FAKULTÄT FÜR !INFORMATIK

Der Informationskrieg im 21.Jahrhundert und seine Auswirkungen auf die Militärdoktrinen der USA

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Informatik (881)

eingereicht von

Christian Meurers
Matrikelnummer 9726360

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer: Ao.Univ.Prof. Dr. phil. Wolfgang Hofkirchner

Wien, 28.10.2008

_____ _____

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

Für meinen Großvater

"Da draußen tobt ein Krieg, alter Freund! Ein Weltkrieg! Und es geht nicht darum, wer die meiste Munition hat… Es geht darum: Wer kontrolliert die Informationen? Was wir sehen und hören… Wie wir arbeiten… Was wir denken… Es geht alles nur um die Informationen!"
(Ben Kingsley, SNEAKERS, Die Lautlosen)

Danksagung

An dieser Stelle möchte ich mich besonders bei meinen Eltern Margit und Bernhard Meurers bedanken, die mir mein Studium durch ihre Unterstützung und Motivation ermöglicht haben.

Weiters bedanke ich mich bei Hr. Ao.Univ.Prof. Dr. phil. Wolfgang Hofkirchner, der mich im Zuge dieser Arbeit betreut und auf den richtigen Weg geführt hat, sowie stellvertretend für alle Kollegen bei meinem Vater Obst Mag. phil. Bernhard Meurers und Hr. Mjr. Ing. Robert Schwimmer, die mir mit ihrer konstruktiven Kritik immer wieder Ideen und Denkanstösse in militärischen Belangen lieferten. Mein weiterer Dank gilt Hr. Mag. phil. Paul Ertl, der Militärbibliothek des Österreichischen Bundesheeres und der Landesverteidigungsakademie für ihre freundliche Unterstützung und den Zugriff auf ihre Archive.

Diese Arbeit widme ich meinem Großvater Emil Doujak, der die Fertigstellung und den Abschluss meines Studiums leider nicht mehr miterleben konnte.

Inhaltsverzeichnis

Einleitung

Die Geschichte der Menschheit ist auch eine Geschichte ihrer Kriege. Durch alle Zeitalter hindurch spiegelten sich Wesen und Struktur einer Gesellschaft in ihren Konflikten wider. Spätestens seit dem Beginn der industriellen Revolution und der damit verbundenen Industrialisierung des Krieges ist der Krieg selbst, bedingt durch die damit verbundene Letalität und Endgültigkeit zu einem Machtinstrument geworden, das in der modernen Gesellschaft längst nicht mehr als letztes Mittel zum Erreichen eigener Ziele gesehen wird.

Dennoch ist aber gerade in den letzten Jahren die Hemmschwelle zum Waffeneinsatz deutlich geschwunden, wie uns die jüngsten Konflikte im Irak und Afghanistan zeigen. Längst haben wirtschaftliche Interessen wie Öl und Kohle die Urängste der Gesellschaft wie eigenes Überleben oder Schaffung von Lebensraum als Kriegsgrund abgelöst, und man möchte fast meinen, der Einsatz von Waffen würde als obligates Mittel zur Erreichung von solchen Zielen angesehen.

Transformation und Vernetzung

Die Wechselwirkung zwischen Militär und Zivilgesellschaft hat in den letzten Jahrzehnten nicht nur ihren Höhepunkt genommen, gerade am militärischen Sektor ist eine Anpassung der Strukturen und Hierarchien an die zivilen Entwicklungen in immer schnellerem Ausmaß sichtbar. Nahezu jede Armee der führenden Nationen befindet sich heute in einer Transformationsphase, in der der Entwicklung der Gesellschaft, dem daraus resultierenden Bedrohungsbild in Hinsicht auf konventionelle und neue, asymmetrische Konfliktformen sowie den sich bietenden technologischen Möglichkeiten Rechnung getragen wird. Der Weg hin zu einer Informationsgesellschaft, wie sie Gesellschaftstheoretiker wie Bell und Toffler[1] sehen, findet ihre Ausprägung auch im Militär und seinen Doktrinen.

So spricht beispielsweise der Präsident der Clausewitz-Gesellschaft, General a.D. Dr. Klaus Reinhardt in Zusammenhang mit der Transformation der deutschen Streitkräfte von einem *„signifikanten Umdenken mit dem Ziel, die Fähigkeiten der Bundeswehr auf die Auftragslage hin neu zu orientieren und sie mit dem Gesamtbegriff Network Centric Warfare (NCW)[2] miteinander zu verknüpfen, um mit den vorhandenen Plattformen durch engere Vernetzung mehr Leistung zu erzielen.“*[3]

Laut dem Militärattaché der deutschen Luftwaffe in London, Brigadegeneral DKfm Rüdiger Heeg, spiegelt sich *„der gesellschaftliche Wandel vom Industrie- in das Informations- und Wissenszeitalter(…) auch in der Kriegführung wider. Der klassische Faktor »Kräfte« verliere zunehmend an Bedeutung, während Zeit und Information bei der heutigen Projektion von Macht in den Vordergrund des Interesses rückten. NCW sei aber mehr als die reine Theorie von Netzwerken, betonte Heeg, es sei vielmehr ein Führungs- und Organisationsprinzip, eine Philosophie der zukünftigen Kriegführung im speziellen und der Machtentfaltung im Allgemeinen. (…)*
NCW umfasse ganzheitliche Veränderungen für Führungsprozesse, Aufbau- und Ablauforganisation und Technologie, für Operationsführung, Ressort übergreifendes

[1] Vgl: Toffler, Alvin; Toffler, Heidi; Überleben im 21.Jhdt; Übersetzt aus dem Amerikanischen „War and Anti-War“ von Helmut Dierlamm et al. Deutsche Verlags Anstalt, 1994
[2] NCW: Network Centric Warfare; Konzept zur vernetzten Operationsführung, vgl Kapitel 5;
Network Centric Warfare kann als ein zentrales Konzept des Informationskrieges gesehen werden
[3] Zeitschrift „Europäische Sicherheit“ Heft 2/2004, Artikel „Forum 2003 der Clausewitz-Gesellschaft“, S60ff

Handeln, Führungskultur und Führungsverhalten. Am Beispiel Führungskultur gezeigt, heiße das, dass die neuen Fähigkeiten nicht nur einfach eine Verbesserung des alten Modells seien, sondern vielmehr neue Denkweisen, eine Potenzierung des bisherigen linearen Informationsmodells und eine Gelegenheit, neuartige flexible Führungsverfahren umzusetzen."[4]

Daraus lässt sich ableiten, worum es bei der Transformation der Streitkräfte und abstrahiert auch zumindest im militärischen Teil des Informationskriegs[5] eigentlich geht, nämlich um eine Änderung des „Denkens", der Doktrin im Zusammenhang mit dem Prozess der Führung unter Einbindung von technologischen Entwicklungen. Diese drei Faktoren befinden sich im gegenseitigen Wechselspiel, denn der Einfluss der Technik findet seinen Niederschlag in den Doktrinen, die wiederum eine Grundlage der Führung darstellen. Umgekehrt passt sich aber gerade die Führung in ihrem Bestreben Führungsüberlegenheit zu erlangen immer mehr den technischen Möglichkeiten an und nimmt so wieder Einfluss auf die Doktrin. Strukturelle Änderungen sowie Auswirkungen auf die Organisation der Streitkräfte resultieren als Begleiterscheinungen aus diesen Zusammenhängen.

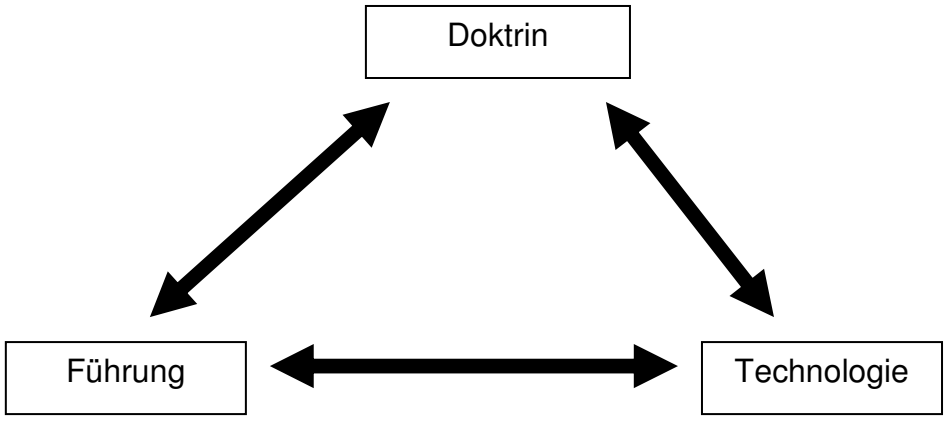


Abbildung 1: Zusammenhang Führung, Doktrin, Technologie; Eigene Darstellung

Doktrin! Technologie! Führung?

Gerade die Beziehung zwischen Doktrin und Technologie ist im Rahmen der Transformation der Streitkräfte in den Fokus der Betrachtung gerückt. So schreibt das Fachjournal „Air Power Revue" der Schweizer Armee: „*Doktrin und Technologie stehen in so engem Zusammenhang, dass man sie als Geschwister betrachten kann."* Und weiter: „*Eine Überlegenheit in Doktrin und Technologie hat eine multiplizierende Wirkung auf den Einsatz der Streitkräfte."*[6] Gleichzeitig aber stellt das Magazin auch fest, dass zwar ein gleichzeitiger Entwicklungsschritt dieser Faktoren eine Revolution auslöst, aber das „*Ungleichgewicht zwischen doktrineller und technologischer Entwicklung*"[7] eher die Regel als die Ausnahme

[4] Heeg, Rüdiger, Zeitschrift „Europäische Sicherheit" Heft 2/2004, Artikel „Forum 2003 der Clausewitz-Gesellschaft", S60ff
[5] Alle anderen Formen des Informationskriegs, der sich auf allen Ebenen der Gesellschaft abspielen kann, bleiben davon unberührt. Kapitel 3 beschäftigt sich näher mit diesem Thema.
[6] Artikel „Doktrin und Technologie: Zwillings- oder Halbschwestern" in Zeitschrift Air Power Revue der Schweizer Armee Nr.3, Beilage zur Allgemeinen Schweizerischen Militärzeitschrift ASMZ 12/2004, S.5
[7] Artikel „Doktrin und Technologie: Zwillings- oder Halbschwestern" in Zeitschrift Air Power Revue der Schweizer Armee Nr.3, Beilage zur Allgemeinen Schweizerischen Militärzeitschrift ASMZ 12/2004, S14

darstellt. Erst mit den laufenden Transformationsprozessen versucht man die Entwicklung dieser Faktoren bewusst zu steuern und so die symbiotischen Effekte zu maximieren.

Ich bin allerdings der Meinung, dass in die Gleichung Doktrin und Technologie auch die Führung als Variable einzubringen ist. Laut Krepinevitch[8] zeichnet sich eine Weiterentwicklung am militärischen Sektor unter anderem an einer Anpassung der Organisation und einer Änderung des Streitkräftesystems aus. Nun ist aber gerade die Führung bzw. das Führungssystem wesentliche Grundlage der militärischen Organisation bzw. des Streitkräftesystems im Allgemeinen und jeder Entwicklungsschritt der Faktoren Doktrin und Technologie, ob im Rahmen der Transformation oder außerhalb dessen, findet seine Ausprägung im Versuch des Erreichens der Führungsüberlegenheit.

Weiters ist das Führungssystem nicht zwingend in einer Doktrin begründet und wie das historische Beispiel des Blitzkrieges[9] zeigt, kann Führung in Verbindung mit Technologie sogar selbst Doktrinen schaffen. Umgekehrt ist aber „*ein technologischer Vorteil alleine keine ausreichende Bedingung, um ein entscheidendes Resultat zu erreichen.*“[10]

Wenn aber der Blitzkrieg ursprünglich gar keine Doktrin war und Technologie alleine nicht genügt, diese Entwicklung zu begründen, so ist zumindest ein weiterer wesentlicher Faktor nötig, um den Aufstieg eines strategischen Konzeptes zur Doktrin zu erklären. Laut Frieser[11] war dies (auch) das Führungssystem mit seiner ausgeprägten Auftragstaktik, das den Offizieren intuitives und selbstständiges Handeln am Gefechtsfeld ermöglichte und so den Führungsvorteil multiplizierte.
Führung ist daher in dieser Beziehung als gleichwertiges Element und ebenso entscheidender Faktor anzusehen.

Ziel dieser Arbeit

Der Fokus dieser Arbeit liegt, wie sich unschwer erkennen lässt, auf den militärischen Teilbereichen des Informationskrieges, auf dem Zusammenhang zwischen Führung, Technologie und Doktrin, sowie den strukturellen und organisatorischen, also auch doktrinellen Auswirkungen der neuen Entwicklungen. Die zentralen Fragen, die es zu klären gilt, sind:

- Inwieweit haben sich Doktrinen bereits durch den Einfluss des Informationskrieges verändert? Wo ist der Informationskrieg im Militär bereits messbar? Welche Kriterien könnte man für zukünftige Beurteilungen ableiten? Finden wir bereits einen echten und umfassenden Informationskrieg?
- Wie sieht der Zusammenhang zwischen Führung-Technologie-Doktrin aus? Wie lassen sich jüngste Entwicklungen anhand eines Modells beschreiben? Lässt sich aus

[8] Krepinevitch, zit. nach Air Power Revue der Schweizer Armee Nr.3, Beilage zur Allgemeinen Schweizerischen Militärzeitschrift ASMZ 12/2004, S7f; Krepinevitch spricht in diesem Zusammenhang zwar von einer Revolution of Military Affairs, der Artikel stellt aber in weiterer Folge klar, dass auch der Begriff „Evolution“ (Entwicklung) zulässig ist.
[9] Siehe Kapitel 2.8.2; Der Blitzkrieg war keineswegs von Beginn des 2.WK an eine Doktrin, sondern vielmehr ein strategisches Konzept, dessen Erfolg erst unter anderem durch den Einsatz von Technologie möglich gemacht wurde. Erst während des Krieges wurde das Konzept zur Doktrin erhoben.
[10] Zeitschrift Air Power Revue der Schweizer Armee Nr.3, Beilage zur Allgemeinen Schweizerischen Militärzeitschrift ASMZ 12/2004; Artikel „Doktrin und Technologie: Zwillings- oder Halbschwestern“; S9
[11] Frieser, Karl Heinz, Blitzkrieg-Legende, Der Westfeldzug 1940; R.Oldenburg Verlag München, 1995

diesem Zusammenhang ein Ansatz für eine Definition für Revolutionen in Militärischen Angelegenheiten finden?

Beschreibung der Abschnitte

Die Arbeit gliedert sich in zwei Abschnitte. Abschnitt I bildet den theoretischen Teil, in dem Grundlagen allgemeiner und militärischer Art erörtert werden. Es wird zunächst in Kapitel 1 der Informationsbegriff sowie seine Verwendung im Zuge dieser Arbeit definiert, Kapitel 2 beschäftigt sich mit der militärischen Führung und Organisation sowie ihren Zusammenhang im Kontext Führung-Doktrin-Technologie. Kapitel 3 widmet sich zunächst dem Informationskrieg aus gesellschaftstheoretischer Sicht und behandelt kurz die Theorien von Bell und Toffler. Weiters wird versucht, dem bislang doch sehr theoretischen Begriff des Informationskrieges eine Gestalt zu geben und ihn zu konkretisieren. Dazu werden unter Anderem die sieben Formen beleuchtet, die der Informationskrieg laut Libicki annehmen kann[12], und die Theorien Arquillas und Ronfeldts beleuchtet. Kapitel 4 stellt das militärische System C4I vor, welches seine stärkste Ausprägung im Konzept der Network Centric Warfare (NCW) findet, das in Kapitel 5 vorgestellt wird.

In Abschnitt II wird dann anhand des Beispiels der US Army untersucht, inwieweit sich die Elemente des Informationskrieges bereits in strategischen Überlegungen und Doktrinen finden lassen. Die Untersuchung beschäftigt sich primär mit dem Einfluss des Informationskrieges auf die Doktrinen und endet mit der Beantwortung der Forschungsfragen. Danach widmen wir uns dem Zusammenhang zwischen den Faktoren Führung, Technologie und Doktrin und versuchen ein Modell für diese Beziehung zu beschreiben, das auch in Zukunft seine Gültigkeit besitzt.

[12] Libicki, Martin C.; What is IW?; National Defense University; Library of Congress Cataloging-in-Publication Data; 1995; S*ix*f

I.Teil

1. Der Informationsbegriff

Mut ist oft Mangel an Einsicht, während Feigheit nicht selten auf guten Informationen beruht.
Sir Peter Ustinov

Der Begriff „Information" ist nur schwer zu erfassen und im Laufe der Geschichte haben viele Philosophen und Wissenschaftler den Versuch einer Definition gewagt, auch wenn wohl keine das gesamte Spektrum des Begriffs abdecken kann. Dennoch ist es nötig, sich zunächst einmal bewusst zu machen, was „Information" eigentlich bedeutet, um den Begriff in weiterer Folge mit der modernen Kriegsführung in Zusammenhang bringen zu können.

1.1. Die Geschichte des Informationsbegriffes

Der Informationsbegriff ist sehr alt und vielschichtig und geht sprachlich gesehen auf die Antike zurück. Im Lateinischen fand das Wort „informatio" seine Verwendung, was mit *Vorstellung, Begriff*, aber auch *Deutung, Erläuterung* übersetzt werden kann[13]. Das dazugehörige Zeitwort „informare" lässt sogar noch mehr Übersetzungen, wie z.B. *formen, gestalten, darstellen, unterrichten, sich denken* oder *sich vorstellen* zu.[14]

Im Laufe der Geschichte, besonders aber in der Neuzeit, beschäftigten sich eine Reihe von Wissenschaftlern und Philosophen mit dem Begriff „Information" und versuchten ihn zu erklären und zu definieren. Die Notwendigkeit der wissenschaftlichen Beschreibung von Information ergab sich einerseits aus dem Bedürfnis, Informationsstrukturen quantifizierbar und messbar zu machen, andererseits aus dem technologischen Fortschritt am Nachrichtensektor und der Diskrepanz, dass die Technik zwar einen hohen Standard erreicht hatte, ihr zugrunde liegende Grundbegriffe wie „Nachricht" und „Information" aber nach wie vor unbearbeitet geblieben waren. So waren es Shannon und Weaver, zwei Mitarbeiter der Bell Laboratories, die mit ihrer Informationstheorie, die nach und nach von der Wissenschaft akzeptiert wurde, ein neues, selbstständiges Wissensgebiet begründeten und prägten. Der Shannon'sche Informationsbegriff gewann am Nachrichtensektor entscheidend an Bedeutung, griff aber für viele Wissenschaftler zu kurz, da er nur die Übertragung von Information behandelte, nicht aber auf deren Inhalt und Bedeutung Rücksicht nahm.

Mittlerweile haben sich viele Gebiete der Wissenschaft mit dem Informationsbegriff beschäftigt und ihre eigenen Betrachtungen und Definitionen publiziert. Die Verwendung des Informationsbegriffs differiert je nach Betrachtungsweise, eine allgemein gültige Definition, die das gesamte Spektrum von „Information" abdeckt, gibt es allerdings scheinbar nicht.
Der lateinamerikanische Informationstheoretiker Rafael Capurro beschreibt die Schwierigkeiten bei der Suche nach einem allgemeingültigen Informationsbegriff in seinem „Capurro'schen Trilemma"[15].

---

[13] Vgl.: Stowasser J.M. et al., Der kleine Stowasser, 3.Auflage, Verlag Hölder-Pichler-Tempsky, 1991, S.233
[14] Vgl.: Fleissner, Peter, et.al.; Der Mensch lebt nicht vom Bit allein; Europäischer Verlag der Wissenschaften, 2.Auflage, 1997, S. 3ff
[15] Vgl.: Capurro, Rafael, Einführung in den Informationsbegriff, URL: http://www.capurro.de/infovorl-kap3.htm#6.%20Das%20Capurrosche, (Abgerufen: 22.07.2007)

Nach Capurro gibt es in allen Bereichen drei Möglichkeiten der Bedeutung des Informationsbegriffs. Er bedeutet

- entweder genau dasselbe
- oder etwas ähnliches
- oder jeweils etwas ganz anderes.

Er führt in weiterer Folge Gründe an, warum keine dieser drei Möglichkeiten zutreffen kann und definiert dies als Capurro'sches Trilemma.

„Wir müssten annehmen, dass der Wissenschaft nichts anders übrig bleibt, als entweder an der Suche nach einer Weltformel zu scheitern oder mit der subjektiven Beliebigkeit der Projektionen zwischen den unterschiedlichsten Gebieten jeden allgemeingültigen Anspruch aufzugeben oder im Fachidiotentum dahin zu vegetieren. Ein Ausweg aus dem Trilemma scheint nicht zu existieren, ein einheitlicher, vereinheitlichter, einziger Informationsbegriff aus logischen Gründen unmöglich."[16]

Als Ausweg wird hier von Hofkirchner/Fleissner das Paradigma der Selbstorganisation gesehen. *„Ein einheitlicher Informationsbegriff, der Allgemeines und Einzelnes miteinander vermittelt, soll dem evolutionären Informationsgeschehen Rechnung tragen."*[17] Ein Informationsbegriff also, der sich je nach Ebene, auf der er zur Anwendung kommt, durch unterschiedliche Freiheitsgrade auszeichnet und einer selbstorganisierenden Strukturbildung unterliegt. Hier schließt sich der Kreis zum lateinischen Ursprung, denn das Wort *in-fomare* bedeutet auch *„sich formen", „sich organisieren"* oder eben *„selbstorganisieren"*.

1.2. Der nachrichtentechnische Informationsbegriff

Das nachrichtentechnische Modell reduziert Information auf ihren quantitativen Aspekt. Es geht auf den amerikanischen Wissenschaftler R.V.L. Hartley zurück, der Information im Sinne eines physikalischen Vermittlungsprozesses auffasst. Aspekte wie Sachbezogenheit, Inhalt und Relevanz fallen in diesem Kontext weg. Die Nachrichtentheorie sieht also von der Bedeutung und dem pragmatischen Aspekt von Information ab.[18]

1.2.1. Das Sender-Empfänger Modell

Hartley sieht in seinem Modell einen Sender, ein Zeichenrepertoire, Auswahlkriterien und einen Empfänger als Faktoren in einem Nachrichtensystem an. Er behandelt Zeichen nur in formaler oder syntaktischer Hinsicht, die Bedeutung oder Semantik der Zeichen oder ihre Wirkung auf den Empfänger, also die Pragmatik, finden bei Hartley keine Berücksichtigung. *„Mit anderen Worten, Hartley nimmt den Begriff Information aus dem menschlichen Gebrauchskontext heraus. Dementsprechend hat „Auswahl" nichts mit menschlicher Entscheidungsfreiheit zu tun."*[18]

---

[16] Hofkirchner/Fleissner nach CAPURRO,
URL: http://www.capurro.de/infovorl-kap3.htm#6.%20Das%20Capurrosche
[17] Hofkirchner/Fleissner nach CAPURRO,
URL: http://www.capurro.de/infovorl-kap3.htm#6.%20Das%20Capurrosche
[18] Vgl.: Capurro, Raphael; URL: http://www.capurro.de/infovorl-kap3.htm#1.%20Der%20nachrichtentechnische, (Abgerufen: 27.06.2007)

Ein Nachrichtensystem wählt also im Rahmen der vorgegebenen Auswahlkriterien selbst aus und trifft eine Entscheidung wenn es mindestens zwei Elemente oder Zeichen gibt. Existieren vier Elemente, so trifft das System zwei Entscheidungen usw. Diese binäre Darstellung prägte später den Begriff *binary digit* oder kurz *bit*. Da die Bedeutung der Zeichen ja nicht berücksichtigt wird, haben alle Zeichen des Zeichenrepertoires den gleichen Informationsgehalt, das heißt der Informationsgehalt einer Nachricht ergibt sich aus der Anzahl der binären Entscheidungen, die logarithmisch berechnet werden kann. Der Informationsgehalt IG einer Nachricht ergibt sich aus dem Logarithmus Dualis von der Anzahl der Zeichen n in der Einheit bit, also

$$IG = Ld(n) \text{ bit}$$

Nehmen wir als Beispiel das telegraphische System des französischen Wissenschaftlers Beaudot, dessen Zeichnrepertoire aus 32 Zeichen bestand, so ergibt sich für dieses System der Informationsgehalt IG

$$IG = Ld\ (32) = 5$$

Jede Entscheidung des Systems bedeutet eine Präzisierung der von der Quelle ausgesendeten Nachricht und eine Reduzierung der Ungewissheit des physikalischen Systems auf Empfängerseite. Der Informationsgehalt ist daher auch ein Maß für die Ungewissheit.[18]

Die Übermittlung von Information erfolgt in einem Nachrichtensystem durch die Übertragung von Zeichen in einem zuvor definierten *Alphabet*, also der Menge aller Zeichen einer *Sprache*. Jede Sprache hat aber bestimmte Regeln, nach denen eine Nachricht aufgebaut werden muss. Diese *Grammatik* oder *Syntax* bildet die formalen Grundlagen für jede Entscheidung im System. Hier zeigt sich der rekursive Charakter von Information, denn bevor man Information aus der Nachricht herauslesen kann, benötigt man Information über die Grammatik der verwendeten Sprache.[19]

Eine Sprache mit nur zwei Zeichen nennt man Binärsprache, die klassische Sprache der Datenübertragung. Um aber komplexe Nachrichten innerhalb einer Sprache bzw. eines Alphabets übertragen zu können, bedarf es einer Codierung, also einer Abbildung einer Sprache auf eine andere. Als Beispiel sei hier der Morsecode angeführt, der die Buchstaben unseres Alphabets in einer Sprache mit drei Zeichen (*, -, pause) abbildet. Eine so verwendete Sprache wird auch *Metasprache* genannt.

Die Codierung muss eindeutig umkehrbar sein, um zu gewährleisten, dass die Rückübersetzung in das Quellalphabet möglich ist.[20] Ist das Alphabet aber unbekannt oder kann ein Zeichen nach einer Störung bei der Übertragung vom Empfänger nicht mehr eindeutig identifiziert werden, so kommen Zufallsprozesse und Wahrscheinlichkeiten ins Spiel. Daraus ergibt sich das klassische Sender-Kanal-Empfänger-Modell der Nachrichtentechnik, dem sich in weiterer Folge Shannon und Weaver angenommen haben.[14]

[19] Blieberger, Johann et.al., Informatik, Dritte Auflage, SpringerWienNewYork, 1996, S.18f
[20] Blieberger, Johann et.al., Informatik, Dritte Auflage, SpringerWienNewYork, 1996, S.19

Abbildung 2: Sender-Empfänger Modell

1.2.2. Der Shannon'sche Informationsbegriff

In der Shannon'schen Theorie werden diskrete Nachrichtenquellen als Produzenten von Zufallsprozessen angesehen.[21] Nachrichten werden dabei durch einen Sender, der die Information auf eine Metasprache abbildet, also codiert, über einen Kanal zum Empfänger übertragen, der im optimalen Fall diese wieder decodieren und so die Information zurückgewinnen kann. Im Übertragungskanal können nun Störungen auftreten, die ein Decodieren der Nachricht unmöglich machen. Der Sender kann sich gegen diese Art von unvorhersehbaren Einflüssen durch verschiedene Strategien, etwa die Verwendung eines *parity bits* oder dem Einsatz von Übertragungsprotokollen wappnen.

Shannon versucht, (unter Berücksichtigung der Wahrscheinlichkeiten, Anm.) ein Maß für den Informationsgehalt eines Zeichens zu finden, das heißt ein Maß dafür, wie viel Information eine diskrete Nachricht enthält, die von einem Sender an einen Empfänger übermittelt wird.[22] Jedes Zeichen einer Zeichenfolge tritt mit einer bestimmten Wahrscheinlichkeit auf, je seltener also ein Zeichen gesendet wird, desto höher ist sein Informationsgehalt oder anders ausgedrückt: der Informationsgehalt einer Zeichenkette stellt eine monoton wachsende Funktion des Reziprokwertes der Auftrittswahrscheinlichkeit der Zeichen dar. Mathematisch lässt sich dies für ein Zeichen so darstellen, wobei h für den Informationsgehalt, p für die Wahrscheinlichkeit und f für eine monoton wachsende Funktion steht:

$$h = f(1/p)$$

Der Informationsgehalt einer aus mehreren voneinander unabhängigen Zeichen bestehenden Nachricht ergibt sich nun aus der Summe der Informationsgehalte der einzelnen Zeichen. Aus der Unabhängigkeit der Zeichen folgt, dass die Wahrscheinlichkeit des Auftretens gleich dem Produkt der Einzelwahrscheinlichkeiten der die Nachricht bildenden Zeichen ist, das heißt die Funktion f erfüllt die Bedingung:[19]

$$f(x)+f(y) = f(x*y)$$

Wie bereits bei Hartley erfüllt auch hier die logarithmische Funktion diese Vorgaben. Der Informationsgehalt eines Zeichens Z ergibt sich also aus dem Logarithmus Dualis des Reziprokwertes seiner Auftrittswahrscheinlichkeit p(Z).

[21] Fey, P., Informationstheorie, Berlin, 1968, zit. nach (Fleissner, Peter, et.al.; Der Mensch lebt nicht vom Bit allein; Europäischer Verlag der Wissenschaften, 2.Auflage, 1997, S.6)
[22] Blieberger, Johann et.al., Informatik, Dritte Auflage, SpringerWienNewYork, 1996, S. 21

$$h = ld\ (1/p(Z)) = -ld\ p(Z)$$

Als Maßeinheit gilt das Bit, wobei ein Bit einer Auftrittswahrscheinlichkeit von 50 Prozent entspricht. Man kann nun unter der Voraussetzung, dass die Wahrscheinlichkeiten bekannt sind, den Informationsgehalt einer Nachricht berechnen. Oft ist es aber wünschenswert, vor dem Eintreffen eines Zeichens den zu erwartenden Informationsgehalt zu ermitteln. Dies geschieht über den mittleren Informationsgehalt H, der auch als *Entropie* bezeichnet wird. Sei h_i der Informationsgehalt des i-ten Zeichens einer Nachricht mit der Länge M und p_i seine Auftrittswahrscheinlichkeit, so ist die Entropie H gegeben durch:

$$H = -\sum_{i=1}^{M} p_i\ ld\ p_i$$

Die Entropie wird ebenfalls in der Einheit Bit gemessen. Aus dem Informationsgehalt ergibt sich die Codelänge eines Zeichens l_i, je geringer der Informationsgehalt, desto geringer die Wortlänge. Die folgende Tabelle soll dies verdeutlichen:

Zeichen	**h**	**Code**
X	0.50	1
Y	0.25	01
Z	0.25	00

Unter der mittleren Wortlänge eines Codes versteht man die mit den Auftrittswahrscheinlichkeiten gewichtete Summe der Längen der den einzelnen Zeichen entsprechenden Codewörter, d.h.

$$L = \sum_{i}\ p_i * l_i$$

wobei l_i für die Länge des dem i-ten Zeichens entsprechenden Codewortes steht.[23] Mit der mittleren Wortlänge L und dem mittleren Informationsgehalt H lässt sich nun auch die Redundanz eines Codes, also die Zahl der eigentlich überschüssigen Zeichen berechnen. Sie ergibt sich aus der Differenz zwischen der mittleren Wortlänge und dem mittleren Informationsgehalt:

$$R = L - H \text{ mit } R>=0$$

Die Informationstheorie von Shannon und Weaver behandelt also die Übertragung der Information über einen Kanal durch einen Sender genauso wie Fragen der En- und Decodierung sowie Störung der Übertragung. Informationsgehalt, Auftrittswahrscheinlichkeit, Redundanz und das Bit als Maßeinheit stehen dabei in enger Beziehung zu dieser Theorie. Allerdings ist der nachrichtentechnische Informationsbegriff nur auf jenen Gebieten relevant, wo es um

[23] Blieberger, Johann et.al., Informatik, Dritte Auflage, SpringerWienNewYork, 1996, S. 23

Nachrichtenspeicherung und Nachrichtenübertragung geht, da Fragen des Inhaltes und des Zusammenhanges von Information hier keine Rolle spielen.

1.3. Der sprachwissenschaftliche Informationsbegriff

Anders als bei der nachrichtentechnischen Betrachtung des Informationsbegriffes, bei der Information im Sinne einer Zeichenfolge verstanden wird, geht es in der sprachwissenschaftlichen Anschauung um die Bedeutung der Zeichen selbst. Bereits in den 30er Jahren beschäftigte sich die Sprachwissenschaft und die Philosophie mit der menschlichen Kommunikation und der Sprache als solches und führte in weiterer Folge, angelehnt an den amerikanischen Philosophen Peirce, die Unterscheidung zwischen Syntax, Semantik und Pragmatik ein. Diese dreidimensionale *Semiotik*[24] wurde vom Sprachwissenschaftler Charles W. Morris in seinem Werk „Signs, Language and Behavior" definiert und geht dabei von der informativen Wirkung von Zeichen aus.[25]

Diese drei Ebenen lassen sich anhand des Prozesses der Semiose veranschaulichen. Nach Morris wird unter Semiose der Zeichenprozess verstanden, also der Prozess, in dem etwas als Zeichen fungiert.[26]

Die Semiose besteht aus folgenden Komponenten:

- einem Gegenstand oder Designat (**D**), also dem worauf sich das Zeichen bezieht
- einem Abbild oder Zeichenträger (**Z**), also dem, was als Zeichen wirkt
- einem Subjekt oder Interpreten (**S**), also dem, der das Zeichen wahrnimmt
- und dem Verhalten eines Interpretanten (**I**), also dem Effekt, der in irgendeinem Rezipienten ausgelöst wird.

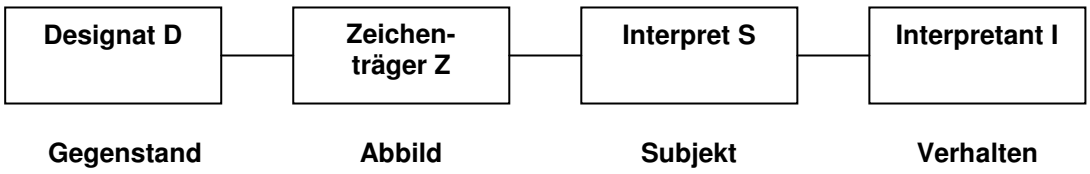


Abbildung 3: Semiose

Morris beschreibt die drei Ebenen in seinem Modell, indem er die Komponente des Zeichenträgers in Relation zu je einer anderen Komponente setzt:

[24] Semiotik: Allgemeine Theorie von den Zeichen und Sprachen
vgl. Fleissner, Peter, et.al.; Der Mensch lebt nicht vom Bit allein; Europäischer Verlag der Wissenschaften, 2.Auflage, 1997, S.10
[25] vgl. Capurro, Rafael, Einführung in den Informationsbegriff, URL: http://www.capurro.de/infovorl-kap3.htm, S5, (Abgerufen: 27.06.2007)
[26] Fleissner, Peter, et.al.; Der Mensch lebt nicht vom Bit allein; Europäischer Verlag der Wissenschaften, 2.Auflage, 1997, S.10ff

Relation Z-S: Die Beziehung zwischen dem Zeichenträger Z und dem Interpreten S wird als *Pragmatik* bezeichnet und stellt die Interpretation eines Zeichens auf der Empfängerseite dar. Der Interpret ist derjenige für den das Zeichen eine Bedeutung hat.

Relation Z-D: Diese Dimension stellt die Bedeutung der Zeichen dar und beschreibt, wofür Zeichen stehen. Sie wird als *Semantik* bezeichnet und ist eine Zuordnung zwischen Zeichen und Designaten, also eine inhaltliche Festlegung der Zeichen. Die Semantik ist die Beziehung der Zeichen zum Sachverhalt.

Relation Z-Z: Die Beziehung des Zeichenträgers zu anderen Zeichenträgern wird *Syntaktik* genannt. Rechtschreibregeln und Grammatik setzen Zeichen in Bezug zueinander, indem sie Regeln für deren Verwendung festlegen.

Fuchs-Kittowski greift die Morris'sche Theorie auf und versucht, die unverbunden nebeneinander gereihten Ebenen zueinander in Beziehung zu setzen und gleichzeitig den Shannon'schen Ansatz des Sender-Kanal-Empfänger Modells beizubehalten. Er geht davon aus, dass Information eine bestimmte Form und einen bestimmten Inhalt hat, also eine Struktur und eine Bedeutung. Diese Unterscheidung wendet er sowohl auf den Ebenen der Semiotik als auch auf der Ebene der Signale an. Sein Schema verbindet menschliche und technische Informationsverarbeitungsprozesse. Verständnis und Begreifen setzen menschliches Bewusstsein voraus, während Interpretation und Erkennung auch ohne subjektives Bewusstsein ablaufen und daher auch von Maschinen ausgeführt werden können.[23]

1.4. Der Informationsbegriff im Sinne dieser Arbeit

Die rein nachrichtentechnische Betrachtung von Information fasst im Sinne dieser Arbeit zu kurz, auch wenn es mit Masse um elektronische Systeme zur Informationsverarbeitung geht und daher dieser Informationsbegriff zunächst nahe liegt. Die nachrichtentechnische Betrachtung von Information findet grundsätzlich überall dort ihren Niederschlag, wo es um Speicherung und Übertragung von Nachrichten geht. Computersysteme, Expertensysteme, Führungsinformationssysteme usw., die in den Konzepten der modernen Kriegsführung zum Einsatz kommen bzw. entwickelt werden, gehen aber weit über dieses Verständnis hinaus, denn sie müssen Information auch nach ihrer Bedeutung und ihrer Wirkung beurteilen, Zusammenhänge herstellen und basierend auf den Ergebnissen Entscheidungen treffen.

Es genügt im subjektiven menschlichen Verständnis nicht, Information nur auf ihre formale Bedeutung zu reduzieren und Aspekte des Inhalts und der Bedeutung außer Acht zu lassen. In dieser Arbeit soll daher von einem intuitiven Begriffsverständnis ausgegangen werden, ähnlich wie in der Physik Wissenschaftler darauf vertrauen, dass jeder Mensch ungefähr weiß, was Masse bedeutet, ohne sie näher definieren zu müssen.[27] Im Zeitalter des Informationskrieges spielen alle Aspekte von Information eine Bedeutung, also sowohl Fragen zur Übertragung als auch Fragen zur Bedeutung und zum Inhalt, daher kommt ein intuitiver oder selbstorganisierender Informationsbegriff den Anforderungen wohl am nächsten. Der Begriff „Information"

[27] vgl. Blieberger, Johann et.al., Informatik, Dritte Auflage, SpringerWienNewYork, 1996, S15

ist in diesem Sinne daher möglichst umfassend zu sehen und wird in dieser Arbeit auch so verwendet.

2. Militärische Organisation und Führung

Die militärische Organisation unterscheidet sich von Organisationen ziviler Unternehmen prinzipiell in geringem Ausmaß. Man kann durchaus die Ebenen des Managements mit den Führungsebenen der militärischen Organisation vergleichen und wird feststellen, dass diese nur in den Ausprägungen der Prozesse differieren. Gesellschaftliche Konventionen, Werte und Vorgaben nehmen gleichermaßen Einfluss auf Organisationen ziviler und militärischer Natur. Was im zivilen Bereich das E-Business, ist im Bereich des Militärs der Informationskrieg und in weiterer Folge die Konzepte zum militärischen Nervensystem C4I[28].

Führung und Führungsüberlegenheit sind wesentlichste Elemente im Informationskrieg und die Anforderungen an Führungsinformationssysteme und Konzepte zur modernen Kriegsführung ergeben sich aus den Prozessen und Strukturen des Militärs.

2.1. Führung – Allgemeine Betrachtung

Um die militärische Arbeitsweise verstehen und die Notwendigkeit von Autorität, straffer Organisation sowie den Wechsel aus Fremd- und Selbstbestimmung innerhalb der Armee einerseits, die Notwendigkeit von Netzwerkstrukturen im Hinblick auf die moderne Kriegsführung andererseits erfassen zu können, ist es zunächst nötig, sich bewusst zu machen, was Führung im allgemeinen bedeutet.

In praktisch jedem Bereich des Lebens und der Gesellschaft ist Führung nötig, um ein geordnetes und friedliches Miteinander zu ermöglichen. Überall dort, wo mehr als zwei Menschen versuchen, ein Ziel zu erreichen, und sei es nur die Bildung einer Fahrgemeinschaft, ist Koordination und Organisation nötig. In allen Kulturen und Epochen der Geschichte, angefangen bei den stammesähnlichen Formen des Zusammenlebens in der Frühgeschichte der Menschheit, bis hin zu den zivilisierten Hochkulturen der Antike, des Mittelalters und der Neuzeit hat es klarer gesellschaftlicher Strukturen mit all ihren unterschiedlichen Richtlinien und Autoritäten bedurft, um die Entwicklung der Zivilisation und Kultur an sich überhaupt erst zu ermöglichen.[29] Organisationsstrukturen, Staatsformen, aber auch Familienformen und Wertebegriffe der Kulturen unterlagen und unterliegen dabei einem ständigen Wandel, so wie sich auch die Gesellschaft selbst in einem steten Prozess des Wandels und der Anpassung befindet. Einflussfaktoren wie Religion, wirtschaftliche Entwicklungen, Umweltfaktoren, Ressourcenverfügbarkeit, aber auch Forschung und Wissenschaft spielen eine zentrale Rolle in der Ausprägung von Werten und in weiterer Folge bei der Entstehung von Strukturen und Autoritäten innerhalb der Gesellschaft. Betrachtet man beispielsweise die Religion als einen der zentralen Faktoren, so kann man gerade heute die prägende Bedeutung des religiösen Wertebegriffs für die Gesellschaft feststellen. War der Einfluss der Religion im mittelalterlichen Europa noch treibender Motor für die Weiterentwicklung der Gesellschaft, der sich klar in den Strukturen und Machtverhältnissen des christlichen Abendlandes niederschlug, so ist, auch wenn die Säulen der gesellschaftlichen Strukturen nach wie vor auf den religiösen Grundwerten basieren, an ihre Stelle

[28] Siehe Kapitel 4

[29] vgl. Meurers, Mag., Bernhard, Führungs- und Organisationslehre, Truppendiensttaschenbuch Nr36, Herold Verlag, Wien, 1998, S.6

Wissenschaft und Wirtschaft als treibende Kraft getreten. Im Vergleich dazu betrachte man Kulturkreise, die sich, stark fokussiert auf ihre Religion, in ihren Werten, Organisationen, Strukturen und Zielen klar von den aufgeklärten, liberalen Demokratien mit ihrem ausgeprägten Menschenrechtsbegriff unterscheiden.

