Cyberwar", sondern auch in ihrer Konfliktintensität. So wird "Netwar" im Bereich der Gewalt unterhalb der Kriegsschwelle geführt und somit neben Staaten auch von nichtstaatlichen Akteuren getragen.

Dank der Informationsrevolution können sich diese Akteure in Netzwerken transnational organisieren, um durch ihre Dezentralisation weniger verwundbar zu sein (vgl. Kap. 2.1.). Aber um dennoch ihre Kräfte konzentrieren zu können, bedingt diese Dezentralisation der taktischen Ebene eine einheitliche Doktrin und enger Informationsaustausch. Diese Organisationsform findet ihre Anwendung sowohl im "Netwar" als auch im "Cyberwar". Die Parallelen zur Guerillaorganisation von Mao Tse-tung sind offensichtlich. Die Vorteile, die aus einem Organisationsnetz resultieren, sind denn auch dieselben:

Offensive potential: Adaptable, flexible, versatile vis à vis opportunities

- Functional differentiation with interoperability
- Impressive mobilization and penetration capabilities
- Capacities for stealth and for swarming

Defensive potential: Redundant, robust, resilient in the face of adversity

- difficult to crack and defeat as a whole
- great deniability

Offense and defense often blurred and blended

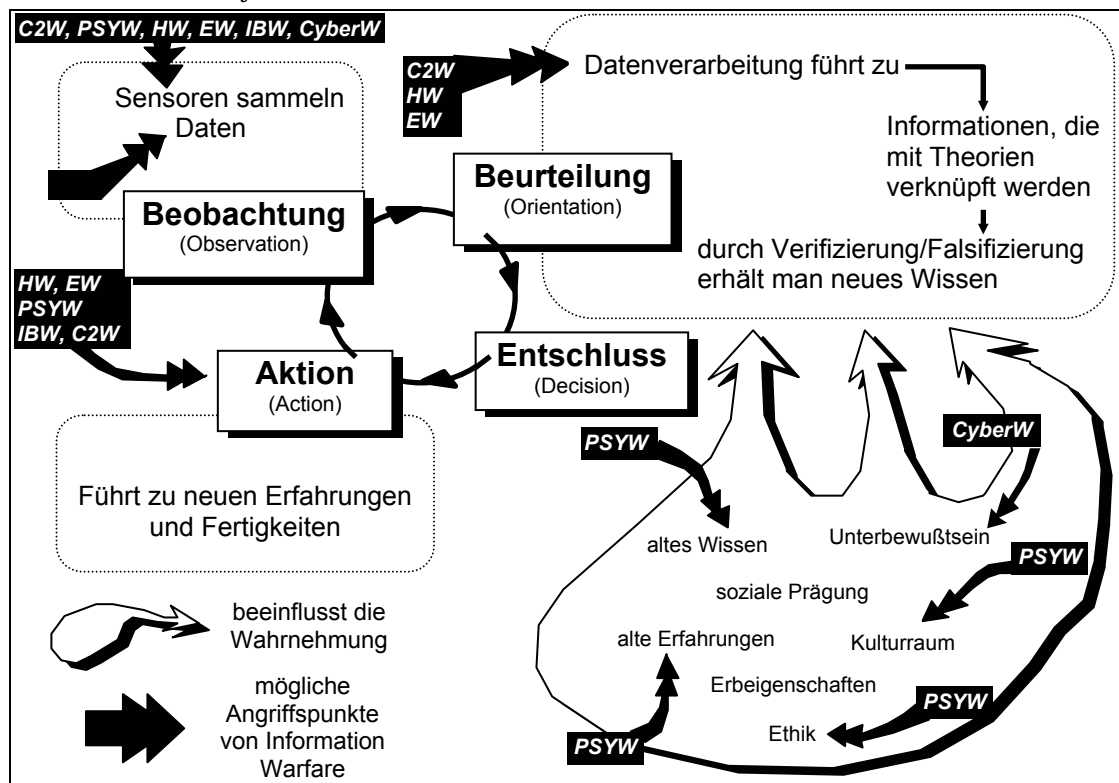
(Arquilla et al., 1996, S. 11)

Dispersion, concentration, constant change of position — it is in these ways that guerrillas employ their strength (Griffith, 1978, S. 91)

Die Netzorganisation ist also nicht ein neues Konzept, das Ende des 20. Jahrhunderts hervorgebracht worden ist. Vielmehr bewährte sich dieses schon bei Drogenkartellen und Schmugglerringen, aber auch in der Kriegsgeschichte (Arquilla et al., 1996).

In Abbildung 3 werden die möglichen Ansatzpunkte von "Information Warfare" im Entscheidungszyklus dargestellt:

Abbildung 3: Entscheidungszyklus mit möglichen Ansatzpunkten von "Information Warfare"



Quelle: in Anlehnung an Rona, 1996, S. 57; Boyd, 1987 nach Szafranski, 1996, S. 3.

Diese Darstellung verdeutlicht, dass nicht nur Datenerfassung getäuscht, in deren Verarbeitung manipulativ eingegriffen und deren Verbreitung gestört werden können, sondern dass "Information Warfare" die Wahrnehmung der Ergebnisse und deren Bewertung durch den Menschen indirekt verändern soll:

Information warfare, in its essence, is about *ideas and epistemology*-big words meaning that information warfare is about the way humans think and, more important, the way humans make decisions. And although information warfare would be waged largely, but not entirely, through the communication nets of a

society or its military, it is fundamentally not about satellites, wires, and computers. It is about influencing human beings and the decision they make (Stein, 1996, [//.../stein.html](#), S. 1).

Offensichtlich ist "Information Warfare" kein neues Konzept. So kann in der Guerillakriegführung von Mao Tse-tung ein praktisches Beispiel von "Information Warfare" gesehen werden:

Guerrilla leaders spend a great deal more time in organization, instruction, agitation, and propaganda work than they do fighting, for their most important job is to win over the people. "We must patiently explain," said Mao Tse-tung. "Explain," "persuade," "discuss," "convince" — these words recur with monotonous regularity in many of the early Chinese essays on guerrilla war (Griffith, 1978, S. 27).

Mit der Informationsrevolution veränderte sich also lediglich die qualitative Anwendbarkeit von "Information Warfare". So vereinigt ein Autor alle Elemente von "Information Warfare", indem er folgendes Vorgehen gegen Guerillakräfte in eine Allegorie fasst:

If a fish (guerrillas) has got to be destroyed it can be attacked directly by rod or net, providing it is in the sort of position which gives these methods a chance of success. But if rod and net cannot succeed by themselves it may be necessary to do something to the water (people) which will force the fish into a position where it can be caught. Conceivably it might be necessary to kill the fish by polluting the water, but this is unlikely to be a desirable course of action (Kitson, 1991, S. 49).

Die ganze Diskussion um "Information Warfare" unterstreicht etwas mit Bestimmtheit: Allgemein wird im westlichen Denken der Schwerpunkt der Kriegführung neu deutlich auf die Seite der Täuschung gesetzt. Die Bedeutung der Täuschung im zwischenmenschlichen Handeln und besonders im Krieg haben aber schon einige Denker betont. So sagt Sun Tzu, dass Kriegführung auf Täuschung beruhe (Griffith, 1971, S. 66). Jomini gewichtet die Täuschung besonders auf taktischer Ebene als bedeutender Kraftmultiplikator:

On réussira d'autant mieux dans ces entreprises (les manoeuvres) si l'on parvient à les cacher à l'ennemi jusqu'au moment de l'assaillir ([Jomini](#), 1994, S. 219).

Auf operativer Ebene meint [Liddell Hart](#) (1991), dass die Militärstrategie zum Ziel hat, den gegnerischen Widerstand zu verringern und zu lähmen, um so die Kampfhandlungen auf ein Mindestmass zu beschränken. Dies soll durch Täuschung und Ablenkung, durch Operationen in den Rücken des Gegners, durch Unterbrechen der gegnerischen Verbindungs- und Operationslinien sowie durch Aufsplitterung des Gegners erreicht werden.