Führung findet in allen Bereichen der Gesellschaft statt, allein ihre Ausprägung in Führungssysteme und Führungsgrundsätze differiert also je nach gesellschaftlichen Einflussfaktoren und Werten.

In unserer modernen Gesellschaft mit ihrem ausgeprägten sozialen Gefüge und der starken Rolle des Individuums steht das Wohl des Menschen als solches nicht nur im Zentrum des täglichen Lebens, sondern hat auch im Bereich der Führung Gewicht.[30] Der Begriff „Führung" umfasst grundsätzlich die Einflussnahme auf Personen, um gewisse Ziele zu erreichen bzw. Aufträge zu erfüllen, beinhaltet in unserer Auffassung aber auch Rücksichtnahme auf die Person selbst. Der Wert des Menschen, seine Bedürfnisse, Ängste, Sorgen und Wünsche werden in den Führungsprozess mit eingebunden und das Wohl des einzelnen Mitarbeiters oder Untergebenen ist im Rahmen der vorgegebenen Grenzen mindestens ebenso wichtig, wie das Erreichen des Zieles selbst. Dazu zählen Maßnahmen, die dem Geführten ein Gefühl der Wertschätzung und Anerkennung vermitteln, aber auch Handlungsfreiheit gewähren und so dem Geführten Selbstständigkeit und Selbstbestimmung suggerieren

Nun könnte man kritisch anmerken, dass sich Bedürfnisse von Menschen gegenseitig im Wege stehen könnten und es gar nicht möglich wäre, zu führen, ohne Nachteile für Andere in Kauf zu nehmen, was ja einen Widerspruch zu oben Gesagtem darstellen würde. Weiters könnte man annehmen, dass in Hinblick auf die Rolle des Kommandanten oder Führers, diese *„Führungskräfte lediglich reagieren, dass Führung lediglich von den Erwartungen inner- und ausserorganisatorischer Anspruchsgruppen abhängt (…)"*[31].
Gerade die Balance zwischen dem Erreichen des Zieles, dem Erfüllen des Auftrages und den Widersprüchen, die sich aus den verschiedenen menschlichen Bedürfnissen und Wünschen ergeben, sowie das Bewegen innerhalb der der Rolle des Führers zugedachten Grenzen, um eben den angesprochenen Erwartungen gerecht zu werden, macht die Kunst des Führens aus und unterstreicht die Komplexität und Dynamik des Prozesses der Führung.

Führung dient daher nicht nur zur Erreichung eines Zieles, sondern soll es auch dem Einzelnen ermöglichen, sich im Rahmen der vorgegebenen Grenzen und Normen frei bewegen und entfalten zu können. Das Anpassen des einzelnen Menschen an diese Normen, Werte und Regeln der Gesellschaft setzt Akzeptanz voraus, die genau durch solche Maßnahmen geschaffen wird. Andererseits werden die Normen, Werte und Regeln der Gesellschaft zwar durch diese eingefordert, allerdings ist es der Mensch als Individuum, der diese prägt und verändert.

„Zwar wird der Mensch als Individuum in seinen Verhaltensweisen durch die Gruppe beeinflusst, deren Normen, Zwänge und Institutionen werden aber wiederum durch den einzelnen Menschen geprägt und verändert. Darin ist nicht nur ein sozialer Werte- und Normenwandel begründet, sondern es wird damit auch klar, dass es des

[30] vgl. Meurers, Mag., Bernhard, Führungs- und Organisationslehre, Truppendienst Taschenbuch Nr. 36, Reihe Ausbildung und Führung, Herold Verlag, Wien, 1998, S.6f
[31] Siebert, Jörg, Führungssysteme zwischen Stabilität und Wandel. Gabler Verlag, 2006, S25f

einzelnen kreativen, neue Erfindungen setzenden oder Widerstände leistenden bzw. Anpassung zeigenden Individuums bedarf, wenn sich die Gesellschaft weiterentwickeln soll. Immer wieder werden Menschen gebraucht, die Maßstäbe vorgeben, Ideen entwickeln und Visionen haben, bei denen man Orientierung suchen und finden kann – eben solche die führen.“ [32]

Aus diesem Wechselspiel lässt sich die grundlegendste Aufgabe der Führung ableiten, die Weiterentwicklung der Gesellschaft an sich. Ein Grundgedanke der sich auch auf die Organisationen und Institutionen der Gesellschaft und deren interne Strukturen abbilden lässt.

2.2. Militärische Führung

Sieht man die Gesellschaft als System, das die Menschen (Elemente) mit ihren Verhältnissen (Relationen) bilden, so kann man das Militär als ein Subsystem der Gesellschaft verstehen[33].

Funktion und Struktur dieses Subsystems sind aufgrund der Aufgabenstellung an das Militär sehr speziell. So kann man als Funktion des Militärs das Erzeugen von Sicherheit (innen und außen) sehen, als Struktur sind die Soldaten (Personal) sowie die Ausrüstung (Material) in ihrer hierarchischen Gliederung zu verstehen. Die Grundstrukturen der Zivilgesellschaft lassen sich auch auf das Militär abbilden, auch wenn die hierarchischen Muster deutlicher ausgeprägt sind. Die hierarchische Organisation sowie die Aufgabenstellung ergeben die Gesamtstruktur des Militärs.

„*Führung ist ein allgemeines, richtungweisendes, steuerndes und motivierendes Einwirken auf Personen oder Organisationselemente, um eine Zielvorstellung zu verwirklichen und die Organisation zu optimieren. Führung setzt Kräfte, Mittel, und Information zielgerichtet nach Zeit und Raum ein.“* [34]

Die Besonderheit militärischer Führung liegt darin, dass sie auch unter außergewöhnlichen Belastungen des Krieges, vor allem im Gefecht, wirksam werden muss. Militärische Führer müssen oft bei Ausfällen von Personal und Material unter Zeitdruck und in ungeklärter Lage handeln. Die Forderung an den Soldaten, sein Leben einzusetzen, und die Pflicht des militärischen Führers, dies von sich und anderen zu verlangen, geben der Menschenführung ein außerordentliches Gewicht. [35]

Militärische Führung ist daher ein sehr komplexer Vorgang, der durch das Führungssystems normiert und optimiert wird.

---

[32] Meurers, Mag., Bernhard, Führungs- und Organisationslehre, Truppendienst Taschenbuch Nr. 36, Reihe Ausbildung und Führung, Herold Verlag, Wien, 1998, S.623

[33] Fleissner, Peter, et.al.; Der Mensch lebt nicht vom Bit allein; Europäischer Verlag der Wissenschaften, 2.Auflage, 1997, S237

[34] Dienstvorschrift für das Bundesheer, Führungsbegriffe, BMLV, 2005, S65

[35] Meurers, Bernhard, Führungsverfahren auf Ebene Brigade und Bataillon, Truppendienst Taschenbuch Nr. 46, Reihe Ausbildung und Führung, Verlag AV + Astoria Druckzentrum GmbH, Wien, 2004, S28

2.3. Militärisches Führungssystem

Die speziellen Anforderungen an das Subsystem „Militär“ haben ebenso spezielle Lösungsansätze und Prozesse innerhalb des Militärs zur Folge, die sich im militärischen Führungssystem widerspiegeln. Stellvertretend für die Arbeitsweise moderner Armeen soll hier das Führungssystem des Österreichischen Bundesheeres betrachtet werden. Österreich ist auf dem Gebiet Führung international anerkannt und schult immer wieder Stabsoffiziere anderer Armeen in diesem Bereich. Unterschiede in den Führungssystemen ergeben sich aus den verschiedenen Aufgaben und Anforderungen an Armeen durch die politischen Vorgaben und Interessen des jeweiligen Staates sowie durch verschiedene Strukturen und Gliederungen.

Unter dem militärischen Führungssystem versteht man den geordneten Zusammenhang zwischen Führungsverfahren, Führungsorganisation und Führungsmitteln[36] .

Es stellt eine geregelte, systematische und strukturierte Arbeitsweise innerhalb des Militärs dar, um die Auftragserfüllung sowohl in der Friedens- als auch in der Einsatzorganisation jederzeit gewährleisten zu können. Jede Entscheidung und Führungsmaßnahme wird im Rahmen dieses Führungssystems getroffen, die besonderen Anforderungen an das Führungssystem ergeben sich aus den Aufgaben und der Natur des Militärs an sich. Es muss flexibel sein und sich an ständig ändernde Anforderungen anpassen können und es muss zu jeder Zeit die rasche Entscheidungsfindung auf allen Ebenen ermöglichen. Dazu ist neben der Abbildung von Strukturen und der Normierung von Entscheidungsprozessen auch ein Informationsmanagement nötig, dass in weiterer Folge dem Kommandanten Information nach Relevanz, Priorität, Vollständigkeit und Echtheit aufbereitet.

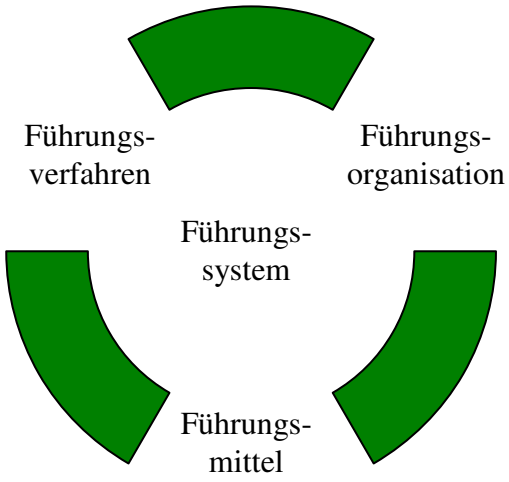


Abbildung 4: Das Führungssystem; Eigene Darstellung

[36] Meurers, Bernhard, Führungsverfahren auf Ebene Brigade und Bataillon, Truppendienst Taschenbuch Nr. 46, Reihe Ausbildung und Führung, Verlag AV + Astoria Druckzentrum GmbH, Wien, 2004, S36ff

2.3.1. Führungsorganisation

Die Führungsorganisation, die auf äußeren Faktoren wie Militärdoktrinen, internationalen Abkommen, Wehrsystem, Verfassung etc. basiert, folgt Regeln betreffend Führungsfunktionen, Führungsinformation und Führungsstruktur.

Die Führungsorganisation umfasst als Teil des Führungssystems des Bundesheeres die Bereiche der Führungsfunktionen und deren Aufgaben, der Führungsinformationen, der Führungsmittel und der Führungsstruktur.[37]

Die Führungsorganisation ist also die Grundstruktur der Armee. Sie regelt aber nicht nur Aufbau und Gliederung von Kommanden und Ebenen, sondern auch den gesamten Ablauf innerhalb der Strukturen. Sie koordiniert alle Tätigkeiten und Vorgänge wie beispielsweise Befehls- und Meldewege und regelt den Informationsfluss und das Informationsmanagement. Die Komponenten der Führungsorganisation sind hier kurz erläutert:

- *Führungsfunktionen* sind die dem Kommandanten einer Führungsebene zugeordneten Führungsgehilfen, die in ihren Fachbereichen Informationen aufbereiten und zur Unterstützung des Kommandanten in seiner Entscheidungsfindung dienen. Sie sind die Führungskräfte im Führungssystem, die durch ihre Leistungsfähigkeit und Ausbildung den Betrieb des Führungssystems sicherstellen.

- *Führungsstruktur* ist die grundsätzliche Einteilung der Führungsebenen hinsichtlich der Befehlsverhältnisse und Autoritäten.

- *Führungsinformationen* sind alle relevanten Daten und Informationen, die dem Kommandanten zur Entscheidungsfindung dienen. Sie sind Voraussetzung jeder Führungstätigkeit.

Gerade der Informationsbegriff spielt hier eine zentrale Rolle, da Information sowohl in inhaltlicher als auch zeitlicher Hinsicht die Grundlage für jede Führungstätigkeit darstellt. Der Informationsfluss, dem Struktur und Aufbau von Gefechtsständen und Organisationselementen angepasst sind, stellt einen Normprozess dar, der dazu dient, Information ohne Zeitverzug, inhaltlich richtig und zur weiteren Verarbeitung vorbereitet allen Führungsfunktionen (Kommandanten, Stab) verfügbar zu machen. Die Lenkung des Informationsflusses und ein Informationsmanagement, welches für Informationsgewinnung, Informationsverarbeitung und Informationsweitergabe verantwortlich ist, sind daher nicht nur die größten Anforderungen an die militärische Führungsorganisation als solches, sondern auch insbesondere an elektronische Führungsinformationssysteme der Zukunft.

[37] Dienstvorschrift für das Bundesheer, Führungsbegriffe, BMLV, 2005, S68

2.3.2. Führungsmittel

Das Führungsmittel ist das einer Führungsebene zur Verfügung stehende System, Gerät und/oder Verfahren, mit dem Informationen gewonnen, verarbeitet, gespeichert, dargestellt und übermittelt werden, um die eigene Führungsfähigkeit zu gewährleisten und die gegnerische zu beeinträchtigen.[38]

Erst Führungsmittel ermöglichen es, die für die Führungstätigkeit nötigen Informationen zu sammeln, aufzubereiten und in Befehle umzusetzen. Sie dienen auch der Übertragung der Befehle und stellen somit ein Bindeglied zwischen dem Führer und den Geführten dar. Sie sollen den Kommandanten in seiner wesentlichsten Aufgabe unterstützen und ihn bei Normabläufen und Routinetätigkeiten entlasten. Die Umsetzung von Führungsgrundlagen, also militärischen Anordnungen und Lagedarstellungen, die überhaupt erst Führungstätigkeiten auslösen, ist ohne Führungsmittel nicht möglich.

2.3.3. Führungsverfahren

Das Führungsverfahren ist ein festgelegter Denk- und Handlungsablauf zur Erfüllung militärischer Aufgaben.[39]

Es bildet einen Informationsverarbeitungsvorgang, bei dem Informationen über den Gegner, Aufklärungsergebnisse, Informationen über die eigenen Kräfte (Stärke, Verfügbarkeit etc.), Umfeldbedingungen (Wetter, Jahreszeit, Gelände etc.) in neue Informationen in Form von Aufträgen und Befehlen umgesetzt werden. Es ist also ein geregelter, normierter Prozess, der allen Entscheidungsträgern den Weg zur Entschlussfassung unter Berücksichtigung aller Einflussfaktoren ermöglicht. Es wird grundsätzlich auf allen taktischen Führungsebenen eingesetzt, kann aber auch vom einzelnen Soldaten im Gefecht zur Anwendung gebracht werden und findet sich in ähnlicher Ausprägung auch in der zivilen Welt wieder.

Das Führungsverfahren bildet einen ständigen Kreislauf in festgelegten Phasen, um eine vorgegebene Zielsetzung zu erreichen. Der Regelkreis beginnt mit dem militärischen Auftrag, also dem Ziel, das erreicht werden soll, und endet mit dem Befehl des Kommandanten, also dem Weg wie dies zu bewerkstelligen sei. Die Phasen der Lagefeststellung und der Planung sind die beiden wesentlichen Elemente dieses Regelkreises (Abbildung 5).

[38] Dienstvorschrift für das Bundesheer, Führungsbegriffe, BMLV, 2005, S68
[39] Olischer, Ing., Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003, S29

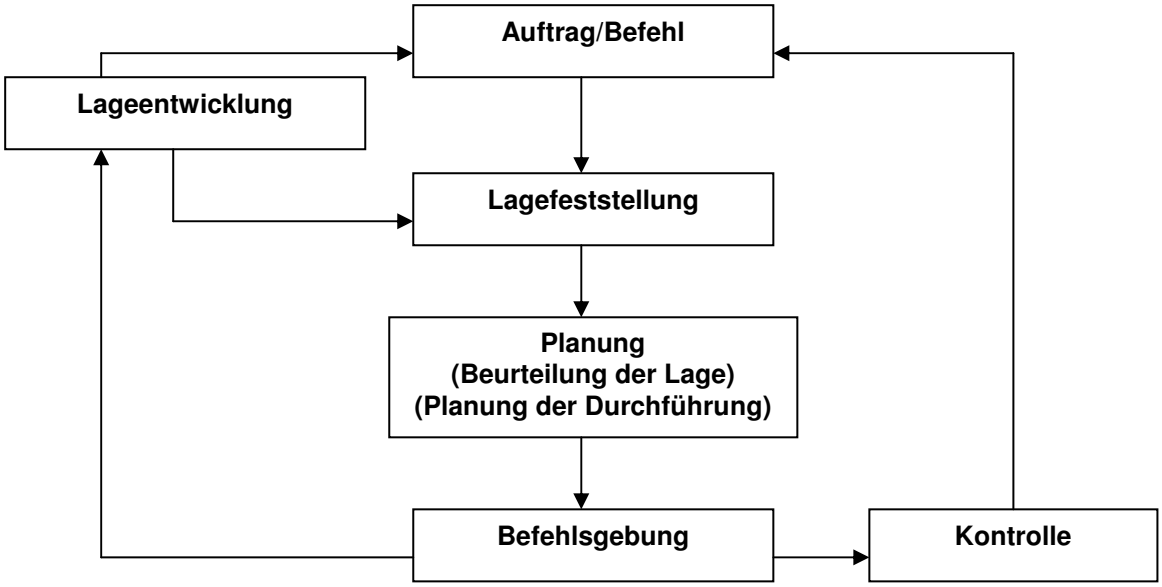


Abbildung 5: Regelkreis Führungsverfahren; Eigene Darstellung[40]

Die Phase der Lagefeststellung ist dabei jener Abschnitt, der zur Informationsgewinnung, -verarbeitung und –weitergabe dient.

Darauf folgt die Planungsphase, in der einzelne mögliche Varianten zur Erreichung des Ziels bzw. Umsetzung des erhaltenen Befehls gegeneinander abgewägt werden und an deren Ende der jeweilige Kommandant die Entscheidung in Form eines Entschlusses trifft. Folgende Arbeitsschritte sind in die Planung integriert und in Abbildung 6 dargestellt.

[40] Vgl. BMLV Merkblatt, Das taktische Führungsverfahren, BMLV, 2001

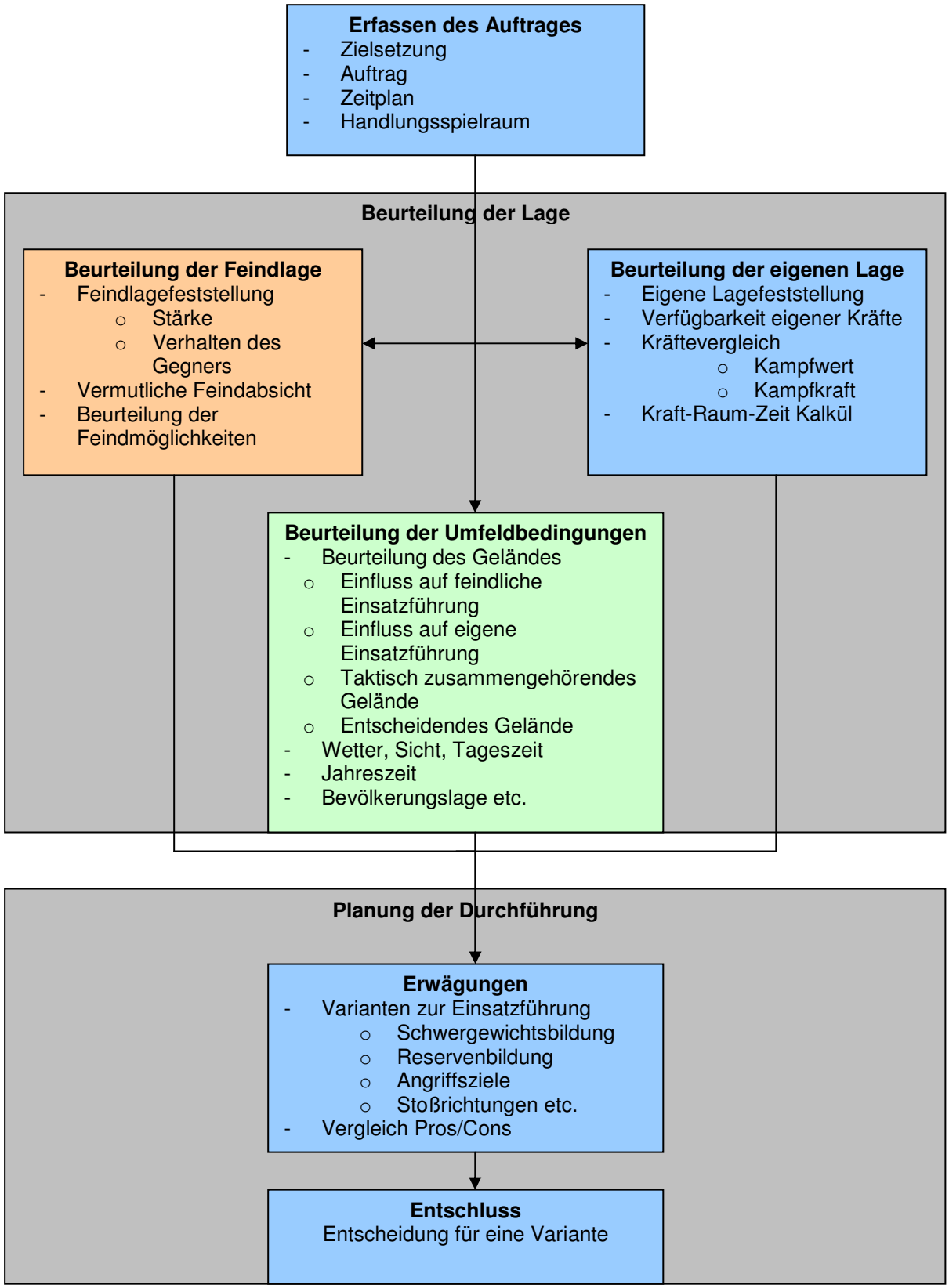


Abbildung 6: Beurteilung der Lage im Führungsverfahren; Eigene Darstellung[41]

[41] Vgl. Landesverteidigungsakademie, Handakt/Taktik, LAVAk, 2001, S5ff

Der Entschluss ist die Grundlage für die Befehlserstellung, die weitere Führungsverfahren auf unteren Ebenen zur Folge hat. Der Kreislauf beginnt dann von Neuem, denn die unmittelbare Auswirkung am Gefechtsfeld, also das Erreichen oder Nicht-Erreichen des Zieles sowie die Kontrolle der korrekten Umsetzung des Befehls oder Auftrags bedingt eine Folge- bzw. Neubeurteilung und somit ein neues Führungsverfahren.

2.4. Führungsverfahren – Ein alltäglicher Prozess

Das militärische Führungsverfahren lässt sich auch im zivilen Leben anwenden und wird, ob bewusst oder unbewusst in fast allen Bereichen zur Entscheidungsfindung eingesetzt. Es ist ein wohl alltägliches Verfahren, dass sowohl in Unternehmen als auch im Privatleben seine Entsprechung findet, sich aber resultierend aus den unterschiedlichen Aufgabenstellungen und Anforderungen natürlich in den Ausprägungen der einzelnen Phasen unterscheidet.

Die Entsprechung der klar strukturierten Vorgangsweise zur Entschlussfassung, die das Militär zur Vereinheitlichung und Normierung der Entscheidungsprozesse definiert hat, lässt sich anschaulich am Beispiel eines SW-Projektes darstellen.

Betrachtet man ein Projekt nach dem Unified Process Modell, so gliedert sich die Abwicklung in vier Phasen, Konzeptionsphase, die Entwurfsphase, die Konstruktionsphase und die Übergangsphase.[42]

Die militärische *Lagefeststellung und Planung* umfasst in diesem Sinne die Konzeption und den Entwurf, also jene Phasen, die vor der eigentlichen Umsetzung des Projektes, nämlich dem *Erfüllen des Auftrages* stehen. Es wird geprüft worum es eigentlich bei dem zu entwickelnden Produkt geht (*Erfassen des Auftrages*), ob es am Markt Konkurrenzprodukte gibt (*Beurteilung der Feindlage*), welche Ressourcen dem Unternehmen zur Verfügung stehen (*Beurteilen der Umfeldbedingungen)*, die Machbarkeitsanalyse (*Beurteilung der eigenen Lage*), Analysen- und Designphasen (*Erwägungen)*, sowie die Entscheidung das Projekt in der geplanten Form zu starten (*Entschluss*).

Sind es im militärischen Bereich Faktoren wie Gelände, feindliche Truppenstärke, Kraft-Raum-Zeitkalkül der eigenen Kräfte etc., die im Führungsverfahren abgearbeitet werden, so sind es im Unternehmen je nach Aufgabenstellung Marktanalysen, Kundengespräche, Personalplanung usw. die zur Beurteilung der Durchführbarkeit und der Art und Weise der Umsetzung in der Phase der Projektplanung durchlaufen werden.

Die Konstruktionsphase ist in weiterer Folge mit der anschließenden *Erfüllung des Auftrages* vergleichbar, die Übergangsphase kann mit dem Erreichen des strategischen bzw. taktischen Zieles verglichen werden.

[42] vgl.: Grechenig, Dipl-Ing. Dr., Thomas, at al.; Software Engineering, 2.Auflage, 2004, S.78ff

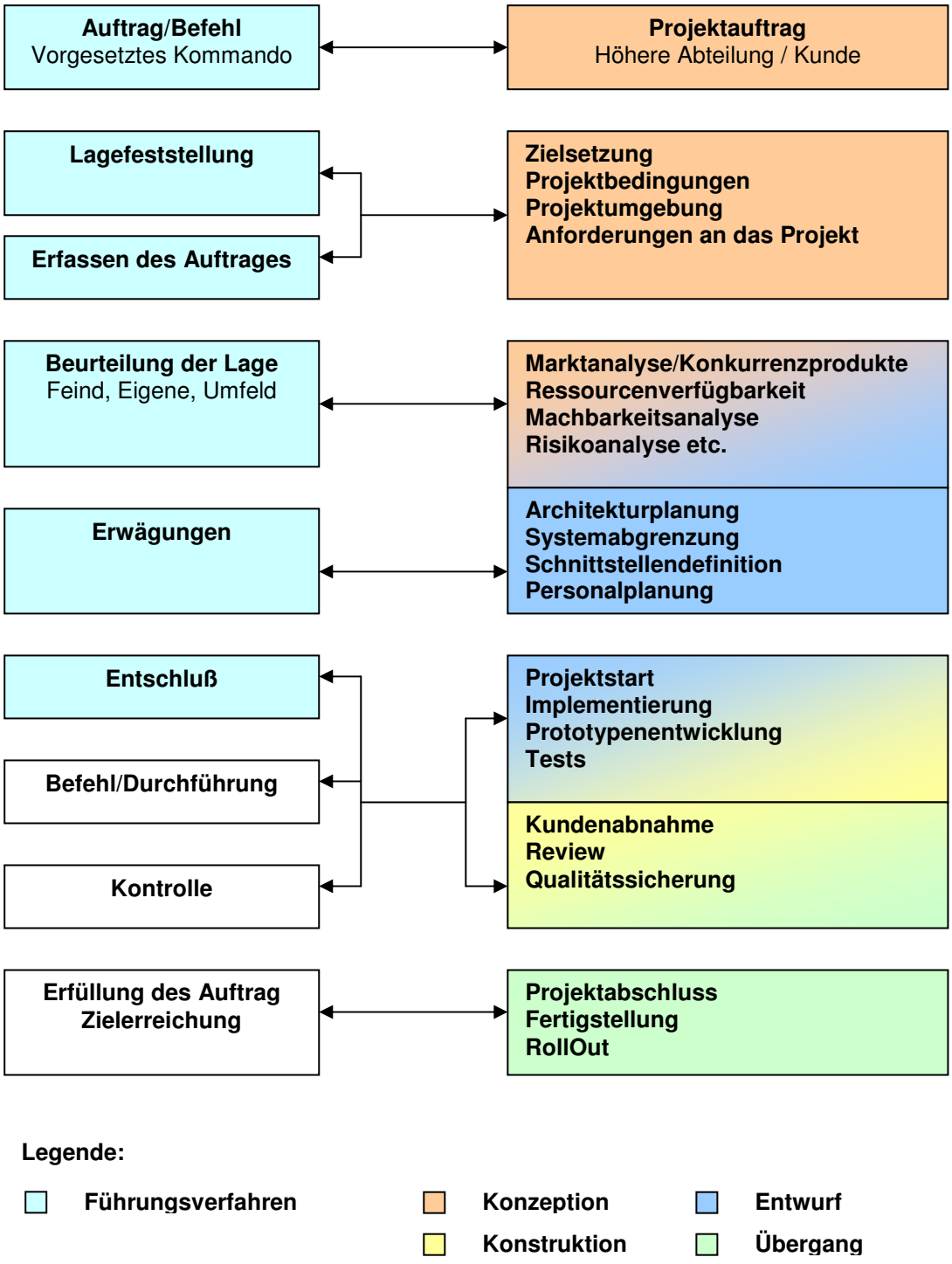


Abbildung 7: Schematischer Vergleich militärisches Führungsverfahren / SW-Projekt; Eigene Darstellung

Selbst Projektmeetings und Iterationsschritte innerhalb der Projektphasen finden ihre Entsprechung in den Befehlausgaben und Stabsbesprechungen, um Arbeitsschritte

gleichzuschalten und verschiedene Fachbereiche zu synchronisieren, sowie einen ständigen Informationsaustausch zu gewährleisten.[43]

2.5. Führungsebenen

Grundsätzlich wird zwischen drei Führungsebenen unterschieden, der strategischen, der operativen und der taktischen Ebene.

Strategie ist nach Carl von Clausewitz die *„Lehre vom Gebrauch der Gefechte zum Zweck des Krieges“*, Taktik nach seiner Definition *„die Lehre vom Gebrauch der Streitkräfte im Gefecht.“* [44].

Die Strategie *muss also dem ganzen kriegerischen Akt ein Ziel setzen, welches dem Zweck desselben entspricht, d.h. sie entwirft den Kriegsplan, und an dieses Ziel knüpft sie die Reihe der Handlungen an, welche zu demselben führen sollen, d.h. sie macht die Entwürfe zu den einzelnen Feldzüge und ordnet in diesen die einzelnen Gefechte an.*[45]

In der heutigen Zeit wird die strategische Ebene von der höchsten militärischen, aber auch politischen Führung gebildet, die durch ihre Zielvorgaben den Einsatz militärischer Mittel als strategische Maßnahme beschließt und die Kriegshandlungen akkordiert.

Die taktische Ebene ist dagegen der Einsatz militärischer Mittel im Gefecht zur Erreichung eines kurzfristigen Zieles. Sie ist die unmittelbare Führungsebene im Gefecht und ist für die Einsatzdurchführung verantwortlich. Taktik ist also nichts anderes, als die geplante Vorgehensweise am Gefechtsfeld.

Zwischen der strategischen und taktischen ist die operative Ebene angesiedelt. Sie ist für die Einsatzführung verantwortlich und koordiniert den Einsatz von Truppen über mehrere Gefechte hinweg. Sie definiert Angriffsziele und koordiniert den Kräfteeinsatz, immer dem strategischen Ziel folgend.

Aus den unterschiedlichen Aufgaben der Ebenen ergibt sich auch deren Informationsbedarf, dargestellt als Detaillierungsgrad von Aufklärungsergebissen:

[43] Der Unterschied zwischen dem militärischen Führungsverfahren und einem SW-Projekt liegt natürlich auch in der chronologischen Abarbeitung der Schritte im Militär, während in einem SW-Projekt bestimmte Arbeitsschritte auch vorgezogen werden können. Der methodische Vergleich bietet sich zur Veranschaulichung der Arbeitsweise dennoch an und untermauert zusätzlich das „Subsystem“ Militär der Gesellschaft.
[44] Clausewitz, Carl von, Vom Kriege, Insel Verlag, 2005, S.113
[45] Clausewitz, Carl von, Vom Kriege, Insel Verlag, 2005, S.205

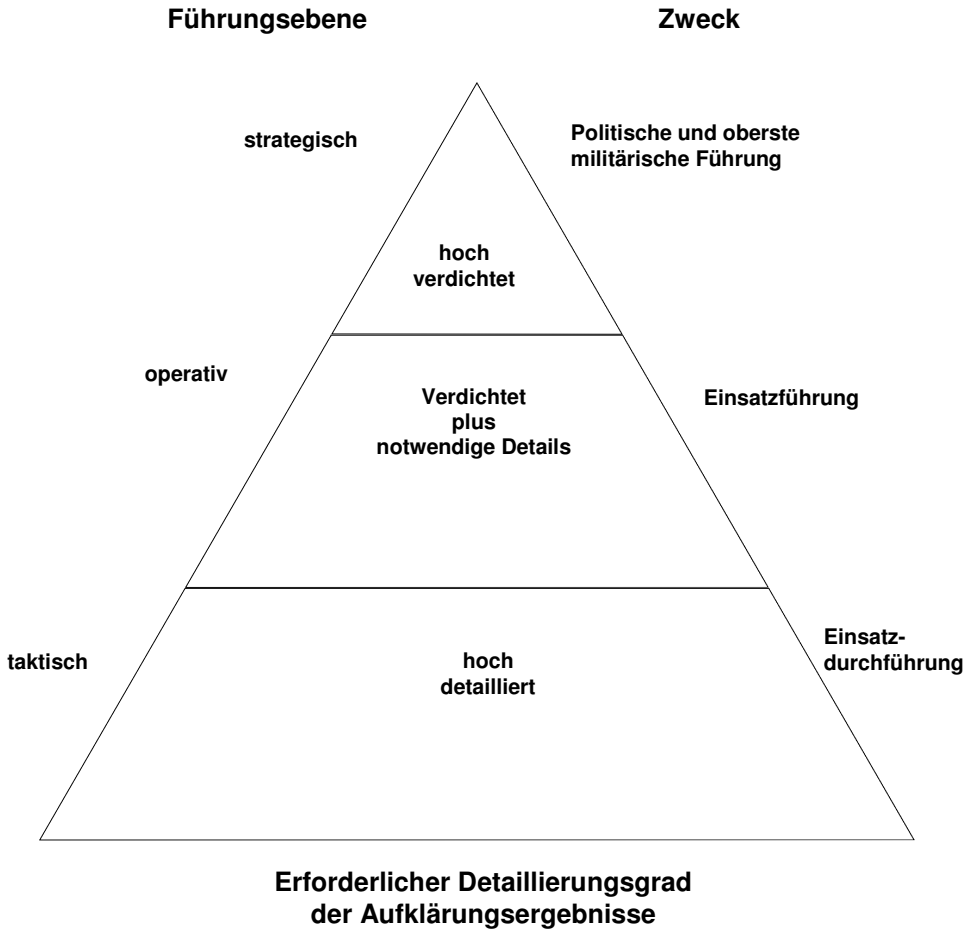


Abbildung 8: Informationsbedarf der Führungsebenen[46]

2.6. Informationsfluss

Ähnlich wie der Ablauf im Straßenverkehr ist der Informationsfluss über das vorhandene Netz an Kommunikationseinrichtungen so zu koordinieren, dass Information rasch und zeitgerecht den jeweiligen Empfänger erreicht. Dies betrifft alle Arten von Information, sowohl elektronische Meldungen, als auch postalische Schriftstücke, die analog über eine Einlaufstelle (Meldesammelstelle, Hauptkanzlei) erfasst, registriert und anschließend dem Empfänger zugestellt werden.

Der Normablauf zur Behandlung schriftlicher Schriftstücke, ob postalisch oder elektronisch, ist in der so genannten Geschäfts- oder Kanzleiordnung geregelt. Über diese wird, ähnlich wie in zivilen Betrieben, Information ihrem Bearbeiter zugeordnet, Bearbeitungswege gesteuert und der Informationsfluss an sich sichergestellt.

Darüber hinaus gibt es natürlich Information, die aufgrund ihrer Dringlichkeit bzw. ihrer Beschaffenheit nicht über eine zentrale Sammelstelle gesteuert werden kann. Eine Einheit im Gefecht hat nicht die Zeit, um Lagemeldungen schriftlich zu verfassen, ebenso kann im unmittelbaren Gefecht nur über mündliche Befehle geführt

[46] Olischer, Ing., Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003, S. 38

werden, da auf aktuelle Lageentwicklungen so schnell wie möglich reagiert werden muss. Hier wird der Informationsfluss über die Fernmeldemittel und die Vorgaben für ihren Betrieb gesteuert, um einen geordneten Ablauf der Informationsübertragung zu gewährleisten sowie eine Überlastung der vorhandenen Kommunikationsmittel zu verhindern.

2.7. Informationsmanagement

Um das Führungsverfahren überhaupt erst zu ermöglichen, ist ein Informationsmanagement vonnöten, das gezielt Maßnahmen zur Informationsgewinnung, Informationsverarbeitung und Informationsweitergabe setzt.

Informationsgewinnung
Information wird durch Maßnahmen der Aufklärung, Überwachung, durch Lagemeldungen eigener Teile, aber auch durch nachrichtendienstliche Ergebnisse sowie auch aus Medienberichten und der Zusammenarbeit mit nicht-militärischen Organisationen gewonnen. Dadurch entsteht ein breiter Pool an Information, die in weiterer Folge erst ausgewertet und aufbereitet werden muss, um Redundanzen, Fehler, Widersprüche, aber auch Informationsdefizite zu erkennen und zu beheben.

Informationsverarbeitung
Information zu bewerten, Zusammenhänge herzustellen und Priorisierungen zu treffen ist die Hauptaufgabe der Informationsverarbeitung. Sie ist prinzipiell an die Phase im Führungsverfahren gebunden und muss ein unmittelbares Einfließen von Ergebnissen in das laufende Führungsverfahren ermöglichen, denn nur so kann ein vollständiges Lagebild geschaffen werden.

In diesem Zusammenhang kann Information nach Relevanz und Präsenz unterschieden werden:

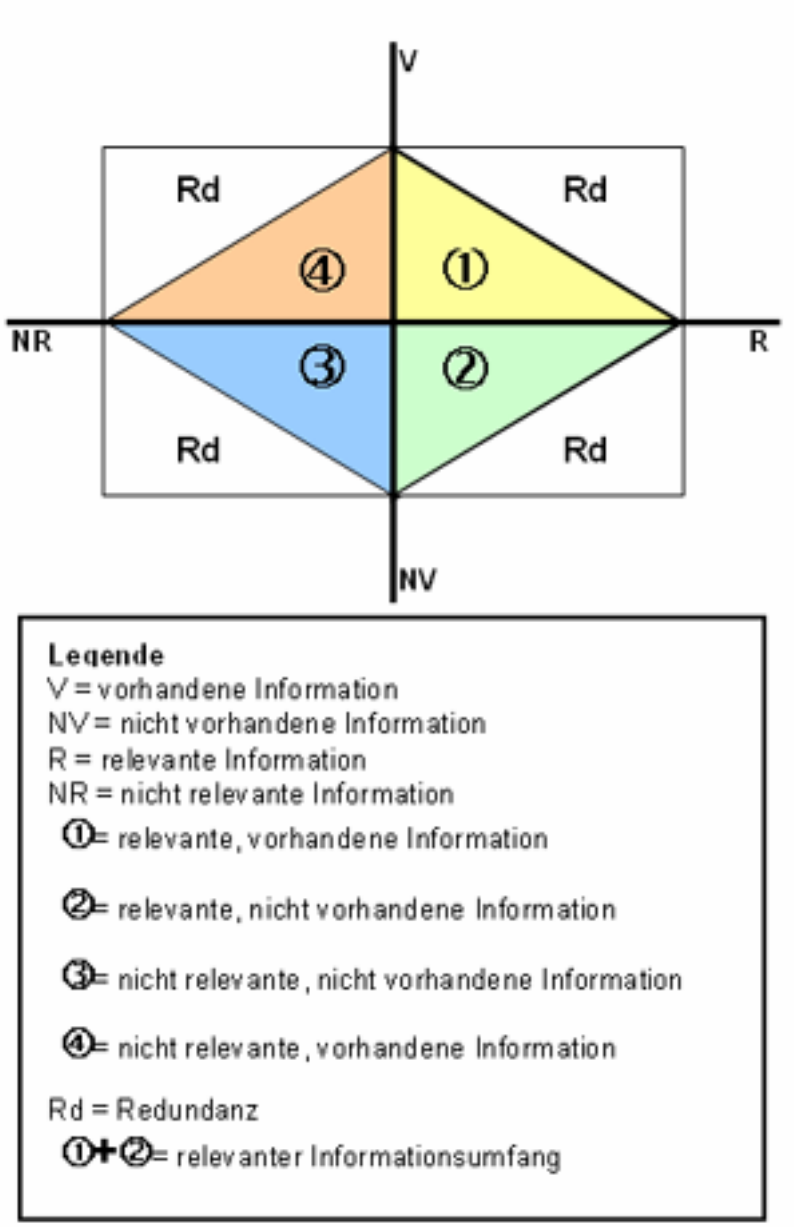


Abbildung 9: Darstellung der Informationsanteile[47]

Ist der Bereich der relevanten, aber unbekannten Information zu groß, kann das Führungsverfahren nicht abgewickelt werden und der Auftrag nicht erfüllt werden.
Daraus ergibt sich der *kritische Informationsbedarf*, also das Minimum an Information, das nötig ist, um eine erfolgreiche Entschlussfassung des Kommandanten und eine Umsetzung derselben überhaupt erst zu ermöglichen.

Informationsweitergabe
Eine weitere wichtige Anforderung an das Informationsmanagement ist die vollständige und zeitgerechte Weitergabe der Information an die richtigen Stellen und Personen, um ihnen dadurch die Erfüllung ihrer Aufgaben zu ermöglichen. Das Informationsmanagement muss dabei so flexibel sein, dass bei besonders dringlichen

[47] Meurers, Bernhard, Führungsverfahren auf Ebene Brigade und Bataillon, Truppendienst Taschenbuch Nr. 46, Reihe Ausbildung und Führung, Verlag AV + Astoria Druckzentrum GmbH, Wien, 2004, S.161

Informationen und Meldungen eine Umgehung der üblichen Melde- und Kommunikationswege möglich wird.

2.8. Die Bedeutung des Begriffs „Führung“ im Informationskrieg

2.8.1. Allgemeine Betrachtung

Führung spielt im Informationskrieg eine sehr zentrale Rolle. Das Wesen der Führung als Abbild der militärischen Strukturen lässt sich in allen Konzepten des Informationskrieges wieder finden und bildet wohl den Kern jeglicher Neuentwicklung auf diesem Sektor. Jedes Führungsinformationssystem, jede Entwicklung von vernetzten Strukturen, jede Tätigkeit zur Informationsgewinnung, aber auch die bloße Weiterentwicklung technischer Systeme dient dem höheren Ziel, die eigene Führungsfähigkeit zu optimieren und effizienter zu gestalten.
Selbst alle Maßnahmen zum Erreichen der Informationsüberlegenheit, alle Störmaßnahmen gegnerischer Einrichtungen, alle Intentionen, dem Feind wichtige Informationen über sich selbst vorzuenthalten werden erst nach der Beurteilung der Lage als bewusste Führungsmaßnahme gesetzt.

Bereits vorhandene elektronische Führungsinformationssysteme sammeln Information und bereiten diese unter Berücksichtigung der Führungsorganisation und in Hinblick auf die Relevanz für die einzelnen Ebenen auf, um so den Kommandanten durch möglichst umfassende, aber auch gezielte Informationen die Führung der eigenen Kräfte zu ermöglichen und ihn Entscheidungen treffen und Führungsmaßnahmen setzen zu lassen, die ohne den Einsatz solcher Systeme nicht bzw. nicht rechtzeitig getroffen bzw. gesetzt werden könnten.

Führung ist daher nicht nur Teil, sondern Grundlage des Informationskrieges. In diesem Zusammenhang kann man den Informationskrieg[48] durchaus auch als Wettstreit um die effizientere, optimiertere Führung bzw. als Kampf um die Führungsüberlegenheit sehen, denn schlussendlich steht Führung hinter jeder einzelnen Maßnahme im militärischen Konflikt, sei er nun konventionell oder im Zusammenhang mit dem Informationskrieg zu betrachten. Die Verbesserung der Führungsfähigkeit bzw. das Erreichen der Führungsüberlegenheit ist Ziel und Zweck in den Konzepten der modernen Kriegsführung.

[48] siehe Kapitel 3

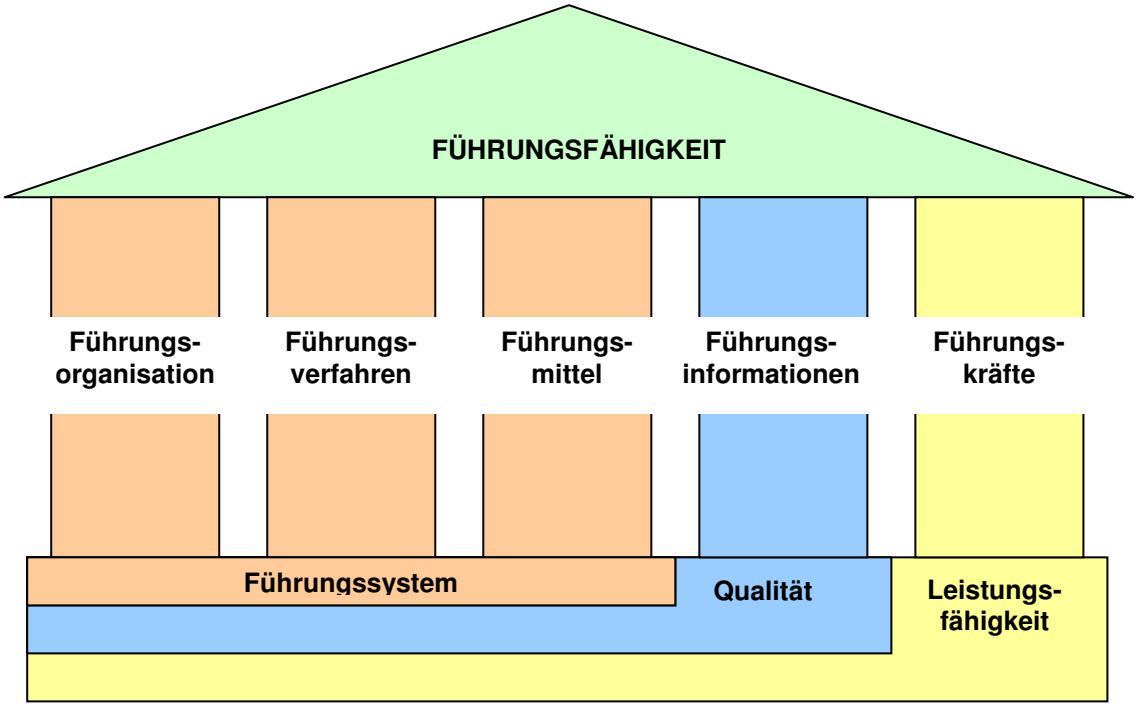


Abbildung 10: Führungsfähigkeit [49]

Hier lässt sich aber auch der Zusammenhang zwischen Führung, Technologie und Doktrin herstellen. Während die theoretischen Führungssysteme als solche sich grundsätzlich an den Doktrinen des Militärs orientieren, fußt dessen praktische Umsetzung in technologischen Systemen, eben den Führungsinformationssystemen, die ihrerseits eine Optimierung und effizientere Gestaltung der Führung und in weiterer Folge der Doktrinen zulassen. Aus diesen Synergieeffekten resultieren Änderungen der Organisationsstruktur, die Vernetzung von Kommunikationswegen und Hierarchien, neue, teilstreitkräfteübergreifende Führungsverfahren und natürlich auch strukturelle Veränderungen der Streitkräfte sowie eine ständige Anpassung der strategischen Ziele und Doktrinen. Man erkennt also deutlich die reziprokale Einflussnahme der Faktoren Führung, Doktrin und Technologie.

2.8.2. Führung-Technologie-Doktrin am Beispiel des Blitzkrieges

Sehr deutlich lässt sich dieser Zusammenhang auch am Beispiel des so genannten „Blitzkrieges“ im Westfeldzug der Deutschen Wehrmacht während des Zweiten Weltkriegs veranschaulichen. Die Entwicklung der „Blitzkrieg-Doktrin“ gilt als Wendepunkt in der Militärgeschichte, war allerdings – entgegen der heute weit verbreiteten Meinung, Hitler hätte diese Doktrin schon lange vor dem Krieg entwickelt - in dieser Form nie geplant und ist aus den historischen Ereignissen heraus entstanden.[50] Die deutsche Führung und der

[49] Olischer, Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003
[50] Frieser, Karl Heinz, Blitzkrieg-Legende, Der Westfeldzug 1940; R.Oldenburg Verlag München, 1995

deutsche Generalstab waren, ebenso wie ihre Gegner auf alliierter Seite, noch stark den Denkmustern des Ersten Weltkrieges mit seinem Stellungs- und Abnutzungskrieg verhaftet und nach den Theorien des italienischen Generals Douhet ging man sogar davon aus, dass Kriege in der Zukunft ebenfalls als Abnutzungskriege geführt werden würden.[51]

Auch war die Wehrmacht zahlen- und materialmäßig den Alliierten Streitkräften unterlegen, nach den Beschränkungen der Versailles-Verträge erst im hektischen Aufbau begriffen und wurde selbst vom eigenen Generalstab als „nicht kriegsfähig" beurteilt. Dies zwang die Generäle schon früh alternative Strategien zu entwickeln, die frei nach Clausewitz durch die Vernichtung der feindlichen Kräfte eine schnelle Entscheidung herbeiführen sollten.[52]

Aufgrund der zahlen- und materialmäßigen Unterlegenheit und der gleichzeitigen Bedrohung von mehreren Seiten entdeckte man daher die im Ersten Weltkrieg vernachlässigte operative Ebene wieder:
„Das operative Denken des deutschen Generalstabs entwickelte sich unter dem Alptraum eines immer wieder drohenden Zwei-Fronten-Krieges. Hierbei musste man (…) folgendes Ziel verfolgen: Wenn es gelang, einen Gegner in einer sofortigen Entscheidungsschlacht niederzuwerfen, konnte man sich anschließend voll auf den anderen konzentrieren. So ließ sich ein Krieg an zwei Fronten auseinanderdividieren in zwei aufeinanderfolgende Kriege an einer Front."[53]

Ein völlig anderer Konflikt als der Stellungskrieg des Ersten Weltkrieges zeichnete sich also ab, ein Konflikt, in dem dem Element „Bewegung" zu Lasten des Elements „Feuer" wieder wesentlich mehr Bedeutung zukam, für den die technischen Vorraussetzungen allerdings schon längst geschaffen waren, wenn auch unter anderen Vorgaben.[54]
Als logische Konsequenz daraus ergab sich der operative Einsatz der Panzerwaffe, der ein Konzept darstellte, dass bis zu diesem Zeitpunkt in dieser Form keinen Einzug in strategische Überlegungen fand, zum einen, weil der Stellungskrieg im Ersten Weltkrieg einen solchen Einsatz sinnlos machte, zum anderen, weil auch die technische Reife der Fahrzeuge fehlte.

Mit dem Prinzip des Durchbruchs weit hinter die feindlichen Linien und dem Angriff in den Rücken des Feindes sollte schnell die Entscheidung am Schlachtfeld herbeigeführt werden, den daraus resultierenden Anforderungen

---

Karl-Heinz Frieser widerlegt in diesem Buch die These, dass die Doktrin des Blitzkriegs als solche bereits vor dem Zweiten Weltkrieg entstanden ist.

[51] vgl. Frieser, Karl Heinz, Blitzkrieg-Legende, Der Westfeldzug 1940;R.Oldenburg Verlag München, 1995, S.428

[52] Es gibt nach Clausewitz zwei Grundsätzliche Möglichkeiten, einen Krieg zu gewinnen:
- durch einen Vernichtungssieg oder
- einen Erschöpfungssieg.

Ersteres lässt sich in einer schnell herbeigeführten Entscheidungsschlacht erreichen, letzteres durch einen lange anhaltenden Abnutzungskrieg.
Und vgl. Frieser, Karl Heinz, Blitzkrieg-Legende, Der Westfeldzug 1940; R.Oldenburg Verlag München, 1995; S412
und Clausewitz, Carl von, Vom Kriege, Insel Verlag, 2005, S308ff

[53] Frieser, Karl Heinz, Blitzkrieg-Legende, Der Westfeldzug 1940; R.Oldenburg Verlag München, 1995; S416

[54] Hier ist die ursprüngliche Entwicklung der Panzerwaffe als Begleitwaffe für die Infanterie gemeint. Der Einsatz der Panzerwaffe als operative Kraft war bis zum Zweiten Weltkrieg nicht angedacht.

an das Führungssystem begegnete man unter anderem mit Technologie. Die Entwicklung entsprechender Panzer mit ausreichender Schnelligkeit und Fahrreichweite sowie der Einsatz von Fernmeldemitteln auch über weite Distanzen hinweg stellten die beiden wichtigsten Faktoren dar. Die Möglichkeit per Funk jeden einzelnen Panzer direkt führen und so effizient und in Sekundenschnelle auf Lageänderungen reagieren zu können sorgte für einen enormen Führungsvorteil im Gefecht.
Dabei waren die technischen Möglichkeiten der Deutschen nicht besser als die der Alliierten, allein die Einsatzgrundsätze waren unterschiedlich. Hatte die Panzerwaffe für die Alliierten beispielsweise nur unterstützenden Charakter, so bildete sie für die Deutschen die Grundlage für ihre strategischen Angriffspläne. So konzentrierte die Wehrmacht ihre Panzer in 10 neugeschaffenen Panzerdivisionen, während die Alliierten ihre Panzer gleichmäßig in Kompaniestärke an den Verteidigungslinien verteilten.

Die Strategie ging auf und der deutsche Schlag traf die Alliierten mit einer solchen Wucht, dass die Front rasch zusammenbrach - so rasch, dass man selbst in Deutschland von einem Wunder sprach, da man mit einem solchen Erfolg nicht gerechnet hatte.[55] Erst durch diese Erfolge und nach dem Westfeldzug im Mai 1940 wurde diese Strategie zur Doktrin erhoben und durch die Propaganda-Maschinerie zur Legende hochstilisiert.

Die Deutschen hatten also die neuen sich durch den gezielten Einsatz damals moderner Technologie bietenden Möglichkeiten erkannt und reagiert. Sie schufen neue Strukturen und Kommunikationsnetze und entwickelten mit dem Konzept des operativen Bewegungskrieges eine völlig neuartige Strategie der Kriegsführung. Vor dem Hintergrund des Zusammenhangs zwischen Führung-Technologie-Doktrin werden hier nicht nur die bereits angesprochenen Wechselwirkungen deutlich, man kann auch noch einen Schritt weitergehen und sagen, dass durch die technischen Entwicklungen am Rüstungssektor und die dadurch erreichte Führungsüberlegenheit die Strategie des Blitzkrieges überhaupt erst zur Doktrin werden konnte.[56] In Abschnitt II werden wir diesen Zusammenhang noch einmal aufgreifen und hinreichend darstellen.

2.9. Führungsinformationssysteme und Fachinformationssysteme

Die Bemühungen zur Erreichung der Führungsüberlegenheit sowie zur Optimierung der Abläufe und Prozesse innerhalb der Führungsorganisation hat ähnlich wie in der zivilen Gesellschaft Lösungen und Lösungsansätze hervorgebracht, lange bevor man vom Informationskrieg als solches sprechen konnte. Die Entwicklung einzelner Systeme vor allem der Amerikaner führte zu Insellösungen, wobei jede für sich eine Kampfwertsteigerung mit sich brachte. Eine Zusammenarbeit zwischen den einzelnen Systemen und somit zwischen verschiedenen Waffengattungen war aber aufgrund fehlender Schnittstellen und unterschiedlicher Systemarchitekturen nur beschränkt möglich. Erst die Gewichtung der „Joint Operations“, also dem Zusammenwirken und

[55] Selbst Adolf Hitler sprach im Zusammenhang mit den Erfolgen an der Westfront von einem *„ausgesprochenen Wunder“*.
vgl Frieser, Karl Heinz, Blitzkrieg-Legende, Der Westfeldzug 1940; R.Oldenburg Verlag München, 1995; S3
[56] Anm.: In der heutigen Zeit spricht man übrigens nicht mehr vom Blitzkrieg, sondern vom „operativen Bewegungskrieg“.

Zusammenarbeiten der Teilstreitkräfte ließ nach und nach die Notwendigkeit eines homogenen Konzepts erkennen, dass die Vernetzung der Streitkräfte zur Folge hat.

Betrachtet man die Entwicklung parallel dazu am Sektor des E-Business, das als zivile Schiene parallel zum Informationskrieg durchaus mit den Konzepten zur vernetzten Kriegsführung vergleichbar ist, so kann man feststellen, dass die Gesellschaft in allen ihren Bereichen diese Entwicklung vollzieht. Management-Informationssysteme erfüllen in Unternehmen die gleichen Aufgaben wie die Führungsinformationssysteme im militärischen Bereich, sie stellen effizientere Prozessabläufe sicher, managen den Informationsfluss, optimieren Entscheidungsprozesse und schaffen so eine Informations-, Führungs-, und Wirkungsüberlegenheit gegenüber anderen Unternehmen, durch die auf die Entwicklungen des Marktes schneller und somit gewinnbringender reagiert werden kann.

Beispiele für Führungsinformationssysteme sind

- ADLER — Artillerie Daten-Lage-Einsatz-Rechnerverband (Bundeswehr)
- SATIR — System zur Auswertung Taktischer Informationen auf Raketenschiffen
- IFAB — Integrierte Feuerleitung Artillerie Batterie (Bundeswehr)
- NADGE — NATO Air Defense Ground Environment
- FüInfSysLw — Das Führungsinformationssystem der deutschen Luftwaffe
- HEROS — Das Führungsinformationssystem des deutschen Heeres
- INTAFF — Integriertes Artillerie Feuerführungs- und Feuerleitsystem (Schweiz)

Anhand dieser Beispiele lässt sich aber auch die Problematik der Abgrenzung des Begriffs Führungsinformationssystem erkennen[57]. Viele Quellen verwenden fälschlicherweise den Begriff Führungssystem[58], was aber gemäß unserer Definition aus 2.3 falsch ist. Oft werden weiters Waffen- und Aufklärungssysteme als Führungsinformationssysteme oder eben fälschlicherweise als Führungssysteme bezeichnet[59], was zwar in Hinblick auf die Insellösungen nicht falsch ist, in Bezug auf eine Generalisierung des Begriffs aber hinderlich ist. Im Verständnis der netzwerkgestützten Kriegsführung und der damit verbundenen Transformation der

[57] Vgl. Hofmann, Hans (Hrsg.), Führungs- und Informationssysteme, Probleme, Erfahrungen und Technologien im militärischen Bereich, Oldenburg R. Verlag Gmbh, 1982, S.41f

[58] Vgl. Fraunhofer Institut Intelligente Analyse und Informationssysteme, URL: http://www.iais.fraunhofer.de/ps.html (Abgerufen: 11.10.2008); Das Institut spricht im Zusammenhang mit seinen Geschäftsfeldern von „Lösungen für (…)Simulations-, Einsatzunterstützungs- und Führungssystemen“ Und vgl. Linke, Peter, Ungleichgewicht des Schreckens, In Freitag, 16.02.2001 URL: http://www.freitag.de/2001/08/01080901.htm (Abgerufen: 11.10.2008); Linke spricht ebenfalls im Zusammenhang mit technischen Systemen von Führungssystemen

[59] vgl. Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr, German Improved Air Defence System (GIADS), URL: http://www.it-amtbw.de/portal/a/itamtbw/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLNzKKN_Sy8AFJgjlejoH6kQjhoJRUfV-P_NxUfW_9AP2C3IhyR0dFRQCzn0K2/delta/base64xml/L3dJdyEvd0ZNQUFzQUMvNElVRS82XzIyXzFKOEw! (Abgerufen: 11.10.2008)
Und: vgl: EADS, Flugabwehrführungssystem SAMROC, URL: http://www.eads.net/1024/de/businet/defence/dcs/solutions/air_defence%20Copy/samoc%20Copy/samoc%20Copy.html (Abgerufen: 11.10.2008)

Streitkräfte kann ein Führungsinformationssystem nur mehr als homogenes Informationsverarbeitungssystem aller Waffengattungen verstanden werden, das sowohl die Strukturen der Führungsorganisation abbildet, als auch die Aufgaben der bisherigen Insellösungen wahrnimmt. Bestehende Waffen- und Aufklärungssysteme können dabei integraler Bestandteil neuer Führungsinformationssysteme sein, nicht aber ein solches für sich.[60]

Allerdings ist zu beachten, dass damit nur Systeme zur Einsatzführung gemeint sein können, da die Einführung und Anwendung solcher fortgeschrittenen Systeme in allen militärischen Bereichen, also auch beispielsweise in der Verwaltung, zu kostenintensiv und aufwandsintensiv wären und wohl auch nicht gefordert sind. In diesen Bereichen kommen ähnliche Fach- oder Management-Informationssysteme zum Einsatz, wie man sie aus Wirtschaftsbetrieben kennt. Die Unterschiede sind in Abb. 2.3 dargestellt.

Führungsinformationssysteme CCIS (Command&Control Information Systems)	**Fachinformationssysteme MIS (Management Information Systems)**
- **Realzeitverarbeitung** - **Verzuglose Kommunikation durch mehrere Führungsebenen** - **Überlebensfähigkeit**	- **Geringere Zeitanspruch** - **Massenverarbeitung** - **Eingeschränkte Überlebensfähigkeit (bestimmte Datenbestände)**
tendenziell **HOHER Realisierungsaufwand** - **besondere Hardware** - **große Redundanz** - **Überlebensmaßnahmen** o **Bunker** o **Auflockerung (Back-up)** o **Mobilität** o **EMP-Härtung**	**tendenziell** **GERINGERER Aufwand** - **Handelsübliche Hardware** - **keine Redundanz** - **Auslagerung der Info** - **Ausweichen auf zivile Rechner**

Abbildung 11: Typisierung von Informationssystemen[61]

[60] In diesem Zusammenhang sei auch auf die Bedeutung des Begriffs „System of Systems“ aus der NCW verwiesen.

[61] Vgl. Hofmann, Hans (Hrsg.), Führungs- und Informationssysteme, Probleme, Erfahrungen und Technologien im militärischen Bereich, Oldenburg R. Verlag Gmbh, 1982, S.33

3. Der Informationskrieg

Si vis pacem, para bellum.
(Asterix, Band XXIII, Obelix GmbH & Co. KG, S33)

Schon früh begann der Mensch, Gewalt als Lösung zu sehen und seine Konflikte kriegerisch zu lösen. Von Anfang an stand dabei, wenn auch erst durch die Maßstäbe der heutigen Zeit erkennbar, der Begriff Information im Mittelpunkt. So versuchte man in frühen Konflikten, durch Späher und Boten möglichst Standort und Stärke der feindlichen Truppen zu erfahren und die eigene Kommunikation aufrecht zu erhalten, während der Feind über die eigene Stärke und Standort möglichst im Unklaren gelassen wurde, um durch den so gewonnenen Informationsvorteil die eigenen Kräfte besser zum Einsatz zu bringen. Die Mongolen, deren Strategie fast ausschließlich auf dieser Vorgangsweise beruhte, konnten so die großen Armeen der Christen, des Islam und des chinesischen Kaiserreichs besiegen. Die Bedeutung von Information im Kampf ist also so alt wie der Krieg selbst.[62]

„Im Laufe der Geschichte haben militärische Doktrin, Organisation und Strategie tiefgreifende Veränderungen durchgemacht, die zum Teil auf bahnbrechenden technischen Neuerungen begründet waren.“[63] Die Erfindung des Schießpulvers beispielsweise beendete die Kämpfe Mann-Gegen-Mann mit Schwert und Speer und etablierte eine neue Schlachtordnung am Felde, die Erfindung des Maschinengewehres zwang die Soldaten in die Schützengräben und der Einsatz früher Kommunikationstechnologie erhöhte schon die Koordinations- und Führungsfähigkeit der napoleonischen Truppen entscheidend.

Mit der Industrialisierung des Krieges und den großen Schlachten des Ersten und Zweiten Weltkrieges gewann der Begriff des Informationsvorteils auch im Bewusstsein der Strategen an Bedeutung. Information wurde nach und nach zu einem zentralen militärischen Element. So konnten beispielsweise die Truppen des Deutschen Kaiserreichs die Schlacht bei Tannenberg (1914) nicht zuletzt deshalb gewinnen, weil sie durch ihre fortschrittliche Funk- und Luftaufklärung über jede Handlung der Zarentruppen im Klaren waren, während die Russen ihrerseits den Standort der 8.Armee unter der Führung der Generäle Hindenburg und Ludendorff völlig falsch einschätzten.[64]

Clausewitz sprach einst vom „Nebel des Krieges“[65] und beschreibt damit nichts anderes, als den enormen Nachteil, der durch Unwissenheit von Standort, Stärke, Lage des Feindes etc. entsteht. Diesen „Nebel des Krieges“ versuchen moderne Armeen durch den Einsatz von Informationstechnologie zu lichten und sich damit einen

---

[62] Arquilla, John; Ronfeldt, David; „Der Cyberkrieg kommt“ in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork, 1998, S35
und: Schätz, Alfred, Nachrichtendienste im Transformationsprozess in Österreichische Militärzeitschrift, Ausgabe 4/2007, S.395

[63] Arquilla, John; Ronfeldt, David; „Der Cyberkrieg kommt“ in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork, 1998, S25

[64] vgl.: Artikel *Schlacht bei Tannenberg (1914).* In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 5. Oktober 2008, 04:11 UTC. URL: http://de.wikipedia.org/w/index.php?title=Schlacht_bei_Tannenberg_(1914)&oldid=51484791 (Abgerufen: 6. Oktober 2008, 02:05 UTC)
und: Dirks, Ekhardt, *Die Schlacht von Tannenberg,* URL: http://www.tannenberg1914.de/ (Abgerufen: 6. Oktober 2008)

[65] Clausewitz, Carl von, Vom Kriege, Insel Verlag, 2005, S67f

Informationsvorteil in Friedens- sowie in Kriegszeiten zu sichern. Moderne Aufklärungsflugzeuge, Satellitenaufklärung, Peil- und Ortungssysteme, Radaranlagen sowie die nötigen Gegenmaßnahmen etc. haben längst Einzug in die moderne Kriegsführung gehalten und das Bild des Krieges als solches massiv verändert.

Aber der Informationskrieg ist mehr als der bloße Einsatz elektronischer Kampfmaßnahmen am Gefechtsfeld, er ist ein umfassendes Gesamtkonzept, dass sowohl den zivilen als auch militärischen Bereich gleichermaßen betrifft. Er ist eine *„(…) immanente Erscheinung unserer Gesellschaft, deren Motor Technologien sind, die aus dem militärischen Zusammenhang entwickelt wurden."*[66]

Wenn wir heute also vom Informationskrieg sprechen, so müssen wir konsequenterweise auch von der Informationsgesellschaft sprechen, einem Gesellschaftstyp, in dem *„Information als Produktionsfaktor und Konsumgut, als Kontroll-, Herrschafts- und Steuerungsmittel bedeutsamer wird."*[67]

3.1. Der Informationskrieg als Konfliktform der Informationsgesellschaft

Krieg ist auch ein Abbild der Gesellschaft. In der Geschichte der Menschheit war die Art und Weise, Krieg zu führen, immer eng verbunden mit dem sozialen System, den wirtschaftlichen Voraussetzungen, dem technischen Standard und den gesellschaftlichen Strukturen ihrer Zeit.[68] Analog zum gesellschaftlichen Wandel hat sich auch der Krieg immer wieder verändert und neue Formen der Konfliktführung hervorgebracht, die ihren Niederschlag in Doktrinen und Führungssystemen gefunden haben.

In seiner Studie „The Third Wave" gliedert Alvin Toffler[69] die Geschichte der Menschheit in drei Transformationsprozesse, die durch Innovationswellen ausgelöst wurden. Die Erste Welle sieht er in der Agrarrevolution begründet, die dem Menschen den Ackerbau brachte und das Agrarzeitalter einläutete. Die industrielle Revolution brachte die zweite Innovationswelle und begründete die Industriegesellschaft und bereits heute seien die Auswirkungen der Dritten Welle, des Informationszeitalters, zu spüren. *„Jede Welle schuf eine neue Art von Zivilisation. Heute (…) sind wir im Begriff, eine revolutionäre Zivilisation der Dritten Welle hervorzubringen, mit ihrer eigenen Wirtschaft und Politik, eigenen Familienformen und Medien."*[70]
Toffler spannt nun den Bogen von der Entwicklung der Gesellschaft hin zur Transformation der Kriegsführung und beschreibt auch die Evolution des Krieges mit Hilfe seines Stadienmodells.[71]

---

[66] Stocker, Gerfried (Hrsg.), „Information.Macht.Krieg" in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork, 1998, S16
Mit dem Hinweis auf die Technologien, die im militärischen Zusammenhang entwickelt wurden, meint der Autor hier Computer und Internet, deren Entwicklung vor allem durch das Militär betrieben wurde
[67] Bühl, Achim; Die virtuelle Gesellschaft; Westdeutscher Verlag, 1997; S33
[68] Begriffe wie „Werte" oder „Ethik" lasse ich hier bewusst außer Acht
[69] vgl. Toffler, Alvin; Toffler, Heidi; Überleben im 21.Jhdt; Übersetzt aus dem Amerikanischen „War and Anti-War" von Helmut Dierlamm et al. Deutsche Verlags Anstalt, 1994; S22
[70] Toffler, Alvin; Toffler, Heidi; Überleben im 21.Jhdt; Übersetzt aus dem Amerikanischen „War and Anti-War" von Helmut Dierlamm et al. Deutsche Verlags Anstalt, 1994; S22
[71] Das Stadienmodell Tofflers beschreibt die Entwicklung der Gesellschaft in drei Stufen: der Agrar-, Industrie- und Informationsgesellschaft

3.1.1. Die Evolution des Krieges

Toffler geht dabei von einem ökonomisch-technischen Ansatz aus und zieht Parallelen zwischen der Form der Arbeit und der Art Krieg zu führen. So war Kriegshandwerk im Agrarzeitalter oft saisonal bedingt, da die Soldaten auch zu Hause ihre Felder bestellen und so das Überleben der Gesellschaft sichern mussten. Die harte Arbeit der Bauern am Felde fand ihr Korrelat im Kampf Mann gegen Mann am Gefechtsfeld, die Waffen waren so wie das Ackerwerkzeug nur zum Teil standardisiert und die eigentliche Kriegshandlung bestand hauptsächlich aus dem Nahkampf unter dem Einsatz von Muskelkraft. Oft wurden die Soldaten statt mit Geld mit Land entschädigt, der wichtigsten Ressource der Agrargesellschaft. Eine Tradition, die sich in Teilen Europas sogar bis ins 19.Jahrhundert hielt.[72]

Die zweite Welle begann mit der Industrialisierung der Gesellschaft vor rund 300 Jahren und dieser Transformationsprozess ist laut Toffler in vielen Ländern der Erde selbst heute noch nicht abgeschlossen. Die Möglichkeit, Güter in Massenproduktion zu fertigen und Maschinen zu bauen schuf nicht nur völlig neue Arbeitsplätze, sie prägte auch die gesellschaftlichen Strukturen und Staatsformen neu. Eine Entwicklung, die sich analog dazu auch auf die Kriegsführung auswirkte, denn fortan waren es nicht mehr Lehnsherren, Clanführer oder Grundbesitzer, die Armeen aufstellten, sondern der moderne Nationalstaat, der sein Volk in den Kriegsdienst stellte. Die Industrialisierung des Krieges fand parallel zu der Industrialisierung der Gesellschaft statt, neue Waffen konnten schnell und in großer Stückzahl produziert werden, der Kampf Mann gegen Mann machte Materialschlachten Platz. Es ging um gezielte flächendeckende Vernichtung, in seiner ausgeprägtesten Form sogar um Massenvernichtung, wie die Entwicklung und auch der Einsatz der Atombombe deutlich machen.

Mit der zunehmenden Bedeutung der Informationstechnologie begann nun um 1900 die Dritte Welle, also der Wandel von der Industriegesellschaft zur Informationsgesellschaft. Eine Entwicklung, die immer noch anhält und deren Auswirkungen nicht nur in unserem täglichen Leben, sondern auch beim Militär durchaus schon beobachtet werden können.
Nicht mehr Feuerkraft und Reichweite, sondern Information stehen nun im Mittelpunkt militärischer Überlegungen und die Dritte Welle, die gerade stattfinden soll, wird unsere Gesellschaft und die Art, Krieg zu führen, massiv verändern. Der Informationskrieg ist also nichts anderes als die logische Konsequenz aus der Entwicklung der Beziehung Gesellschaft-Krieg.

3.1.2. Bells Postindustrielle Gesellschaft und postindustrieller Krieg

Anders als Toffler reduziert Bell den sozialen Wandel der Gesellschaft nicht auf ökonomisch-technische Aspekte, sondern begreift ihn als multidimensionalen Prozess. In der post-industriellen Gesellschaft, die für ihn die Informationsgesellschaft ist, sieht er einen einschneidenden Wandel der

[72] vgl. Toffler, Alvin; Toffler, Heidi; Überleben im 21.Jhdt; Übersetzt aus dem Amerikanischen „War and Anti-War“ von Helmut Dierlamm et al. Deutsche Verlags Anstalt, 1994; S56f

Sozialstruktur, nicht aber der ganzen Gesellschaft. Die Informationsgesellschaft stellt für ihn einen Idealtypus dar im Gegensatz zu Toffler, der damit einen realen Gesellschaftstypus beschreibt.[73]

Bell schlüsselt die Informationsgesellschaft in fünf Dimensionen auf:

a. wirtschaftlicher Sektor: Übergang von einer güterproduzierenden zur Dienstleistungswirtschaft
b. Berufsstruktur: Vorrang für professionalisiert und technisch qualifizierte Berufe
c. Axiales Prinzip: Zentralität theoretischen Wissens als Quelle von Innovationen und Ausgangspunkt der gesellschaftlich-politischen Programmatik
d. Zukunftsorientierung: Steuerung technischen Fortschritts und Bewertung der Technologie
e. Entscheidungsbildung: Entwicklung intellektueller Technologien, die komplexe Entscheidungen auf Basis von gesichertem Wissen treffen können

Für Bell ist die postindustrielle Gesellschaft aber keine Formel für eine konkrete Gesellschaft, sie ist vielmehr *„ein analytisches Konstrukt, ein Paradigma, ein Konzept, das neue soziale Organisations- und Schichtungsachsen der fortgeschrittenen westlichen Gesellschaft aufzeigt.“*[74]

Der deutsche Sozialwissenschaftler Achim Bühl kritisiert in seinem Buch *„Die virtuelle Gesellschaft“* Bell dahingehend, dass gerade die symbiotische Beziehung zwischen Militär und Informatik im 20.Jahrhundert und die bislang überwiegend militärische Prägung der Technologie die Vorstellung Bells, Modalität und Dynamik der Informationsgesellschaft würden durch theoretisches Wissen, wie etwa einer Technikfolgenabschätzung, bestimmt und nicht primär durch Profitmaximierung, Wettbewerb und technologischen Anpassungsdruck, als Wunschtraum denn als realistische Politikanalyse erscheinen lässt.[75]

Ich glaube aber, dass wir zu diesem Zeitpunkt noch gar nicht sagen können, wohin uns die Entwicklung führen wird. Natürlich leben wir in einer Zeit, in der Fortschritt und Entwicklung nach wie vor von Wettbewerb und Anpassungsdruck bestimmt werden, in der zivilen Welt genauso wie am militärischen Sektor. Gerade der Informationskrieg könnte unter Berücksichtigung von Bells Modell aber sehr wohl die militärische Denkweise grundlegend ändern und durch zunehmende Bedeutung der Militärwissenschaften die gleiche multidimensionale Entwicklung hervorrufen, die er in der Informationsgesellschaft sieht. Daraus könnten sich folgende Dimensionen für den Wandel eines industriellen militärischen Systems hin zu einem post-industriellen oder informatisierten Militär ergeben:

a. Wirtschaftlicher Sektor: Übergang vom massierten Einsatz von Waffen in einem breiten Spektrum hin zu serviceorientiertem, spezialisierten Einsatz

[73] vgl. Bühl, Achim; Die virtuelle Gesellschaft; Westdeutscher Verlag, 1997; S36ff
[74] Bell, Daniel, Die nachindustrielle Gesellschaft, Frankfurt, New York, 1975 zit. nach (Bühl, Achim; Die virtuelle Gesellschaft; Westdeutscher Verlag, 1997, S38)
[75] Bühl, Achim; Die virtuelle Gesellschaft; Westdeutscher Verlag, 1997; S38

effeiktiver, kleiner Waffensysteme; Umstellung der Rüstungsindustrie auf spezialisierte, technisch hoch entwickelte elektronische Systeme

b. Berufsstruktur: Das Berufsbild des Soldaten ändert sich, technisch hochqualifiziertes Personal in Bereichen der elektronischen Aufklärung, Ingenieurwesen, Fernmeldewesen, Waffentechnik usw. wird zunehmend an Bedeutung gewinnen
c. Axiales Prinzip: Theoretisches Wissen als Quelle von Innovationen auch auf dem militärischen Sektor. Die Militärwissenschaften gewinnen an Stellenwert und werden in diesem Bereich zentrale Quelle für Innovationen.
d. Zukunftsorientierung: gezielte Steuerung der Rüstungsindustrie, Entwicklung von Systemen auch unter Einfluss von ethischen Aspekten
e. Entscheidungsbildung: Entwicklung von intelligenten Führungsinformations- und Waffensystemen bis hin zur Künstlichen Intelligenz, um Kommandanten Entscheidungen zu erleichtern oder abzunehmen

Der Informationskrieg ließe sich damit ebenfalls als einschneidender Wandel im militärischen System erklären, der aber nicht das gesamte Militär betrifft. So könnte man den dualen Krieg Tofflers[76] auch unter der Prämisse verstehen, dass in einem Konflikt daher klarerweise Elemente sowohl der industriellen als auch der postindustriellen Kriegsführung zu finden sind, da ja die Transformation der Kriegsführung nicht umfassend, sondern nur zum Teil geschieht. Der Informationskrieg, so wie wir ihn heute kennen und wahrnehmen, wäre daher per definitionem dual und gemäß Bell ein analytisches Konzept und Paradigma, das neue Organisations- und Schichtungsachsen im gesellschaftlichen Subsystem Militär aufzeigt.

3.1.3. Was ist eine Revolution?

Im Zusammenhang mit dem Informationskrieg ist immer wieder von einer „Revolution in der Kriegsführung" die Rede, selbst die USA als führende Nation und Vordenker in der Entwicklung von Konzepten zur Kriegsführung sprechen von einer „*Revolution in Military Affairs*". Dabei ist es durchaus umstritten, ob es sich bei dieser Entwicklung tatsächlich um eine Revolution handelt, oder ob sie vielmehr evolutionären Charakter hat.[77] Während Bell durchaus auch von einer „dritten technologischen Revolution"[78] spricht, negiert Toffler diesen Terminus außerhalb seiner Innovationswellen völlig. Gerade für das Dreieck Führung-Technologie-Doktrin ist es aber notwendig, den Begriff „Revolution" einer – zumindest für diese Arbeit – gültigen Definition zuzuführen.

[76] vgl. Toffler, Alvin; Toffler, Heidi; Überleben im 21.Jhdt; Übersetzt aus dem Amerikanischen „War and Anti-War" von Helmut Dierlamm et al. Deutsche Verlags Anstalt, 1994; S99ff
und Simeoni, Thomas; War der Golfkrieg der erste Informationskrieg?, Diplomarbeit; Wien, 1997; S79f

[77] vgl Eckert, Dirk; Kölner Arbeitspapiere zur internationalen Politik Nr1/2001; Theorie und Praxis der Information Warfare in den USA, S9

[78] Bell, Daniel, Die dritte technologische Revolution und ihre möglichen sozialökonomischen Konsequenzen, in: Merkur, 44 (1990) zit. nach (Hohls, Rüdiger; „Über die Werkbank zur tertiären Zivilisation" in Europa und die Europäer. Quellen und Essays zur modernen Europäischen Geschichte; Stuttgart; Franz Steiner Verlag; 2005, S104)

Das Problem an Tofflers Wellentheorie ist meines Erachtens, dass sie einerseits eine sehr großzügige Auslegung und Interpretation historischer Entwicklungen zulässt, um diese in den Typus einer Gesellschaft einordenbar zu machen, andererseits aber Begriffe wie „Revolution“ sehr eng definiert. Demnach sind alle technischen Entwicklungen, die das Militär und die Kriegsführung in ihren Grundfesten verändert haben, zwar durchaus signifikant, aber nicht revolutionär.

„Auch wird der Begriff „revolutionär“ häufig auf neue technische Errungenschaften wie etwa das Schießpulver, (…) angewandt. Diese Errungenschaften haben die Kriegsführung zugegebenermaßen tiefgreifend verändert (…). Gleichwohl waren sie nicht so gravierend, dass man sie als Revolution bezeichnen könnte.“[79] Toffler definiert an dieser Stelle das Wesen einer Revolution selbst und sagt, sie verändere *„das Spiel selbst, seine Regeln, das erforderliche Gerät, die Größe und Organisation der beteiligten „Mannschaften“, ihre Ausbildung und Doktrin, ihre Taktik(…)“* und letztendlich sogar das „(…)*Verhältnis der Gesellschaft zum Spiel.“*[80]

Hier widerspricht sich Toffler meiner Meinung nach, denn gerade die Entwicklung des Schießpulvers, um dieses Beispiel hier explizit aufzugreifen, hatte genau diese Auswirkungen auf die Kriegsführung. Sie änderte Doktrinen und Taktiken, hatte Auswirkungen auf Organisation, Struktur und Größe der Armeen und fand ihren Niederschlag auch im Verhältnis der Gesellschaft zum Krieg, der plötzlich viel tödlicher wurde und neue Konzepte erforderte - das Konzept des absoluten Krieges[81] kann hier wohl als sehr gutes und deutliches Beispiel gesehen werden. Daher kann technologische Entwicklung – sogar nach der Definition Tofflers - durchaus revolutionär sein und die Anwendung des Begriffs „Revolution“ auf neue technische Errungenschaften müsste durchaus zulässig sein.