Einerseits ermöglicht die Technologierevolution unter günstigen Bedingungen eine noch nie dagewesene Schlachtfeldtransparenz, andererseits bietet dieselbe Technologie die notwendige Chance, den Gegner auf eine noch kaum erreichte Qualität zu täuschen, so dass Überraschung auch auf dem modernen Schlachtfeld erzielt werden kann:

While many developments, particularly in surveillance technology, make the achievement of surprise by traditional means more difficult, as many others contribute towards the achievement of surprise, or at least can be exploited so to do.
(...)

In the light of the increased destructive power of modern forces, surprise is more important than ever.

The principal reason why surprise works is the fallibility of the human mind especially whilst under pressure. Whilst certain technological advances might help ease this problems, the vast majority of developments are actually adding to the difficulty by creating a 'data deluge' (Isbell, 1993, S. 162-163).

Wie aufgezeigt, umfasst das Konzept "Information Warfare" eine weite Bandbreite, die vom zwischenstaatlichen Krieg im Clausewitz'schen Verständnis als "Fortsetzung der Politik mit anderen Mitteln" ([Clausewitz](#), 1952, S. 108) d.h. mit physischer Gewalt, bis hin zum Interessenskonflikt ganz allgemeiner Natur reicht. Darin werden Staaten, sprich deren Streitkräfte, Non-Governmental Organizations (NGOs), Trans-National Corporations (TNCs), Trans-National Criminal Organizations (TCOs) (organisierte Kriminalität), Guerillakämpfer, Verbrecher und Terroristen sowie Abenteuer suchende Jugendliche als mögliche Akteure betrachtet. Dabei umfasst die Konfliktintensität ein

Spektrum, das von friedlicher Koexistenz, d.h. Wettbewerb und Konkurrenz, über Gewalt unterhalb der Kriegsschwelle (LIC) bis hin zum klassischen Krieg (HIC) reicht. Die zur Konfliktaustragung eingesetzten Mittel umfassen ein Arsenal, das vom Wort und Bild bis zum NEMP alles beinhaltet. Die Schwierigkeit den Urheber einer "Information Warfare" Attacke zu lokalisieren, ja selbst eine Attacke als solche zu erkennen, verwischt die Grenzen zwischen Krieg und Frieden, Kriminalität und Krieg sowie zwischen innerer und äusserer Sicherheit. Es liegt deshalb nahe, "Information Warfare" nicht mit dem eingeschränkten Begriff der Informationskriegführung zu übersetzen, sondern diesen auf die ganzheitliche Betrachtungsweise der Strategie von General Beaufre (vgl. Anhang 5.3.) auszuweiten:

...la stratégie ne doit pas être une doctrine unique, mais une *méthode de pensée* permettant de classer et de hiérarchiser les événements, puis de choisir les procédés les plus efficace (Beaufre, 1963, S. 11).

Indem Strategie als eine Denkmethode betrachtet wird, löst sie Beaufre von ihren ursprünglich kriegerischen Fesseln und weitet dieselbe in ihrer Anwendbarkeit auf jedes zwischenmenschliche Handeln aus.

Grundsätzlich definiert Beaufre Strategie als die Kunst der Dialektik des Willens, indem Macht zur Lösung des Konfliktes von Streitparteien verwendet wird (Beaufre, 1963, S. 16). Ziel der Strategie ist es, den Gegner davon zu überzeugen, dass es zwecklos sei, in einen Kampf einzutreten oder diesen weiterzuführen (Beaufre, 1963, S. 17). Die Entscheidung wird dann fallen, wenn man eine Situation geschaffen hat und diese als Gelegenheit ausnützt, in welcher die moralische Desintegration des Gegners soweit herbeigeführt worden ist, dass er zur Annahme unserer Bedingungen gezwungen werden kann (Beaufre, 1963, S. 18). In Sun Tzus Worten:

To subdue the enemy without fighting is the acme of skill.

Thus, what is of supreme importance in war is to attack the enemy's strategy (Griffith, 1971, S. 77).

Die Wahl der Mittel dazu hängt sowohl von der Verwundbarkeit des Gegners als auch von den eigenen Möglichkeiten ab. Beaufre unterscheidet dabei zwischen direkter und indirekter Strategie. Während direkte Strategie schwergewichtig militärische Mittel zur Zielerreichung einsetzt, benutzt die indirekte Strategie andere Mittel als militärische Gewalt: So z.B. Diplomatie, politische und wirtschaftliche Sanktionen aber auch einen revolutionärer Aufstand, um eine Intervention von aussen vorzubereiten oder um eine Regierung zu stürzen, sowie ein Guerillakrieg in Verbindung mit internationalen Aktionen (Beaufre, 1963, S. 19). Hier ist denn auch die Informationstechnologie-und mit dieser die Informatik-als zusätzlicher Machtfaktor neben Diplomatie, Wirtschaft, Kultur, Ideologie und Streitkräfte dazuzusetzen. Kurz, das Konzept "Information Warfare" beinhaltet also je nach Anwendungsart Elemente der indirekten wie auch der direkten Strategie.

3. Ein strategisches Modell

Dieses Kapitel soll dem Konzept "Information Warfare" eine inhaltlich hierarchische Ordnung geben, indem es in ein strategisches Modell eingebunden wird. Im folgenden soll "Information Warfare" in die Bereiche strategische, operative und taktische Ebene sowie in die Kategorien direkte und indirekte Strategie gegliedert werden.

3.1. Definitionen

Wie zuvor erwähnt, wird unter direkter Strategie nichts anderes als die Durchsetzung einer Absicht unter hauptsächlichem Einsatz resp. Androhung des Machtfaktors Streitkräfte verstanden.

Im Gegensatz dazu bezweckt die indirekte Strategie, den eigenen Willen unter schwergewichtigem Einsatz aller anderen Machtfaktoren durchzusetzen.

Unter indirektem Vorgehen versteht man eine Art des Einsatzes von Streitkräften auf ein Operationsziel hin. Der Einsatz bezweckt, den Gegner von einer unerwarteten Richtung anzugreifen, so dass die eigene Kräftekonzentration gegen den gegnerischen Schwachpunkt angesetzt werden kann. Indirektes Vorgehen gehört also zur direkten Strategie. Auf den Gegner hat das indirekte Vorgehen zwei Auswirkungen. Die eine liegt im psychologischen Bereich, die andere im physischen. Überraschung und Bewegung sollen den Gegner zuerst aus dem physischen wie auch aus dem psychischen Gleichgewicht bringen. Erst wenn die gegnerische Führung im Glaube der Aussichtslosigkeit gelähmt und erst wenn der gegnerische Widerstand dadurch maximal verringert ist, soll zum entscheidenden Schlag ausgeholt werden ([Liddell Hart](#), 1991).

Wenn hier von der strategischen Ebene einer (Kriegs-)Unternehmung gesprochen wird, so soll man alles dasjenige darunter verstehen, was sich einerseits in konzeptioneller, theoretischer Art und Weise mit der

Kriegführung (Interessenskonflikt) beschäftigt und andererseits alle Faktoren einer (Kriegs-)Unternehmung, die sich nicht durch das Resultat eines Zusammenstosses der Streitkräfte ergeben.

So schliesst die strategische Ebene die Politik und die Strategie im weiteren Sinne ein. Die Politik formuliert die Zielsetzung eines kriegerischen Unternehmens (resp. eines Interessenskonflikts). Die Strategie im weiteren Sinne formuliert im Rahmen der direkten und indirekten Strategie die strategische Vorgehensweise und bedient sich im Hinblick auf die Zielerreichung aller zur Verfügung stehenden Machtmittel wie Diplomatie, Wirtschaft, Kultur, Ideologie, Informationstechnologie, Informatik und Streitkräfte.