Wenn wir also hier von einer Revolution sprechen, dann können wir dies nur tun, wenn wir uns von der engen Auslegung Tofflers verabschieden und annehmen, dass Revolutionen auch abseits der großen Innovationswellen stattfinden können. In diesem Zusammenhang dürfte es jedoch zu kurz greifen, zehntausend Jahre Menschheitsgeschichte in nur einer einzigen Epoche zusammenzufassen, auch wenn dies nicht grundlegend falsch sein mag. Selbst Toffler sagt ja, dass es durchaus auch Ausnahmen gegeben hat, die aus dem typischen Bild herausgefallen sind und führt gerade in der Ersten Welle beispielsweise die Römische Armee als eine für das Agrarzeitalter grundsätzlich untypisch gut organisierte Armee an.[82]

Jedes neue Zeitalter ist das Produkt einer technologischen Revolution und jede technologische Revolution ist das Vorspiel eines neuen Zeitalters.[83] Führt man diesen

---

[79] Toffler, Alvin; Toffler, Heidi; Überleben im 21.Jhdt; Übersetzt aus dem Amerikanischen „War and Anti-War“ von Helmut Dierlamm et al. Deutsche Verlags Anstalt, 1994; S47f

[80] Toffler, Alvin; Toffler, Heidi; Überleben im 21.Jhdt; Übersetzt aus dem Amerikanischen „War and Anti-War“ von Helmut Dierlamm et al. Deutsche Verlags Anstalt, 1994; S47f

[81] Clausewitz, Carl von, 2005, Vom Kriege, Insel Verlag, Achtes Buch;
Clausewitz spricht von der Theorie des „absoluten Krieges“, also eines Krieges, auf allen Ebenen des Staates und der Gesellschaft ausgetragen wird. Im Zweiten Weltkrieg wurde die Abwandlung dessen als „totaler Krieg“ zum faschistischen Propaganda-Instrument. Zwar sagt Clausewitz auch, dass sein absoluter Krieg praktisch unmöglich wäre, dennoch zeigt allein die wissenschaftliche Beschäftigung mit dem Thema auch den Einfluss des Krieges auf die Gesellschaft und ihre Auseinandersetzung damit.

[82] Vgl. Toffler, Alvin; Toffler, Heidi; Überleben im 21.Jhdt; Übersetzt aus dem Amerikanischen „War and Anti-War“ von Helmut Dierlamm et al. Deutsche Verlags Anstalt, 1994; S55

[83] Weiguang, Shen; Der Informationskrieg; in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork, 1998; S68

Gedanken weiter, so könnte man sagen, dass auch jede technologische Entwicklung einen Schritt hin zur Transformation in ein neues Zeitalter darstellt und die großen Innovationswellen erst in der Summe ihrer Revolutionen selbst revolutionären Charakter entwickeln.

Für unser Dreieck Führung-Technologie-Doktrin rufen wir uns in Erinnerung, dass nur ein gleichzeitiger Entwicklungsschritt dieser Faktoren eine Revolution auslösen kann.[84] Eine Revolution im Verständnis dieser Arbeit findet im militärischen Bereich daher immer dann statt, wenn zumindest zwei dieser Faktoren einen nahezu gleichzeitigen Entwicklungsschritt vollziehen und so den dritten Faktor ebenfalls zu einem Entwicklungsschritt zwingen. Umgekehrt betrachtet kann eine alleinige Entwicklung eines Faktors als evolutionär bezeichnet werden. Dieser Hypothese werden wir uns später noch einmal widmen.

3.2. Der Informationskrieg – Begriffsbestimmung und Definition

Nachdem wir den Informationskrieg aus gesellschaftstheoretischer Sicht betrachtet haben, beschäftigen wir uns in diesem Kapitel mit den konkreten Formen und Auswirkungen wie wir sie heute bereits kennen. Leider wird in vielen Quellen der Begriff des Informationskrieges nur sehr indifferenziert und kontextbezogen verwendet, was eine allgemein gültige Begriffsbestimmung erschwert. Die Frage, was nun dem Informationskrieg zuzurechnen sei und was nicht, beschäftigt schon lange die Wissenschaft und die Debatte darüber ist noch lange nicht zu Ende.

Den Informationskrieg ausschließlich als militärische Konfliktform zu betrachten, ist ebenso zu kurz gefasst wie die reine Reduzierung desselben auf die Entwicklungen der Informationstechnik. Infowar kann sich auf allen Ebenen der Gesellschaft abspielen und ist wohl die größte Bedrohung der heutigen Zeit. Nie zuvor war der Mensch so abhängig von Technologie und nie zuvor war es so einfach, ganze Systeme zu Fall zu bringen. Die Gefahr liegt aber nicht nur im großen Angriffspotential, das Technologie per natura bietet, sondern auch in der Möglichkeit, den Konflikt von der staatlichen Ebene auf eine individuelle zu transferieren. Diese Art der asymmetrischen Kriegsführung[85] ist neu und stellt eine der größten Herausforderungen an die zivile, aber auch militärische Konfliktführung dar. Man stelle sich beispielsweise einen Hacker-Angriff auf die New Yorker Börse vor und die Folgen eines dadurch verursachten wirtschaftlichen Zusammenbruchs auf die Welt, oder gar den Abschussbefehl für eine Atomrakete nach einem erfolgreichen Angriff auf ein militärisches Computersystem. Diese Szenarien mögen vielleicht nach Science-Fiction klingen und zugegebenermaßen aufgrund zahlreicher Sicherungsmaßnahmen eher unwahrscheinlich sein, allerdings zeugt allein schon die Existenz dieser Sicherungsmaßnahmen davon, dass diese Bedrohungen durchaus real und keinesfalls zu unterschätzen sind.
Es ist ein gesellschaftspolitisches Problem, dem wir uns in Zukunft abseits aller militärischen Konflikte sicher noch vermehrt widmen werden müssen. In der Zwischenzeit wollen wir uns hier an dieser Stelle aber dennoch mit der staatlichen Ebene und dem Informationskrieg als neuer Konfliktform zwischen Staaten beschäftigen.

[84] Zeitschrift Air Power Revue der Schweizer Armee Nr.3, Beilage zur Allgemeinen Schweizerischen Militärzeitschrift ASMZ 12/2004; Artikel „Doktrin und Technologie: Zwillings- oder Halbschwestern“; S14
[85] Von asymmetrischer Kriegsführung spricht man, wenn sich die militärische Stärke zweier Parteien signifikant unterscheidet. In der heutigen Zeit wird vor allem ein Konflikt eines Staates gegen eine Organisation oder Gruppierung als asymmetrischer Konflikt bezeichnet.

Einen ersten Eindruck der Vielfalt der Gebiete des Informationskrieges liefert dazu Wikipedia:

Informationskrieg *(engl. Infowar oder Information warfare) ist eine Bezeichnung für die gezielte Nutzung und Manipulation von gesteuerten Informationen, um in der Wirtschaft oder in der Politik Vorteile gegenüber Konkurrenten und Gegnern zu erzielen. Dazu gehört auch die Beeinflussung von Medien durch gezielte Falschinformationen, Teilinformationen oder Propaganda mit dem Ziel der Medienmanipulation im eigenen Interesse.*

Außerdem werden Methoden, die dazu dienen, "feindliche" Kommunikationssysteme auszuschalten und zu sabotieren, als Infowar bezeichnet. Dazu gehören z.B. die Zerstörung von Anlagen für Fernseh- und Radiosendungen, die Nutzung fremder Fernseh- und Radiostationen für die Ausstrahlung eigener Informationen, die Zerstörung der Kommunikationslogistik oder die Manipulation von Transaktionen an der Börse durch Interventionen per Computer, Nutzung privilegierten Wissens oder gezielt gestreute Falschinformationen.[86]

Hier wird bereits deutlich, dass es nicht immer die Politik und schon gar nicht immer das Militär sein muss, das Information Warfare betreibt. Gerade der Wirtschaft, aber auch den Medien kommt hier eine entscheidende Rolle zu, die sie auch in Friedenszeiten erfüllen.

3.2.1. Arten des Informationskrieges nach Libicki

Der amerikanische Militärwissenschaftler Martin Libicki unterscheidet sieben Arten des Informationskrieges[87], die wir in der Folge kurz erläutern wollen:

(i) Command-and-Control Warfare
(ii) Intelligence-based Warfare
(iii) Electronic Warfare
(iv) Psychological Warfare
(v) Hacker Warfare
(vi) Economic Information Warfare
(vii) Cyberwarfare

3.2.1.1. Command-and Control Warfare (C2W)[88]
(which strikes against the enemy's head and neck)

Diese Art der Kriegsführung verfolgt das Ziel, die generische Führung und deren Führungseinrichtungen auszuschalten bzw. entscheidend zu stören. Dies kann auf zwei Arten erfolgen, einerseits, indem Führungspersonal oder Führungseinrichtungen direkt bekämpft werden *(antihead)* und andererseits, indem Kommunikationseinrichtungen ge- oder zerstört werden *(antineck).*

---

[86] Artikel *Informationskrieg*. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 24. Mai 2008, 13:50 UTC. URL: http://de.wikipedia.org/w/index.php?title=Informationskrieg&oldid=46438284 (Abgerufen: 6. Oktober 2008, 02:12 UTC)

[87] Libicki, Martin C.; What is IW?; National Defense University; Library of Congress Cataloging-in-Publication Data; 1995; S*ix*f

[88] vgl. Libicki, Martin C.; What is IW?; National Defense University; Library of Congress Cataloging-in-Publication Data; 1995; S9ff

3.2.1.2. Intelligence-based Warfare (IBW)[89]
(which consists of the design, protection and denial of systems that seek sufficient knowledge to dominate the battlespace)

Darunter versteht man das direkte Einfließen von Aufklärungsergebnissen in die Kampfführung in Echtzeit. Dadurch wird eine höhere Koordinationsfähigkeit der eigenen Kräfte während Operationen erreicht und Ziele können schneller und unmittelbar bekämpft werden. Mittels Sensoren soll Schlachtfeldtransparenz (battlespace visibility) entstehen und ein entsprechendes umfassendes Lagebild (situational awareness) vermittelt werden.

3.2.1.3. Electronic Warfare (EW)[90]
(radio-electronic or cryptographic techniques)

Electronic Warfare oder *„Elektronische Kampfführung ist die Gesamtheit aller militärischen Maßnahmen unter Ausnützung elektromagnetischer Strahlung*

- *zur Informationsgewinnung über den Gegner*
- *zur Verhinderung der Nutzung des elektromagnetischen Spektrum durch den Gegner sowie*
- *zur Sicherstellung der Nutzung des elektromagnetischen Spektrums für eigene Anwendungen. „*[91]

Kapitel 4.3.4 befasst sich ausführlich mit diesem Thema.

3.2.1.4. Psychologoical Warfare (PSYW)[92]
(in which information is used to change the minds of friends, neutrals and foes)

Mit den Entwicklungen am Sektor der Informationstechnologie haben auch die Möglichkeiten und Mittel zur psychologischen Kriegsführung neue Ausmaße erreicht. Information und Desinformation können wesentlich leichter einem breiteren oder gezielt einer bestimmten Zielgruppe näher gebracht werden. Psychologische Kriegsführung richtet sich dabei sowohl gegen Feinde nach außen hin, als auch nach innen gegen das eigene Volk. Libicki unterscheidet vier Formen der psychologischen Kriegsführung:

- counter will: gegen den nationalen Willen eines Staates/Volkes gerichtet; beinhaltet alle Intentionen, das öffentliche Meinungsbild zu beeinflussen; in diesem Zusammenhang können z.B. die

[89] vgl. Libicki, Martin C.; What is IW?; National Defense University; Library of Congress Cataloging-in-Publication Data; 1995; S19ff
[90] vgl. Libicki, Martin C.; What is IW?; National Defense University; Library of Congress Cataloging-in-Publication Data; 1995; S27ff
[91] Olischer, Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003, S.82
[92] vgl. Libicki, Martin C.; What is IW?; National Defense University; Library of Congress Cataloging-in-Publication Data; 1995; S35ff

Militärparaden der Sovjets gesehen werden, die die militärische Macht in das Bewusstsein der westlichen Bevölkerung bringen sollten, aber auch Bush's *„Achse des Bösen"* oder die partielle, zensierte Berichterstattung aus dem jüngsten Irakkrieg. In diesen Bereich fallen auch Medien und Unternehmen, die versuchen, die öffentliche Meinung für ihre Zwecke zu beeinflussen.

- counter forces: gegen feindliche Kräfte gerichtet; hierzu zählen beispielsweise Versuche, feindliche Soldaten zum Aufgeben oder Überlaufen zu bewegen oder das Vertrauen in die eigene Führung zu unterminieren; auch hier findet man im Irak viele Beispiele, in denen die Koalitionsstreitkräfte den irakischen Soldaten die Aussichtslosigkeit ihres Kampfes dargelegt haben und sie so zur Aufgabe überredet haben

- counter commander: gegen feindliche Kommandanten gerichtet; Verwirrung und Täuschung werden hier große Bedeutung zugemessen; durch Verwirrung erzeugt man Überraschung, durch das scheinbare Vorgehen nach einer vom Gegner erwarteten Handlungsweise wird diesem Sicherheit suggeriert

- counter culture: Kulturkampf; ist eigentlich als Form der psychologischen Kriegsführung umstritten; Grundsätzlich versteht man darunter den Einfluss fremder Normen und Werte im eigenen Kulturkreis unter Angst des Verlustes der eigenen Identität bzw. umgekehrt das Schüren von Ängsten, Nationalismus und „Wir-Gefühl" und die damit verbundene Ausgrenzung des Fremden. Hier kommt neuen, schwer steuerbaren Medien wie dem Internet große Bedeutung zu.

3.2.1.5. Hacker Warfare (HW)[93] (in which computer systems are attacked)

Diese Art des Informationskrieges umfasst das Ausnutzen von Sicherheitslücken ziviler Computer-Netzwerke für Angriffe auf Infrastruktur, Wirtschaft und Finanz. Die geringen Kosten verbunden mit der großen zu erzielenden Wirkung machen gerade diesen Bereich zu einem zentralen Feld für den Informationskrieg. Das militärische Pendant dazu ist eigentlich eher im C2W zu finden, wobei diese Grenze sicher nicht eindeutig gezogen werden kann.

[93] vgl. Libicki, Martin C.; What is IW?; National Defense University; Library of Congress Cataloging-in-Publication Data; 1995; S49ff

3.2.1.6. Economic Information Warfare (EIW)[94]
(blocking information or channelling it to pursue economic dominance)

EIW ist die Verbindung zwischen Economic Warfare und Information Warfare. Dabei unterscheidet Libicki zwischen zwei Formen, der Informationsblockade und des Informationsimperialismus. Einerseits soll analog zur Wirtschaftsblockade ein Land durch die Blockade von Wissen und Information gezwungen werden, eigenen Interessen zu folgen. Andererseits soll durch die Spezialisierung auf bestimmte Industriesektoren die Konkurrenzfähigkeit erhalten und diese Position durch hohe Wissensintensität und Know-How gesichert werden.

3.2.1.7. Cyberwarfare (CW)[95]
(a grab bag of futuristic scenarios)

Libicki spricht in diesem Zusammenhang von Informationsterrorsimus, semantischen Angriffen, Simulationskriegsführung und Gibson-Warfare.

- Informationsterrorismus: eigentlich eine Weiterführung der HW, zielt aber nicht auf die Netze selbst, sondern auf Personen und Organisationen dahinter ab

- semantische Angriffe: ein scheinbar einwandfrei funktionierendes System soll getäuscht werden und so zu gewissen Reaktionen provoziert werden; z.B. kann die Täuschung der seismischen Sensoren eines Atomkraftwerkes zu dessen Abschaltung führen

- Simulationskriegsführung: Der Grundgedanke ist, dass Krieg nicht mehr real am Schlachtfeld stattfindet, sondern im virtuellen Raum simuliert wird, wobei das Ergebnis für alle Konfliktparteien bindend ist.

- Gibson-Warfare: Basierend auf dem Science Fiction Autor William Gibson stellt die Gibson Warfare eine Weiterentwicklung der Simulationskriegsführung dar. Der Autor lässt hierbei seine Protagonisten zu Gestalten einer virtuellen Welt werden, die sich bekämpfen.

Ob Simulationskriegsführung und Gibson-Warfare jemals Realität werden ist mehr als fraglich und eindeutig dem Bereich der Science Fiction zuzuordnen. Würde ein Krieg, der seinen größten Schrecken, nämlich die Letalität verliert, nicht auch seinen Machtfaktor verlieren und eher zu einem Spiel degenerieren als ein Instrument der Politik darstellen?

---

[94] vgl. Libicki, Martin C.; What is IW?; National Defense University; Library of Congress Cataloging-in-Publication Data; 1995; S67ff

[95] vgl. Libicki, Martin C.; What is IW?; National Defense University; Library of Congress Cataloging-in-Publication Data; 1995; S75ff

3.2.2. Netzkrieg – Cyberkrieg nach Arquilla/Ronfeldt

Einen anderen, für unseren Gebrauch pragmatischeren, Ansatz wählen die beiden Mitarbeiter der RAND-Corporation[96], John Arquilla und David Ronfeldt. Sie stellen die These auf, *„dass sich aufgrund der Informationsrevolution[97] für einzelne Gesellschaften neue Konfliktformen sowie für ihre Truppen neue Formen der Kriegsführung ergeben werden.“*[98] Dabei unterscheiden sie zwischen dem „Netzkrieg“ (engl. Netwar), der ideelle gesellschaftliche Konflikte beschreibt, und dem „Cyberkrieg“ (engl. Cyberwar), also der militärischen Ebene zukünftiger Auseinandersetzungen.

3.2.2.1. Netzkrieg[99]

Im Kontext des Netzkriegs werden nicht militärische, informationsbezogene Konflikte zwischen Gesellschaften oder Staaten verstanden, die sich unterhalb der Kriegsschwelle abspielen. Ziel in solchen Auseinandersetzungen ist es, das tatsächliche oder vermeintliche Wissen einer Zielbevölkerung über sich und ihre Umwelt zu stören, zu beschädigen oder zu modifizieren. Staatliche diplomatische Maßnahmen, Täuschung oder Störung lokaler Medien, Infiltration von Datenbanken, Förderung von regierungsfeindlichen bzw. oppositionellen Netzwerken oder auch Propaganda- und psychologische Maßnahmen stellen lediglich einen Teilbereich der Möglichkeiten dar, die sich Konfliktparteien eröffnen. Netzkriege zeichnen sich dadurch aus, dass sie anders als andere Konfliktformen auf Information und Kommunikation abzielen. Dabei ist zu beachten, dass sie sich großteils im nicht-militärischen Bereich abspielen, auch wenn nach Arquilla und Ronfeldt eine Überschneidung mit militärischen Konflikten durchaus möglich ist. Parallel zu einem Wirtschaftskrieg, der sich rein in Handelsbeschränkungen, Embargos, Technologiediebstahl etc. äußern kann, der aber auch zu einer bewaffneten Blockade oder zur strategischen Bombardierung von Wirtschaftsgütern führen kann, könnte es im Verlauf eines Netzkrieges durchaus auch zu militärischen Informationsoperationen kommen. Dies ist insofern von Interesse, da Netzkriege mit großer Wahrscheinlichkeit gewaltfrei ablaufen und von Arquilla und Ronfeldt sogar als Instrument gesehen werden, mit dem man in Zukunft echte Kriege im Keim ersticken kann. *„In einer chaotischen Welt kann Abschreckung ebenso gut eine Funktion der Cyberbereitschaft und Cyberpräsenz wie der Truppenbereitschaft und Truppenpräsenz sein.“*[100]

---

[96] Die RAND Corporation (Research And Development) ist eine non-profit Organisation, die sich mit globalen Entwicklungen in Politik und Rüstung beschäftigt. Ihre Analysen und Forschungen wurden ursprünglich nur für die US Armed Forces durchgeführt, mittlerweile arbeitet die Corporation auch für fremde Regierungen sowie private, kommerzielle und internationale Organisationen.

[97] Auch Arquilla und Ronfeldt sprechen in diesem Zusammenhang von einer Revolution und beziehen sich dabei in der Folge ebenfalls auf William Bell;

[98] Arquilla, John; Ronfeldt, David; „Der Cyberkrieg kommt“ in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork 1998, S28

[99] vgl. Arquilla, John; Ronfeldt, David; „Der Cyberkrieg kommt“ in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork 1998, S28ff

[100] vgl. Arquilla, John; Ronfeldt, David; „Der Cyberkrieg kommt“ in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork 1998, S31

3.2.2.2. Cyberkrieg[101]

Das militärische Pendant zum Netzkrieg ist der Cyberkrieg, also die informationsbezogene Planung bzw. Durchführung militärischer Operationen. Es ist das Bemühen, möglichst alles über den Feind zu erfahren und so wenig wie möglich über sich selbst preiszugeben, sowie die Zerstörung der für das Selbstverständnis des Gegners (d.h. Zur Beantwortung der Fragen: wer er ist, wo er ist, was er wann tun kann, warum er kämpft, welche Bedrohungen er sich zuerst stellen soll etc) unerlässlichen Kommunikations- und Informationssysteme. Dabei können verschiedenste Technologien zur Anwendung kommen, die Information, Kommunikation, Positionierungssysteme, Freund-Feind-Kennung oder intelligente Waffensysteme ebenso umfassen, wie elektronische Kampfmaßnahmen zur Störung, Täuschung oder Zerstörung gegnerischer Informations- oder Kommunikationssysteme. Aber der Cyberkrieg ist mehr als nur der Einsatz von Technologie und wird von Arquilla und Ronfeldt auch klar von der automatisierten, robotischen oder computerisierten Kriegsführung abgegrenzt.[102]

„*Im Cyberkrieg geht es ebenso sehr um Organisation wie um Technologie.“* Das bedeutet, dass sich auch Doktrin, Strategie, Taktik und sogar Hierarchien ändern. Der Übergang zu vernetzten Strukturen und die damit verbundene Dezentralisierung von Kommando und Kontrolle erfordert eine institutionelle Neugestaltung des Militärs innerhalb und zwischen den einzelnen Teilstreitkräften, ein verbessertes Komplexitätsmanagement schafft ein besseres, zentrales Verständnis der Gesamtsituation und Cyberkrieg kann sogar die Entwicklung neuer Doktrinen bedeuten. Cyberkrieg verändert das Wesen des Krieges selbst und *„im Sinne von Clausewitz zeichnet sich der Cyberkrieg durch das Bestreben aus, Wissen in Kampfkraft umzumünzen.“*[103]

3.3. Informationskrieg als militärische Konfliktform

Im Sinne dieser Arbeit beschäftigen wir uns mit dem Informationskrieg als militärischer Konfliktform, also jenem Bereich, den Arquilla und Ronfeldt unter dem Begriff „Cyberkrieg“ zusammengefasst haben. Dabei können die Begriffe „Cyberwar“ und „Informationskrieg“ synonym verstanden werden.
Diese Art der Konfliktführung setzt vor allem in der operativen und taktischen Führungsebene an, beeinflusst aber dort, wo sie Doktrinen schafft oder modifiziert, auch die strategische Ebene. Abgeleitet von Arquilla/Ronfeldt beschreiben drei zentrale Punkte den Cyberkrieg, nämlich:

---

[101] vgl. Arquilla, John; Ronfeldt, David; „Der Cyberkrieg kommt“ in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork, 1998, S31ff
und Arnett, Eric; Welcome to Hyperwar, zit. nach (Arquilla, Ronfeldt; Der Cyberkrieg kommt, S33)
[102] Dies steht im Widerspruch zu einer Sichtweise, die im „Cyberkrieg“ oder „Hyperkrieg“ eine Zukunft zeichnet, in der Roboter und autonome Computer Konflikte am automatisierten Schlachtfeld austragen, in der der Mensch sich der Maschine unterordnet und Kriege aus der Distanz durch eine Vielzahl von Angriffen geführt werden, was laut Arquilla und Ronfeldt die Auswirkungen der Informationsrevolution völlig falsch interpretiert. In diesem Zusammenhang kann man auch die oben angeführte Gibson-Warfare sehen, der demnach ebenfalls eine Fehlinterpretation der Informationsrevolution zugrunde liegt.
[103] Arquilla, John; Ronfeldt, David; „Der Cyberkrieg kommt“ in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork, 1998, S33

- Einsatz von Technologie
- Organisation, Strategie, Dezentralisierung, Vernetzung
- Komplexitätsmanagement

Diese Charakteristika sind durchaus Analogismen zur Verbindung Führung-Technologie-Doktrin und finden in Abbildung 12 ihre Entsprechung. Anhand dieses Vergleichs wird wieder der revolutionäre Charakter des Informationskrieges sichtbar, sowie dessen enge Verbindung zu diesem Dreieckskonstrukt.

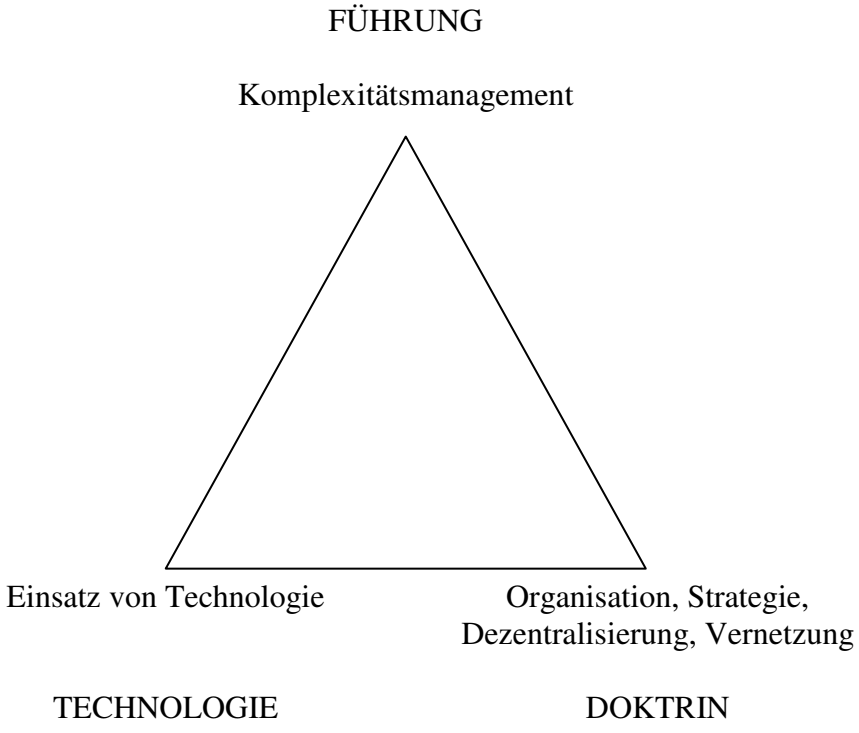


Abbildung 12: Kriterien Informationskrieg und Zusammenhang mit Führung, Doktrin, Technologie; Eigene Darstellung

Die Entwicklung des Cyberwar als militärischer Form des Informationskriegs ist daher, ohne hier das Untersuchungsergebnis aus Abschnitt II vorweg nehmen zu wollen, bereits in realen Entwicklungen der Streitkräfte auf allen Ebenen beobachtbar. Deutliche Strukturänderungen, Doktrinen für Informationsoperationen oder die Vernetzung der Streitkräfte über die Grenzen der Teilstreitkräfte hinweg sind nur die offensichtlichsten Auswirkungen dieser revolutionären Entwicklung. Umgekehrt formuliert könnte man auch sagen, dass anhand der Transformationsprozesse der Streitkräfte und der damit verbundenen tiefgreifenden Änderungen des Militärs der Cyberkrieg bereits klar erkennbar ist.

4. C4I(SR)

Die Welt wird nicht mehr von Waffen beherrscht, nicht mehr von Geld und Erdöl, sondern von kleinen Einsen und Nullen! Von Bits und Daten! Nur von kleinen Elektroden…"
(Ben Kingsley, SNEAKERS, Die Lautlosen)

Der Begriff C4ISR ist ein militärisches Akronym, das von den US-Streitkräften geprägt wurde und für *Command, Control, Communication, Computer (C4), Intelligence, Surveillance, Reconnaissance (ISR)* steht. Es beschreibt nichts anderes, als den Kampf um die Informationsüberlegenheit bzw. die Führungsüberlegenheit in militärischen Konflikten mit elektronischen Mitteln, die in Führungsunterstützungssystemen eingebettet sind. Es geht um die Informationsgewinnung, -verarbeitung und –weitergabe bzw. –übertragung und um die Intention den Gegner in genau diesen Bereichen zu behindern.

Die technologische Entwicklung der Moderne und Postmoderne spiegelt sich auch im Bereich der militärischen Kriegsführung wider. Bereits im zweiten Weltkrieg wurden erste Systeme entwickelt, die zwar in ihren Anwendungsgebieten lokal eingeschränkt waren und nur im entferntesten Sinn unter C3I[104] eingestuft werden konnten, aber dennoch den Beginn der hochtechnologisierten Kriegsführung einläuteten. In diesem Zusammenhang kann beispielsweise die Entwicklung von RADAR-Systemen zum frühzeitigen Erkennen von Feindflugzeugen, das Long-Range Positionierungssystem LORAN-C oder die Dechiffriermaschine Enigma gesehen werden. Das erste „echte" C3I-System fand später im Vietnam-Krieg seinen Einsatz, als ein Netzwerk aus Minen und Sensoren installiert wurde, um Nachschubwege des Vietcong kontrollieren zu können[105].

Die rapide Entwicklung am Computersektor fand ihren Niederschlag nicht nur im neuen Begriff C4I, sondern auch in den technologischen Entwicklungen des Kalten Krieges. Das Zusammenwirken verschiedener Waffengattungen sowie die Effizienzsteigerung durch Vernetzung der eigenen Truppen ließen ein großes Potential für eine echte Revolution in der Kriegsführung erkennen. Im Jahre 1994 rief das US Militär die „Revolution of Military Affairs" aus, mit der wir uns im Zuge der Analyse in Teil II noch beschäftigen werden, und gab so die bis dato größte Initialzündung für den Umbau der Armee unter Abstützung auf moderne C4I-Systeme.

4.1. Entwicklung des Begriffes C4ISR

So wie die technologische Entwicklung am militärischen Sektor ein fortlaufender Prozess ist, unterlag auch der Begriff C4ISR für militärische Führungssysteme einem ständigen Wandel. War ursprünglich mit der Bezeichnung C2 nur der Bereich Führung und Kontrolle umfasst (Command & Control), so wurde bald die Bedeutung der Kommunikation als Schlüsselkomponente erkannt und der Begriff auf C3 erweitert. Die Intelligence als informationsbeschaffende Quelle prägte lange den Begriff C3I, erst später wurde auch die Bedeutung des Computers erkannt und das Akronym C4I war geboren. Die durchaus sinnvolle Differenzierung zwischen nachrichtendienstlicher und militärischer Aufklärung und Überwachung führte zu dem heute gängigen Begriff C4ISR.

---

[104] vgl Kapitel 4.1 – Entwicklung des Begriffes C4ISR

[105] vgl Weizenbaum, Joseph, Die Macht der Computer und die Ohnmacht der Vernunft, Frankfurt, 1978 zit. nach (Bernhardt, Ute; Ruhmann, Ingo, Informatik und Militär, in Friedrich, J. et al (Hrsg.), Informatik und Gesellschaft, Spektrum u.a., Heidelberg, 1995, S.100)

Viele Quellen sprechen heute bereits von C4ISTAR, C4I2 oder sogar C5I. C4ISTAR beinhaltet zusätzlich noch die so genannte *Target Acquisition (TA)*, also das Identifizieren und Bewerten von möglichen Angriffszielen. Im Falle von C4I2 spricht man von Interoperabilität (*Interoperability)*, bei C5I ist der Begriff *Combat Systems* miteinbezogen worden. Die neuen Variationen stellen eher eine Gewichtung einzelner Bereiche als Schlüsselkomponenten dar, die allerdings auch in einer allgemeineren Betrachtung durch den Begriff C4ISR abgedeckt werden.

4.2. Die Elemente von C4ISR

4.2.1. Command & Control

Die erste Ebene der Führung und Kontrolle bezieht sich auf die Befehlsgebung und deren Umsetzung. Führung und Kontrolle kann als eine Einheit gesehen werden und ist die grundlegendste Aufgabe in der militärischen Struktur, die auf allen Ebenen stattfindet.

Führung ist ein richtungsweisendes und steuerndes Eingreifen auf Kommanden, Truppen, Dienststellen und einzelne Soldaten, um einen Auftrag zu erfüllen oder Ziele zu erreichen[106], also im Wesentlichen das Ausgeben von Befehlen und Aufträgen. Führung findet sowohl im Frieden, als auch im Einsatz statt und stellt hohe Anforderungen an Kommandanten aller Ebenen.

Führung braucht aber Kontrolle, um die Richtigkeit der Befehle, die korrekte Umsetzung sowie die unmittelbaren Auswirkungen prüfen zu können, aber auch um die Flexibilität bei Änderungen in den Zielvorstellungen, des Auftrages oder der Lage zu gewährleisten.

Da ein kontinuierlicher Austausch von den führenden zu den geführten Ebenen und umgekehrt stattfindet, lässt sich Führung und Kontrolle in Form einer informationellen Schleife darstellen (Abb. 1). Führung bildet hier den Feedforward-Teil der informellen Schleife, Kontrolle den Feedback-Teil.[107]

[106] Meurers, Bernhard, Führungsverfahren auf Ebene Brigade und Bataillon, Truppendienst Taschenbuch Nr. 46, Reihe Ausbildung und Führung, Verlag AV + Astoria Druckzentrum GmbH, Wien, 2004, S.40ff
[107] vgl.: Fleissner, Peter, et.al.; Der Mensch lebt nicht vom Bit allein; Europäischer Verlag der Wissenschaften, 2.Auflage, 1997, S.208

Abbildung 13: Regelkreis aus Führung und Kontrolle; Eigene Darstellung

4.2.2. Communication

Das wichtigste Führungsmittel ist die Verbindung[108]**.** Damit Führung und Kontrolle in den komplexen hierarchischen Gliederungen der Armee durchführbar werden, bedarf es Kommunikation und den dazu nötigen Kommunikationstechnologien. Gerade der Sektor der Kommunikation ist einer der wichtigsten Komponenten des C4ISR Systems und bezieht sich längst nicht mehr auf den unmittelbaren Funkverkehr am Gefechtsfeld. Information muss den jeweiligen Fachorganen und Kommandanten zugeführt werden, um ein möglichst umfassendes Lagebild erstellen zu können und die Entscheidungsfindung und Befehlserstellung zu beschleunigen.

Das aussagekräftigste Aufklärungsergebnis und die erfolgversprechendsten Befehle sind wertlos, wenn sie zu spät oder gar nicht an ihre Bestimmungsstelle gelangen. [109]

Aufbau und Betrieb der dazu nötigen Kommunikationseinrichtungen und Netzwerke sind daher eine der größten Herausforderungen an moderne Streitkräfte, zumal auch Datenverbindungen sowie LANs und WANs das Rückgrat der modernen Kriegsführung bilden. Der vernetzte Gefechtsstand ist längst Realität geworden, Fernmeldemittel und die dazugehörige Truppe stellen die nötigen Verbindungen sicher.

4.2.3. Computer

Seit dem zweiten Weltkrieg hat der Computer Einzug parallel zur zivilen Gesellschaft auch die militärische Welt erobert. Heute kommt Computern in fast allen Bereichen eine große Bedeutung zu. Es ist nicht nur die Aufgabe von Computern, den gesamten Nachrichtenverkehr zu koordinieren, sondern auch Information nach Art, Verlässlichkeit und Wichtigkeit zu filtern und aufzubereiten, um so Entscheidungsprozesse zu optimieren und zu beschleunigen[110].

[108] Vgl. Dienstvorschrift für das Bundesheer, Die FM-Truppe, FMTS, 1986, S2
[109] Olischer, Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003, S.42
[110] Fleissner, Peter, et.al.; Der Mensch lebt nicht vom Bit allein; Europäischer Verlag der Wissenschaften, 2.Auflage, 1997, S.209f

Die Gewinnung von Daten ist in der heutigen Zeit weniger das Problem als ihre zeitgerechte Verarbeitung. Computer bereiten Aufklärungsergebnisse auf, werten Satellitenbilder aus, treffen Priorisierungen bei der Zielauswahl, verarbeiten in Echtzeit Informationen und Daten eigener Truppen (Freund-Feind-Kennung, Status bez. Munition und Betriebsmittel), und helfen Kommandanten, den Überblick über das Geschehen am Gefechtsfeld zu wahren, um nur einige Anwendungsbereiche zu nennen. Computer sind integraler Bestandteil moderner Technologien und militärische Führung ohne rechnergestützte Abläufe in der Einsatzführung oder Logistik ist nicht nur am Gefechtsfeld selbst, sondern auch im Friedensbetrieb unmöglich, auch wenn die Komplexität der Führung an sich die Entwicklung eines ganzheitlichen Systems zur Unterstützung des gesamten Führungsvorganges bis jetzt noch nicht zugelassen hat. Die Forschung an einem Gesamtsystem zur weitgehenden Automatisierung im Führungsprozess ist Grundlage von Zukunftskonzepte wie zum Beispiel der Netzwerkgestützten Kriegsführung[111].

4.2.4. Intelligence, Surveillance, Reconaissance

„Wenn du den Feind und dich selbst kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten.“[112]

Die Beschaffung von Informationen ist so alt wie der Krieg selbst. Bereits in den frühen Urkunden der Menschheit finden sich Hinweise auf Nachrichtenbeschaffung. Die Heerführer der damaligen verwendeten Kundschafter, um Informationen über Stärke und Stellungen der Gegner zu beschaffen und damit die eigenen Kräfte besser zum Einsatz bringen zu können.

Nach Gunzenhäuser[113] versteht man unter *„Intelligence“* *„besonders die Sammlung, Beurteilung von (öffentlich zugänglichen oder geheimgehaltenen) Informationen in besonderen Dienststellen für Zwecke der militärischen und politischen Führung, wobei die Berücksichtigung und Verwertung dieser Nachrichten bei militärischen und politischen Entscheidungen der oberen Führung überlassen bleiben“*.

Die durch die nachrichtendienstliche Aufklärung (*Intelligence*), die Überwachung von bestimmten Bereichen, etwa durch Radaranlagen (*Surveillance*), sowie die militärische Aufklärung (*Reconaissance*) beschafften Informationen bilden die Grundlage jedes Führungsprozesses. Die Entscheidungen von Kommandanten und somit das Schicksal der eigenen Kräfte hängen von der Schaffung eines Informationsvorteils ab, der durch den Einsatz von modernen Technologien gewonnen werden soll. ISR umfasst sowohl die Informationsgewinnung in Friedenszeiten durch die militärischen und nicht-militärischen Nachrichtendienste, als auch die aktive militärische Aufklärung im Ernstfall.

Man unterscheidet hier einerseits zwischen der *Human Intelligence* (HUMINT), also der Aufklärung durch den Menschen, etwa durch den Einsatz von Spionen und Agenten, aber auch Analytikern, die Medienberichte, politische Entwicklungen,

[111] vgl. Kapitel 5 – Network Centric Warfare
[112] Sun Tsu, Die Kunst des Krieges, S.14
[113] Gunzenhäuser, Max zit. nach ÖMZ, Österreichische Militärzeitschrift, Ausgabe 04/2007, Verlagspostamt Wien, S.396

Truppenbewegungen etc. auswerten und einschätzen. Andererseits spricht man von der *Technical Intelligence* (TECHINT), die Aufklärung mit technischen Mitteln, die eine große Bandbreite zur Informationsgewinnung sowohl im Frieden als auch zu Kriegszeiten bieten. Auf diesem Gebiet kommt der Sensorik eine große Bedeutung zu.[114]

4.3. Sensorik

Sensoren sind die Augen und Ohren der Kriegsmaschine[115]. Um dem System bzw. in weiterer Folge den Kommandanten aller Ebenen möglichst viele Informationen liefern zu können, ist es zunächst nötig, diese Informationen zu gewinnen. Für die militärische Entscheidungsfindung ist es wichtig, möglichst viele Parameter wie Position, Geschwindigkeit, Terrain, Wetter (Bewölkung, Sicht, Sonnenauf- & -untergang, Wind, Temperatur, Wasserstand, Niederschlag), Truppenstärke, Feindansatz usw. zu kennen. Neben der menschlichen Komponente bei der Informationsgewinnung, bei der Soldaten, Analysten, Spione und Agenten als Sensoren fungieren, kommt im C4I System eine breite Palette an technischen Errungenschaften zum Einsatz, die die Aufgaben der Überwachung und Aufklärung sowie der Zielerfassung übernehmen.

Aktive Sensoren
Als aktive Sensoren werden Sensoren bezeichnet, die ein Signal emittieren und das Echo wieder auffangen, um so Informationen über Geschwindigkeit, Entfernung, Richtung und Größe eines oder mehrerer Objekte gewinnen zu können. Zu solchen Sensoren zählen beispielsweise Radaranlagen, Laseranlagen, Echolot- und Sonaranlagen.

Passive Sensoren
Sensoren die Signale ausschließlich auffangen und diese auswerten, nennt man passive Sensoren. Dazu zählen optische Sensoren, Infrarot-Systeme, Restlichtverstärker, Funkpeiler, Abhöranlagen und akustische Sensoren.

Im militärischen Bereich wird außerdem noch zwischen *abbildender* und *signalerfassender* Sensorik unterschieden, wobei die Zuordnung in aktive und passive Sensoren übergreifend ist.