Die operative Ebene beinhaltet denjenigen Bereich, der sich mit der praktischen Umsetzung der Vorgaben der strategischen Ebene beschäftigt. Sie beinhaltet demnach die Strategie im engeren Sinne (Militärstrategie). Militärstrategie ist der Bereich der Armeespitze, welcher die Vorgaben der strategischen Ebene in operative Ziele für die Streitkräfte umformuliert. Dabei stimmt die Armeespitze die Zwischenziele und Einsatzarten auf die vorhandenen Mittel im Hinblick auf das Endziel ab.

Unter taktischer Ebene sollen alle Dinge subsumiert werden, die in die Sphäre des Gefechts fallen. Die taktische Ebene setzt die Zielsetzungen der operativen Stufe um, indem sie ihre Mittel im bestmöglichen Zusammenwirken auf dem Gefechtsfeld einsetzt.

Die operative Ebene übt also eine Scharnierfunktion zwischen strategischer und taktischer Ebene aus.

3.2. Ebenen des strategischen Denkens und Information Warfare

Werden die beschriebenen Mittel und Möglichkeiten von "Information Warfare" mit den Ebenen des strategischen Denkens in eine Tabelle vereint, so erhält man als Ergebnis die unten stehende Tabelle:

Tabelle 2: Inhaltlich hierarchische Ordnung von "Information Warfare"

Information Warfare					
Strategische Ebene	<p>❶ Politik: Zielvorgabe</p> <p>❷ Strategie im weiteren Sinne:</p> <ul style="list-style-type: none"> ⇒ Formulierung der strategischen Vorgehensweise, ⇒ Einsatz der zur Verfügung stehenden Machtmittel: <ul style="list-style-type: none"> ❶ Diplomatie ❷ Wirtschaft ❸ Kultur/Ideologie <i>Mittel:</i> PSYW (i, iv) ❹ Informationstechnologie/Informatik <i>Mittel:</i> Netwar (HW, EIW, CyberW) ❺ Streitkräfte 				
Operative Ebene	<p>❶ Strategie im engeren Sinne (Militärstrategie):</p> <ul style="list-style-type: none"> ⇒ Umformulierung von den Vorgaben der strategischen Ebene in operative Zielsetzungen, ⇒ Abstimmung der Zwischenziele, Mitteleinsatz und Vorgehensweisen im Einklang mit dem Endziel <p><i>Mittel:</i> Cyberwar (CyberW, PSYW (ii))</p>				
Taktische Ebene	<p>Sphäre des Kampfes und dessen Durchführung</p> <p><i>Mittel:</i> C²W, IBW, PSYW (iii), EW</p>				
Vorgehen	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; width: 50%;">offen</th> <th style="text-align: center; width: 50%;">verdeckt</th> </tr> </thead> <tbody> <tr> <td style="vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> • HW (destruktiv) • C²W • EW • CyberW • EIW (Sanktionen) • Dissuasion (Androhung massiver Vergeltung gegen die Informationsinfrastruktur) </td> <td style="vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> • HW (konstruktiv) • IBW • PSYW • CyberW </td> </tr> </tbody> </table>	offen	verdeckt	<ul style="list-style-type: none"> • HW (destruktiv) • C²W • EW • CyberW • EIW (Sanktionen) • Dissuasion (Androhung massiver Vergeltung gegen die Informationsinfrastruktur) 	<ul style="list-style-type: none"> • HW (konstruktiv) • IBW • PSYW • CyberW
offen	verdeckt				
<ul style="list-style-type: none"> • HW (destruktiv) • C²W • EW • CyberW • EIW (Sanktionen) • Dissuasion (Androhung massiver Vergeltung gegen die Informationsinfrastruktur) 	<ul style="list-style-type: none"> • HW (konstruktiv) • IBW • PSYW • CyberW 				

Als verdecktes Vorgehen sollen alle Handlungen im Bereich "Information Warfare" verstanden werden, die beabsichtigen, die Informationsinfrastruktur und Informationsprozesse unbemerkt zu seinen eigenen Gunsten auszunützen. Darunter können u.a. Massnahmen fallen, die darauf abzielen, Annahmen und Wissen der Gegenpartei mittels "Psychological Warfare" (PSYW) zu beeinflussen (Szafranski, 1996). Weiter sollen darunter auch Aktionen im Bereich "Hacker Warfare" (HW) gezählt werden, die als konstruktiv bezeichnet werden. Damit ist die Beschaffung von Geld, Informationen, Hard- und Software gemeint, ohne dass die Informationsinfrastruktur dadurch von

Ausfällen beeinträchtigt würde. Sympathisanten sowie Nachrichten und Aufklärungsergebnisse sollen mit "Psychological Warfare" (PSYW) bzw. mit "Intelligence based Warfare" (IBW) ebenfalls vom Gegner unbemerkt beschafft werden können. Auch alle defensive Massnahmen zum Schutz der eigenen Informationsinfrastruktur und der eigenen Informationsprozesse fallen in den Bereich des verdeckten Vorgehens, falls diese erfolgreich sein wollen.

Unter dem Begriff des offenen Vorgehens sollen alle Massnahmen verstanden werden, welche die Informationsinfrastruktur und Informationsprozesse zu stören beabsichtigen, so dass diese wegen Überlastung, hard- oder softwareinduzierte Systemausfälle oder gar wegen physischer Zerstörung aussetzen. Schon die Androhung solcher Massnahmen soll unter die Bezeichnung des offenen Vorgehens von "Information Warfare" fallen.

Auf strategischer Ebene wird abgewogen, ob resp. wie die Mittel von "Information Warfare" im Rahmen von "Netwar" zur Zielerreichung eingesetzt werden können. In der Form von "Netwar" findet man wahrscheinlich diejenige Möglichkeit, welche Sun Tzu als die höchste Vollkommenheit eines Strategen bezeichnet, nämlich indem dieser die Gegenpartei durch Angriff auf dessen Strategie überwindet (Griffith, 1971). Hier, wie auch auf operativer Ebene, gilt es im besonderen, die Mittel und Vorgehensweisen mit dem Endziel abzustimmen. Das Endziel darf dabei nie aus den Augen verloren gehen:

1. *Adjust your end to your means.* (...)
2. *Keep your object always in mind*, while adapting your plan to circumstances. Realize that there are more ways than one of gaining an object, but take heed that every objective should bear on the object ([Liddell Hart](#), 1991, S. 335).

Bei jeder Konfliktaustragung sollte der Zweck ein besserer Friede sein. Deshalb darf der Stratege auch im Krieg niemals den Blick für den erstrebten Frieden verlieren, wenn er seine Pläne schmiedet:

The object in war is a better state of peace — even if only from your own point of view. Hence it is essential to conduct war with constant regard to the peace you desire ([Liddell Hart](#), 1991, S. 338).

Das Besagte gilt es besonders dann zu berücksichtigen, wenn man sich zur Anwendung von "Netwar" entscheidet. Denn "Netwar" nimmt nicht nur Formen des totalen Krieges an, sondern ist in seiner Wirkung mit derjenigen eines Nuklearkrieges zu vergleichen (Stein, 1996, //.../chn6.html). Die Wirkung einer "Netwar"-Attacke ist in Kollateral- und Folgeschäden schwer einschätzbar. Dabei wird nicht zwischen Kombattanten und Zivilisten unterschieden. In einer zunehmend interdependenten Welt lässt sich zudem nicht ausschliessen, dass man selbst von Folgeschäden der eigenen "Netwar"-Offensive betroffen sein wird. So liegt ein weltweiter Börsencrash durchaus im Bereich des Möglichen, wenn man z.B. die Börse in Tokyo durch "Hacker Warfare" mit imaginären Devisentransaktionen überschwemmt. Die Folgekosten sind wie beim Nuklearwinter nach dem nuklearen Schlagabtausch kaum absehbar. So wirft "Netwar" gleich wie der Einsatz von Nuklearwaffen Fragen des Kriegsvölkerrechts auf. Neben den legalistischen Aspekten gesellt sich aber auch die Frage der Ethik. Dank der Informationsrevolution sind Angriffe im Bereich der Semantik und Epistemologie in einer noch nie dagewesenen Qualität möglich. So ist das Opfer eines "Netwars" von hoher Intensität letztlich die Wahrheit:

...the very possibility of "truth" is being replaced with "virtual reality"; that is, "information" which produces effects independent of its physical reality. What is being attacked in a strategic level netwar are not only the emotions, or motives, or beliefs of the target population, but the very power of objective reasoning. (...) The idea of "societal-level ideational conflict" may need to be considered with all the care given to the conduct of nuclear war, as the "end state" of netwar may not be bloodless surrender but total disruption of the targeted society. Victory may be too costly as the cost may be truth itself (Stein, 1996, //.../chn6.html).