Die folgende Abbildung zeigt die Möglichkeiten eines typischen Sensoreinsatzes in Verbindung mit der jeweiligen Führungsebene:

[114] vgl. Olischer, Ing., Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003, S.58f
[115] Fleissner, Peter, et.al.; Der Mensch lebt nicht vom Bit allein; Europäischer Verlag der Wissenschaften, 2.Auflage, 1997, S210

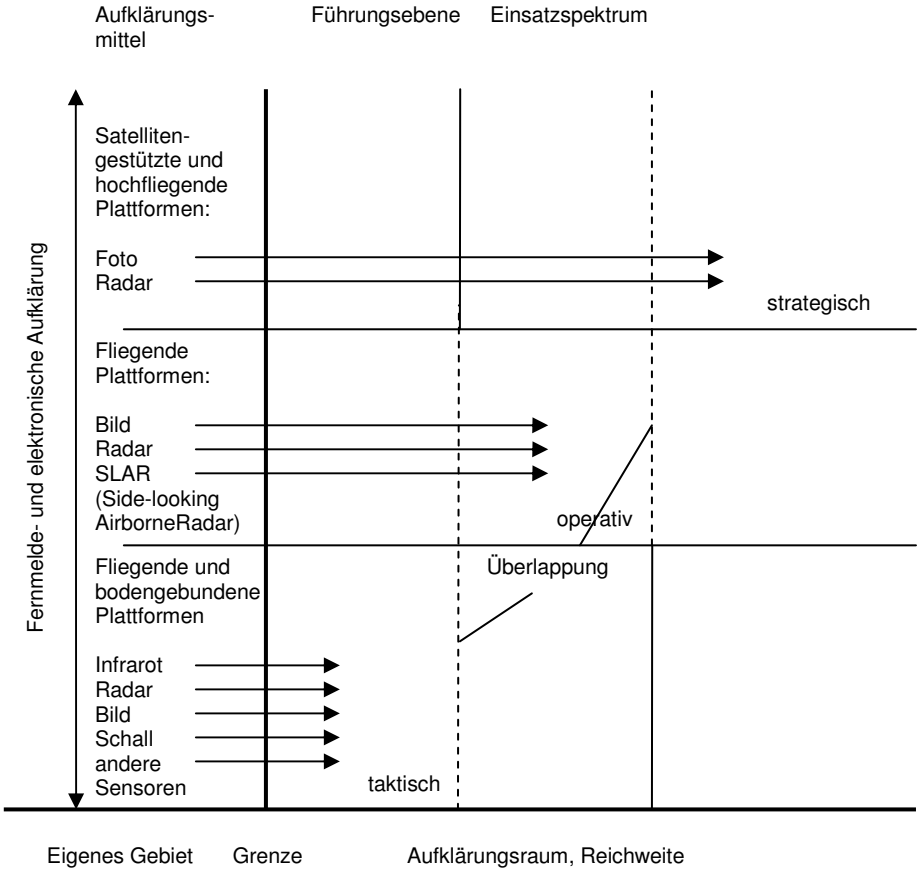


Abbildung 14: Möglichkeiten zum Sensoreinsatz[116]

4.3.1. Satelliten[117]

Mit der Eroberung des Weltalls kam auch Satelliten aller Art gerade im militärischen Bereich eine immer größere Bedeutung zu. Heute sind Satelliten ein unverzichtbarer Bestandteil jedes C4ISR Systems und liefern bereits zu Friedenszeiten wertvolle Informationen über gegnerische Truppenbewegungen, Stärke, Taktik des Feindes und ähnliches. Sie dienen zur Kommunikation, Navigation, Waffensteuerung, Zielerfassung, Überwachung, Aufklärung, aber auch zur Störung gegnerischer Systeme.

4.3.1.1. Navigationssatelliten

Navigationssysteme ermöglichen die genaue Positionsbestimmung und ermöglichen so die korrekte Navigation und Routenplanung eigener Einheiten. Die Satelliten senden dazu ständig Daten wie ihre sich ändernde Position und Zeitparameter aus, die Empfangsgeräte empfangen und verarbeiten. Über die Signallaufzeit kann dann so die eigene Position bestimmt werden, wobei

[116] Vgl.: Olischer, Ing., Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003, S.60

[117] Um die immer größer werdende Bedeutung von Satelliten in der Sensorik zu unterstreichen, wird dieser Bereich detaillierter behandelt.

atmosphärische Einflüsse, Reflexionen und andere Abweichungen mathematisch eliminiert werden können, so dass heute bereits eine sehr hohe Genauigkeit erreicht wird.

Das wohl bekannteste, weil mittlerweile auch zivil genutzte, Anwendungsgebiet ist das globale Positionierungssystem GPS. Das von der US Air Force unter dem Namen NAVSTAR-GPS (Navigational Satellites with Time and Ranging – Global Positioning System) entwickelte System sollte ursprünglich den eigenen Streitkräften die Navigation auf See, bei Flugzeugen und Fahrzeugen ermöglichen und so den Rückgriff auf andere eigene und fremde Funknavigationsdienste ersparen. Eine zivile Nutzung war ursprünglich nicht geplant[118]. Erst politische Entscheidungen im Laufe der Zeit machten auch die zivile Nutzung des Systems möglich.

Bereits 1967 wurde der Startschuss für das Programm gegeben, vom Erstbetrieb 1973 bis zur vollen Funktionsfähigkeit dauerte es allerdings 25 Jahre. Erst 1997 konnte NAVSTAR/GPS seine volle Kapazität ausschöpfen und das Vorgängersystem TRANSIT endgültig ablösen. Die genaue Positionsbestimmung ist am zivilen Sektor auf bis zu maximal 15m Abweichung möglich, im militärischen Bereich ist dieser Wert nicht bekannt, die Abweichung dürfte aber bereits im Zentimeter-Bereich liegen.

Mittlerweile besteht das System aus einem Netz von 24 Satelliten auf 6 Bahnebenen, die von der Schriever Air Force Base in Colorado gesteuert werden und deren militärische Nutzung weit über die reine Positionsbestimmung hinausgeht. Das GPS-System ist Teil des so genannten *Nuclear Detection Systems*, das über Sensoren für Gamma- und Infrarotstrahlung sowie Detektoren zum Aufspüren eines Elektromagnetischen Impulses (EMP) Atomexplosionen sowie Starts von Interkontinentalraketen aufspüren soll.[119]

Heute ist das GPS-System unverzichtbarer Bestandteil der zivilen Navigation zu Luft, See und Land und hat auch die privaten Haushalte längst erobert. Allerdings regt sich in Europa und der Welt auch Widerstand gegen die Vormachtstellung der Amerikaner auf diesem Sektor.

Die vermehrte Nutzung dieser Technologie, ob militärisch oder zivil, bedeutet auch eine höhere Abhängigkeit des Militärs und der Wirtschaft von der Politik einer fremden Macht. Eine Situation, die gerade im Kalten Krieg nicht tragbar war und die Russen Mitte der 70er Jahre zur Entwicklung ihres militärischen Positionierungssystem GLONASS veranlasste. 1982 wurde der erste Uragan-Satellit ins Weltall geschossen, mit dem Zerfall der Sowjetunion scheiterte aber auch beinahe der Vollausbau des Systems. Die kurze Lebensdauer der Satelliten und die politische Situation in Russland am Weg zu einer Demokratie führten nahezu zum Scheitern des Projekts, heute ist man aber wieder massiv am Aufbau des GLONASS-Systems interessiert. Momentan befinden sich 18 Satelliten in der Erdumlaufbahn, bis zum Jahre 2010 soll die Vollausbaustufe aus 24 Satelliten

[118] Dodel, Hans; Häupler Dieter; Satellitennavigation, Hütig – Telekommunikation, 2004, S.161
[119] Artikel *Global Positioning System.* In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 5. Oktober 2008, 21:24 UTC. URL: http://de.wikipedia.org/w/index.php?title=Global_Positioning_System&oldid=51517918 (Abgerufen: 6. Oktober 2008, 02:14 UTC)

erreicht werden. Allerdings stellt die beschränkte Lebensdauer der russischen Satelliten von knapp drei Jahren ein Problem dar. Um die nötige Konstellation von 24 Satelliten zu erhalten, müssten jährlich 8 Satelliten in die Umlaufbahn gebracht werden. Die dafür notwendigen Finanzen hat die russischen Regierung bis dato nicht aufgebracht.[120]

Seit den 90er Jahren entwickelt die Europäische Union gemeinsam mit der Raumfahrtbehörde ESA das Navigationssystem GALILEO, das seine volle operationale Konstellation vermutlich zwischen 2008 und 2012 erreichen wird und mit 30 Satelliten (27 aktive Satelliten, 3 Reserveeinheiten) auf 3 Bahnen arbeitet. Obwohl das System grundsätzlich für den zivilen Markt vorgesehen ist, ist eine militärische Nutzung aber gerade in Hinblick auf eine Gemeinsame Außen- und Sicherheitspolitik (GASP) der EU-Mitgliedsstaaten sowie der Entwicklung und Umsetzung einer Europäischen Verteidigungs- und Sicherheitspolitik (EVSP) nicht nur denkbar, sondern mit hoher Wahrscheinlichkeit anzunehmen.

Tabelle 1*:* Übersicht der wesentlichen Generationen von Navigationssystemen[121]

Generation	Jahr	Name	Beschreibung
Ia	1960	TRANSIT	Anstoß der Satellitentechnik; Entfernungsmessung auf Dopplereffekt im UHF-Bereich; Betrieb durch US-Marine
Ib	1962	TSYKADA	Kopie von TRANSIT; Betrieb durch Marine der UdSSR
IIa	1996	GPS/NAVSTAR	Weiterentwicklung von TRANSIT zur Einwegentfernungsmessung; Betrieb durch US-Luftwaffe
IIb	1996	GLONASS	Kopie von GPS, Betrieb durch GUS-Luftwaffe
III	2010	GALILEO	GNSS-2; Satellitennavigation der dritten Generation

4.3.1.2. Satellitenkommunikation

Kommunikationssatelliten bilden gemeinsam mit den terrestrischen Kommunikationsbahnen das zentrale Nervensystem jeder militärischen Organisation. Ohne Kommunikationsmöglichkeiten, die im Bedarfsfall garantieren, dass Nachrichten sicher, vollständig und zeitgerecht übermittelt werden, würde die Führungsfähigkeit jedes Systems zusammenbrechen. Kommunikationssatelliten garantieren diese Eigenschaften im militärischen, aber auch im zivilen Bereich und ermöglichen globale Kommunikation und Erreichbarkeit auch an den entlegensten Orten der Erde.

4.3.1.3. Aufklärungssatelliten

Am militärischen sowie zivilen nachrichtendienstlichen Sektor werden spezielle Satelliten für Aufklärungs- und Spionagezwecke herangezogen. Sie sind mit

[120] Dodel, Hans; Häupler Dieter; Satellitennavigation, Hütig – Telekommunikation, 2004, S.176
[121] Vgl.: Dodel, Hans; Häupler Dieter; Satellitennavigation, Hütig – Telekommunikation, 2004, S.10

Kameras, Radar, Infrarot und ähnlichen Sensoren ausgestattet und können bei Bedarf in einen niedrigeren Orbit abgesenkt werden, um die Auflösung zu verbessern. Die so erzielten Bilder werden elektronisch aufbereitet und ausgewertet, so dass es angeblich sogar möglich sein soll, die Nummerntafel eines Autos lesen zu können. Aus dem Internet kann man sich heute Bilder seines Hauses, Gartens oder von Sehenswürdigkeiten in einer Auflösung herunterladen, die militärisch relevant und nutzbar ist. Dies eröffnet auch Nationen, die keinen Zugriff auf diese Technologie haben, gewisse Möglichkeiten, sich über die Nutzung von Satellitenbildern Vorteile zu verschaffen.

4.3.1.4. Geostationäre Satelliten

Unter allen Bahnen ist die in der Äquatorialebene liegende Kreisbahn mit der Periode 24 Stunden die herausragende und bildet den so genannten „Geostationären Erd-Orbit“ oder kurz „GEO“. Satelliten, die sich auf dieser Bahn befinden, bewegen sich mit der Erdrotation mit und erscheinen daher ihrem Beobachter auf der Erde stationär. Die GEO-Bahn ist für die Kommunikation mit ortsfesten Erdfunkstellen von großer Bedeutung, da die auf den Satelliten gerichteten Antennen nicht nachgerichtet werden müssen, was Aufwand und Kosten erspart. Ein Geo-Satellit sieht aufgrund seiner großen Entfernung von ca. 35.880km ca. 42% der Erde, mit zwei geschickt positionierten Satelliten kann nahezu die gesamte bewohnte Erde abgedeckt werden.[122]

Aufgrund ihrer Eigenschaften werden geostationäre Satelliten gerne als Kommunikations- bzw. Rundfunksatelliten genutzt, durch ihre fixe Position können sie zur Navigation, Aufklärung oder als Wettersatelliten nicht oder nur beschränkt herangezogen werden.

4.3.1.5. Militärische Satellitensysteme

Zahlreiche Länder verfolgen neben einer zivilen Nutzung von Satellitentechnologie auch ein militärisches Satellitenprogramm.

MILSTAR
1994 nahm das *Military Strategic, Tactical And Relay Satellite System* seinen Betrieb auf. Es war das erste System, das die Kommunikation und Zusammenarbeit unter den Teilstreitkräften Army, Navy, Air Force, Marine Corps und National Guard erlaubte, die bisher eigenständige Systeme betrieben. Es ist ein gut geschütztes, relativ störunanfälliges System, das für eine feindliche Umgebung geschaffen wurde. Es soll gegen Störmaßnahmen und nukleare Angriffe geschützt sein (EMP-Sicherheit) und kann aufgrund seines *Communications, Comman, Control and Information Distribution Mission* Moduls bis zu sechs Monate völlig autonom agieren.

MOLNIJA & MERIDIAN
Das MOLNIJA-System wurde noch von der ehemaligen Sowjetunion eingeführt und ist seit 1965 in Betrieb. Es ist ein auf die Bedürfnisse Russlands

[122] vgl.: Dodel, Hans; Häupler Dieter; Satellitennavigation, Hütig – Telekommunikation, 2004, S.82

zugeschnittenes Kommunikationssystem, das auch die nördlichen Polargebiete abdeckt und so die Kommunikation in Gesamtrussland sicherstellt. Das System MERIDIAN, dessen erster Satellit zu Weihnachten 2006 ins All geschossen wurde, soll das alte MOLNIJA-System ablösen.

SKYNET
Neben den USA und Russland ist das britische SKYNET das dritte dediziert-militärische System einer Einzelnation mit weltweiter Verfügbarkeit.[123]. Der erste Satellit war 1969 im Orbit, das System wird von der Royal Air Force betrieben.

SYRACUSE
Die französischen Streitkräfte betreiben das *Systeme de Radio-Communications Utilisant un Satellite.* Das System arbeitet als Passagiernutzlast der französischen TELECOM-Satelliten und erreicht dadurch eine weltweite Abdeckung. Marine und Heer betreiben verschlüsselte, sichere Kanäle mit Bodenstationen und Schiffsanlagen.

HISPASAT
Ähnlich dem französischen System betreibt auch Spanien sein eigenes Satellitenprogramm, das das zivile Fernmeldesystem HISPASAT der spanischen Postverwaltung nutzt.

XINUUO 2
Das aggressive Raumfahrtprogramm Chinas hat in den letzten Jahren viel Aufsehen erregt. China will unter Einsatz massiver finanzieller Mittel den Anschluss an die Spitze der Weltraumnationen schaffen, hat aber immer bestritten, an militärischen Systemen zu arbeiten und ist offiziell stets gegen die Militarisierung des Weltalls aufgetreten. China stand aber schon lange im Verdacht, an derartigen Systemen zu arbeiten, der Abschuss eines Wettersatelliten hat diesen Verdacht bestätigt. Über die Nutzung von Kommunikationssatelliten für die Volksarmee ist wenig bekannt, offiziell stand bei der militärischen Nutzung von Satellitentechnologie die Erdbeobachtung im Vordergrund. China hatte zuletzt das System XINUUO 2 installiert, technische Probleme führten aber zur Abschaltung des bislang einzigen Satelliten des Systems.

NATO
Das Satellitensystem der NATO erfolgt nicht unter Abstützung auf bereits vorhandene Systeme der Bündnisstaaten, sondern mit eigenen Satelliten, die aber von den USA und Großbritannien beschafft werden und zu den nationalen Systemen kompatibel sind.

EU
Von den fünf großen Staaten in der europäischen Union ist Deutschland das einzige Land, das keine eigene Satellitenkommunikation für seine Streitkräfte hat. Im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik ist aber eine gemeinsame militärische Nutzung sehr wahrscheinlich. Nationen, die eigene Satellitenprogramme betreiben, könnten Partnerstaaten die Mitnutzung ermöglichen und gerade im Rahmen der Aufstellung des EUROCORPS könnte die Einbringung militärischer Satellitenkommunikationsmöglichkeiten eine

[123] vgl.: Dodel, Hans; Häupler Dieter; Satellitennavigation, Hütig – Telekommunikation, 2004, S.225

wesentliche Rolle spielen. Ein eigenes militärisches Kommunikationssystem der EU-Staaten ist momentan nicht geplant.

4.3.1.6. Anti-Satellitenwaffen und Störmaßnahmen

Ein Satellit ist grundsätzlich verletzbarer als ein in der Erde verlegtes Kabel und bietet seinen Feinden zahlreiche Angriffspunkte. Ein Angriff auf einen Satelliten muss aber nicht immer mit der Zerstörung desselben enden, auch wenn diese langfristig gesehen zum Erreichen der eigenen Ziele am meisten Erfolg versprechen würde.

Der Abschuss eines Satelliten vom Boden aus ist leistungsaufwendig und der Beobachtung durch den Gegner ausgesetzt. Es können jedoch auch Smart Bullets von Railguns in der Umlaufbahn auf z.B. 40km/s beschleunigt und auf einen Satelliten abgeschossen werden. Diese wären schwer aufzuhalten und ein Ausweichen ist fast unmöglich[124].

Nuklearattacken bieten theoretisch ebenfalls die Möglichkeit, Satelliten auch aus großer Entfernung außer Gefecht zu setzen. Die Abhärtung des Satelliten gegen solche Angriffe ist aber bereits möglich und die Konsequenzen eines nuklearen Schlags sind wesentlich weitreichender als dass sich ein Einsatz von Nuklearwaffen nur zum Abschuss eines Satelliten rentieren würde.

Eine sehr gute Möglichkeit, Satelliten sauber und gezielt abzuschießen, bieten so genannte Anti-Satelliten Raketen, die von der Erde aus in den Orbit geschossen werden und dort über ein Signal-Tracking in ihr Ziel finden. China erprobte am 11. Januar 2007 unter großem internationalem Protest und sehr zum Ärgernis der USA eine solche Waffe und schoss einen seiner alten Wettersatelliten erfolgreich ab. Zum ersten Mal in der Geschichte wurde bekannt, dass eine solche Waffe, wenn auch nur zu Testzwecken, eingesetzt wurde.

Anti-Satelliten-Raketen erreichen in der Regel Satelliten im Low-Earth-Orbit (LEO), also Spionage- und Aufklärungssatelliten. Die Anti-Satelliten-Rakete wird entweder vom Boden oder einem Trägersystem wie beispielsweise einem Kampfjet in die Umlaufbahn geschossen und erreicht seine Zerstörungskraft nicht zwingend mit einem Sprengkopf. Als oberste Stufe einer solchen Rakete kann ein so genanntes MHV (Miniatur Homing Vehicel) dienen, das in den Satelliten gesteuert wird und durch seine kinetische Energie alleine diesen zerstört.

[124] vgl.: Dodel, Hans; Satellitenkommunikation, dpunkt Verlag, 1999, S.216

Abbildung 15: Amerikanische Anti-Satellitenrakete, die von einer F-15 Eagle in den Orbit geschossen wird

Wesentlich kosteneffizienter und mit weniger Aufwand durchführbar ist aber nicht der Abschuss, sondern die Störung eines Satelliten. Am effektivsten ist es, den Satelliten abschalten bzw. in eine andere Umlaufbahn dirigieren zu können. Verschlüsselte Datenübertragung und Kommunikation soll genau dies verhindern, im militärischen Ernstfall können Satelliten daher auch das Kommandomodul abschalten und bis zu 60 Tage autark arbeiten[125].

Aber auch die gezielte Störung der Satellitenübertragung kann zum Erfolg führen. Wie jede andere Funkstrecke kann auch die Satellitenübertragung mit einem ausreichend starken Störsender unterbrochen oder behindert werden. Dazu ist es gar nicht nötig, die gesamte Kommunikation bzw. Sendeleistung des Satelliten an sich zu unterbinden, es reicht bereits aus, am unmittelbaren Gefechtsfeld - beispielsweise durch Einsatz eines Breitbandstörers - den Empfang von Satellitensignalen zu stören und so Navigation und Kommunikation zwischen den Einheiten zu behindern. Der große Vorteil der technischen Überlegenheit einer Partei kann hier schnell zu einem großen Nachteil werden.

[125] vgl.: Dodel, Hans; Satellitenkommunikation, dpunkt Verlag, 1999, S.217

Abbildung 16: Mögliche Bedrohungen von Satelliten[126]

4.3.2. Roboter und Unmanned Vehicels

Drohnen und Roboter bieten für die Armee der Zukunft eine gute Möglichkeit Ressourcen und Kosten einzusparen und vor allem den Menschen zu schonen. Steckt die Entwicklung von echten Robotern noch in den Kinderschuhen, so sind erste Drohnen und ferngesteuerte Einheiten, so genannte „*Unmanned Vehicels*" sowohl in der Luft als auch zu Lande bereits im Einsatz. Sie dienen vorrangig noch der Informationsbeschaffung und Aufklärung, in weiterer Folge ist aber auch ein Einsatz als Waffe vorgesehen. Wichtig ist dabei die schnelle Reproduzierbarkeit, die Wiederverwendbarkeit und die Tatsache, dass der Soldat die Drohne fernsteuert oder programmiert, selbst aber weit vom Aktionsgebiet entfernt und sich somit nicht in unmittelbarer Lebensgefahr befindet.

4.3.2.1. UAVs – Unmanned Air Vehicels

Unbemannte Flugobjekte werden schon seit Jahren vor allem zu Aufklärungszwecken eingesetzt. Die deutsche Bundeswehr benutzt solche Drohnen, um ihre Grenzen zu überwachen, aber auch im unmittelbaren Kriegseinsatz wie im Kosovo (Einsatz der Aufklärungsdrohne CL-289) oder Irak haben sich diese Fluggeräte bereits bewährt. Sie werden entweder ferngesteuert oder verfolgen einen fix programmierten Kurs und können sogar temporär autark agieren. Mittlerweile gibt es eine breite Palette an UAVs, und die Entwicklung neuer Systeme ist zu einem wichtigen Sektor in der Rüstungsindustrie geworden. Selbst in Österreich werden Drohnen und UAVs entwickelt und gebaut, so ist

[126] Grafik des US-Verteidigungsministeriums aus dem *Space Technology Guide* FY 2000/2001

beispielsweise der Camcopter S-100 eine Drohne, die bis zu 6 Stunden völlig autark eine bestimmte Route abfliegen und überwachen kann.

In Zukunft sollen UAVs alle Aufgaben von modernen Kampfflugzeugen erfüllen können, das bedeutet, neben der Spionage, Aufklärung, Überwachung und Markierung von Zielen, ist auch die aktive Bekämpfung dieser Fokus in der Entwicklung. Dabei werden sie nicht nur auf sich allein gestellt agieren, sondern auch im Verbund oder Schwarm eingesetzt werden. Die BOEING X-45, welche noch 2008 in Dienst gestellt werden soll, erfüllt alle Eigenschaften eines Angriffsflugzeuges. Europa arbeitet parallel an der EADS Barracuda, die sogar als voller Ersatz für konventionelle Kampfflugzeuge zum Einsatz kommen soll. Solche UAVs werden militärisch als UCAVs bezeichnet, also als *Unmanned Combat Air Vehicels*.

Abbildung 17: Deutsche Aufklärungsdrohne CL-289 beim Start[127]

4.3.2.2. UGVs – Unmanned Ground Vehicels

Was in der Luft schon klare Gestalt annimmt, nämlich die Entwicklung von ferngesteuerten wieder verwendbaren Waffenträgersystemen, dürfte am Boden aufgrund der komplexeren Anforderungen noch etwas auf sich warten lassen. Faktoren wie Gelände oder die Überwindung von Hindernissen, Minen, Sperren, aber auch die im Vergleich zu UAVs höhere Verwundbarkeit stellen die wesentlichen Probleme solcher Gefährte dar. Dennoch sind UGVs ebenfalls schon seit Jahren im Einsatz, sie dienen aber weniger der Informationsgewinnung als dem Räumen von Minenfeldern oder Entschärfen von Bomben am zivilen Sektor.

[127] Artikel *CL 289*. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 28. September 2008, 13:38 UTC. URL: http://de.wikipedia.org/w/index.php?title=CL_289&oldid=51246563 (Abgerufen: 13. Oktober 2008, 01:15 UTC)

4.3.2.3. Roboter

Echte Roboter, die absolut autonom agieren, selbstständig Informationen über ihre Umwelt sammeln, navigieren, Objekte erkennen und Entscheidungen treffen können, sind heutzutage noch Utopie. Langfristig ist aber der Einsatz solcher Systeme auch im militärischen Kontext durchaus denkbar, wobei immer die ethische Frage gestellt werden muss, ob es sinnvoll und vor allem moralisch vertretbar ist, eine Maschine alleine über Leben und Tod entscheiden zu lassen.

4.3.3. Radarsysteme

Radarsysteme sind heute ein nicht mehr wegzudenkender Bestandteil sowohl in der zivilen als auch der militärischen Welt. Sie erlebten ihren entscheidenden Entwicklungsschub im Zweiten Weltkrieg, als die Luftschlacht um England die Entwicklung und Forschung sowohl auf deutscher als auch auf britischer Seite vorantrieb. Mit Radarsystemen kann man die Geschwindigkeit, Bewegungsrichtung, Entfernung, Flughöhe und Größe von Objekten, also Flugzeugen, Schiffen, Zügen und anderen Fahrzeugen aus einer sicheren Distanz bestimmen und so rechtzeitig auf Entwicklungen und Bedrohungen reagieren. Dabei wird eine elektromagnetische Welle emittiert, die vom Objekt reflektiert und vom System wieder aufgefangen wird. Aufgrund der Phasenverschiebung, der Laufzeit der Welle und dem Abstrahlwinkel können die genannten Parameter berechnet und weiterverarbeitet werden. Im Schiffs- und Flugverkehr haben Radarsysteme eine sehr große Bedeutung erlangt, da ohne sie ein geordneter und unfallfreier Betrieb wohl nicht mehr möglich wäre.

4.3.3.1. Militärisches Radar

Im Unterschied zur zivilen Luftraumüberwachung kann das militärische Radar auch Objekte erkennen, die sich im Radarschatten eines anderen Objektes bewegen und so für die zivilen Stellen unsichtbar sind. Dies wird durch ein Multi-Radar-Tracking System möglich, das auch auf die zivilen Radarstationen zurückgreift. In Österreich ist das so genannte System „Goldhaube“ im Einsatz, dessen 5 militärische Mittelstreckenradarsysteme und 6 militärische Tiefflugradarsysteme mit 3 zivilen Mittelstreckenradarsystemen zusammenarbeiten.

4.3.3.2. Tiefffliegererfassungsradar

Eine wesentliche Komponente im militärischen Frühwarnsystem stellt das Tiefffliegererfassungsradar dar. Mit konventionellem Einsatz von Radartechnologie ist es nicht möglich, alle Bereiche des Luftraums lückenlos zu überwachen. Gebirgszüge und Täler stellen dabei natürliche Hindernisse dar, die es Flugzeugen ermöglichen, sich unter dem Radarsignal anzunähern. Dies zu verhindern ist die Aufgabe von mobilen Tiefffliegererfassungssystemen, die gezielt zur Überwachung von exponierten Geländeteilen und Radarschatten eingesetzt werden. Ist ein Feindflugzeug erkannt und als solches identifiziert worden, können so genannte Zielzuweisungsradarsysteme zum Einsatz kommen, die ein koordiniertes Zusammenwirken der Fliegerabwehrkräfte ermöglichen sollen.

4.3.3.3. Gefechtsfeldradar

Bodenradarsysteme stellen eine weitere Möglichkeit dar, Informationen über das Gefechtsfeld zu gewinnen. Sie werden auf kurze Distanz eingesetzt und ermöglichen es Kommandanten, entscheidende Geländeteile zu überwachen, Annäherungen des Feindes rechtzeitig zu erkennen, eigene Truppen zu führen und das Lagebild entsprechend zu vervollständigen.

4.3.3.4. Passives Radar

Radartechnologie wie wir sie heute kennen, könnte schon bald der Vergangenheit angehören. Eine wahre Revolution im Bereich militärischer Radaranlagen zeichnet sich ab, nämlich die Einführung des so genannten passiven Radars. Dabei handelt es sich um ein System, das bereits vorhandene elektromagnetische Wellen wie etwa Handy- oder Rundfunksignale nutzt und über diese die Position von Objekten bestimmen kann. Genauso wie ein Fisch im Wasser die Wellenausbreitung beeinflusst, tun das auch Objekte aller Art mit elektromagnetischen Wellen. So soll nicht nur die Ortung von Flugzeugen sondern auch von Fahrzeugen und sogar Menschen mit einer militärisch relevanten Genauigkeit möglich sein.

Zahlreiche Firmen und Nationen forschen bereits an der Entwicklung solcher Systeme und konnten bereits Erfolge erzielen. Das tschechische Passiv-Radar System *Vera-E* hat offenbar bereits Serienreife erreicht, der amerikanische Rüstungskonzern *Lockheed Martin* hat dem Pentagon bereits 2002 das System *Silent Sentry* vorgestellt, das den gesamten Luftraum über Washington unter Nutzung von Rundfunksignalen überwachen konnte.[128]

Der Einsatz von Passiv-Radar Systemen könnte in der militärischen Kriegsführung einen großen Umbruch auslösen, denn erstmals wäre es möglich, Objekte zu überwachen ohne selbst „gesehen“ zu werden. Da keine Signale abgestrahlt werden, wären Anti-Radar Waffen, die über den Ortungsstrahl von Radaranlagen ins Ziel gelenkt werden, plötzlich wirkungslos, die kostenintensive Entwicklung der Stealth-Technologie wäre mit einem Schlag sinnlos geworden, selbst heute nahezu „unsichtbare“ Objekte wie z.B. der B2 Tarnkappenbomber oder der Stealthjäger F-117 würden ihren größten Vorteil verlieren und nicht einmal registrieren, dass sie längst erfasst wurden. Der Erfolg der heute vor allem von den Amerikanern in den jüngsten Konflikten verfolgten Strategie, vor einer Bodenoffensive die Lufthoheit zu gewinnen, wäre massiv gefährdet. Feindliche Luftabwehranlagen könnten nicht mehr detektiert und bekämpft werden, passiv-radar gesteuerte Luft-Boden Raketen könnten nahezu unbemerkt zuschlagen und der Begriff Lufthoheit müsste neu definiert werden.

[128] vgl.: Schildt, Gerhard Helge, Impulstechnik Grundlagen und Anwendungen, LYK-Informatiktechnik Gmbh, 2006, S.229ff

4.3.4. Elektronische Kampfführung (Electronic Warfare)

Elektronik und Elektronikanwendungen unterstützen im C4I-System die Gewinnung, Verarbeitung und Weitergabe von Information auf allen Führungsebenen und haben so erheblichen Anteil beim Erreichen der Informations-, Führungs- und in weiterer Folge auch Wirkungsüberlegenheit. Elektronikanwendungen bringen für das Führungssystem enorme Vorteile mit sich, bieten aber auch große Angriffsflächen für die gegnerische Seite. Die Kampfführung wird daher durch die Einbeziehung der gesamten Elektronikanwendungen um neue Möglichkeiten ergänzt. Diese sind:

- *Erhöhung der eigenen Führungs- und Wirkungsfähigkeit* infolge Schaffung eines Informationsvorsprunges aus den gegnerischen Elektronikanwendungen und
- *Herabsetzung der gegnerischen Führungs- und Wirkungsfähigkeit* durch Verhinderung einer effizienten Funktionsweise der gegnerischen Elektronikanwendungen.

Es geht also sowohl um die Erschließung neuer Informationsquellen für die eigene Führung, als auch um den Kampf gegen die feindliche Führungsfähigkeit. Angriffsziele sind hierbei insbesondere die elektronischen Anlagen und Einrichtungen gegnerischer C4I-Systeme. [129]

Die Elektronische Kampfführung bildet daher eines der Kerngebiete im C4I-System, da sie gezielt unter Nutzung bzw. Störung von Informations- und Kommunikationstechnik die eigene Führungsfähigkeit erhöhen, wobei hier klar zu unterscheiden ist, dass das bloße zur Verfügung stellen von Kommunikationstechnik zum Zwecke der eigenen Einsatzführung noch nicht der EloKa[130] zuzuordnen ist. Kampfmaßnahmen sind auch immer als solche zu sehen, das heißt als aktiv gesetzte Aktionen, um den Gegner in seiner Handlungsfähigkeit einzuschränken.

Elektronische Kampfführung ist die Gesamtheit aller militärischen Maßnahmen unter Ausnützung elektromagnetischer Strahlung

- *zur Informationsgewinnung über den Gegner*
- *zur Verhinderung der Nutzung des elektromagnetischen Spektrum durch den Gegner sowie*
- *zur Sicherstellung der Nutzung des elektromagnetischen Spektrums für eigene Anwendungen.* [131]

Mit dieser Definition wird klar, was unter dem Begriff EloKa zu verstehen ist. Einerseits sind dies alle Maßnahmen zur Aufklärung und Informationsgewinnung aus gegnerischen Elektronikanwendungen, andererseits werden aber auch alle Mittel, mit denen gegnerische Anwendungen beeinflussbar sind, durch den Begriff umfasst. Dazu zählen unter anderem neben Störung und Täuschung (*Softkill*[132]) in weiterer Folge

[129] Vgl. Olischer, Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003, S79ff;
[130] EloKa – Abkürzung für „Elektronische Kampfführung"; analog dazu EW für „Electronic Warfare"
[131] Olischer, Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003, S.82
[132] Softkill: Be- und Verhinderung gegnerischer Kommunikationsanlagen

auch die Zerstörung durch elektromagnetische hochenergetische Strahlung (*Hardkill*[133]).

4.3.4.1. Elektronische Aufklärung (Electronic Intelligence)

Die Informationsgewinnung im Sinne der EloKa erfolgt über die Aufklärung elektromagnetischer Wellen und die Identifikation, Auswertung und Klassifizierung von Signalen. Dazu zählen einerseits die klassische Funkaufklärung, also das Abhören und Auswerten gegnerischen Funk- und Datenverkehrs (*COMMINT*[134]*),* sowie die Ortung und Klassifikation sonstiger elektromagnetischer Abstrahlungen wie Radar-, Feuerleit- oder Lenkeinrichtungen (*ELINT*[135]*)*. Die beiden Bereiche sind eng miteinander verbunden, so dass sie an dieser Stelle unter dem Begriff *Elektronische Aufklärung (EloAufkl)* zusammengefasst werden.

Der gezielte Einsatz von Elektronischer Aufklärung hat Tradition und findet auch in Friedenszeiten statt. Ständig werden von allen Staaten der Welt auch Verbündete aufgeklärt, um so Erkenntnisse und Daten über Andere zu gewinnen und potentielle Bedrohungsbilder erstellen zu können.

Das amerikanische Echolon-System ist nur eines von vielen Beispielen, die international bekannt sind, aber interessanterweise ohne Protest und diplomatischer Folgen bleiben. Der große internationale Aufschrei sowie diplomatische oder militärische Folgen bleiben aber wohl auch aufgrund mangelnder Sensibilität für die Thematik der Elektronischen Kampfführung aus. Heute scheint gerade dieser Eingriff in die Souveränität anderer Staaten allgemein geduldet und gebilligt zu sein, obwohl mittlerweile sogar die persönliche Freiheit des Einzelnen unter dem Deckmantel des Kampfes gegen den Terrorismus in Frage steht. Eine Entwicklung die ethisch bedenklich und moralisch zu hinterfragen ist.

Die Elektronische Aufklärung erfolgt auf der strategischen Ebene[136] über die Nachrichtendienste, auf der operativen und taktischen Ebene über eigens ausgerüstete Truppenteile, die der Fernmeldetruppe zugeordnet sind. Man spricht hier auch von so genannten *Electronic Support Measures*[137], oder Elektronischen Unterstützungsmaßnahmen. Der Unterschied zwischen EloAufkl und EloUM liegt in der Zielsetzung, *Elektronische Aufklärung und FM-Aufklärung sind sozusagen die elektronischen Aufklärungskomponenten im Informationskrieg, der bereits im Frieden geführt wird. Elektronische Unterstützungsmaßnahmen sind die elektronischen Aufklärungskomponenten des elektronischen Kampfes im Einsatz.*[138]

---

[133] Hardkill: Zerstörung von Anlagen und elektronischen Bauteilen

[134] COMMINT: Communications Intelligence oder Fernmeldeaufklärung (FMAufkl) im deutschen Sprachgebrauch

[135] ELINT: Electronic Intelligence oder Elektronische Aufklärung (EloAufkl) im engen Sinn

[136] vlg.¨Kapitel 2.5 – Führungsebenen

[137] Electronic Support Measures (ESM), im deutschen Sprachraum Elektronische Unterstützungsmaßnahmen (EloUM)

[138] Olischer, Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003, S.101

4.3.4.2. Elektronische Gegenmaßnahmen (Electronic Counter Measures)

Alle Maßnahmen zur Be- und Verhinderung der wirksamen Nutzung des elektromagnetischen Spektrum durch den Gegner, sowie alle Maßnahmen zur Zerstörung gegnerischer Anlagen und elektronischer Einrichtungen über hochenergetische Abstrahlungen werden unter dem Begriff Elektronische Gegenmaßnahmen zusammengefasst. Das Ziel ist es dabei, die Funktionsweise von Geräten und Systemen so zu beeinträchtigen, dass jeglicher kampfwertsteigernder Nutzen für den Gegner verloren geht. Dies kann über die Tätigkeiten des Täuschens, Störens oder Zerstörens erfolgen, wobei sich diese in ihren Auswirkungen und Zielsetzungen unterscheiden.

4.3.4.2.1. Täuschen

Darunter versteht man das gezielte Irreführen des Gegners, das Vorspielen falscher Tatsachen, um den eigenen Einsatz und die eigene Kampfführung zu verschleiern. Dies kann beispielsweise über das Senden „falschen" Funkverkehrs erfolgen, um so dem Gegner Standort und Stärke vorzugaukeln, während die eigentlichen Einheiten Funkstille halten und sich bereits woanders befinden. Die Auswirkung erfolgreicher Täuschung soll folgendes Beispiel verdeutlichen:

Im Golfkrieg bereiteten die USA ihren Angriff vor und landeten dazu in KUWAIT, von wo aus der erste Stoß erfolgen sollte. Tagelang vor der eigentlichen Offensive wurde die irakische Aufklärung amerikanischem Funkverkehr ausgesetzt, aus dem die Vorbereitung des Angriffes mit zwei Panzerdivisionen aus südlicher Richtung zu schließen war. In Wahrheit hielten die Truppen strikte Funkstille und während die Iraker mit dem Stoß von Süden aus rechneten, verschoben die Amerikaner ihre Einheiten Richtung Westen, von wo aus sie bei Angriffsbeginn in die Flanke der Iraker stießen und so bereits früh tief in den Irak eindringen konnten.

4.3.4.2.2. Stören

Die zeitlich und örtlich beschränkte Be- und Verhinderung der Nutzung des elektromagnetischen Spektrums nennt man stören. Dabei unterscheidet man grundsätzlich unter aktiven und passiven Stören. Bei der passiven Störung entsteht die Störwirkung lediglich durch Beeinflussung der Energie, die durch Reflexion zum Empfänger zurückgelangen soll. Dies erfolgt beispielsweise über Düppelstreifen bei Flugzeugen, die Radarsignale verfälschen, auch die Tarnkappentechnologie kann als passive Täuschungsmaßnahme gesehen werden.
Die aktive Störung erfolgt durch Abstrahlung elektromagnetischer Energie und soll beim Empfänger ein stärkeres Signal erzeugen als sein Nutzsignal. Verschiedene Störverfahren unterbinden so gegnerischen Funk- und Datenverkehr und schränken damit die Führungsfähigkeit ein.

4.3.4.2.3. Zerstören

Die nachhaltige Verhinderung der Nutzung des elektromagnetischen Spektrums durch den Gegner bedingt die Zerstörung seiner Anlagen und Einrichtungen. Am Sektor der EloKa erfolgt dies über hochenergetische Abstrahlung wie gebündelten Mikrowellen- oder Laserstrahlen, aber auch dem Elektromagnetischen Impuls (EMP). Die Entwicklung in diesem Bereich ist freilich noch im Anfangsstadium, bietet aber großes Potential für die zukünftige Elektronische Kampfführung.

4.3.4.3. Elektronische Schutzmaßnahmen (Electronic Protection Measures)

Der letzte Bereich in der Elektronischen Kampfführung umfasst die Elektronischen Schutzmaßnahmen (EloSM), die früher auch als ECCM[139] bezeichnet wurden. Darin finden sich alle Tätigkeiten, um feindliche Gegenmaßnahmen wirkungslos zu machen und die eigene Führungsfähigkeit zu erhalten. Man unterscheidet hier zwischen taktischen, betrieblichen und technischen Schutzmaßnahmen.

Die *taktischen Schutzmaßnahmen* beinhalten Überlegungen zum Einsatz elektronischer Mittel in Hinblick auf die Einsatzführung. Beispiele dafür sind die Wahl der richtigen Antenne, der Aufstellungsort in Hinblick auf die Abstrahleigenschaften, die Frequenzwahl, Ausgangsleistung oder den Einsatz von Relais-Stationen.

Betriebliche Schutzmaßnahmen sind Tätigkeiten die das bedienende Personal während des Betriebes durchführen kann. Hierzu zählen zum Beispiel die Verwendung von Sprechtafeln oder Decknamen im Funkverkehr.

Technische Schutzmaßnahmen sind gerätespezifische Lösungen zur Erhöhung der Betriebssicherheit. Dazu zählen Anti-Störmaßnahmen wie das Frequency-Hopping[140] oder das geräteseitige Verschlüsseln von Informationen.

4.3.5. Der Soldat als Sensor

Nicht nur Elektronik, auch der Soldat selbst agiert im modernen Gefecht als Sensor und wird in Zukunft immer mehr als solcher eingesetzt werden. Dabei sind damit nicht nur Aufklärungstrupps und Eliteeinheiten, die weit hinter den feindlichen Linien eingesetzt werden und so sensible Information zu gewinnen suchen, gemeint, sondern jeder einzelne Soldat selbst. Beobachtungen, die Soldaten machen oder Informationen, die sie aus Gesprächen mit der Bevölkerung gewinnen runden das Gesamtbild ab und tragen zu einer umfassenderen Lagefeststellung bei.

[139] ECCM: Electronic Counter Counter Measures; Im Prinzip Gegenmaßnahmen zu den Gegenmaßnahmen, der Begriff umfasst aber nur technische Mittel, die eingesetzt werden, nicht aber Maßnahmen zum Schutz des Nachrichteninhaltes, woraufhin man heute von EPM spricht

[140] Frequency Hopping: Frequenzsprungverfahren: Betriebsart bei Funkgeräten, die während der Übertragung innerhalb kürzester Zeit in einem bestimmten Bereich des Bandes die Frequenz wechseln und so den Einsatz von Störern erschweren

Ein weiteres Konzept ist allerdings der Soldat als Sensorträger, der ausgerüstet mit PDA, GPS, Kameras und ähnlichem Kommandanten und Gefechtsständen einen realen Eindruck von den Geschehnissen im unmittelbaren Kampf liefert.[141]

4.4. Entscheidungsfindung

4.4.1. Informationsaufbereitung und - verarbeitung

Nicht nur die Informationsgewinnung, auch die Informationsverarbeitung ist essentieller Bestandteil von C4I-Systemen. Die gewonnene Information muss dem Kommandanten nicht nur zeitgerecht zur Verfügung stehen, sie muss auch von Widersprüchen und Fehlern bereinigt und auf wesentliche Punkte reduziert werden. Zusätzlich muss der Entscheidungsträger aber in der Lage sein, die Granularität der Information auf Wunsch zu erhöhen und Varianten durchspielen zu können. Die Verantwortung, die dabei solchen Systemen zukommt, lässt sich anhand eines viel zitierten Beispieles verdeutlichen:

Am 03. Juli 1988 befand sich der amerikanische Kreuzer USS Vincennes zur Sicherung der Öllieferungen für die USA in iranischen Hoheitsgewässern und wurde von iranischen Kanonenbooten angegriffen. Plötzlich meldete das Battle Management System AEGIS[142] ein sich näherndes Flugzeug, das auf Funkkontakt nicht reagierte und auch kein Transpondersignal sendete. Innerhalb von nur sieben Minuten befahl der Kommandant unter Abstützung auf das Führungsinformationssystem den Abschuss des vermeintlich feindlichen Flugzeuges. Es handelte sich dabei allerdings um eine iranische Linienmaschine, die Auswirkungen dieses Fehlers waren mit 290 Toten verheerend.[143]

In weiterer Folge wurde ein Softwarefehler für den Abschuss der Maschine verantwortlich gemacht, die schwere Verantwortung dieser Entscheidung liegt aber auch in der reinen Abstützung des Kommandanten auf sein Battle-Management-System. Das System hatte den Airbus als feindliche F-14 erkannt und eine Bedrohung ausgemacht, ohne aber alle relevanten Informationen zu besitzen. So waren zivile Flugpläne nicht einprogrammiert und die Verfahrensregeln für ein Flugzeug, das kein Transpondersignal sendet, waren ebenso mangelhaft.

Die fehlende und falsche Informationsaufbereitung ließ den Kommandanten, der sich auf sein System voll und ganz verlassen hatte, diese fatale Entscheidung treffen. Das Beispiel macht aber auch deutlich, wie wichtig die Informationsaufbereitung im C4I-System ist. Ein korrekt und umfassend arbeitendes System hätte das Fehlen an Information erkannt und zumindest die Möglichkeit berücksichtigt, dass es sich um eine zivile Maschine handeln könnte und nicht den sofortigen Abschuss des Flugzeugs vorgeschlagen.

4.4.2. Battle-Management

Der Regelkreis von Führung und Kontrolle ist durch C4I-Systeme so weit wie möglich zu unterstützen, eine automatisierte Abwicklung des Vorganges der Führung kann aber auch von einem C4I-System nie vollständig übernommen werden. Dem steht

[141] siehe Kapitel 4.5 - Der neue Soldat
[142] AEGIS: Airborne Early Warning Ground Environment Integration System
[143] vgl. Simeoni, Thomas; War der Golfkrieg der erste Informationskrieg?, Diplomarbeit; Wien, 1997, S.41f

nicht nur die Komplexität des gesamten Führungsvorganges an sich entgegen, sondern auch die ethische und moralische Frage, ob es Computersystemen gestattet sein soll, ohne menschlichen Einfluss Schlachten und Gefechte zu lenken und so Entscheidungen über Leben und Tod zu treffen.

Allerdings liegt in der Beantwortung dieser Frage auch die große Herausforderung der Zukunft an das C4I-System, denn natürlich ist es technisch möglich, komplexe Entscheidungen von Expertensystemen nach vorgegebenen Entscheidungshilfen wie beispielsweise den „Rules of Engagement“[144] treffen zu lassen, was in gewissen Teilbereichen auch durchaus Sinn macht. Betrachtet man beispielsweise die Abwehrmaßnahmen eines modernen Kriegsschiffes gegen Anti-Schiffs-Raketen, so wird man feststellen, dass es dem Feuerleitoffizier bzw. Kommandanten gar nicht möglich ist, zeitgerecht die Berechnungen zum Ziel zu erstellen und die entsprechenden Feuerbefehle zu erteilen, ohne den rechtzeitigen Abschuss der Rakete zu gefährden. Solche Verteidigungssysteme sind daher sehr wohl rein durch das C4I-System zu steuern, überall dort wo es aber um komplexere Entscheidungen und größere Zusammenhänge geht, ist der menschliche Faktor allerdings unersetzbar.

Der Grad der Automatisierung hängt also von der jeweiligen Führungsebene und Art der Führungsstelle ab, so ist für Entscheidungsfindungen im technischen Bereich wie eben zum Beispiel innerhalb von Waffensystemen bei zeitkritischen Anwendungen ein höherer Automatisierungsgrad erforderlich als bei Entscheidungen zur Führung von Truppen. Die endgültige Entscheidung muss aber immer der Mensch selbst, in diesem Falle der Kommandant, treffen können. Die Einbindung der menschlichen Intelligenz muss auch bei Expertensystemen möglich sein und selbst bei vollautomatischen Führungsprozessen muss die Möglichkeit für den Kommandanten gegeben sein, jederzeit Einfluss auf Entscheidungen des Systems nehmen zu können.[145]

Das Battle Management stellt daher eine Art „Gratwanderung“ dar zwischen der Frage, was Systeme selbstständig dürfen und können sollen und was nicht. Die Problematik liegt aber auch darin, dass Computersysteme nie wirklich erfassen können, wie ein Befehl, den sie geben, sich im Gefecht auswirkt und welche direkten und indirekten Konsequenzen sich daraus ergeben. „*They can never know the real physical and social world of accidents, tensions and battlefield chaos. They cannot reason about the intensions of an adversary.*“[146]

4.4.3. Interoperabilität

Der Kampf der „verbundenen Kräfte“, also das Zusammenwirken der verschiedenen Waffengattungen als homogenes System ist ein Konzept, das seit dem zweiten Weltkrieg verfolgt wird. Durch die Vernetzung von Kommunikationswegen soll die Effizienz der Waffengattungen durch koordinierten Kräfteeinsatz erhöht werden. Im C4I-System soll dieser Synergieeffekt durch Vernetzung der einzelnen Truppenteile

[144] ROE – Rules of Engagement: Verfahrensregeln für den Kampfeinsatz, in denen die Befugnisse der Soldaten je nach Einsatzart klar definiert sind

[145] Olischer, Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003, S54f

[146] Bellin, D., Chapman G.(Eds): Computer in Battle – Will they Work?, Hartcourt Brace Jovanovich, Boston 1987 zit. nach (Simeoni, Thomas; War der Golfkrieg der erste Informationskrieg?, Diplomarbeit; Wien, 1997, S41)

erreicht werden, der Begriff „*Force Multiplier*“ ist eng mit dem Einsatz von vernetzten Systemen und der Interoperabilität verbunden. Die sich aus der Vernetzung von Truppenteilen und in weiterer Folge von Information ergebende Kampfwertsteigerung stellt eine wesentliche Komponente im Erreichen der Führungs- und Wirkungsüberlegenheit dar.

4.4.4. Elektronische Lagekarten

Elektronische Lagekarten, die in Echtzeit geführt werden, geben Entscheidungsträgern jederzeit ein umfassendes Lagebild. In diese Lagekarten fließen neben Standort und Stärke der eigenen Kräfte natürlich auch Aufklärungsergebnisse ein. Sie ermöglichen ein Verfolgen von Gefechten nahezu in Echtzeit, ähnlich wie in einem Computerspiel, wobei hier den Benutzern solcher Lagekarten die moralische Verantwortung jederzeit bewusst sein muss, geht es doch immer um Menschenleben. Auch in diesem Bereich ist die Frage der Granularität zu berücksichtigen, denn je nach Führungsebene unterscheidet sich die relevante Information, die aus solchen Lagekarten gewonnen werden soll.

4.4.5. Simulatoren

Moderne Simulatoren lassen das Geschehen am virtuellen Gefechtsfeld üben und optimale Strategien zur Kriegsführung erarbeiten. Der Umgang mit komplexen modernen Waffensystemen kann ebenso kostengünstig und materialschonend geprobt und erlernt werden, wie der Einsatz in realitätsnahen Szenarien. Für nahezu alle militärischen Bereiche gibt es mittlerweile Simulatoren und Software-Systeme, die mögliche Szenarien nachbilden und so Soldaten aller Ebenen optimal auf ihren Einsatz vorbereiten können.

4.5. Der neue Soldat

Ein sehr interessantes Konzept für den Einsatz von Technologie und einer damit verbundenen Kampfwertsteigerung stellt der so genannte „Land Warrior“ dar. Dieses von der US Army betriebene Projekt soll den einzelnen Soldaten zu einer Sensor- und Waffenplattform machen, die über die normalen menschlichen Grenzen hinaus wirken kann. Der Land Warrior soll dabei in der Lage sein, Ziele zu bekämpfen, die außerhalb seines Sichtfeldes liegen oder aufgrund von Umwelteinflüssen oder Tarnmaßnahmen grundsätzlich nicht in seiner Reichweite liegen. Er soll weiters mittels PDA und Notebook fähig sein, sich jederzeit ein für ihn relevantes Lagebild zu verschaffen und umgekehrt seine Beobachtungen am Gefechtsfeld in die Beurteilungs- und Führungsprozesse der übergeordneten Kommanden einbringen können. So soll es ihm beispielsweise möglich sein, auf Beobachtungsergebnisse der ihm benachbarten Einheiten zuzugreifen und so Gefahren, aber auch Ziele rechtzeitig zu erkennen und bekämpfen zu können. Mittels Kameras soll er in der Lage sein, um die Ecke zu schießen, Sensoren geben weiters ständig über den Status des Soldaten Auskunft, so können auch medizinische Daten überwacht und ausgewertet werden.
Die Entwicklungen gehen sogar soweit, dass bereits mit „second skins“, also Tarnanzügen, die sich chamäleonähnlich an ihre Umgebung anpassen oder mit exoskelettarer Stärkung der

Körperkräfte experimentiert wird. Auch wenn viele dieser Entwicklungen noch utopisch und nach Science Fiction klingen, so arbeitet die *„Science daran, die Fiction zu überbieten“*[147].

4.6. Intelligente Waffensysteme

Neue „intelligente“ Waffensysteme sollen zusätzlich für Effizenz und Kampfwertsteigerung sorgen. Präzisionsgesteuerte Bomben und Raketen sollen gezielte Schläge aus der Distanz ermöglichen, um so eigene Kräfte schützen und den Gegner trotzdem entscheidend treffen zu können. Die Reichweite reicht dabei von RADAR-, Laser-, Infrarot- bis hin zu Satelliten- und GPS-gesteuerter Munition, die bei höherer Treffergenauigkeit weniger Begleitschäden oder Kollateralschäden anrichten soll. Seit dem Golfkrieg 1990/91 wurde in diesem Zusammenhang der Begriff der *„chirurgischen Kriegsführung“* geprägt, der suggerieren sollte, dass Kampfhandlungen ohne zivile Opfer oder unbeabsichtigten Schäden an Infrastruktur möglich wären. Militärische Schläge sollten gemäß dieser Notation so präzise wie ein Skalpell bei einer medizinischen Operation geführt werden können, allein die Praxis zeigt, dass diese Vorstellung irreal ist. So wurde dieser Mythos beispielsweise im Kosovo-Konflikt zerstört, wo an die 30 Fälle von Kollateralschäden dokumentiert sind.[148] Zivile Opfer sind wohl in keinem Krieg gänzlich zu vermeiden, auch wenn der Einsatz präzisionsgesteuerter oder intelligenter Waffen diese reduzieren kann.
Eine weitere Überlegung bringt Thomas Simeoni ein, der in seiner Untersuchung des Golfkrieges 1990/91 unter anderem zu dem Schluss kommt, dass der Einsatz nicht-intelligenter Waffensysteme dem Informationskriegscharakter dieses Konfliktes widerspricht[149].
Folgerichtig bedeutet dies im Umkehrschluß, dass der Einsatz intelligenter Waffensysteme der industriellen Kriegsführung widerspricht und daher als Indikator für den Informationskrieg gewertet werden kann. Führt man diesen Gedanken fort, so könnte man sagen, dass in einem umfassenden Informationskrieg keine konventionellen Waffen mehr eingesetzt werden dürften, ob diese Vorstellung allerdings real ist, bleibt abzuwarten und wird erst die Zukunft zeigen.

[147] vgl. Kaufmann, Stefan, „Electronic Soldier“ – Der Infanterist der Zukunft In: Der Offizier Nr3/3006, S8ff
[148] vgl. Neuneck, Götz, Scheffran, Jürgen, Die Grenzen technischer Kriegsführung, Spektrum der Wissenschaft 01/2000, S90ff
[149] Vgl. Simeoni, Thomas; War der Golfkrieg der erste Informationskrieg?, Diplomarbeit; Wien, 1997, S.142

5. Network Centric Warfare

Nicht groß zu sein ist ausschlaggebend, sondern als kleine Einheiten große Netzwerke zu bilden.
Dr. Lothar Späth, Ministerpräsident Baden-Würthemberg 1978-1991

In der Vergangenheit sind wir im Zusammenhang mit dem Informationskrieg immer wieder auf den Begriff der „Vernetzung" der Gesellschaft und in weiterer Folge auch des Militärs gestoßen. Diese Entwicklung hat bereits in neuen Konzepten der Kriegsführung, den damit verbundenen doktrinellen Veränderungen und in fortgeschrittenen Reformations- bzw. Transformationsprozessen innerhalb der Streitkräfte vieler Nationen ihren Niederschlag gefunden. Vor allem die USA nehmen auf diesem Gebiet eine Vorreiterrolle ein und haben ihre Theorie der *„Network-Centric Warfare" (NCW)* entwickelt, die wohl eine neue Ära ganz im Sinne des Informationskrieges einläuten wird. Aber auch europäische Staaten haben sich das Konzept der Amerikaner zum Vorbild genommen, um international wettbewerbsfähig zu bleiben und die „*Gap of Capability*" gerade innerhalb der NATO gering zu halten. So entwickelt die deutsche Bundeswehr beispielsweise eine *vernetzte Operationsführung*, die Briten nennen ihr Modell hingegen *Network Enabled Capabilities (NEC)* und sogar in Österreich hat man die Zeichen der Zeit erkannt und versucht im Rahmen der Reform ÖBH 2010 zumindest einen ersten Schritt in diese Richtung zu setzen.

Konkret versteht man unter Network Centric Warfare (NCW) die Kombination von Strategien, gemeinsamen Taktiken, Techniken, Prozeduren und Organisationen, die eine teilweise oder voll vernetzte Streitmacht etablieren kann, um einen entscheidenden Vorteil im Gefecht zu ziehen.[150] Durch den Einsatz moderner Technologien (C4ISR) wird eine Informationsüberlegenheit erreicht, die den Protagonisten[151] der NCW in weiterer Folge eine teilstreitkräfteübergreifende Überlegenheit in der gesamten Reichweite aller militärischen Operationen vom klassischen Gefecht bis hin zu friedenserhaltenden Einsätzen garantieren soll. NCW ist die militärische Antwort auf das Informationszeitalter und genießt im Militär den Status, den in der modernen Wirtschaft das E-Business innehat.[152]

5.1. NCW als *Revolution in Military Affairs*

Nach dem Ende des Kalten Krieges und der beginnenden Globalisierung wurde schnell klar, dass auch auf das Militär grundlegende und tiefgreifende Änderungen zukommen werden. Wie bereits in Kapitel 3 kurz erwähnt wurde diese Entwicklung Anfang der 90er Jahre in den USA unter dem Begriff „*Revolution in Military Affairs* (RMA)" thematisiert. Ganz im Sinne der Begriffsbestimmung dieser Arbeit[153] wird darunter eine Entwicklung verstanden, *die in der Art der Kriegsführung in zumindest einer Teilstreitkraft einen Paradigmenwechsel hervorruft und alte Operationsformen obsolet werden lässt. Dabei können sowohl*

[150] vgl. Cebrowski Arthur, Vice Admiral US Navy, The Implementation of NCW, Office for Force Transformation, Secretary of Defense, 2005, S3
[151] Der Fokus liegt hier klar bei den USA und ihren Streitkräften. In diesem Kapitel ist der Begriff „Militär" vor allem in Bezug zu den US-Streitkräften zu setzen, da gerade in Europa trotz aller Bemühungen die Entwicklung und auch der Stellenwert der NCW den USA hinterher hinkt.
[152] vgl. Cohen, S., William, Secretary of Defense, Annual Report to The President and The Congress, Department of Defense, 1999, S.107ff
[153] vgl. Kapitel 3.1.3

technologische Innovation als auch neue strategische Konzepte Grundlage dieser Vorgänge sein.[154]

Die Theorie der NCW als fundamentalste und wichtigste RMA brachte erstmals Vice Admiral Arthur Cebrowski der US Navy 1998 ins Spiel, der Parallelen zwischen militärischer Entwicklung und der Wirtschaft zog. In Anlehnung zu Toffler sprach er davon, dass Gesellschaften so Krieg führen, wie sie Gewinn erwirtschaften und orientierte sich dabei an den Organisationsprinzipien der New Economy.

Für ihn, mittlerweile Beauftragter der US-Regierung für Force Transformation. ist daher die Vernetzung der Streitkräfte und somit der Übergang von der plattformbasierten zur netzwerkbasierten Kriegsführung die wichtigste RMA seit der Einführung der *levée en masse* während den Napoleonischen Kriegen.[155]

Tatsächlich ist aber der revolutionäre Charakter der NCW, der augenscheinlich durch den Paradigmenwechsel und den doktrinellen tiefgreifenden Änderungen entsteht, durchaus nicht so eindeutig, wie er scheinen mag. Der Begriff der „Transformation" beinhaltet nämlich das Abgehen von klassischen Modernisierungsschritten und Anpassungen an technologische Entwicklungen und impliziert vielmehr eine evolutionäre, zeitgerechte Entwicklung des Militärs, das sich nunmehr ständig in einem Prozess der Veränderung befinden soll. So sieht beispielsweise die Deutsche Bundeswehr in der Transformation „*die Gestaltung eines fortlaufenden, vorausschauenden Anpassungsprozesses, um die Einsatzfähigkeit, der Bundeswehr zu erhöhen und auf Dauer zu halten*"[156] und das US-Amerikanische Verteidigungsministerium (Department of Defense – DOD) definiert Transformation als „*evolution and deployment of combat capabilities that provide revolutionary or asymmetric advantages to our forces.*"[157]

Die eigentliche Revolution in Militärischen Angelegenheiten abseits von Doktrinen, Organisation, Führung und Technologie wird daher in Zukunft auch in der evolutionären Entwicklung des Militärs liegen.

5.2. Struktur der Network Centric Warfare

Die eigentliche Grundidee besteht nun in der Vernetzung der einzelnen Teilstreitkräfte und der Schaffung neuer Kommunikationswege. Eine neue Informationsstruktur und ein leistungsstarkes Netzwerk sollen eine zentrale Verfügbarkeit der gesamten Information gewährleisten und so Führungsverfahren beschleunigen, ein umfassendes Lagebild vermitteln und den *Kampf der Verbundenen Kräfte*[158] optimieren. Frei nach dem Metcalfeschen Gesetz, das ja besagt, dass der Nutzen eines Netzwerkes mit dem Quadrat der Anzahl seiner Teilnehmer steigt, muss also der Übergang von der plattform- zur netzwerk-gestützten Kriegsführung, also hin zu einem hochvernetzten Militär, eine entsprechende Kampfwertsteigerung zur Folge haben.

---

[154] vgl Decker Julio, *Seminararbeit Network Centric Warfare. Ein neues Konzept der Kriegsführung*, 2003, URL: http://www.politik.uni-koeln.de/jaeger/downloads/decker_ha.pdf, S4, (Abgerufen: 21.04.2008)

[155] vgl URL: http://www.politik.uni-koeln.de/jaeger/downloads/decker_ha.pdf, S5, (Abgerufen: 21.04.2008) und Cebrowksi, Arthur, Vice Admiral US Navy, Network Centric Warfare, It's Origins and Future, US Naval Insitute,1998, S1

[156] vgl Benz Friedrich, Vernetzte Operationsführung, Zeitschrift Wehrtechnik V/2005, S26

[157] Network Centric Warfare, Department of Defense, Report to Congress, 2001, S2-2

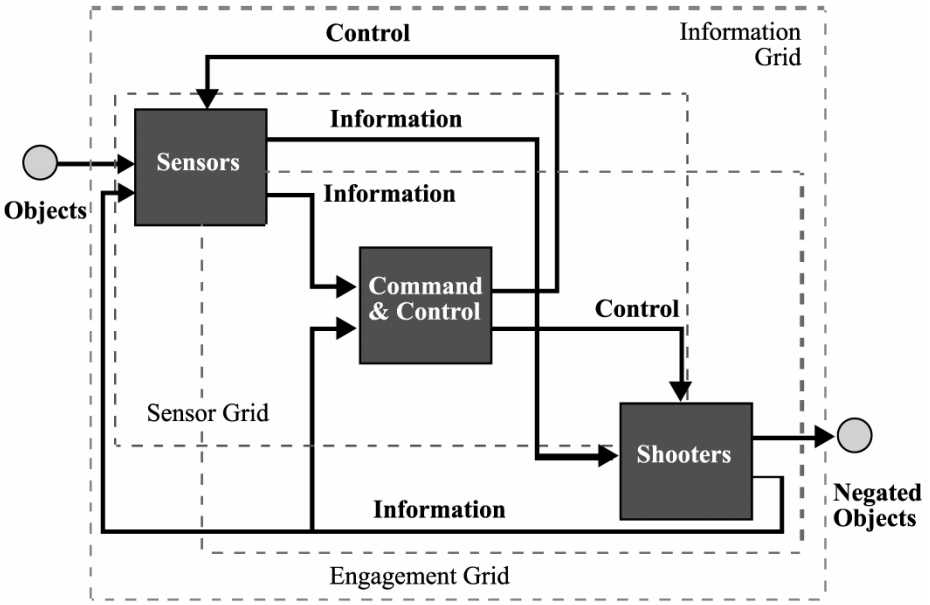
[158] Als Kampf der Verbundenen Kräfte wird das Zusammenwirken der einzelnen Teilstreitkräfte bezeichnet; Dieser Begriff ist synonym mit dem englischen Joint Forces

Um dies zu veranschaulichen, müssen wir zunächst erklären, was man unter plattformgestützter Kriegsführung versteht. Früher agierten auf dem Gefechtsfeld luft-, boden- und seegestützte Streitkräfte mit ihren jeweiligen Sensor- und Waffensystemen unabhängig voneinander und ein Informationsaustausch bzw. ein Zusammenwirken der Kräfte (z.B. Luftunterstützung) war, wenn überhaupt, nur durch hohen Koordinierungsaufwand auf höchster Ebene und entsprechendem Zeitverzug möglich. Jede Plattform oder Teilstreitkraft entwickelte eigene Systeme und operierte im Rahmen ihrer Aufträge weitgehend autark. Erst im Sinne der Idee des Kampfes der Verbundenen Kräfte wurden integrierte Einzelsysteme entwickelt, die so konzipiert wurden, dass sie im Verbund ihre spezifische Aufgabe erfüllen konnten.[159]

Dieser Ansatz ist nun nicht grundsätzlich neu und hat mit dem Konzept der NCW nur bedingt zu tun. Es wäre falsch, NCW mit dem Kampf der Verbundenen Kräfte völlig gleichzusetzen, allerdings gibt die NCW dem Kampf der Verbundenen Kräfte eine völlig neue Dimension, indem durch die Vernetzung der Truppen *allen Akteuren ermöglicht wird, die Fähigkeiten der anderen je nach Bedarf und Berechtigung einzusetzen.*[160]

Es geht um *„Führung und Einsatz auf der Grundlage eines streitkräftegemeinsamen, führungsebenenübergreifenden und interoperablen Informations- und Kommunikationsverbundes, der alle relevanten Personen, Stellen, Truppenteile und Einrichtungen sowie Sensoren und Effektoren miteinander verbindet. Diese neue Dimension des Verbundes von Aufklärung, Führung und Wirkung erlaubt es, durch enge und schnelle Abstimmung von Handlungsoptionen militärisches Handeln im gesamten Aufgabenspektrum schneller, effektiver und effizienter im Sinne des Auftrages zur Wirkung zu bringen.“*[161]

Erreicht wird dies durch die Bildung dreier Teilnetzwerke, den so genannten Grids, die die Grundstruktur der NCW bilden und wie folgt aussehen:



[159] vgl. Moschin Andreas, Obstlt i Gst, Network Enabled Operations, Land Power Revue der Schweizer Armee Nr 3, Blg. zur ASMZ 12/2005, S8
[160] Moschin Andreas, Obstlt i Gst, Land Power Revue der Schweizer Armee Nr 3, Blg. zur ASMZ 12/2005, S8
[161] vgl Benz Friedrich, Vernetzte Operationsführung, Zeitschrift Wehrtechnik V/2005, S26

Abbildung 18: Struktur der Network Centric Warfare [162]

5.2.1. Information Grid

Der Information Grid bildet die Basis der Teilnetzwerke und bettet die beiden anderen in sich ein. Diese Ebene ist verantwortlich für die Verwaltung von Information in Form von Daten, die gesendet, empfangen, gespeichert und aufbereitet werden müssen. Dazu ist eine komplexe Netzwerkarchitektur erforderlich, die neben einer mehrfachen Redundanz und hoher Ausfallssicherheit auch Kommunikationswege mit entsprechenden Kapazitäten etabliert. Die zeitgerechte und bedarfsorientierte Übermittlung von Daten ist dabei ebenso wichtig wie eine entsprechende Datensicherheit und Datenintegrität.

Dabei ist es aber nicht der Grundgedanke, dass jeder ständig mit jedem Daten austauscht, sondern dass aufgrund der Vernetzung eine sich im Laufe der Operation dynamische Kommunikation entwickelt. Hier zeichnet sich bereits ein Paradigmenwechsel ab, dem wir später bei den Grundprinzipien für den Einsatz vernetzter Streitkräfte[163] noch einmal begegnen werden, und zwar die Organisation entgegen der traditionellen hierarchischen Ordnung (top-down) im Militär, nämlich von unten nach oben (bottom-up). In Zukunft wird es nämlich nicht mehr am Besitzer der Information sein, diese an den richtigen Empfänger zu bringen, vielmehr wird es der Empfänger sein, der zweckdienliche Informationen proaktiv abruft. Kommandanten werden daher nicht mehr auf Lageinformationen, Befehle usw. warten, sondern diese selbstständig bei Bedarf abrufen.[164]

5.2.2. Sensor Grid

Dieses Teilnetzwerk homogenisiert alle relevanten Daten, die von Sensoren aller Art gesammelt werden und ermöglicht so ein für alle Einheiten synchronisiertes, umfassendes Lagebild, das kontinuierlich aktualisiert wird. Als Sensoren dienen dabei alle bereits bestehenden see-, luft-, land- und weltraumgestützten Systeme, die sich zwar in ihren Reichweiten und grundsätzlichen Aufgaben unterscheiden, deren gewonnene Daten aber vom Sensor Grid nach Relevanz und Priorität aufbereitet werden. Die Herausforderung besteht hier im Filtern von wichtigen Daten aus einer enormen Datenmenge sowie im gegenseitigen Abgleichen der Daten über mehrere Sensorsysteme hinweg. Mit Hilfe des Sensor Grids kann beispielsweise ein so genannter *composite track* erstellt werden, der die Verfolgung eines Objekts über mehrere Sensorsysteme (also z.B. der Anflug eines Feindflugzeugs, das per Schiffs- und Bodenradar geortet wird) ermöglicht und so den Wert der Information in Hinsicht auf Relevanz und Präzision multipliziert.

---

[162] Quelle: URL: http://www.emeraldinsight.com/fig/0730130501001.png, (Abgerufen: 04.05.2008)
[163] vgl. 5.3.3.4 Self-Synchronisation: bottom-up Organisation
[164] vgl. Moschin Andreas, Obstl i Gst, Land Power Revue der Schweizer Armee Nr 3, Beilage zur ASMZ 12/2005, S10

5.2.3. Engagement Grid

Die eigentlichen Kampfhandlungen finden über das Engagement Grid statt, das die durch den Sensor Grid gewonnene Information und die daraus resultierende hohe Übersicht über das Kampfgeschehen (battlespace awareness) direkt in erhöhte Kampfkraft umsetzt.[165] Dies geschieht über die gezielte Bekämpfung von strategisch bedeutsamen Zielen über die Grenzen der Teilstreitkräfte hinweg, also im Kampf der Verbundenen Kräfte. Die so gewonnene Kampfkraft, also die *Cooperative Engangement Capability* (CEC), ergibt sich aus der Maximierung des Effekts bei Minimierung des Aufwandes. Waren die militärischen Kapazitäten in der plattform-gestützten Kampfführung mit ihren fast konkurrierenden Teilstreitkräften schon allein durch die zeitliche Verzögerung durch notwendige Koordinierungsmaßnahmen auf höchster Ebene limitiert, so können nun mehrere Ziele in kürzerer Zeit in gemeinsamen Schlägen bekämpft werden. Dauerte es im Kalten Krieg noch einige Tage, bis ein Aufklärungsziel bekämpft werden konnte, waren es im Afghanistankonflikt nur mehr 20 Minuten, wobei nur 2 Minuten systembedingt waren und der Rest der Zeitspanne durch menschliche Entscheidungsprozesse verursacht wurde.
Hier tritt nun ein neues Ziel der Kriegsführung zu Tage, denn im Zeitalter der NCW geht es in erster Linie gar nicht mehr darum die gegnerische Armee zu vernichten, sondern die Strategie des Feindes zu brechen. Werden mehr als die Hälfte von strategisch wichtigen Einrichtungen zerstört, so bricht die Strategie des Feindes zusammen und der Konflikt ist in der Regel entschieden.[166]

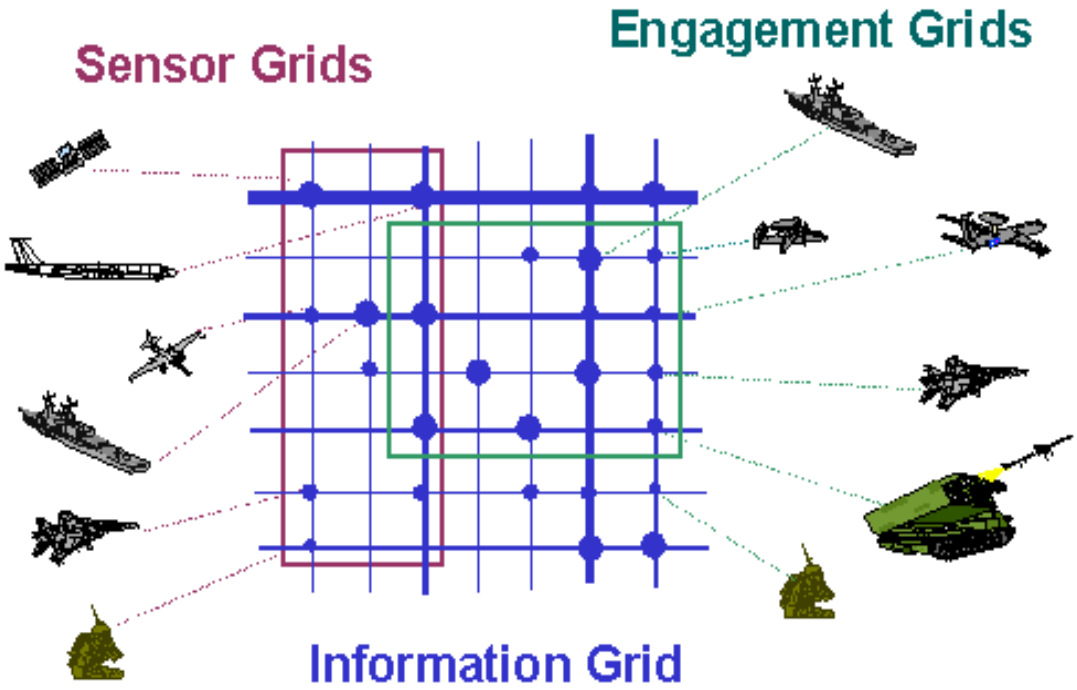


Abbildung 19: Zusammenhang der Grids[167]

[165] vgl. Cebrowksi, Arthur, Vice Admiral US Navy, Network Centric Warfare, It's Origins and Future, US Naval Insitute,1998, S6
[166] vgl. Cebrowksi, Arthur, Vice Admiral US Navy, Network Centric Warfare, It's Origins and Future, US Naval Insitute,1998, S6
[167] URL: http://www.fas.org/irp/program/collect/docs/pax_auvsi_1-2/sld033.htm, (Abgerufen: 08.05.2008)

5.2.4. Global Information Grid

Als Weiterentwicklung des Information Grids, von Kritikern aber stark angezweifelt, wird von den US Streitkräften der Aufbau eines globalen Informationsnetzwerks (GIG) forciert, welches netzwerk-gestützte Kriegsführung in globalem Ausmaß ermöglichen soll. Ziel ist es, Bündnispartner und Alliierte in das Netzwerk zu integrieren und so die Bildung von Koalitionen auch weiterhin zu ermöglichen. Die US Streitkräfte haben diese Ziele im Joint Vision 2020 festgelegt, ob dies aber auch so umgesetzt werden kann, hängt auch von der Investitionsbereitschaft der Bündnispartner ab und ist wohl eher eine politische, denn technische Frage.

5.3. Operative und Taktische Einsatzführung

Die Vernetzung der Truppen und das Zusammenwirken der Kräfte über alte Grenzen hinweg hat konsequenterweise auch weitreichende Änderungen am Gefechtsfeld und in den Einsatzgrundsätzen zur Folge. Das DOD definiert in diesem Zusammenhang vier Paradigma und neun Grundsätze, die als Grundlage der NCW gelten und die positiven Auswirkungen auf die Kampfführung deutlich machen sollen.[168]

5.3.1. Grundsätze für den Einsatz vernetzter Truppen

Die vier Paradigma für den Einsatz vernetzter Truppen ergeben sich in Anlehnung an das Handbuch „The Implementation of Network Centric Warfare“ wie folgt:

- A robustly networked force improves information sharing.
- Information sharing enhances the quality of information and shared situational awareness.
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command.
- These, in turn, dramatically increase mission effectiveness.[10]

Abbildung 20: Paradigma der NCW[169]

[168] Cebrowski Arthur, Vice Admiral US Navy, The Implementation of NCW, Office for Force Transformation, Secretary of Defense, 2005, S7ff
[169] Cebrowski Arthur, Vice Admiral US Navy, The Implementation of NCW, Office for Force Transformation, Secretary of Defense, 2005, S7

In diesen vier Paradigma lassen sich bereits die Grundsätze für die Einsatzführung erkennen. Als erstes geht es um Information und deren Austausch, wodurch ein allgemeineres Lagebild vermittelt werden kann, das die Truppen in die Lage versetzt, über die Grenzen ihres Auftrages hinweg mit anderen Zusammenzuarbeiten und wiederum ihre Aufträge selbstständig an Lageentwicklungen anzupassen. Dies hat schnellere Führungsabläufe zur Folge, wodurch die Truppen schneller und besser am Gefechtsfeld agieren können. Die neun Grundsätze für den Einsatz vernetzter Truppen ergeben sich daher wie folgt:

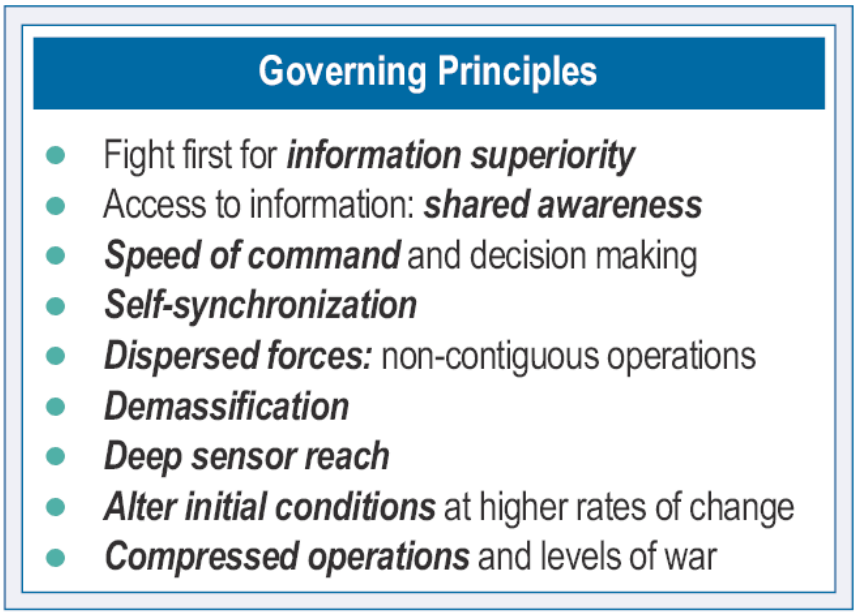


Abbildung 21: Grundsätze für den Einsatz vernetzter Truppen[170]

5.3.1.1. Information Superiority

Informationsüberlegenheit bildet das zentrale und grundlegendste Element der NCW. Kann Informationsüberlegenheit nicht erreicht werden, scheitert das ganze System, daher ist ihr besondere Bedeutung beizumessen. Erreicht werden soll sie durch hohe Akkuratesse, Pünktlichkeit und Relevanz der Information, was einen verminderten Informationsbedarf durch den Zugriff auf vernetzte Quellen und Sensoren zur Folge hat. Gleichzeitig wird versucht, den Informationsbedarf des Gegners zu maximieren und den Zugang zu Information zu minimieren.

5.3.1.2. Shared Awareness

Die Informationsüberlegenheit soll ein allgemeines, situationsbedingt umfassendes Lagebild vermitteln, das jede Einheit im Rahmen ihrer Bedürfnisse abrufen kann. Dabei sind Informationsempfänger gleichzeitig Sender und verantwortlich für das zeitgerechte Übermitteln von Information in das Netzwerk. Hier sehen wir wieder die bottom-up Hierarchie, denn Einheiten werden zwar nach wie vor von den

[170] Cebrowski Arthur, Vice Admiral US Navy, The Implementation of NCW, Office for Force Transformation, Secretary of Defense, 2005, S8

vorgesetzten Kommanden mit Informationen versorgt, rufen aber die für sie relevanten Daten selbstständig und auf ihre Bedürfnisse zugeschnitten ab.

5.3.1.3. Speed of Command

Durch die Informationsüberlegenheit wird Führungsüberlegenheit in Form von schnelleren, besseren Entscheidungsfindungsprozessen erreicht, die sonst nicht möglich gewesen wären. Kommandanten können aufgrund der Gesamtheit der Information schneller und effizienter agieren und befehlen. Unter Speed of Command wird aber der gesamte Prozess vom Erhalt eines Auftrages bis hin zu seiner Erfüllung verstanden.

5.3.1.4. Self-Synchronisation

Der wohl revolutionärste Grundsatz ist aber die Self-Synchronisation, daher wollen wir uns mit ihr ein wenig näher beschäftigen. Self-Synchronisation bedeutet, dass Einheiten am Gefechtsfeld aufgrund der hohen *shared awareness* in der Lage sind, Befehle selbstständig im Sinne des Auftrages abzuändern und so auf die komplexen und nicht vorhersagbaren Entwicklungen während einer militärischen Operation schneller reagieren können.