In einer Konfliktaustragung ist aber nicht Chaos, sondern die Bewahrung der Kontrolle über die Geschehnisse das oberste Gebot. Dabei gilt

es, auf jede mögliche Handlung die Gegenreaktionen vorauszudenken, um dadurch die geeigneten Gegenmassnahmen zu entwickeln:

...il faut prévoir les réactions adverses possibles à chacune des actions envisagées et se donner la possibilité de parer chacune d'elles (Beaufre, 1963, S. 19).

Will man die Handlungsfreiheit in jeder Situation bewahren, ist dabei unter allen Umständen eine einzige Kausalkette zu vermeiden.

Ob die Androhung von "Netwar" ähnlich wie Atomwaffenarsenale eine Dissuasionswaffe auf strategischer Ebene sein kann, hängt von zwei Faktoren ab: Erstens muss die Wirkung von "Netwar" in ihrer Durchschlagskraft die Gegenseite so überzeugen, dass diese die Kosten einer möglichen Konfliktaustragung deutlich höher als irgendwelchen Nutzen daraus einschätzt. Zweitens muss der Gegenseite mittels einer glaubhaften Einsatzdoktrin bewusst gemacht werden, dass "Netwar" sie ab einer bestimmten Eskalationsstufe eines Konfliktes treffen würde. Neben einer Demonstrationswirkung in Form von Tests oder in Form eines Echteinsatzes, muss "Information Warfare" in eine glaubhafte Einsatzdoktrin gefasst werden, damit sie dissuasive Wirkung erzielt.

Neben dieser direkten Bedrohung besteht aber durchaus die Möglichkeit einer indirekten Bedrohung. Wenn im Landkrieg unter direkter Bedrohung die Besetzung resp. eine Androhung der Besetzung eines Landes, unter indirekter Bedrohung ein Durchmarsch resp. eine Androhung eines Durchmarsches durch ein Drittland zum Zwecke einer Besetzung des gegnerischen Territoriums verstanden wird, so soll im Bereich "Information Warfare" unter indirekter Bedrohung, das Ausnutzen der Informationsinfrastruktur und Informationsprozesse eines Drittlandes zum Zwecke von "Netwar" gegen die gegnerische Informationsinfrastruktur und Informationsprozesse verstanden werden. Staaten, die besonders von diesem Bedrohungsszenario eines Konfliktes betroffen sind, besitzen eine ausgezeichnete sowie vernetzte Informationsinfrastruktur,

die durch geringe defensive Massnahmen gekennzeichnet ist und dadurch grosse Sicherheitslücken aufweist.

Wie schon vorgängig vermerkt erweist sich das Erkennen einer "Netwar"-Attacke aus technischen Gründen als äusserst schwierig. Bestimmte Vorgehen auf operativer Stufe können diese Tatsache zusätzlich verstärken. Eine wagen Identifikation des Aggressors legt aber eine schlechte Basis zur Legitimation eines bewaffneten Vorgehens als mögliche Gegenreaktion auf eine "Netwar"-Attacke. Ein kollektives Vorgehen der Völkergemeinschaft via UNO ist wohl somit von vornherein ausschliessbar. Aber auch ein unilaterales Vorgehen wird kaum auf grosse Unterstützung seitens Alliierte treffen. Denn ein Alliiertes, wenn nicht schon selbst indirekt von den "Netwar"-Attacken betroffen, wird spätestens dann direkt Opfer von "Netwar", falls er die Pflichten der Allianz erfüllen sollte:

Difficulty of building and sustaining coalitions: Reliance on coalitions is likely to increase the vulnerabilities of the security postures of all the partners to strategic IW attacks (netwar), giving opponents a disproportionate strategic advantage (Molander, Riddile und Wilson, 1996, S. 3).

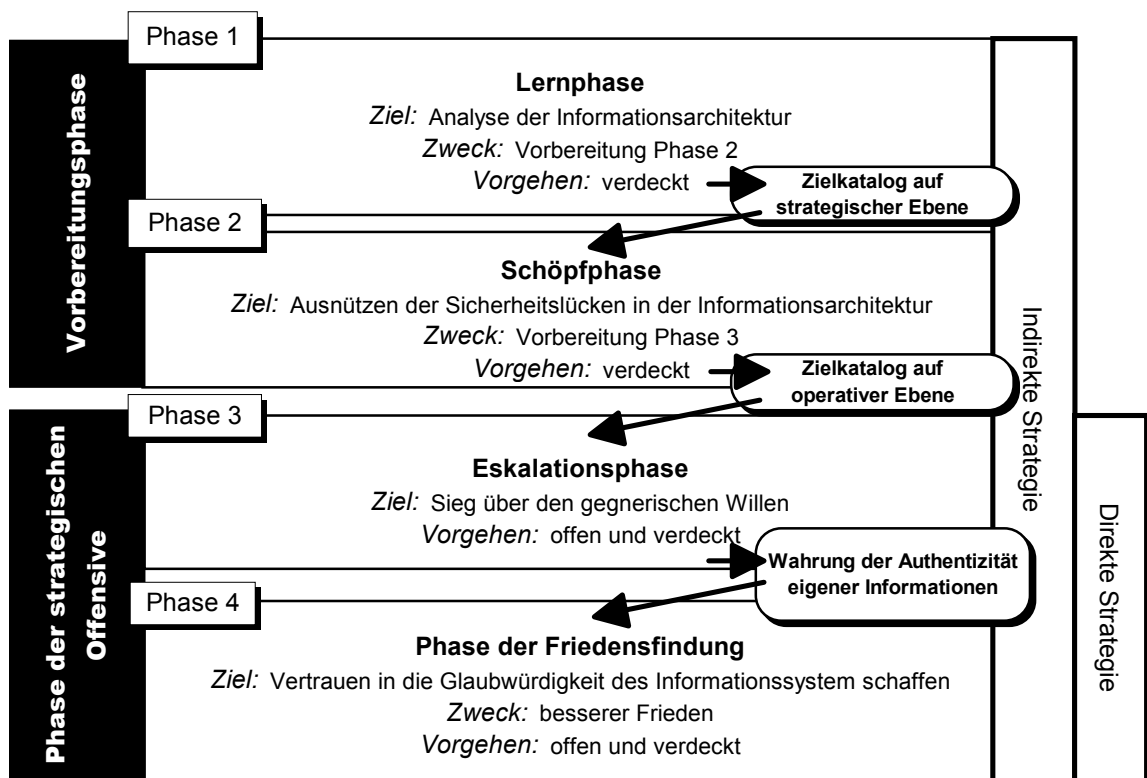
Auf operativer wie auf taktischer Ebene sollen die Mittel von "Information Warfare" nicht nur, wie dies bei "Command-and-Control Warfare" (C²W) bis anhin der Fall gewesen ist, als Kraftmultiplikatoren eingesetzt werden, sondern müssen zur vollständigen Verwirrung der gegnerischen Streitkräfte-im besonderen deren Führung-verwendet werden. So gilt es auf operativer und taktischer Ebene die Mittel von "Information Warfare" gezielt, konzentriert und in allen ihren Formen koordiniert gegen den Entscheidungszyklus der Gegenseite massiv einzusetzen. Nur so kann folgende von Jomini beschriebene Zielsetzung einer Schlacht erreicht werden: "...la première chose est de gagner la bataille sans chercher toujours la destruction totale de l'ennemi" ([Jomini](#), 1994, S. 376). Nicht die physische Vernichtung der gegnerischen Streitkräfte liegt im Vordergrund, sondern der Sieg über diese. Das ist

dann erreicht, sobald die Gegenseite den Willen zum Widerstand aufgegeben hat. Mit anderen Worten ausgedrückt, liegt der Sieg über einen Widersacher nicht im physischen, sondern vielmehr im psychologischen Bereich. Darin liegt der Grund, wieso das indirekte Vorgehen und die indirekte Strategie gerade im Zuge der erweiterten Möglichkeiten durch die Informationsrevolution neuen Impetus erhalten haben.

"Information Warfare" auf operativer Ebene durchbricht in der Kriegführung althergebrachte Vorstellungen von Raum und Zeit. Dank verdecktem Vorgehen können Kriegsvorbereitungen monatelang, ja über Jahre hinweg, unbemerkt durchgeführt werden. Taktische Vorausaktionen im Bereich "Hacker Warfare" wie das Implantieren von Trojanischen Pferden, Zeitbomben oder Bedingungsbomben lassen sich vorgängig ausführen. Die Wirkung dieser Implantate kann dann auf einen bestimmten Zeitpunkt, mit einer spezifischen Operation koordiniert, Monate später ausgelöst werden. In der räumlichen Dimension umfasst das potentielle Kriegstheater nicht mehr lediglich den Raum, in dem sich Antagonisten physisch angreifen können, also Operationstheater, Operationsbasis inkl. Verbindungslinien sowie im Zeitalter der Interkontinentalraketen den Heimatboden, sondern beinhaltet wegen der indirekten Bedrohung die ganze Welt inkl. Weltraum. Da Bits und Bytes praktisch zeitverzugslos überall hin verschoben werden können, liegt die Annahme nahe, dass im Bereich von "Netwar" das Ausnutzen der äusseren sowie konzentrischen Linien immer zum Vorteil gereichen wird. Denn diese Operationslinienwahl ermöglicht der offensiven Partei, die Gegenseite aus verschiedenen Richtungen gleichzeitig zu attackieren. So können denn auch die Spuren, die zum Aggressor hinführen könnten, zusätzlich verwischt werden, so dass die Identifikation desselben überaus schwierig sein dürfte.

3.3. Phasen der Dialektik des Willens

Tabelle 3: Phasenverlauf eines künftigen Konfliktes



Der Inhalt des Konzeptes "Information Warfare" umschrieben und in ein strategisches Gedankengebäude verarbeitet, steht es nun an, zu hinterfragen, welche Phasen die künftige Kriegsführung durchlaufen werde.

Wie in Tabelle 3 dargestellt, kann der Verlauf von "Information Warfare" in vier Phasen unterteilt werden: Erstens in eine Lernphase, zweitens in Schöpfphase, drittens in eine Eskalationsphase und schliesslich viertens in eine Phase der Friedensfindung resp. Deeskalation. Die ersten zwei Phasen sind dadurch gekennzeichnet, dass in diesen schwerewichtig verdeckt und mittels indirekter Strategie vorgegangen wird. Denn Lernphase und Schöpfphase bilden zusammen die eigentliche Vorbereitungsphase einer strategischen Offensive, die erst mit der Eskalationsphase eingeleitet wird.

In der Lernphase soll die Informationssystemarchitektur des Zielraumes, d.h die Architektur der gegnerischen Entscheidungsfindung, auf

strategischer, operativer und taktischer Ebene analysiert werden, so dass "Information Warfare" wirksam geführt werden kann:

The dependence of information warfare on the other side's architecture suggests that its effectiveness is only as good as ist intelligence on that architecture. (...) Information warfare waged without regard for the architecture of decisionmaking is no better than a shot in the dark (Libicki, 1996, [//.../a003ch11.html](#)).

Eine Informationsarchitektur umfasst nicht nur die physischen Elemente wie Sensoren und Empfänger mit deren technischen Spezifikationen sowie die Verbindung dieser Teile untereinander. Eine Informationssystemarchitektur beinhaltet auch Massnahmen, die ergriffen werden, damit die Authentizität von Information gewährleistet bleibt. Weiter erklärt die Informationssystemarchitektur, wie Daten zu Information werden und wie Information zu Entscheidung führt:

Architecture links information to decision: how readings are interpreted, what readings are correlated to one another, what constitutes recognition, where boundaries are set to eliminate false positives and false negatives, and under what circumstances sensor bit streams are given higher relative priority. Are data from heterogeneous streams melded to influence decision or to support them after the fact? The sensor-to-shooter complexes of tomorrow are but one channel; other channels include political direction, rules of engagement, and the status of one's own forces (Libicki, 1996, [//.../a003ch11.html](#)).

Eine Informationssystemarchitektur besteht also neben einer technischen Komponente aus einem komplexen, von der Kultur geprägten Element.

Der Zweck dieser Phase besteht also darin, die zweite Phase vorzubereiten, indem man analysiert, wie im Zielraum Meinungen, Werte, Ideen und Wissen zustande kommen und wie das Resultat an ein bestimmtes Zielpublikum am geeignetsten vermittelt wird. Neben der Analyse der Kultur, wird in der Lernphase eine eingehende Schwachpunktanalyse der Informationsinfrastruktur des Zielraumes einen weiteren Schwerpunkt darstellen. Diese Schwachpunktanalyse soll nicht nur Sicherheitslücken aufdecken, sondern gleichzeitig Daten wie Codewörter,

Identifikationsprotokolle elektronischer Datenübertragung, Lösungsschlüssel zum Dechiffrieren u.ä. zu deren Ausnützung aggregieren. Der Abschluss dieser Phase bilden Zielkataloge auf strategischer Ebene für den Einsatz der verschiedenen Mittel von "Information Warfare".

In der zweiten Phase können die in der Lernphase gesammelten Informationen zur Beschaffung von weiteren Informationen, von Geldmitteln sowie von Hard- und Software benutzt werden. In der Schöpfphase soll die eigene Position konsolidiert werden, indem ein ausgedehntes Organisationsnetz aufgebaut wird und die geeigneten Ausgangsbedingungen für die strategische Offensive geschaffen werden. Ziel dieser Phase ist neben der Konsolidierung, Zielkataloge auf operativer Ebene zusammenzustellen sowie den eigenen Zugriff auf authentische Informationen zu gewährleisten.

Je nach strategischer Zielsetzung eines Akteurs kann ein Konflikt über Jahre hinweg in der Schöpfphase verharren. So kann es durchaus sein, dass ein weniger entwickeltes Land oder TCO sich damit begnügt, lediglich von unbemerkt abgezweigten Finanzströmen aus dem Zielraum oder von der eigenen Macht über die Entscheidungsfindung der Gegenseite durch Manipulation zu profitieren.

Erst in der Eskalationsphase wird zum offenen Vorgehen sowie zur direkten Strategie übergegangen. Je nach beabsichtigter Konflikttintensität reicht diese strategische Offensive von Dissuasion durch Androhung von "Netwar", über Erpressung, Terrorismus bis hin zum offenen Krieg mittels "Cyberwar". Für diese Phase werden die während der Vorbereitungsphase vorgängig implantierten und zum Teil ausgetesteten Mechanismen zum Eindringen in das gegnerische Informationssystem koordiniert ausgelöst. Ziel der Eskalationsphase ist der Sieg des eigenen Willens über denjenigen der Gegenpartei. Nicht die Vernichtung des Gegners steht dabei im Vordergrund, sondern die Bewahrung der Authentizität der eigenen Informationbeschaffung und -verarbeitung.