Das Österreichische Bundesheer definiert Selbst-Synchronisation wie folgt:
„Selbst-Synchronisation ist die Fähigkeit von Führungsebenen, komplexe Aufgaben auf dem Gefechtsfeld selbst „bottom up" zu organisieren und zu synchronisieren. Die Prinzipien zur Umsetzung dieser Organisation des Gefechtes sind ein gemeinsames Ziel, klarer Auftrag durch den Kommandanten, ein gemeinsames umfassendes Lagebild und vor allem anwendbare „Rules of Engagement". Selbst-Sychronisation kann sich entwickeln wenn das Wissen über die Eigenen, den Feind und andere Einflussfaktoren auf dem Gefechtsfeld hoch ist."[171]

Auch Cebrowski spricht von der hohen Komplexität militärischer Operationen und davon, dass die Komplexitätslehre zeigt, dass sich komplexe Unternehmen am besten von unten nach oben organisieren.[172] Dies steht aber in krassem Widerspruch zur streng hierarchischen Ordnung im Militär und stellt daher einen klaren Paradigmenwechsel mit revolutionärem Charakter dar.

In Kapitel 2 haben wir das Führungsverfahren[173] kennen gelernt, dass im Gefecht eine Art Kreislauf darstellt, der immer wieder durchlaufen wird. Cebrowski sagt nun, dass es während einer Operation aufgrund dieser geplanten Synchronisationsschritte zu Operationspausen kommt, die dem Feind Möglichkeiten eröffnen.[174]

---

[171] Militärstrategisches Konzept des Österreichischen Bundesheeres, BMLV, 2006, S59
[172] vgl. Cebrowksi, Arthur, Vice Admiral US Navy, Network Centric Warfare, It's Origins and Future, US Naval Insitute,1998, S6
[173] siehe Kapitel 2.3.3; Cebrowski spricht hier vom OODA-Loop, dem amerikanischen Äquivalent zum vorgestellten österreichischen Verfahren
[174] Wobei Cebrowski an dieser Stelle aber nicht sagt, dass der Gegner diesem Rhythmus ja ebenso unterliegt

Der Verlauf einer Operation entwickelt sich also grundsätzlich schrittweise, wobei die Zeit zwischen den Schritten als Verlust an Kampfkraft zu werten ist. Mit Hilfe einer bottom-up Organisation kann diese stufenweise Entwicklung an eine Kurve, die die optimale Operationsdurchführung in Relation zur Zeit darstellt, angenähert werden. Abbildung 22 veranschaulicht dies:

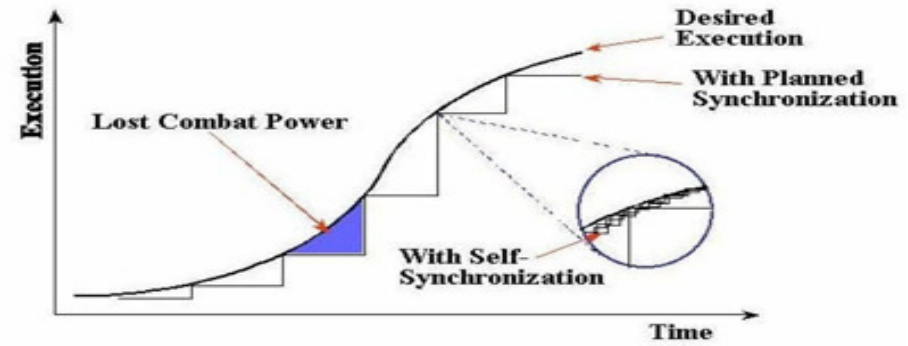


Abbildung 22: Durchführungs-Zeit Diagramm[175]

Wie die Graphik zeigt, wird die Operationsführung optimiert, was klarerweise einen entscheidenden Vorteil im Kampf gegen nicht vernetzte Truppen bringt, die noch unter Einhaltung der traditionellen Hierarchie ihrem „alten" Rhythmus unterliegen.

Allerdings ist zu gewährleisten, dass das selbstständige vorgehen der Truppen koordiniert bleibt und bestimmten Rahmenbedingungen folgt. Die wegfallenden Autoritäten und Kommanden müssen zumindest bis zu einem bestimmten Grad ersetzt werden, dies geschieht einerseits durch klare, präzisierte Aufträge, durch gemeinsame operative Ziele, die auch der taktischen Ebene bekannt sein müssen und vor allem durch Verhaltensregeln und Anweisungen, die den Kommandanten den Rahmen für Kampfhandlungen in Hinsicht auf das Beginnen, Fortführen und den Einsatz von Waffengewalt vorgeben – den *Rules of Engagement*.

5.3.1.5. Dispersed Forces

Eine gezielte Kräfteverteilung soll die Kampfkraft steigern, anstatt einer physikalischen Dominanz durch Konzentration der Kräfte in einem bestimmten Gefechtsstreifen sollen Truppen im richtigen Moment an Ort und Stelle sein und effektiv und gezielt zuschlagen können. Dazu ist eine enge Verknüpfung zwischen Aufklärung, Operation und Logistik anzustreben, um temporären Vorteil über den Gegner zu gewinnen.

[175] Van den Berghe, F., Wiesendahl, U., Funktionsweise der Network Centric Warfare, 2003, S9, URL: www.armscontrol.de/publikationen/**ws0203ncw**.pdf, (Abgerufen: 08.05.2008)

5.3.1.6. Demassification

Der aufgrund der Vernetzung der Kräfte gewonnene Informationsvorteil, soll dazu genutzt werden, um mit kleineren Einheiten effektiver und gezielter wirken zu können. So können die in einem bestimmten Gefechtsstreifen eingesetzten Truppen limitiert und verkleinert werden, weiters soll es feindlichen Kräften durch die höhere Mobilität erschwert werden, eigene Kräfte anzugreifen.

5.3.1.7. Deep Sensor Reach

Die Abstützung auf ein Sensornetzwerk schafft Informationsüberlegenheit, jede Waffenplattform, vom einzelnen Soldat bis zum Satelliten, agiert dabei als Sensor.

5.3.1.8. Alter Initial Conditions at Higher Rates of Change

Vernetzte Streitkräfte sind durch oben angeführte Grundsätze in der Lage, die Gefechtsbedingungen zu beeinflussen und so die Entwicklung der gegnerischen Operation zum eigenen Vorteil zu verändern.

5.3.1.9. Compressed Operations at Levels of War

Prozesse und organisatorische Abläufe sind so zu optimieren, dass strukturelle Hindernisse abgebaut, Kapazitäten erhöht und so eine schnelle und effektive Einsatzführung möglich werden.

5.3.2. Der Weg zur Full Spectrum Dominance

Auf Basis des Konzeptes der NCW hat in den US-Streitkräften eine Entwicklung eingesetzt, die Schaffung einer neuen Streitkraft, der Joint Force, zum Ziel hat, die im gesamten Spektrum militärischer Operationen dominieren kann. Diese „*Full Spectrum Dominance"* soll durch vier operative Grundsätze erreicht werden, die basierend auf der Informationsüberlegenheit und der NCW in der *Joint Vision 2020*[176] festgelegt sind.

5.3.2.1. Dominant Maneuver

Durch überlegene Geschwindigkeit und Bewegung sowie der Fähigkeit, das Feuer von weit dezentralisierten Effektoren zu konzentrieren und zu skalieren wird Überlegenheit im Manöver erreicht.

[176] Joint Vision 2020 ist die Weiterentwicklung der Joint Vision 2010 und ein doktrinelles Strategiepapier zur Streitkräfteentwicklung, wir kommen später auf beide zurück

5.3.2.2. Precision Engagement

Der präzise Kräfteeinsatz beschreibt die Fähigkeit vernetzter Truppen, Ziele und Objekte zu lokalisieren, zu erkennen, auszuwählen und das richtige System zum Einsatz zu bringen. Das bedeutet das Ziele mittels kooperativen Einsatzes der Streitkräfte präzise und effektvoll bekämpft werden können.

5.3.2.3. Focused Logistics

Benötigte und zur Verfügung stehende Ressourcen und Dienstleistungen können durch die Vernetzung der Truppen effizient und rechtzeitig dem Bedarfsträger zugeführt werden.

5.3.2.4. Full Dimensional Protection

Der Eigenschutz der Truppen wird erhöht, indem gegnerische Aktivitäten frühzeitig erkannt und unterbunden werden. Weiters werden alle Maßnahmen getroffen, um Operationen mit dem geringsten Risiko für eigene Kräfte durchführen zu können.[177]

5.4. Kritik an NCW

Obwohl das Konzept NCW einen der größten Entwicklungsprozesse in der Geschichte des amerikanischen Militärs eingeläutet hat, werden auch kritische Stimmen laut, die sich der allgemeinen Euphorie nicht anschließen wollen. So sei die Idee der streitkräfteübergreifenden Einsatzführung nicht grundlegend neu, außerdem sei NCW nichts anderes als die Wiederverwertung alter Konzepte unter neuem Namen, um mit vermeintlich neuen Projekten die Geldflüsse aus dem Kongress aufrechtzuerhalten. Andere kritisieren wiederum die Störungsanfälligkeit und die Systemsicherheit des Konzeptes. Die entstehende Abhängigkeit von neuen Technologien mache die eigenen Truppen bei Ausfällen verwundbarer und es würden neue Angriffspunkte für gegnerische Information Warfare geschaffen.[178]

Diese Kritiken sind zweifelsohne nicht ganz von der Hand zu weisen, denn tatsächlich hat es die Idee des Kampfes der Verbundenen Kräfte, wie schon erwähnt, bereits zu Zeiten, als der Begriff „Informationskrieg“ noch unbekannt war, gegeben. Auch die Abhängigkeit von elektronischen Systemen, die erst bei Ausfall selbiger deutlich wird, sowie die daraus resultierende Verwundbarkeit eigener Kräfte ist als logische Konsequenz anzunehmen.

Allerdings, so meine ich, können all diese Kritikpunkte, so berechtigt sie auch sein mögen, nicht über die Tatsache hinwegtäuschen, dass durch die NCW ein Quantensprung in der Entwicklung der Kriegsführung passiert, der nicht nur die operative und taktische

[177] vgl. Moschin Andreas, Obstlt i Gst, Network Enabled Operations, Land Power Revue der Schweizer Armee Nr 3, Blg. zur ASMZ 12/2005, S9

[178] Vgl. Cebrowski Arthue, Vice Admiral US Navy, Network Centric Warfare, An Emerging Military Response to the Information Age, Military Technology 5/2003, S.20f
Und vgl: Lauring, Mag., Bernhard, Network Centric Warfare, Österreichische Militärische Zeitschrift 6/2003, S763f

Einsatzführung betrifft, sondern darüber hinaus in höchstem Maße doktrinelle, strukturelle und systeminterne Entwicklungsprozesse hervorgerufen hat, die in dieser Form historisch kaum vergleichbar sind und die die Grundprinzipien des Militärs mit seiner streng hierarchischen Ordnung in Frage stellen. Vielleicht mag die Entwicklung in den USA zu schnell gehen, vielleicht sind die Kapazitäten in punkto Datenübertragung, Systemintegrität und Ausfallsicherheit noch nicht hoch genug, aber diese Probleme sind in naher Zukunft sicher lösbar. Wir können zum jetzigen Zeitpunkt noch nicht abschätzen, wohin diese Entwicklung führen wird, aber wir können, so glaube ich, erkennen, dass NCW die wohl konkreteste Form des Informationskrieges ist und all jene in Kapitel 3 behandelten Kriterien für eine revolutionäre Entwicklung, sei es nach Toffler oder Bell, erfüllt, so dass wir durchaus vom Beginn eines neuen Zeitalters sprechen können.

II.Teil

Wir haben uns im ersten Abschnitt dieser Arbeit unter Anderem mit den Grundlagen des Informationskrieges beschäftigt und wollen nun untersuchen, wie weit die Entwicklung schon fortgeschritten ist und sich in den Doktrinen der modernen Armeen niederschlägt. Als Referenz wollen wir uns dabei auf die Streitkräfte der USA und hier hauptsächlich auf die US Army konzentrieren.
Die wohl unbestrittene Führungsrolle der USA in Hinblick auf militärische Entwicklungen eröffnet uns die Möglichkeit, anhand der Streitkräfte der Vereinigten Staaten von Amerika den Einfluss des Informationskrieges auf Doktrinen zu untersuchen. Dabei werden wir uns einem Vergleich der Entwicklung seit dem Ende des Kalten Krieges widmen, um so die Unterschiede herauszuarbeiten und den Informationskrieg anhand seiner Elemente nach Arquilla/Ronfeldt messbar zu machen. Allerdings sei an dieser Stelle bemerkt, dass wir nicht alle Entwicklungen der Streitkräfte auf den Informationskrieg zurückführen werden können, da gerade in den USA budgetäre und geopolitische Vorgaben die Streitkräfteentwicklung sehr beeinflussen.
Der Zusammenhang zwischen Führung-Technologie-Doktrin wird am Ende des Abschnitts noch einmal zusammenfassend erläutert und bildet den Abschluss der Beantwortung der Forschungsfragen.

1. Einfluss des Informationskrieges auf die Doktrinen

1.1. Rahmenbedingungen für die Untersuchung

Wenn wir die geschichtliche Entwicklung der Kriegsführung seit dem Zweiten Weltkrieg betrachten, so lässt sie sich in mehrere Phasen gliedern. Der Kalte Krieg als großes Wettrüsten zweier globaler Machtsysteme hat ein einsatzorientiertes, aber unflexibles Denken der Militärs als Begleiterscheinung hervorgebracht, das klar auf einen globalen, konventionellen Konflikt zwischen nahezu gleich starken Parteien ausgerichtet war. Große Änderungen in den Doktrinen, revolutionäre Ansätze in der Kriegsführung wurden zwar theoretisch angedacht, deren praktische Umsetzung blieb aber zumeist aus, da ja immer auch eine Verschiebung des Gleichgewichtes der Macht zu befürchten war. Erst der Zusammenbruch der Sowjetunion und des Warschauer Paktes ermöglichte bzw. erzwang ein Aufbrechen dieser Strukturen und ebnete dem Informationskrieg im heutigen Verständnis den Weg. Die Phasen in der Entwicklung der Kriegsführung, die wir hier betrachten wollen, gliedern sich daher wie folgt:

- Phase I: Endphase Kalter Krieg 1982 bis 1991[179]
- Phase II: Neue Weltordnung 1991-2000
- Phase III: Eine neue Dimension in einem neuen Jahrtausend 2000-heute

[179] Es soll hier allerdings nicht der Eindruck entstehen, dass es im Kalten Krieg keine Entwicklungen gegeben hat. Ganz im Gegenteil war dieser Konflikt, der Gott sei Dank nie real ausgefochten werden musste, Motor und Antrieb für enorme Fortschritte im Bereich der Kriegsführung. Allerdings fanden revolutionäre Ansätze und damit verbundene große Umstrukturierungen erst nach Ende des Kalten Krieges ihren Niederschlag, wodurch diese Abgrenzung meines Erachtens nach durchaus Sinn macht. Es sei hier auch zu erwähnen, dass der Grundstein für die heutigen Entwicklungen auch bereits während des Kalten Krieges gelegt wurde. Wir wollen uns in dieser Phase auch nicht mit dem gesamten 35-jährigen Verlauf dieses Konfliktes beschäftigen, sondern vielmehr markante Punkte als Vergleichswerte für die anliegende Untersuchung betrachten.

In der Analyse bleiben wir bei Arquilla und Ronfeldt und deren Definition des Informationskrieges. Die Elemente, anhand derer wir den Grad des Informationskrieges untersuchen wollen, sind daher - wie bereits in Abschnitt I erwähnt – abgeleitet von Arquilla und Ronfeldt und in Anlehnung an den Zusammenhang Führung-Doktrin-Technologie:

- Einsatz von Technologie
- Organisation, Strategie, Dezentralisierung, Vernetzung
- Komplexitätsmanagement

Wir werden für jede Phase diese Elemente untersuchen und die Streitkräfte sowohl in ihrer Friedensorganisation als auch, wenn möglich, in realen Konflikten betrachten, um dann die Ergebnisse herauszuarbeiten. Um die Begriffe abzugrenzen, legen wir fest, dass die Existenz von Führungsunterstützungskräften ab Verbandsebene[180], Kräften zur Elektronischen Kampfführung sowie Bemühungen, den Kampf der Verbundenen Kräfte zu forcieren (z.B. über die Schaffung eigener Kommanden und Führungseinrichtungen), zusätzlich als Elemente und Indikatoren des Informationskrieges zu werten sind.

Streitkräftemäßig werden wir uns auf die US Army, ihre Doktrinen und ihre Organisation beschränken und nur dort wo es sinnvoll erscheint einen Blick auf die anderen Teilstreitkräfte werfen, da für die US Army gilt:

- sie bildet die größte der Teilstreitkräfte
- die Belastung durch Einsätze im Vergleich zu den anderen Teilstreitkräften ist überproportional hoch[181]
- sie trägt die Hauptlast im Transformationsprozess
- und hat in der Einsatzführung als einzige alle Dimensionen abzudecken

1.2. Grundlagen zur Organisation der US Streitkräfte

Um die einzelnen Ebenen der Kommanden und Verbände zu verstehen und einschätzen zu können, beschreibt dieses Unterkapitel kurz die grundlegende Struktur und die Befehlskette der US Streitkräfte.

Bei der Organisation der Streitkräfte ist zwischen der Administration und der militärischen Kommandokette zu unterscheiden, die nicht identisch sind. Oberster Befehlshaber ist der Präsident, der mit dem Verteidigungsminister die *National Command Authority (NCA)* bildet. Ihnen beigestellt ist das *Joint Chiefs of Staff Command (JCS),* das die Kommandanten aller Teilstreitkräfte in sich vereinigt und dessen Vorsitzender beratende Funktion für die National Command Authority hat. Die operativen Kräfte sind unterteilt in regionale Kommanden, den *Unified Combatant Commands (UCC)*, die verschiedene Aufgaben und Aufträge verfolgen, und den *Specified Commands,* die spezielle Funktionen in der Armee sicherstellen. Die regionalen Kommanden sind in den Interessenssphären der Amerikaner über den Erdball verteilt, so gibt es zum Beispiel das *US European Command (USEUCOM)*, das *Pacific*

[180] Der Aufbau von Kommunikationsnetzen auf Divisions- und Brigadeebene wird von Fernmelde- bzw. Führungsunterstützungsverbänden und – einheiten sichergestellt. Führungsunterstützungskräfte innerhalb von Bataillonen und Kompanien/Batterien/Staffeln jeglicher Waffengattung stellen Verbindungen innerhalb dieser Bataillone sicher, spielen für uns aber eine untergeordnete Rolle und werden daher nicht berücksichtigt.

[181] Vgl. Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006“, Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.153

Command (USPACOM), das *US Central Command (USCENTCOM)* für die Golfregion oder das *US Southern Command (USSOUTHCOM)* für Südamerika. In einem solchen UCC sind Komponenten von zwei oder mehr Teilstreitkräften einem Kommandanten unterstellt. Im Anhang findet sich eine Grafik der einzelnen Verantwortungsbereiche der Kommanden.

Die *Specified Commands* sind für spezielle Aufgaben aufgestellt und befehligen in der Regel nur Komponenten einer einzelnen Teilstreitkraft. Beispiele sind das *Strategic Command (STRATCOM)*, zuständig für die Nuklearwaffen oder das *US Special Operations Command (USSOCOM)* für den Einsatz der Spezialkräfte.

Diese Organisationsstruktur ist an sich streitkräfteübergreifend angelegt, daher weisen die einzelnen Teilstreitkräfte noch einmal ähnliche Strukturen auf.

Abseits davon existiert noch die militärische Befehlskette, die wir anhand der Landstreitkräfte kurz erläutern wollen. Die US Army besteht aus sechs *Major Commands (MACOM)*, die unterschiedliche Truppenstärken führen, folgende Skizze stellt die Kommandostruktur der Teilstreitkraft Army dar:

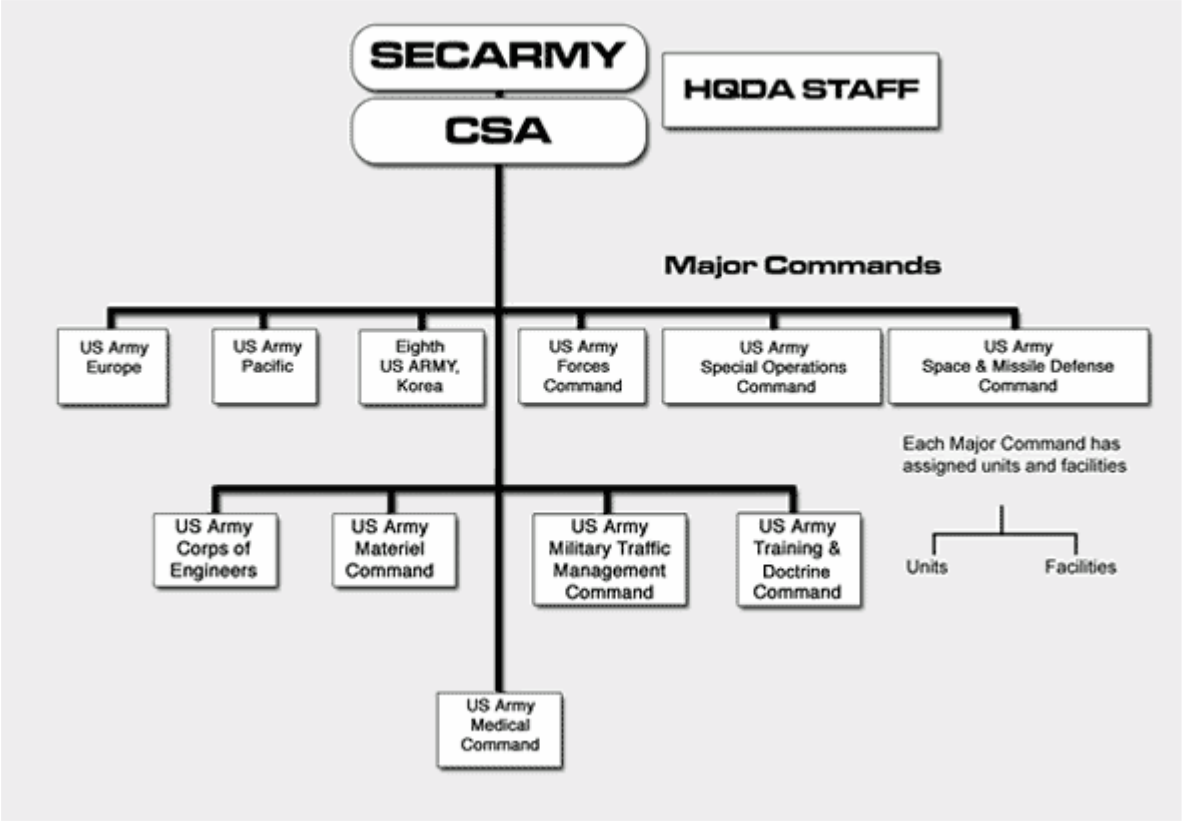


Abbildung 23: Kommandostruktur US Army[182]

An der Spitze steht der *Secretary of the Army (SECARM)*, der im Verteidigungsministerium sitzt und der *Chief of Staff of the Army (CSA)*, der Mitglied im JCS ist. Jedem Major Command ist eine bestimmte Anzahl an Verbänden unterstellt, beispielsweise kommandiert das *US Army Forces Command (FORSCOM)* die Erste bis Sechste Armee. Allen diesen

[182] Artikel *United States Army*. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 30. September 2008, 10:24 UTC. URL: http://de.wikipedia.org/w/index.php?title=United_States_Army&oldid=51315323 (Abgerufen: 6. Oktober 2008, 02:26 UTC)

Armeen sind wiederum Verbände und Einheiten unterstellt, die Hierarchie stellt sich wie folgt dar:

- Armee: ca. 100.000-150.000 Mann
- Korps: ca. 30.000 Mann
- Division: ca. 15.000 Mann
- Brigade: ca. 3500 Mann
- Regiment/Bataillon: ca. 1000 Mann

Weiters finden wir noch Allgemeine Kommanden der Army, wie das *US Army Training and Doctrin Command (TRADOC)*, das für die Ausbildung der Truppen und die Entwicklung und Bewertung von Doktrinen verantwortlich ist.
Dies ist die grundlegende Struktur, einzelne Punkte von Interesse werden im Zuge der Untersuchung betrachtet.

1.3. Phase I – Endphase Kalter Krieg

1.3.1. Einsatz von Technologie

Der Faktor Technologie spielte im Kalten Krieg eine sehr bedeutende Rolle. Das gegenseitige Wettrüsten zwischen Ost und West rief immer wieder Innovationswellen im Bereich der Raketen-, Waffen-, aber auch der Informationstechnik sowie auf Gebieten wie Biologie und Chemie hervor und fand im Gleichgewicht des Schreckens seinen traurigen Höhepunkt. Enorme Ressourcen und Mittel wurden über Jahrzehnte in die Etablierung neuer Kriegstechnologie gepumpt, die die Menschheit am Rande des Abgrunds einer permanenten nuklearen Bedrohung wandeln ließ.
„*Krieg ist der Vater aller Dinge!*“[183] sagte einst der griechische Philosoph Heraklit und der Erfindungsgeist der Menschheit in der Entwicklung von Waffen und Technologie zum Zwecke der Kriegsführung sucht tatsächlich seinesgleichen. Die Palette ist groß, von Flugzeugen, Panzern, Raketen, lasergesteuerten Präzisionsbomben bis hin zu biologischen und chemischen Waffen oder der Atombombe brachte der Kalte Krieg Technologien hervor, die teils so schrecklich waren, dass sie ihn nie ausbrechen ließen. Aber nicht nur die Vernichtung stand im Fokus der Forschung und so verdankt die Menschheit gerade dem Kalten Krieg auch zahlreiche Innovationen, die uns heute selbstverständlich sind, wie wir kurz am Beispiel des Internet verdeutlichen wollen.

Das Internet, eines der wohl wichtigsten Kommunikationsmittel unserer Zeit, wurde in den 1960er Jahren von der damaligen amerikanischen ARPA[184] entwickelt, um die knappen Rechnerkapazitäten sinnvoll nutzen und eine ausfallssichere Kommunikation zu ermöglichen. Einige Quellen behaupten, dass das Ziel der Entwicklung war, im Falle eines Atomkrieges und der danach zerstörten Infrastruktur Kommunikation trotzdem zu ermöglichen, dies klingt zwar glaubhaft, ist aber nicht gesichert.[185] Das

[183] Heraklit, 500vChr
[184] ARPA: Advanced Research Project Agency, heute DARPA, wobei das D für Defense steht; eine im US-Verteidigungsministerium angesiedelte Behörde für Forschungsprojekte im Bereich Militär- und Raumfahrttechnologie; Sie wurde 1957 gegründet um den USA den technologischen Vorsprung gegenüber der Sowjetunion zu sichern und arbeitete eng mit Universitäten und zivilen Forschungseinrichtungen zusammen
[185] vgl: Artikel *Wie das Internet entstand* In: Bundesamt für Sicherheit und Informationstechnik, URL: http://www.bsi-fuer-buerger.de/internet/01_02.htm, (Abgerufen : 20.08.2008)

innovative war dabei, dass Datenpakete sich durch ein Netzwerk ihren Weg zum Empfänger suchen und erst im Endgerät wieder zur ursprünglichen Nachricht vereint werden. Die ARPA war dabei im Departement of Defense angesiedelt, wo sie auch heute noch untergebracht ist. Das heutige Internet, wie wir es kennen, ist das Ergebnis jahrelanger kommerzieller Nutzung und Forschung durch zivile und militärische Stellen. Es ist, obwohl ursprünglich für das Militär entwickelt, zu einem der wichtigsten Medien und Kommunikationsmittel unserer Zeit aufgestiegen.

Es ging hier also nicht nur um Waffen und Waffensysteme, die auf beiden Seiten immer wieder weiterentwickelt wurden, sondern es ging auch um Kommunikations- und Informationstechnologie und andere technische Infrastruktur, deren Entwicklung ebenfalls in ständigem Wettrüsten vorangetrieben wurde. Der Einsatz solcher Technologien führte zum Teilgebiet der „elektronischen Kampfführung“ und fand seinen Höhepunkt in den 1980er Jahren, als unter dem Deckmantel der „elektronischen Gegenmaßnahmen“ bzw. der „elektronischen Gegen-Gegenmaßnahmen“ versucht wurde, das gesamte elektromagnetische Spektrum nutzbar zu machen und dem Gegner genau dies zu verwehren. Diese Strategie ist aber bereits ein Anzeichen erster doktrineller Überlegungen für den Informationskrieg, auch wenn sie eingebettet in die Doktrinen und Strategien der konventionellen Kriegsführung nur einen kleinen Teilbereich darstellten und eines der wesentlichsten Ziele der „information warfare“, der Kampf gegen die Führung, nicht primäres Ziel in den damaligen Konzepten und Doktrinen war.

„Diese Entwicklung war allerdings in der Situation der nuklearen Abschreckung politisch nicht besonders interessant und wurde daher vor allem technologisch getrieben. Darüber hinaus fielen solche Maßnahmen in den Bereich der "Operations Security" und waren bei den Militärgeheimdiensten und Aufklärungseinheiten angesiedelt. Deren institutionelle Sonderrolle - nicht den Kommandeuren der kämpfenden Truppen unterstellt zu sein - verhinderte ein Nachdenken darüber, ob und wie man die Kriegführung mit Hilfe moderner Elektronik grundlegender verändern kann.“[186]

Das Fehlen einer homogenen, gesamtgesellschaftlichen Sicht auf die möglichen Auswirkungen der Technologie auf die Kriegsführung hatte auch zur Folge, dass es keine auf ein Gesamtsystem gezielte Entwicklung und Forschung gab und viele Führungs- und Waffensysteme als Insellösungen der Teilstreitkräfte entwickelt wurden. Der heterogene Blickwinkel und die systembedingte Unflexibilität der Strategen, die ihren alten Denkmustern der Kriegsführung verhaftet waren, ließ das Potential der neuen Technologien im Kalten Krieg vielleicht erahnen, war aber nicht in konkreten Konzepte erkennbar.

---

und URL: http://www.internet4jurists.at/intern1a.htm, (Abgerufen: 20.08.2008)

[186] Vgl, Bendrath, Ralph, „Krieger in den Datennetzen“, URL: http://www.heise.de/tp/r4/artikel/7/7892/1.html, 2001, (Abgerufen: 6. Oktober 2008)

1.3.2. Organisation, Strategie, Dezentralisierung, Vernetzung

1.3.2.1. AirLand Battle Doktrin

Betrachten wir zunächst die Doktrin jener Zeit. Die Rivalität der Teilstreitkräfte und der durch den Vietnamkrieg verursachte technologische Rückstand[187] leitete einen Umdenkprozess im amerikanischen Militär ein, der bereits in den 1970er Jahren erste Ansätze zu einer neuen Doktrin hervorbrachte, die dann 1982 offiziell eingeführt wurde und die alte „Active Defense Doctrine" ablöste – die AirLand Battle Doktrin. Sie wurde zur grundlegenden Doktrin des US-Heeres[188] für jegliche Kampfhandlungen und ging von einem Krieg aus, der vorherige Konflikte in Geschwindigkeit und Zerstörung übertreffen sollte. Die AirLand Battle Doktrin prägte den Begriff des erweiterten Schlachtfelds, das heißt die Doktrin ging von der mehrdimensionalen Natur[189] der Kriegsführung aus und sollte sicherstellen, dass „*die Kampfkraft der eingesetzten Kräfte und Mittel auf taktischer und operativer Ebene optimal zur Geltung gebracht werden"*[190] Dabei sollte sie flexibel sein, günstige Möglichkeiten für die Operations- und Gefechtsführung schaffen oder ausnutzen, sich Schwächen des Gegners zunutze machen, sich auf die Gravitationszentren des Gegners konzentrieren und die gemeinsamen Handlungen der Teilstreitkräfte und Waffengattungen synchronisieren.
„*The concept called for early offensive action, by air and land, to the full depth of enemy formations to defeat an enemy attack."*[191] Offensive trat an die Stelle von Defensive, es sollte die gesamte Tiefe des Gefechtsfeldes ausgenutzt und der Gegner bereits weit hinter den vordersten Linien angegriffen werden. Die Grundsätze der Doktrin ergaben sich daher wie folgt:

- Erringung der Initiative durch Überraschung, Schnelligkeit, Offensivgeist und Konzentration der Kräfte und Mittel auf den entscheidenden Punkt (Center of Gravity)
- Erreichung einer solchen Beweglichkeit der Führung und des Handelns, die dem Gegner die Initiative nimmt und ihn daran hindern soll, rechtzeitig und koordiniert zu reagieren
- Erlangung der als Tiefe bezeichneten Fähigkeit, die Tiefe des Raumes, die verfügbare Zeit und die vorhandenen Ressourcen maximal auszuschöpfen
- Gewährleistung der Konzentration der Kräfte und Mittel auf den entscheidenden Punkt durch genaue Abstimmung (Synchronisation) aller Handlungen nach Ziel, Zeit und Ort[192]

---

[187] Knapp zehn Jahre Krieg schränkten neue Entwicklungen ein, was der Sowjetunion einen Vorteil verschaffte
[188] vgl Field Manual 100-5 Operations, Headquarter Department of the Army, Washington, DC, 1982, S 7ff
[189] Die Theorie besagt, dass das Schlachtfeld aus mehreren Dimensionen besteht, zB der zeitlichen Dimension, der physischen Dimension, der Dimension des Luftraumes oder aber auch der Dimension von chemischen, biologischen oder nuklearen Waffen
[190] vgl. Wolf, Wolfgang, Der Golfkrieg, Bernard & Graefe Verlag, Bonn, 1992, S.40
[191] vgl Artikel *The Evolution of the AirLand Battle Concept*, In: Air University Review 1984, URL: http://www.airpower.maxwell.af.mil/airchronicles/aureview/1984/may-jun/romjue.html (Abgerufen: 6.Oktober 2008)
[192] Wolf, Wolfgang, Der Golfkrieg, Bernard & Graefe Verlag, Bonn, 1992, S.41

Wir erkennen die zentralen Begriffe der Initiative, der Schwergewichtsbildung[193] (Center of Gravity), des Faktors Bewegung, des Faktors Tiefe und vor allem die Abstimmung und Synchronisation aller Kräfte. Dahinter steht aber ein Zusammenwirken der Teilstreitkräfte auf allen Ebenen, also konkret das Überwinden der alten Trennung zwischen Luftwaffe und Bodentruppen. Um dies überhaupt erst zu ermöglichen, wurden *„integrierte Gefechtsstände, Sensoren und Trägersysteme benötigt, die in der Lage waren, Gefechtsdaten in Echtzeit zu berechnen, zu übertragen und auszuwerten. Diese Aufgabe sollten C3I-Systeme übernehmen.“*[194]

Dazu kamen natürlich Faktoren wie die Aufklärung (Intelligence) auch mit elektronischen Mitteln sowie die Elektronische Kampfführung, die ebenfalls in der Doktrin festgeschrieben, aber nur bedingt in Beziehung zueinander gebracht wurden. So wurden Maßnahmen zur Elektronischen Aufklärung dem Bereich der militärischen Sicherheit zugeschrieben[195], während die Gesamtverantwortung für die Elektronische Kampfführung im Stabsbereich Führung/Einsatzführung[196] angesiedelt und das Element Kommunikation sowie Elektronische Gegenmaßnahmen wieder einem eigenen Stabsbereich zugeordnet waren.[197] Diese Trennung wirkte sich auch auf das Bewusstsein der Kommandanten aus, die ihre Prioritäten auf Feuer, Wirkung, Bewegung und andere Elemente legten und den Bereich der Kommunikation und Elektronischen Kampfführung eher als Randbereich im Spektrum der militärischen Kriegsführung wahrnahmen. Nicht umsonst wird im Field Manual 100-5 explizit auf die Bedeutung der Kommandanten für eine erfolgreiche Integration und somit einen erfolgreichen Einsatz der Elektronischen Kampfführung hingewiesen:

„The commander is the key to successfully integrating electronic warfare into the operational scheme. He must understand its potential impact on the battlefield and provide the continuous guidance necessary to its proper use.”[198]

Es zeichneten sich also bereits gegen Ende des Kalten Krieges die Grundzüge des Informationskrieges in seiner heutigen Form ab, allerdings fehlte nach wie vor die Gesamtsicht auf die Thematik, der Informationskrieg als solches war im Denken des Militärs noch nicht existent, er war weder Theorie noch Idee, allein die Indikatoren der Elektronischen Kriegsführung und der Kampf der Verbundenen Kräfte weisen auf seine frühe Existenz hin. Aber, wie in Kapitel 3 bereits festgestellt, ist der Informationskrieg ja mehr als der bloße Einsatz elektronischer Kampfmaßnahmen am Gefechtsfeld, er ist ein umfassendes Gesamtkonzept, das wir hier keinesfalls finden können. Daher ist die Doktrin als Schlüsselkonzept zwar sehr wohl für die Initialzündung und Schaffung einer ersten grundlegenden Infrastruktur für den Informationskrieg verantwortlich, allerdings war dieser zu jener Zeit kein bewusstes Ziel, sondern vielmehr ein zukunftsträchtiger

[193] „Center of Gravity“ ist mit dem Begriff „Schwergewicht“ vielleicht zu schwach übersetzt und an dieser Stelle keinesfalls mit dem Führungsgrundsatz der taktischen Schwergewichtsbildung zu verwechseln. Vielmehr geht es hierbei um eine Massierung der Kräfte am schwächsten Punkt des Gegners auf einer operativen Ebene

[194] vlg. Bendrath, Ralph, Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Peter Bittner, Jens Woinowski (Hg.): Mensch - Informatisierung - Gesellschaft, Münster: Lit Verlag, 1999, S. 141ff

[195] wahrgenommen durch die Stabsfunktion des S2 bzw. G2

[196] wahrgenommen durch die Stabsfunktion des S3 bzw. G3

[197] wahrgenommen durch den Communication-Electronics Officer (vergleichbar mit dem Fernmeldeoffizier); vgl. Field Manual 100-5 Operations, Headquarter Department of the Army, Washington, DC, 1982, 7-18f

[198] Field Manual 100-5 Operations, Headquarter Department of the Army, Washington, DC, 1982, 7-18

Nebeneffekt. Die Fragen, die sich aus dieser Doktrin an die Zukunft der Kriegsführung ergaben, sollten erst später durch den Golfkrieg 1990/1991 aufgeworfen werden. Wir können diese Doktrin daher nicht als Informationskriegsdoktrin im Sinne der Untersuchung auffassen und müssen folgerichtig auch den Einfluss des Informationskrieges auf die Doktrinen der Streitkräfte in dieser Phase negieren. Allerdings ist durchaus erkennbar, dass die Wurzeln des Informationskrieges in dieser Doktrin liegen, denn die Einsatzgrundsätze von damals sind nach wie vor zentrale Punkte der modernen Kriegsführung von heute und der operative Bewegungskrieg wurde durch diese Doktrin eigentlich neu definiert.

1.3.2.2. Streitkräfteorganisation

Sehen wir uns nun die Organisation der Streitkräfte an, die im Anschluss an die Einführung der AirLand Battle Doktrin eine massive Neustrukturierung und Reform durch den Goldwater-Nichols Act erlebt hat.[199] Dazu ist zunächst zu erwähnen, dass die Teilstreitkräfte bis 1947 zum Teil im Kabinettsrang waren und erst mit dem Security Act dem damals gegründeten Verteidigungsministerium untergeordnet wurden. Daraus resultierte eine Rivalität, die sich nicht nur um Budget und Ausrüstung, sondern auch um politischen Einfluss drehte und die Fähigkeit zu Verbundoperationen massiv einschränkte. Die Parallelität von Kommandostrukturen, Redundanzen und das ständige Wetteifern zwischen den Teilstreitkräften hatten zur Folge, dass sich die Teilstreitkräfte mehr oder weniger unabhängig und in Konkurrenz zueinander sahen. Dies ging sogar soweit, dass sie jeweils eigene Forschungsabteilungen unterhielten, die neue Waffen- und Führungssysteme entwickelten. Erst mit der Streitkräftereform durch den Goldwater-Nichols Act von 1986 sollte diesem Problem massiv begegnet werden, um die Strukturprobleme zumindest einzudämmen und den Kampf im Verbund und somit die volle Umsetzung der AirLand Battle Doktrin überhaupt erst zu ermöglichen.

(a) Joint Chiefs of Staff

Wir stellen zuallererst auffallend fest, dass die Bemühungen durch Synergieeffekte Vorteile im Gefecht zu erzielen, durchaus schon sehr lange gegeben waren. Wie bereits erwähnt ist ja auch der Kampf der Verbundenen Waffen nicht wirklich neu und das amerikanische Militär hat dem bereits kurz nach dem Zweiten Weltkrieg mit der Schaffung seines *Joint Chiefs of Staff* (JCS) Kommandos Rechnung getragen. Dieses höchste, übergeordnete Kommando der US Streitkräfte sollte teilstreitkräfteübergreifend agieren, eine bessere Koordinierung der Streitkräfte ermöglichen und vereinigte damals wie heute die Oberbefehlshaber (Chiefs of Staff) der Teilstreitkräfte in sich. Bis 1986 war das JCS auch für die operative Führung der Streitkräfte verantwortlich, eine Kompetenz die es im Zuge der Reform abgeben musste. Das JCS war nun in erster Linie für die Ausbildung und Einsatzbereitschaft der Teilstreitkräfte verantwortlich.

[199] Ziel der Reform war die so genannte Army 86, die die Armee auf High-Intensity Conflicts (HIC) in Europa, Korea und Südost-Asien vorbereiten sollte.

Im JCS Command ist neben den Oberbefehlshabern der Teilstreitkräfte auch ein ganzer Stab, der *Joint Staff,* angesiedelt, der den Vorsitzenden bei seiner Arbeit unterstützt. Interessant ist, dass bereits zu Zeiten der AirLand Battle Doktrin die Funktion des J6 auch mit C3I[200]-Aufgaben betraut war.