In der Phase der Friedensschliessung gilt es, der Gegenpartei Vertrauen in die Glaubwürdigkeit in ihre eigenen Informationssysteme wieder zu

vermitteln. Der Aufwand dazu ist direkt von der Intensität und Vorgehensweisen von "Information Warfare" während der Eskalationsphase abhängig. Dies führt deutlich vor Augen, dass schon auf strategischer Ebene die Mittel und Vorgehensweisen im Hinblick auf die Zielerreichung, nämlich das Schaffen eines besseren Friedens, wohl überlegt sein muss.

4. Schlusswort

Unter dem Konzept "Information Warfare" darf nicht wie zu Beginn von dessen intellektuellen Durchleuchtung lediglich der Kraftmultiplikator "Command-and-Control Warfare" (C²W) verstanden werden, sondern es umfasst das ganzheitliche strategische Denken wie von Beaufre beschrieben. Je nach Einsatzart fallen die Mittel von "Information Warfare" in die direkte wie auch in die indirekte Strategie. Die Informationsrevolution eröffnet auch in einem Schlachtfeld, das durch wachsende Transparenz und Lagebewusstsein gekennzeichnet ist, neue Chancen der Täuschung. Dabei bildet der Entscheidungszyklus der Gegenseite in seiner Gesamtheit das Angriffsziel. Nicht nur Sensoren sollen getäuscht werden, sondern Datenverarbeitung und -übermittlung, ja die Wahrnehmung und das Beurteilungsvermögen des Gegners mittels Beeinträchtigung seiner althergebrachten Annahmen und seines tradierten Wissens. Das allgemein zugängliche Know-how sowie die dazugehörenden geringen Einstiegskosten eröffnen staatlichen und nicht-staatlichen Akteuren die Möglichkeit, "Information Warfare" zu führen. Durch "Information Warfare" sind kleine und grosse, mächtige wie auch schwache, wenig entwickelte sowie entwickelte Staaten (Akteure) gleich verwundbar. Dabei umfasst die Konfliktintensität sämtliche Eskalationsstufen, die vom Frieden bis zum Krieg reichen. "Netwar" wird auf strategischer Ebene geführt, wobei dessen Einsatzwirkung mit derjenigen eines Nuklearkrieges vergleichbar ist und somit ähnliche Fragen betreffend Dissuasion, Einsatzdoktrin, Ethik und Legalität aufwirft. Auf operativer Ebene wird "Cyberwar" als praktische Umsetzung von "Information Warfare" gesehen. Die Mittel, welche verdeckt oder offen eingesetzt werden, sind sowohl bei "Netwar" als auch bei "Cyberwar" dieselben, ihre Zielräume hingegen unterscheiden sich. "Netwar" wird schwergewichtig gegen eine Gesellschaft als ganze, "Cyberwar" schwergewichtig gegen Streitkräfte geführt. Wegen den technischen Möglichkeiten gepaart mit

geschicktem operativen Vorgehen, erweist sich die Identifikation des Aggressors in einem "Netwar" als ein äusserst schwieriges Unterfangen. Die strategische Offensive gericht dem Aggressor nicht nur aus diesem Grund zum Vorteil, sondern auch weil sich eine kollektive Massnahme oder eine Koalition gegen diesen kaum einleiten resp. formen, geschweige denn nachhaltig unterhalten lässt.

Auf der Seite der Organisationsform verflacht die Informationsrevolution Hierarchien, weil Informationen allen Hierarchiestufen gleichzeitig zur Verfügung stehen. So werden sich Organisationsnetzwerke durch ihre Interoperabilität, Flexibilität, Redundanz und Dezentralisation gegenüber starren Hierarchien, welche leicht durch Guillotinieren (Ausschaltung der Führung) oder Strangulation (Unterbrechen der Verbindung der Führung mit deren Unterstellten) zu neutralisieren sind, durchsetzen.

Die künftige Konfliktaustragung lässt sich in vier Phasen unterteilen. Die Lern- und die Schöpfphase dienen zur Vorbereitung der Eskalationsphase, die durch ihre Anwendung von "Information Warfare" und deren Intensität direkt die abschliessende Phase, die der Friedensfindung, beeinflusst.

Die gute aber moderat geschützte Informationsinfrastruktur macht die Schweiz in Kombination mit ihrer aussenwirtschaftlichen Verstrickungen besonders im Banken- und Versicherungsbereich zu einem natürlichen Ziel für verdeckte "Hacker Warfare". Ebenfalls ist die indirekte Bedrohung durch "Information Warfare" für die Schweiz nicht zu unterschätzen.

Die Konsequenzen aus der Informationsrevolution und aus "Information Warfare" sind nun auf strategischer, operativer und taktischer Ebene umzusetzen. Eine Anpassung der Organisationsstrukturen der Streitkräfte wird dabei eine der notwendigen Umsetzungen dieser Konsequenzen darstellen. Ausbildung und Erziehung der Soldaten, insbesondere der Führungskräfte, müssen ebenfalls den neuen Anforderungen genügen. Sammeln und Verwerten authentischer Informationen wird die

prominente Rolle in Konflikten einnehmen. Dabei erhalten die Nachrichtendienste schon in Friedenszeiten eine neue, gewichtigere Bedeutung.

"Information Warfare" verdeutlicht, dass die Grenzen zwischen Krieg und Frieden nicht klar zu ziehen sind. Das Leben stellt vielmehr einen ununterbrochenen Interessenskonflikt dar. Die Interessenskonflikte unterscheiden sich lediglich in den Mitteln ihrer Austragung, wobei auch diese im Bereich "Information Warfare" dieselben sind. Der Krieg unterscheidet sich von anderen Interessenskonflikten durch die *bewusste* Inkaufnahme des Tötens und des Getötetwerdens zur Verteidigung bestimmter Werten und Normen.

Eine Architekturanalyse des schweizerischen Informationssystems muss Gegenstand einer nachfolgenden Untersuchung sein. Denn nur so kann sich die Schweiz vor "Information Warfare" effektiv schützen und ihre Interessen erfolgreich verfolgen:

Therefore I (Sun Tzu) say: 'Know the enemy and know yourself; in a hundred battles you will never be in peril' (Griffith, 1971, S. 84).

5. Anhang

Tabelle 5.1.: Ursachen unbeabsichtigter Computerausfälle

1. Fehlmanipulationen
2. Stromausfall
3. Kabelbruch (ein Glasfaserkabel kann ca. 375'000 Telephonate übertragen)
4. Feuer, Staub, Asche und Rauch
5. Wasserschaden
6. Erdbeben
7. Solarstrahlung
8. Gewitter, statische Elektrizität
9. Verschieben von Computer
10. Systemunterhalt und ungenügender Unterhalt
11. Austesten des Systems auf Sicherheitslücken
12. Feuchtigkeit
13. Gase, Dämpfe und chemische Reinigungsmittel
14. Systemüberhitzung und Deformationen durch Temperaturschwankungen, Ausfall von Klimaanlage
15. Vibrationen
16. Korrosion

Quelle: Cohen, 1995, S. 33-40.

Tabelle 5.2.: Ursachen beabsichtigter Computerausfälle

Mittel	Vorgehen/Effekt
1. Trojan horses	Unter einem Trojanischen Pferd versteht man einen Nebeneffekt bei Software (z.B. von Gratis-Update-Disketten) oder Hardware (Chipping, Back doors), der es erlaubt, den Zugang zu Dienstleistungen zu verwehren, Informationen zu verfälschen oder klassifizierte Informationen durchsickern zu lassen.
2. Time bombs	Wie ihr physisches Gegenstück, setzt die Wirkung einer Zeitbombe auf einen vorbestimmten Zeitpunkt ein. Eine Softwarezeitbombe kann z.B. versuchen, sämtliche Dateien zu löschen. Eine Hardwarezeitbombe kann den Ausfall einer Systemkomponente hervorrufen.
3. Use or condition bombs	Ist der Zeitbombe ähnlich, nur dass die Bedingungs-bombe durch die Erfüllung einer vorbestimmte Bedingung initiiert wird. So z.B. durch eine bestimmte Ausführungsanzahl eines Befehls.

Tabelle 5.2.: Ursachen beabsichtigter Computerausfälle (Fortsetzung)

Mittel	Vorgehen/Effekt
4. Dumpster diving	Darunter wird das Durchstöbern von Abfall verstanden. Denn oft befinden sich im Abfall alte Disketten, deren Daten für die Vorbereitung einer Hackerattacke nützlich sein können.
5. Fictitious people	Fiktive Namen werden für das Benutzen von Dienstleistungen verwendet. Ebenfalls können durch eine Anhäufung von fiktiven Interessensvertreter Trends ausgelöst werden.
6. Protection limit poking	Beim Erreichen einer gewissen Anzahl von Versuchen ein Passwort einzugeben, verwehren gewisse Systeme jegliche Dienstleistung, so dass es zu ihrer Wiederherstellung aus- und wieder angeschaltet werden muss.
7. E-mail overflow	Elektronische Post wird dazu benutzt, Computersysteme mit Information zu blockieren, so dass diese für andere Zwecke im gleichen Zeitraum nur beschränkt verwendet werden können.
8. Infrastructure interference	Indem Signale zu Satelliten oder an Richtstrahlantennen gesendet werden, können Signale der öffentlichen Informationsinfrastruktur gestört und unterbrochen werden.
9. Infrastructure observation	Abhören von Radiosignalen und Richtstrahlantennensignale.
10. Sympathetic vibration	Durch gegenseitiges automatisches "Packet Feedback" wird ein Netzwerk überlasten und so Dienstleistungen unterbrochen.
11. Human engineering	Anwendung der Überzeugungskunst, um von Mitarbeiter berechtigten Zugang für eine Dienstleistung zu erhalten.
12. Bribes	Bestechung
13. Get a job	Infiltration in eine Organisation als angestellter Mitarbeiter
14. Password guessing	Erraten von Passwörtern
15. Computer viruses	Computerviren sind Programme, die sich reproduzieren. In diesem Prozess befallen sie laufend weitere Programme, was schliesslich zum Ausfall von Dienstleistungen führt.
16. Data diddelling	Daten, die unberechtigterweise verändert werden.
17. Packet insertion	IP (Identifikationsprotokoll) Pakete werden gefälscht, so dass sie den Anschein erwecken, von einer anderen berechtigten Adresse her zu stammen.
18. Packet watching	IP Pakete werden isoliert, um die Kommunikation zwischen Computer-Terminals zu verfolgen und so Benutzeridentifikationen und Passwörter in Erfahrung zu bringen.
19. Van Eck bugging	Möglichkeit, die von Bildschirmen stammende elektromagnetische Strahlung aufzufangen und wiederzugeben.

Tabelle 5.2.: Ursachen beabsichtigter Computerausfälle (Fortsetzung)

Mittel	Vorgehen/Effekt
20. Electronic interference	Elektronische Interferenz
21. Open microphone listening and Video viewing	Multimediageräte können über das Netzwerk so programmiert werden, dass deren Videokameras oder Mikrophone auch im scheinbar ausgeschalteten Status in Betrieb bleiben. So können Gespräche abgehört und Räume beobachtet werden. Ebenfalls können so Eingaben auf der Computertastatur mitverfolgt werden.
22. Repair, replace, and remove information	Einige Computerreparaturwerkstätten verwenden für kaputte Disketten alte, gebrauchte als Ersatzmaterial. Andere entwenden Information, bevor sie die Disketten neu formatieren.
23. Wire closet attacks	Schaltkästen von Informationssystemen oder zur Stromversorgung sind oft einfacher zugänglich als andere Bereiche. Hat man sich einmal Zugang verschafft, können Kabel zerschnitten, angezapft, anders oder miteinander verkabelt werden.
24. Shoulder surfing	Jemanden beim Eintippen von Passwörtern oder PIN-Codes beobachten, um diese dann selbst zu benutzen.
25. Data aggregation	Durch Datenaggregation zu vertraulichen Informationen gelangen.
26. Backup theft	Entwenden von Disketten-Backups
27. Login spoofing	Techniken, um Login-Einträge zu sammeln
28. Hangup hooking	Benutzen einer fremder Telefonverbindung, indem während des Prozesses des Aufhängens eines Modems, die fremde Verbindung von einem selbst übernommen wird.
29. E-mail spoofing	Verändern von elektronischer Postmitteilungen
30. Combined attacks	Die verschiedenen Techniken können miteinander kombiniert werden, um den gewünschten Effekt zu erzielen.

Quelle: Cohen, 1995, S. 40-54.

5.3. Das strategische Denken Beaufres im Überblick

Strategische Ebene	<p>❶ Politik: Zielvorgabe</p> <p>❷ Stratégie Totale: Zweck</p> <ul style="list-style-type: none"> • Erteilt den Auftrag und bestimmt die Zielsetzungen der Stratégie Générale der folgenden Sparten: <ol style="list-style-type: none"> 1. Politik 2. Wirtschaft 3. Diplomatie 4. Armee <p>❸ Stratégie Générale: Zweck</p> <ul style="list-style-type: none"> • Gruppierung und Verteilung der Aufgaben zu den entsprechenden Zweigen innerhalb der Sparte <p>❹ Stratégie Opérationelle: Zweck</p> <ol style="list-style-type: none"> 1. Abstimmung und Entwicklung der Taktik und Technik im Hinblick auf die Stratégie Générale. 2. Abstimmung der Stratégie Générale im Hinblick auf die gegebenen, aber vor allem auch auf die zukünftigen taktischen und technischen Möglichkeiten. <p>Strategie Die Strategie ist die Kunst der Dialektik des Willens, Macht zur Lösung eines Konfliktes anwendend.</p> <p>Zweck</p> <ul style="list-style-type: none"> • Die Entscheidung herbeiführen, indem man eine Situation schafft und diese als Gelegenheit ausnützt, in welcher die moralische Desintegration des Gegners soweit herbeigeführt worden ist, dass dieser zur Annahme von Bedingungen gezwungen werden kann.
Vorgehen	<p>❶ Direkte Strategie:</p> <ul style="list-style-type: none"> • Die Armee ist zur Herbeiführung der Entscheidung mit Schwergewicht eingesetzte Mittel. ⇒ beinhaltet die Ansätze von Clausewitz und Liddell Hart. <p>❷ Indirekte Strategie:</p> <ul style="list-style-type: none"> • Die Indirekte Strategie wird überall dort eingesetzt, wo die Konfliktlösung nicht direkt durch einen militärischen Zusammenstoß gesucht wird, sondern durch einen möglichst indirekten Prozess: <ul style="list-style-type: none"> → politisch (psychologisch) → wirtschaftlich → oder durch aufeinander folgenden militärischen Aktionen, die jedoch durch Gespräche und Verhandlungen unterbrochen und vorbereitet werden ⇒ Salamtaktik <div style="text-align: center; margin: 10px 0;"> $S = K * F * \psi * t$ </div> <p style="text-align: right; margin-right: 50px;">K = Faktor des spez. Umstandes F = materielle Macht ψ = moralische Macht</p> <p>Diese zwei Arten der Strategie schliessen einander nicht aus, sondern sind komplementär; sie harmonisieren im Zusammenspiel.</p> <p>2 Maximen:</p> <ol style="list-style-type: none"> 1. Wahre die Handlungsfreiheit, indem du jede mögliche gegnerische Reaktion auf deine Handlung vorausszusehen versuchst und eine geeignete Gegenreaktion ausarbeitest. 2. Ökonomie der Kräfte

(Beaufre, 1963)

6. Literaturverzeichnis

- Adams, J. (1995). Dawn of the Cyber Soldiers. The Sunday Times, 15. Oktober.
- Alberts, D. S. The Unintended Consequences of Information Age Technologies. <[http:// www .ndu. edu/ ndu/ inss/ books/ uc/ uhome.html](http://www.ndu.edu/ndu/inss/books/uc/uchome.html)>. Oktober 1996.
- Altermatt, U. (1996). Von der Ethnisierung der Politik. Neue Zürcher Zeitung, Nr. 208, 17.
- Arquilla, J. und Ronfeldt, D. (1993). Cyberwar is Coming!. Comparative Strategy, 12, 141-165.
- Arquilla, J. und Ronfeldt, D. (1996). The Advent of Netwar. Santa Monica: RAND.
- Beaufre, A. (1963). Introduction à la stratégie. Paris: Librairie Armand Colin.
- Buchan, G. Information War and the Air Force: Wave of the Future? Current Fad?. <<http://www.rand.org/publications/IP/IP149/#fn1>>. März 1996.
- Burkert, W. (1972). Homo Necans. Berlin: Walter de Gruyter.
- Cairncross, F. (1996). Das Ende der Distanz. NZZ Folio, Nr. 2, 42-47.
- Calvo, M. D. (1996). Digitizing the Force XXI Battlefield. Military Review, Mai-Juni, 68-73.
- Campen, A. D. (1992). Iraqi Command and Control: The Information Differential. In A. D. Campen (Hrsg.), The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War. (S. 171-177). Virginia: AFCEA International Press.
- [Clausewitz von](#), C. (1952). Vom Kriege (16. Auflage). Bonn: Dümmlers Verlag.
- Cohen, F. B. (1995). Protection and Security on the Information Superhighway. New York: John Wiley & Sons.

- Economist (1995). The Softwar Revolution. A Survey of Defence Technology, 10. Juni.
- Elliott, C. L. (1993). The Impact of the Media on the Prosecution of Contemporary Warfare. In B. H. Reid (Hrsg.), The Science of War: Back to First Principles (S. 164-191). London: Routledge.
- Goodell, J. (1996). The Cyberthief and the Samurai. New York: Dell Publishing.
- Graf, C. (1996). IP Packet Filters in SWITCHlan. SWITCHjournal, Nr. 1, 9-10.
- Griffith, S. B. (1971). Sun Tzu- The Art of War. London: Oxford University Press.
- Griffith, S.B. (1978). Mao Tse Tung- On Guerrilla Warfare. New York: Anchor Press.
- Gut, J. (1993). Nukleare elektromagnetische Impulse und Mikrowellenwaffen: Lautlose Schläge. Miliz, 10, 24-29.
- Gut, J. (1987). Ein NEMP-Schutzkonzept für die Gesamtverteidigung. Technische Rundschau, 8, 84-85.
- Huber, W. (1996). IP Spoofing Attacke und deren Abwehr. SWITCHjournal, 1, 11-13.
- IASIW (Institute for the Advanced Study of Information Warfare). What is Information Warfare. <<http://www.seas.gwu.edu/student/retoinfowar/what.html>>. Oktober 1996.
- Isbell, B. R. (1993). The Future of Surprise on the Transparent Battlefield. In B. H. Reid (Hrsg.), The Science of War: Back to First Principles (S. 149-163). London: Routledge.
- Jomini, A. H. (1994). Précis de l'art de la guerre. Paris: Edition Ivrea.
- Kitson, F. (1991). Low Intensity Operations: Subversion, Insurgency, Peace-keeping. London: Farber and Farber.
- Libicki, M. C. Defending the National Information Infrastructure. <<http://www.ndu.edu/ndu/inss/actpubs/niitemp.html>>. Oktober 1996.
- Libicki, M. C. What is Information Warfare. <<http://www.ndu.edu/ndu/inss/actpubs/act003/a003ch00.html>>. Oktober 1996.

- [Liddell Hart](#), B. H. (1991). Strategy. New York: Meridian.
- Lubich, H. P. (1996). Security Problems and Countermeasures in the Current Internet. SWITCHjournal, 1, 4-7.
- Magsig, D. E. Information Warfare in the Information Age. <[http:// www.seas.gwu.edu/ student/ dmagsig/ infowar. html](http://www.seas.gwu.edu/student/dmagsig/infowar.html)>. Dezember 1995.
- Manthorpe, W. H. J. Jr. (1996). From the Editor. In W. H. J. Manthorpe Jr. (Hrsg.), Information Warfare. (S. 3-12). Defense Intelligence Journal, Vol.5, Nr. 1.
- Menoher, P. E. Jr. (1992). Responsive Communications Key to Army Intelligence. In A. D. Campen (Hrsg.), The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War. (S. 71-74). Virginia: AFCEA International Press.
- Molander, R. C., Riddile, A. S. und Wilson, P. A. Strategic Information Warfare: A New Face of War. <[http://www.rand.org./publications/MR/MR661/MR661.html](http://www.rand.org/publications/MR/MR661/MR661.html)>. Oktober 1996.
- Nichiporuk, B. und Builder, C. H. (1995). Information Technologies and the Future of Land Warfare. Santa Monica: RAND.
- Niefong, M. R. (1996). The Key to Information Dominance. Military Review, Mai-Juni, 62-67.
- O'Connell, R. L. (1989). Of Arms and Men: A History of War, Weapons and Agression. Oxford: Oxford University Press.
- Riccardelli, R. F. (1995). The Information and Intelligence Revolution. Military Review, September- Oktober, 82-87.
- Rona, T. P. (1996). Information Warfare: An age-old Concept with new Insights. In W. H. J. Manthrope Jr. (Hrsg.), Defense Intelligence Journal, Vol. 5, Nr. 1, 53-67.
- Schoch, C. (1996). Ausfall sämtlicher Bancomaten der Schweiz. Neue Zürcher Zeitung, Nr. 105, 20.
- Schweizerische Armee (1994). Reglement 51.20 d Taktische Führung 95.
- Stahel, A. A. (1993). Luftverteidigung- Strategie und Wirklichkeit. Zürich: Verlag der Fachvereine.

- Steiger, R. (1990). Lehrbuch der Diskussionstechnik. Frauenfeld: Huber Verlag.
- Stein, G. J. Information War- Cyberwar- Netwar. <<http://www.cdsar.af.mil/battle/chp6.html>>. Oktober 1996.
- Stein, G. J. Information Warfare. <<http://www.cdsar.af.mil/apj/stein.html>>. Oktober 1996.
- Stix, G. (1995). Fighting Future Wars. Scientific American, Dezember, 74-80.
- Summers, M. G. (1995). The New World Strategy. New York: Touchstone.
- Szafranski, R. A Theory of Information Warfare- Preparing for 2020. <<http://www.cdsar.af.mil/apj/szfran.html>>. Oktober 1996.
- Thomson, M. (1995). Plotting a War Game. Time International, 21. Oktober, 32-34.
- Toffler, A. und Toffler, H. (1993). War and Anti-War: Survival at the Dawn of the 21st Century. London: Little Brown.
- Toma, J. S. (1992). Desert Storm Communications. In A. D. Campen (Hrsg.), The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War. (S. 1-5). Virginia: AFCEA International Press.
- United States General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. <<http://www.fas.org/irp/gao/aim96084.html>>. Oktober 1996.
- Van Creveld, M. (1991). On Future War. London: Brassey's.
- Waller, D. (1995). Onward Cyber Soldiers. Time International, 21. Oktober, 26-32.
- Wenger, A. und Köppel, T. Die Auswirkung der Informationsrevolution auf die schweizerische Aussen- und Sicherheitspolitik: Chancen und Risiken. <http://www.fsk.ethz.ch/publ/bulletin/bull_95/b95_ir.html>. Dezember 1995.
- Zeller, R. (1996). Geständnisse im Fall Armee-Überwachungssystem. Neue Zürcher Zeitung, Nr. 46, 13.

EHRENWORT

Hiermit erkläre ich, dass die Diplomarbeit von mir selbst ohne unerlaubte Beihilfe verfasst worden ist.

8118 Pfaffhausen, 1996

Christoph M. V. Abegglen