(b) US Army Information Systems Command

Auf Ebene der Allgemeinen Kommanden der Army finden wir das US Army Information Systems Command (USAISC), das 1985 aus dem US Army Communication Command hervorging und dessen Aufgabe es war, alle Fragen in Hinsicht Informationsmanagement unter einem Kommando zu vereinen. Ihm unterstellt waren das 5th & 7th Signal Command, die 1st Signal Brigade in Seoul und die 11th Signal Brigade in Arizona. Weiters finden wir das US Army Information Systems Engineering Command, das für den Einsatz von Computern und Informationstechnologie im Felde verantwortlich war.[201]

(c) Truppenstärken

Die Truppenstärken ergaben sich nun im Großen wie folgt:[202]

Landstreitkräfte:	**Luftstreitkräfte:**	**Seestreitkräfte**:
Stärke: 770.904 Mann	Stärke: 605.805 Mann	Stärke: 571.053 Mann US Navy + 196.300 Mann US Marine Corps
18 Divisionen, davon – 4 Panzerdivisionen – 6 Mechanisierte Infanteriedivisionen – 6 Infanteriedivisionen – 1 Luftlandedivision – 1 Luftbewegliche Division	24 Strategische Raketenstaffeln 242 Fliegerstaffeln – 22 Strategische Bomberstaffeln – 82 Jagdbomberstaffeln – 4 Jagdstaffeln – 4 Strategische Aufklärungsstaffeln – 8 Taktische Aufklärungsstaffeln – 1 Fernaufklärungsstaffel – 31 Transportstaffeln (17 Strategisch/14 Taktisch) – 41 Sonderstaffeln (Kommunikation, AWACS, Search&Rescue…) – 50 Tankerstaffeln	Wir wollen die Navy an dieser Stelle nicht genauer betrachten, da sie erstens im Sinne der AirLand Battle Doktrin nur unterstützenden Charakter durch ihre taktischen Kräfte (Marineinfanterie, Navy Flieger, Schiffsartillerie etc) hatte und zweitens eine genaue Behandlung der Gliederung der Seestreitkräfte für diese Arbeit keine Relevanz hätte.
Gesamtstärke: Knapp 2,4 Mio Angehörige der Streitkräfte Zusätzlich dazu verfügen die Streitkräfte über Reserven der Nationalgarde und der Army, Air Force, Navy und Marine Reserve, die wir hier ebenfalls nicht näher behandeln wollen.		

Tabelle 2: Truppenstärken der US Streitkräfte 1987

[200] Wir verwenden in diesem Kapitel aus historischen Gründen und aus Gründen der Lesbarkeit den Begriff C3I synonym zum heute gängigen C4ISR

[201] Vgl: Artikel *History of ISEC,* In: US Army Information Systems Engineering Command, URL: http://www.hqisec.army.mil/isec/about/history.asp, (Abgerufen: 20.08.2008)

[202] Wiener, Friedrich, Dr., Truppendienst Handbook Nr.3, The Armies of the NATO Nations, First English Edition, Herold Publishers Vienna, 1987, S. 44ff

Die Landstreitkräfte nahmen ihre Struktur gemäß der Reform 86 ein und waren in Corps, Divisionen und Bataillone gegliedert: [203]

Corps 86	*Division 86*
– HQ & HQ Company – Armored Cavalry Regiment – Corps Combat Aviation Brigade – Corps Artillery – **Corps Signal Brigade** – Military Police (MP) Group – **Combat Electronic Warfare Intelligence (CEWI) Group** – Corps Engineers Brigade – NBC Defense Brigade – Air Defense Brigade – Rear Air Combat Operations Brigade – Corps Support Command	– HQ & HQ Company – Panzerdivision: ▪ 6 gepanzerte Bataillone & 4 mechanisierte Bataillone – Infanteriedivision: ▪ 5 gep. & 5 mech. Bataillone – Combat Aviation Brigade – Division Artillery – Gep. Pionierbataillon – Gep. Fliegerabwehrbataillon – **Signal Battalion** – **CEWI Battalion** – NBC Defence Company – MP Company – Division Support Command
Ca. 85.000 Mann	Ca. 16000-20000 Mann

Tabelle 3: Gliederung Corps/Division 86

Vergleicht man nun diese Struktur mit der vor der Reform 1986[204] so fallen vor allem die Combat Electronic Warfare Intelligence Elemente auf, die sowohl auf Corps- als auch auf Divisionsebene dazugekommen sind. Weiters treffen wir auf Fernmeldeverbände, deren Aufgabe die Herstellung von Kommunikationswegen für ihre Verbände ist.

(d) Bewertung

Abschließend betrachtet lassen sich in den Strukturen durchaus Hinweise auf den Informationskrieg erkennen. Die Einführung von Kommanden höchster Ebenen für die Schaffung von Informationssystemen oder die Etablierung von Electronic Warfare Verbänden auf oberster operativer Ebene zeugen von einer klaren Zunahme der Bedeutung des Faktors Information und Informationsmanagement. Es stand nicht mehr das bloße Herstellen von Kommunikationswegen durch klassische Fernmeldeverbände im Vordergrund, sondern auch aktive Aufklärung und in weiterer Folge aggressive Störung des elektronischen Spektrums. Daraus ergab sich auch ein erhöhter Bedarf an Kommunikationswegen, was durchaus als Indikator für einen höheren Vernetzungsgrad gewertet werden kann. Des Weiteren wurde ja das JCS zugunsten der regionalen Kommanden seiner operativen Führung beraubt, was wir als Tendenz zur Dezentralisierung sehen können. Wir erkennen also Elemente zur Vernetzung und zur Dezentralisierung und die zunehmende Bedeutung des Informationsbegriffes.

[203] Wiener, Friedrich, Dr., Truppendienst Handbook Nr.3, The Armies of the NATO Nations, First English Edition, Herold Publishers Vienna, 1987, S. 66ff
[204] Wiener, Friedrich, Dr., Truppendienst Taschenbuch Nr.3, Fremde Heere: Die Armeen der NATO Staaten, 4.Auflage, Verlag Carl Ueberreuter, 1973, S37ff

Allerdings finden sich diese Elemente nur auf höchster Ebene, haben also auf die taktische Einsatzführung nur wenige Auswirkungen. Die Drehscheiben der operativen Führung zu dieser Zeit waren die Corps und Divisionen, die aber den Einsatz von Elektronischer Kriegsführung auf ihrer Ebene beurteilten und den unterstellten Verbänden nur wenige Einflussmöglichkeiten ließen. Die Synchronisation der Kräfte geschah daher genau in diesen Kommanden, was aber statt einer Dezentralisierung wiederum eine Zentralisierung zur Folge hatte, also genau den gegenteiligen Effekt. Außerdem wurden diese Strukturen nicht unter der Prämisse des Informationskriegs an sich, sondern für die Umsetzung der AirLand Battle Doktrin und die dort verlangte erhöhte Interoperabilität eingenommen.

Allein aus der Betrachtung der Strukturen der Streitkräfte jener Zeit lässt sich die Frage nach dem Einfluss des Informationskrieges daher nicht eindeutig beantworten.

1.3.3. Komplexitätsmanagement

Wie wir bereits bei der Behandlung der Doktrin festgestellt haben, sollten C3I-Systeme den erhöhten Anforderungen des Informations- und Battlemanagement gerecht werden. Schnelligkeit, Vielseitigkeit und Initiative im Gefecht konnten im Bereich der Führung durch zumindest zwei Faktoren erreicht werden.

Der erste Faktor waren Führungsinformationssysteme, die Information schnell und richtig zum Empfänger bringen sollten. Eines dieser Systeme und das erste teilstreitkräfteübergreifende war das *Joint Surveillance Target Attack Radar System (JSTARS).* Dieses System ist insofern interessant, da es als fliegender Gefechtsstand an Bord einer Boeing 707 auf Aufklärungsergebnissen basierende Befehle und Aufträge an verschiedene Truppenteile am Boden, in der Luft oder zur See schnell weiterleiten konnte und somit einen der ersten Versuche der echten Vernetzung und Dezentralisierung der Streitkräfte darstellte.

Zweiter Faktor ist das Führungssystem selbst, das aufgrund der geforderten Schnelligkeit und Vielseitigkeit von seinen Kommandanten Flexibilität einforderte. Die Kommandanten konnten nicht mehr starr von einem übergeordneten Kommando geführt werden und bei jeder nicht vorhersehbaren Änderung der Lage neue Befehle einfordern, sondern hatten selbstständig im Sinne des Auftrages zu handeln, was uns auch hier die Tendenz zur Dezentralisierung erkennen lässt.

Von Seiten des Komplexitätsmanagement ist daher festzustellen, dass durch Doktrin und Technologie die Faktoren Dezentralisierung und Vernetzung auch auf die Führung und in weiterer Folge auf das Komplexitätsmanagement projiziert wurden. Hier können wir eindeutig feststellen, dass sich der Informationskrieg zu manifestieren begann und langsam seinen Weg in das Bewusstsein der Militärs fand.

1.3.4. Einsatzbeispiel 2.Golfkrieg 1990-1991

Wir wollen uns nun kurz dem Ende dieser Phase und an dieser Stelle einem Konflikt widmen, in dem die neue Doktrin, Technologie und das flexible Führungssystem sich beweisen mussten – dem Golfkrieg 1990/1991.

„Der Golfkrieg 1991 war die erste praktische Anwendung der ALB-Doktrin, deren Grundannahmen durch den überlegenen Sieg der USA für die Militärs als bestätigt galten.“[205] In nur 46 Tagen war das Kriegsziel erreicht, der Sieg für die Koalitionskräfte unter Führung der USA gelungen und Kuwait von der irakischen Okkupation befreit. 38 Tage oder 80% der Kampfhandlungen wurden ausschließlich durch die Luftstreitkräfte geführt[206] , die die Bodenoffensive soweit vorbereiten konnten, dass diese nach nur 5 Tagen erfolgreich abgeschlossen werden konnte und die Verlustzahlen weit unter den vor dem Krieg hochgerechneten 15000 lagen. Der Konflikt selbst galt als größte Kampfhandlung seit dem Zweiten Weltkrieg, in Summe standen sich 1,9 Millionen Soldaten gegenüber, davon allein bis zu 540000 Angehörige der amerikanischen Streitkräfte.

Vom technischen Standpunkt her sollen vier Faktoren für den Erfolg der Alliierten verantwortlich gewesen sein:

- zielsuchende Präzisionswaffen, die gegen Punktziele im irakischen Führungsnetz eingesetzt wurden
- der nahezu 100%ige Erfolg bei der Zerstörung von Radaranlagen, Führungsanlagen der irakischen Flugabwehr
- die Wirkung moderner Munition (zielsuchend etc) auf ihre Ziele und die dadurch bedingte Feuerüberlegenheit
- Ortungs- und Informationssysteme der US-Streitkräfte, die eine bewegliche und präzise Operationsführung erlaubten[207]

Um diese Faktoren überhaupt zur Geltung bringen zu können, musste die entsprechende Infrastruktur geschaffen werden, die sich nach folgenden Gesichtspunkten beurteilen lässt:

- Das Informationsaufkommen und der Informationsaustausch waren noch nie zuvor so hoch
- Nie zuvor spielte der Computereinsatz eine größere Rolle; die C3I-Teilnehmer reichten von den höchsten Kommanden bis zu den Feuerleitsystemen der Waffenplattformen sowie weit in den logistischen Bereich im Hintergrund
- Innerhalb der Vorbereitungsphase wurden in Saudi-Arabien mehr Kommunikationswege geschaffen als in Europa in den 40 Jahren zuvor
- C3I-Systeme deckten eine Fläche von mehr als 151000 km2 ab
- Das Haupt C3I-System für die Landkriegsführung war das ATCCS (Army Tactical Command Control System), für die Auswertung von Aufklärungsergebnissen das MIPS (Military Intelligence Processing

[205] vlg. Bendrath, Ralph, Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Peter Bittner, Jens Woinowski (Hrsg.): Mensch - Informatisierung - Gesellschaft, Münster: Lit Verlag, 1999, S. 141ff
[206] vgl. Wolf, Wolfgang, Der Golfkrieg, Bernard & Graefe Verlag, Bonn, 1992, S.103
[207] vgl. Commenda, Othmar, GenMjrdG, „Erste Erfahrungen, Erkenntnisse und Lehren“ in Truppendienst 1/1992, „Golfkrieg 90/91“, Herold Druck und Verlagsges. mbH, Wien, 1992, S.107f

System) und diverse Systeme für Problemlösungshilfen, Missions- und Operationsplanungen[208]

Von doktrineller Seite her kam die AirLand Battle Doktrin zum Einsatz, die wir bereits oben beschrieben haben.

Für das Komplexitätsmanagement, unterstützt durch die beschriebenen und weiteren C3I- und Waffensystemen, war Beweglichkeit und Initiative von größter Wichtigkeit. Gerade im Golfkrieg haben sich die Dezentralisierung und Delegierung von Handlungskompetenz auf die tiefstmögliche Ebene einer zentralisierten Führung überlegen gezeigt. Das Beispiel der irakischen Streitkräfte, die noch einer starren Befehlstaktik und vordefinierten Kampfplänen folgten, zeigt, dass diese nicht mehr in der Lage waren, sich dem hohen Tempo der Gefechtshandlungen anzupassen, insbesondere auch, weil durch Zerstörung und Täuschung der irakischen Gefechtsaufklärung kein umfassendes Lagebild mehr vermittelt werden konnte. Das amerikanische Führungssystem, das den Kommandanten gemäß Doktrin erstmals vermehrte Eigeninitiative zugestand, erwies sich als klar überlegen.[209]

Dieser Einsatz von hoch entwickelter Technologie, die neue Doktrin und ein in dieser Form nicht gekanntes Komplexitätsmanagement veranschaulichten also eindrucksvoll das Potential der neuen Kriegsführung und drängen uns nun die Frage auf, ob dieser Konflikt nicht schon ein Informationskrieg gewesen sein könnte. Aus oben genanntem lassen sich auch tatsächlich Elemente des Informationskrieges ableiten.

- Vernetzung der Truppen
- Dezentralisierung
- Teilstreitkräfteübergreifende Kampfführung
- Einsatz von C3I und Hochtechnologie
- Kampf gegen die feindliche Führung
- Flexible Führung im Sinne des Auftrags
- Elektronische Mittel zur Aufklärung und Kampfführung

Allerdings muss man hier die Bedeutung dieser Elemente im Sinne des Gesamtkonzepts des Informationskrieges betrachten und hier stellt sich die Situation nicht eindeutig dar. Die Frage, welche Auswirkungen es gehabt hätte, hätte der Irak ähnliche Mittel und Kräfte zur Verfügung gehabt, lässt den großen Erfolg der AirLand Battle Doktrin hinterfragenswert erscheinen. Ob der Kampf gegen die feindliche Führung sowie die Flexibilisierung der taktischen Ebene in dieser Form stattgefunden hätte oder ob nicht im Falle einer stärkeren Gegenwehr und eines damit höheren Synchronisationsbedarfs die obere Führung stärker eingegriffen hätte, bleibt dahingestellt. Die Dezentralisierung selbst war ja kein doktrinelles Ziel, Begriffe wie „Selbstsynchronisation“ unbekannt und selbst der Einsatz der Elektronischen Kampfführung konnte in seiner Bedeutung erst während des Konfliktes abgeschätzt werden.

Fakt ist auch, dass dieser Krieg in den Augen vieler Analysten kein Krieg neuer Qualität war. So schreibt zum Beispiel Wolfgang Wolf in seiner Analyse:

---

[208] vgl. Fritz, Friedrich, „C3I – Alte Tatsachen, neue Dimensionen“ in Österreichische Militärische Zeitschrift, Heft 2/1993, Offsetdruck Carl Ueberreuterges. mbH., Wien, 1993, S.140

[209] vgl. Commenda, Othmar, GenMjrdG, „Erste Erfahrungen, Erkenntnisse und Lehren“ in Truppendienst 1/1992, „Golfkrieg 90/91“, Herold Druck und Verlagsges. mbH, Wien, 1992, S.98

„Vom Charakter her wies der Golfkrieg insgesamt keine neue Qualität, aber eine ganze Reihe qualitativ neuer bzw. bisher weitaus weniger ausgeprägter Züge auf, wie den Einsatz neuer Waffentechnologien und die erstmals in diesem Umfang erreichte Zerstörung der militärischen und zivilen Infrastruktur militärischer Bedeutung."[210]

Einen weiteren Aspekt bringt Thomas Simeoni ein, der dem Golfkrieg unter anderem den Charakter des Informationskrieges deshalb abspricht, weil er noch starke Elemente der konventionellen Kriegsführung und Massenvernichtung im Sinne von Flächenbomardements etc. aufwies, was gegen den Charakter des Informationskrieges spricht.[211] (Tatsächlich stehen 76800 Tonnen herkömmlicher Bomben nur 7400 Tonnen Präzisionsbomben gegenüber.[212])

Ich glaube, dass es sich mit der Beurteilung des Golfkrieges ähnlich verhält, wie mit der Beurteilung der Doktrin dieser Zeit. Wir können durchaus Elemente des Informationskrieges erkennen, es sprechen aber auch viele Argumente gegen diese Klassifizierung. Daher ist der Golfkrieg im Sinne dieser Arbeit als konventioneller, aber durchaus zukunftsweisender Konflikt zu sehen, der erst in seinen Analysen die Frage aufgeworfen hat, was durch den Einsatz von integrierten C3I-Systemen noch möglich sei und wie Datenerfassung und –analyse für die Entscheidungsfindung genutzt werden können. Durch den Golfkrieg hatte der Informationskrieg also erst den Kern militärischer Organisationsformen erreicht[213], folgerichtig kann der Golfkrieg noch kein Informationskrieg gewesen sein.

1.3.5. Zwischenfazit

Zu Beginn der 1980er Jahre standen die amerikanischen Streitkräfte vor zahlreichen Problemen, die sie mit Reformen zu beheben versuchten. Neben den Rivalitäten der Teilstreitkräfte zählte dazu auch veraltete Ausrüstung und eine Doktrin, die ebenfalls nicht mehr zeitgemäß zu sein schien. Mit der Einführung der AirLand Battle Doktrin gelang aber mehr als nur die Überwindung dieser Probleme, mit ihr gelang, wenn auch unbewusst, die Begründung einer neuen Art der Kriegführung – des Informationskrieges.

Zusammenfassend lässt sich festhalten, dass die Frage nach dem Einfluss des Informationskrieges auf die Doktrinen dieser Phase schwierig zu beantworten ist. Zahlreichen Indikatoren für den Informationskrieg stehen viele Gegenargumente gegenüber, einzig im Bereich des Komplexitätsmanagement lassen sich eindeutige Merkmale des Informationskrieges finden. Auch das Konfliktbeispiel Golfkrieg hat die Frage, ob es sich bei diesem Krieg schon um einen Informationskrieg handelte, offen gelassen.

Wenn wir die Frage nach dem Informationskrieg aber nicht beantworten können, so wollen wir den Einfluss auf die Kriegsführung doch zunächst einmal verneinen. Was

[210] vgl. Wolf, Wolfgang, Der Golfkrieg, Bernard & Graefe Verlag, Bonn, 1992, S.20
[211] Simeoni, Thomas; War der Golfkrieg der erste Informationskrieg?, Diplomarbeit; Wien, 1997; S142; wobei Simeoni die Frage ob der Golfkrieg ein Informationskrieg ist, nicht eindeutig beantwortet
[212] Wolf, Wolfgang, Der Golfkrieg, Bernard & Graefe Verlag, Bonn, 1992, S.130
[213] vlg. Bendrath, Ralph, Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Peter Bittner, Jens Woinowski (Hrsg.): Mensch - Informatisierung - Gesellschaft, Münster: Lit Verlag, 1999, S. 141ff

bleibt uns also über? Wir finden den Einsatz von Technologie, von ersten Führungs- und C3I-Systemen auf technologischer Seite, weiters die Existenz von Verbundkommanden wie dem JCS, eine neue, schlankere Streitkräfteorganisation und eine Doktrin, die allein deshalb schon eine neue Art der Kriegsführung begründet, weil sie das Schlachtfeld in die Tiefe ausdehnt. Wir haben weiters ein flexibles Führungssystem, das Kommandanten im Gefecht eigenständig auf Änderungen der Lage reagieren lässt, und wir finden erste vernetzte Führungsabläufe durch das JSTARS-System. (Nebenbei bemerkt wird dem aufmerksamen Leser an dieser Stelle nicht entgangen sein, dass wir hier wieder auf die bereits angesprochene trianguläre Struktur Führung-Technologie-Doktrin treffen). Wir erkennen also durchaus schon das Potential, das in jedem dieser Faktoren steckt, was allerdings fehlt ist der Zusammenhang und die Homogenität. Der Konflikt am Golf als Katalysator hat genau diesen Zusammenhang bewusst gemacht und ein neues Denken im Militär begründet. Er hat erst die Fragen aufgeworfen, die nötig waren, um die Entwicklung des Informationskriegs zu ermöglichen.
Die Frage nach dem Einfluss des Informationskrieges auf die Doktrinen jener Zeit mag daher vielleicht nicht eindeutig beantwortbar sein, was wir aber dargelegt haben, sind die Ursprünge des Informationskrieges, die genau in diesen Entwicklungen in der letzten Phase des Kalten Krieges liegen.

1.4. Phase II – Neue Weltordnung

1.4.1. Einsatz von Technologie

Der Golfkrieg förderte das große Potential des Informationskrieges, aber auch viele Probleme und Hindernisse zu Tage. Als eine der wichtigsten Ableitungen aus den Erfahrungen können wir aber die starke Bedeutung der Information erkennen, sei es in Form von einem erhöhten Bedarf an Aufklärungsergebnissen, als Informationsfluss oder fokussiert auf den Begriff der Informationsüberlegenheit. Nicht nur institutionelle Hindernisse, wie die Konkurrenz zwischen den Teilstreitkräften oder jene zwischen den Geheimdiensten und den taktischen Einsatzkräften waren dabei störend, auch die hohe Anzahl an verschiedenen technischen Informationssystemen und der daraus resultierende höhere Koordinationsbedarf wurden als Problemfaktoren identifiziert.

„Die technologische Entwicklung hat hier zu neuen Überlegungen geführt, die Fragmentierung des Aufklärungsapparates zu überwinden und einen besseren Informationsfluss anzustreben. Ein entscheidendes Ereignis dafür war ebenfalls der Golfkrieg 1991, in dem die technischen und sozialen Koordinationsprobleme zwischen Militär und Aufklärungseinheiten deutlich zutage traten. (…)
Diese Entwicklungen zeigen, dass die bisher klaren Grenzen zwischen Politik und Militär oder zwischen Militär, Geheimdiensten und privaten Informationsdienstleistern in der Auflösung begriffen sind. Die USA werden weiterhin darauf setzen, ihre militärische Vormachtstellung auf Feuerkraft zu stützen. Gleichzeitig wird aber die Verfügung über Informationen immer mehr als neue Quelle der Macht begriffen.“[214]

Neben den Entwicklungen am Sektor der Führungsinformationssysteme, die wir später behandeln wollen, stellte sich auch die Frage, wie man schnell und effizient

[214] vlg. Bendrath, Ralph, Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Peter Bittner, Jens Woinowski (Hrsg.): Mensch - Informatisierung - Gesellschaft, Münster: Lit Verlag, 1999, S. 149f

Information gewinnen konnte. Dies sollten neue technische Systeme, wie wir sie im Kapitel 4 kennen gelernt haben, gewährleisten. Hierzu wurde eine eigene Truppe unter anderem mit der Entwicklung von neuer Technologie und deren Evaluierung beauftragt, die Experimental Force (EXFOR) oder später FORCE XXI.[215] Eines der größten und bekanntesten Projekte, das sich hervorragend als Referenzbeispiel eignet, ist das Land Warrior Projekt. Die Bedeutung der Information wurde so hoch eingeschätzt, dass sogar der Soldat selbst zur Sensorplattform werden sollte und umgekehrt eine Kampfwertsteigerung durch neue Fähigkeiten wie das Bekämpfen von Zielen, die außerhalb des Sichtfelds liegen oder durch Umwelteinflüsse verborgen werden, erfuhr. Das Land Warrior Projekt zeigt klar die Prioritäten in der Entwicklung technischer Systeme, nämlich Sensorik und Informationsbeschaffung einerseits und Feuerkraft sowie Kampfwertsteigerung andererseits.

Wir erkennen in dieser Phase einen viel höheren Stellenwert der Information, als sie ihn noch zu Zeiten des Kalten Krieges hatte. Technologische Entwicklungen wurden gezielt auf den Einsatz zur Informationsbeschaffung, Aufklärung oder Kommunikation ausgerichtet. Von technologischer Seite her erkennen wir mit dem Land Warrior Konzept sogar eine Tendenz zu einer Vernetzung der einzelnen Soldaten, also der untersten Ebene. Die gesamte Entwicklung ging also weit über das hinaus, was wir in Phase I noch unter Elektronischer Kampfführung zusammengefasst hatten. Anders als damals wurden jetzt sehr wohl Überlegungen darüber angestellt, wie man durch Technologie und deren Einsatz das Wesen des Krieges ändern könnte und in welchem Ausmaß das möglich wäre. Parallel dazu entwickelte sich, wie wir im nächsten Punkt sehen werden, zumindest im Subsystem Militär eine gesamtgesellschaftliche Sicht auf den Informationskrieg.

Allerdings wurden die Entwicklung neuer Technologien und die Einführung neuer Systeme im Militär von politischer Seite stark gebremst. Die Hochrüstung der vergangenen Jahrzehnte und der Wegfall der ständigen Bedrohung durch den Kalten Krieg hatten in erster Linie Reduktionsgedanken zu Folge und Präsident Clinton beschränkte in seiner Amtszeit das Verteidigungsbudget einschneidend.

„*Die Entwicklung der US-Streitkräfte unter der Clinton-Administration folgte einem ambivalenten Muster: Einerseits wurde der mit der Joint Vision eingeschlagene Technologie-Pfad in konzeptioneller Hinsicht weiterverfolgt. Andererseits bestand seitens der politischen Führung nur eine zögerliche Bereitschaft, die kostenintensive Transformation der US-Streitkräfte auch zu finanzieren.*“[216]

Das Wehrbudget der USA blieb in dieser Phase nahezu konstant und stieg nur langsam an. Dies wirkte sich natürlich auf Möglichkeiten der Streitkräfte aus, die ja nicht nur neue Entwicklungen und Beschaffungsvorgänge zu finanzieren hatten, sondern auch laufende Kosten wie Gehälter, Wohnungen, Treibstoff, Munition, Wartung etc. abzudecken hatten. Daraus ergab sich für die beiden im Sinne der Modernisierung zentralen Haushaltsposten Forschung und Entwicklung sowie Beschaffung folgende Rahmenbedingungen:

[215] vlg. Bendrath, Ralph, Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Peter Bittner, Jens Woinowski (Hrsg.): Mensch - Informatisierung - Gesellschaft, Münster: Lit Verlag, 1999, S. 144f

[216] vgl. Jim Sourter/Loren Thompson, Army Vision and the Transformation of Land Power in the Next Century, in: Strategic Review, Vol.25(1997) 3, S.31-39 zit. nach (Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006“, Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.113)

- Im Bereich Forschung und Entwicklung blieben die Ausgaben relativ konstant, das bedeutet, dass in diesem Bereich die kontinuierliche Weiterentwicklung von Systemen betrieben werden konnte
- Der Bereich der Beschaffung sieht allerdings anders aus: hier sanken die Ausgaben von 34% des Budgets unter Reagan in Phase I auf unter 20% Mitte der 1990er Jahre.

Verschärfend kam hinzu, dass der Großteil der Ausgaben in sekundäre Güter wie Lastkraftwagen, Ersatzteile und Munition investiert wurde. Das Verteidigungsbudget wurde also mit Masse zum Erhalt bestehender Systeme eingesetzt und nicht in neue Technologien investiert. So betrugen 1997 die Ausgaben für neue Kampfwert steigernde Systeme nur 12Mrd US-Dollar im Vergleich zu 250Mrd US-Dollar Gesamtbudget.[217]

Abschließend können wir also feststellen, dass der Informationskrieg mit Fortdauer dieser Phase immer präsenter wurde und dass die technologischen Entwicklungen dieser Zeit auch durchaus in ihm begründet waren. Der politische Wille in dieser Phase bremste allerdings die Entwicklungen stark, so dass auch der Transformationsprozess aufgehalten wurde. Dies sollte sich erst unter der Amtszeit von George Bush Jr. ändern.

1.4.2. Organisation, Strategie, Dezentralisierung, Vernetzung

Von organisatorischer Seite betrachten wir zunächst wieder die Doktrinen dieser Phase. Basis und Ausgangspunkt und auch nach wie vor gültig war immer noch die AirLand Battle Doktrin, an die, vor allem nach den positiven Erfahrungen aus dem Golfkrieg 1990/91 jede neue Entwicklung anknüpfte. Der Krieg am Golf 1990/91 führte letztendlich zu einer Neubewertung der amerikanischen Verteidigungspolitik und damit auch der Art der Kriegsführung.

1.4.2.1. Revolution in Military Affairs (RMA)

Die Debatte über die Möglichkeiten der modernen Kriegsführung und einer damit verbundenen RMA fand ihren ersten Höhenpunkt in einem Memorandum, das Andrew Marshall, Direktor des Office of Net Assessment (ONA) im Pentagon, im Jahre 1993 der damaligen Clinton-Administration zukommen ließ:

„Dessen Grundtenor lautete: Die Waffen des Kalten Krieges, Plattformen wie Flugzeugträger und schwere Panzerdivisionen würden angesichts neuer moderner Informations-, Kommunikations- und Waffensysteme schnell überholt sein. Nach Marshall standen die Vereinigten Staaten durch die neuen Möglichkeiten der Informationskriegsführung am Beginn einer militärischen Revolution.“[218]

[217] Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006“, Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.115f

[218] Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006“, Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.133f

Die Diskussion über die RMA ist in den USA vielschichtig und auf die teils widersprüchlichen Erkenntnisse der bis heute andauernden Debatte soll hier nicht eingegangen werden. Die Frage, ob Entwicklungen als Revolution eingestuft werden können, ist nicht immer eindeutig und lässt sich oft nur aus der Geschichte heraus beurteilen, auch gibt es keine wissenschaftliche Klassifikation der RMA. Von Seiten des Pentagon wurden diese Entwicklungen allerdings als RMA bezeichnet, wir wollen daher auch hier an dieser Notation festhalten.

Was können wir nun aus oben Gesagtem ableiten? Zunächst fallen uns anhand des Zitats zwei Aussagen auf: zum einen geht Marshall davon aus, dass die damals aktuellen Waffen- und Kommunikationssysteme nicht mehr zeitgemäß seien und die Abstützung auf schwere Verbände zugunsten von Informationstechnologie überholt sei. Zum anderen erkennen wir hier bereits zwei Jahre nach dem Golfkrieg und seiner Katalysatorwirkung erstmals den Begriff „Informationskrieg". Das ist insofern bemerkenswert, als die Verwendung des Begriffes alleine oben getroffene Aussage, der Informationskrieg habe den Kern militärischer Operationen erreicht, zusätzlich unterstreicht. Weiters bedeutet dies, dass sehr schnell das Potential dieser Art der Kriegsführung und in weiterer Folge der Weg, den die Army beschreiten musste, um es ausschöpfen zu können, erkannt wurde. Dies äußerte sich konkret zunächst in einer Überarbeitung des Field Manuals 100-5, in dem in der Fassung aus dem Jahr 1993 *„the end of the industrial-age warfare and the beginning of the information-age warfare"*[219] angekündigt wurde. Aber auch zwei weitere doktrinelle Dokumente wurden später in dieser Phase erstellt, nämlich das Konzept der *Joint Vision 2010* und das *Field Manual 100-6 „Information Operations"*, denen wir uns nun kurz widmen wollen.

1.4.2.2. Joint Vision 2010

Die „Joint Vision 2010" wurde 1996 veröffentlicht und war ein Grundsatzpapier für den gedachten Weg der Streitkräfteentwicklung, auch wenn sie keine Doktrin im operativen Sinn darstellte. Vielmehr war und ist sie ein im typisch amerikanisch-plakativen Stil gehaltenes Richtungspapier, in dem Ziele und neue operative Konzepte der zukünftigen Streitkräfteentwicklung definiert wurden. Bereits hier finden wir die zentralen Leitlinien, die uns später bei der *Network-Centric Warfare*[220] bzw. im *Joint Vision 2020* wieder begegnen werden, nämlich

- Dominant Maneuver
- Precision Engagement
- Full Dimensional Protection
- Focused Logistics

und das übergeordnete Ziel der Full Spectrum Dominance. Interessant dabei ist der Weg, wie diese Konzepte umgesetzt werden sollen, so heißt es beispielsweise im Zusammenhang mit dem Precision Engagement:

[219] vgl. Tilford Earl H Jr, The Revolution of Military Affairs: Prospects and Cautions, Carlisle, Pa., 1995, S55f (zit. nach Bendrath, Ralph, Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Peter Bittner, Jens Woinowski (Hrsg.): Mensch - Informatisierung - Gesellschaft, Münster: Lit Verlag, 1999, S. 144)
[220] siehe Kapitel 5.3.2

„Precision engagement will consist of a system of systems that enables our forces to locate the objective or target, provide responsive command and control, generate the desired effect, assess our level of success, and retain the flexibility to reengage with precision when required."[221]

Und weiter zur Full Dimensional Protection:
"*Full-dimensional protection will be built upon information superiority which will provide multidimensional awareness and assessment, as well as identification of all forces in the battlespace. Information warfare will support this effort by protecting our information systems and processes (…)"*[222]

Wir erkennen hier wieder die Notation des Informationskrieges, aber auch die Unterstreichung der Bedeutung der Informationsüberlegenheit und den Gedanken eines „System of Systems", also eines C4I-Systems, das alle Bereiche der Streitkräfte abdecken soll. In diesem Sinne definiert der damalige US-Verteidigungsminister Willian Cohen im *Annual Report to The President and the Congress 1999* sechs Grundkomponenten für zukünftige C4ISR-Systeme:

- A robust multisensor information grid providing dominant awareness of the battlespace.
- A joint communications grid with adequate capacity, resilience, and network management capabilities to rapidly pass relevant information to commanders and forces and to provide for their communications requirements.
- Advanced command and control processes that allow employment and sustainment of globally deployed forces faster and more flexibly than those of potential adversaries.
- A sensor-to-shooter grid to enable distributed joint forces to engage in coordinated targeting, cooperative engagement, integrated air defense, and rapid battle damage assessment and dynamic follow-up strikes.
- An information defense capability to protect the globally distributed sensors, communications, and processing networks from interference or exploitation by an adversary.
- An information operations capability to penetrate, manipulate, or deny an adversary's battlespace awareness or unimpeded use of his own forces.[223]

Auch hier kristallisiert sich klar die Notwendigkeit neuer konkreter Technologie zur Informationsgewinnung, -aufbereitung und -management sowie zur Kommunikation, aber auch die Notwendigkeit neuer Führungsprozesse und die Betonung der teilstreitkräfteübergreifenden Koordination heraus. Der Gedanke der Joint Force, also einer voll[224] integrierten, über den Strukturproblemen und Rivalitäten der Vergangenheit stehenden Streitkraft, wurde dabei als allgemeines Ziel forciert.[225]

---

[221] Joint Vision 2010, Department of Defense, 1996, S.21
[222] Joint Vision 2010, Department of Defense, 1996, S.22
[223] Cohen, S., William, Secretary of Defense, Annual Report to The President and The Congress, Department of Defense, 1999, Part III/10
[224] „voll integriert" bedeutet in diesem Zusammenhang: institutionell, organisatorisch, intellektuell und technologisch
[225] Joint Vision 2010, Department of Defense, 1996, S.2

Daraus abgeleitet lässt sich durchaus auch schon der Bezug zum E-Business herstellen, das ja ähnliche Entwicklungen im Wirtschaftsbereich propagierte. *„Managing-Strategien wie Effizienzsteigerung, Kosteneinsparungen, Rationalisierung, Optimierung, Vernetzung, "Konzentration auf Kernbereiche" werden nun auf das US-Militär angewandt.“*[226] Wichtiger für uns ist an dieser Stelle aber die Forderung nach mehr Flexibilität, Effizienz und Mobilität und damit verbunden die Abkehr von Massenheeren hin zu kleinen effektiven Einheiten.[227]
Die Joint Vision 2010 wurde von den Teilstreitkräften in jeweils eigene doktrinelle Dokumente umgesetzt, so zum Beispiel in die Army Vision 2010 der Landstreitkräfte.

1.4.2.3. FM 100-6 Information Operations

Ein weniger plakatives, dafür wesentlich substantielleres Dokument ist das Field Manual FM 100-6 „Information Operations“ der US Army, das im selben Jahr veröffentlicht wurde wie die Joint Vision 2010.

“Information operations integrate all aspects of information to accomplish the full potential for enhancing the conduct of military operations.”[228]

Das Dokument versucht die volle Bandbreite des Informationskrieges abzudecken, um so das gesamte Potential für die militärische Kriegsführung ausschöpfen zu können. Es spricht eigentlich schon sehr detailliert von Informationsraum, Bedrohungen der Informationsinfrastruktur, Informationssystemen sowie militärischen Operationen in diesem Kontext. Es unterscheidet zunächst zwischen dem Globalen und dem Militärischen Informationsraum:

[226] Pflüger, Thomas, „Neue Armeen für neue Aufgaben“ in Netzwerk Friedenskooperative, Friedensforum 1/1999, Kommission Zukunft der Bundeswehr, URL: http://www.friedenskooperative.de/ff/ff99/1-23.htm, (Abgerufen: 15.09.2008)
[227] vgl. Joint Vision 2010, Department of Defense, 1996, S.17 und
Pflüger, Thomas, „Neue Armeen für neue Aufgaben“ in Netzwerk Friedenskooperative, Friedensforum 1/1999, Kommission Zukunft der Bundeswehr, URL: http://www.friedenskooperative.de/ff/ff99/1-23.htm,
[228] FM 100-6 Information Operations, Department of the Army, 1996, S iv

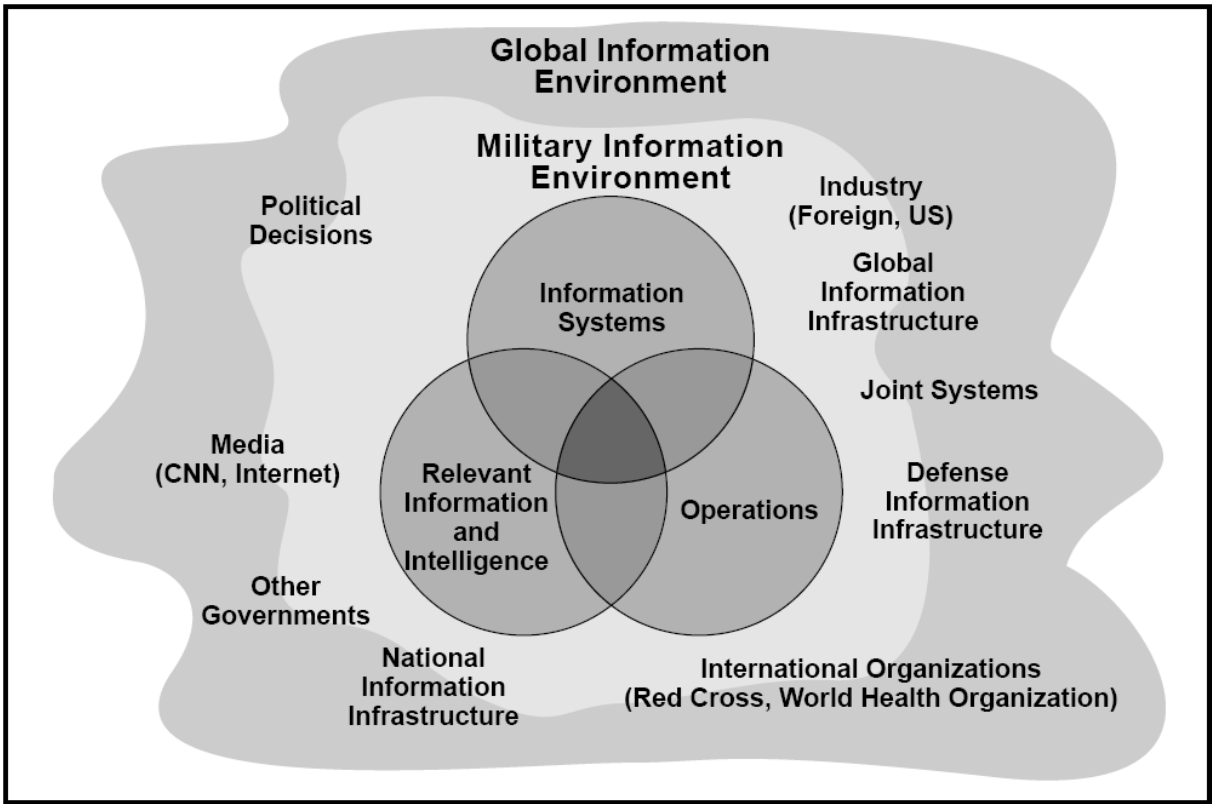


Abbildung 24: Globaler und Militärischer Informationsraum[229]

Alleine anhand dieser Graphik wird bereits deutlich, in welchem großen Rahmen sich Operationen in Zukunft abspielen werden und dass diese längst nicht mehr auf den rein militärischen Bereich beschränkt sind, auch wenn sie sich gemäß Definition im militärischen Informationsraum abspielen sollen.[230] Die gesamte Bandbreite ergibt sich auch aus dem Bedrohungsszenario, das das FM 100-6 gegenüber der Informationstechnologie zeichnet:

[229] FM 100-6 Information Operations, Department of the Army, 1996, S 2-3
[230] Die Grenzen zwischen Globalem und Militärischen Informationsraum sind ja fließend und verschwimmen zusehends

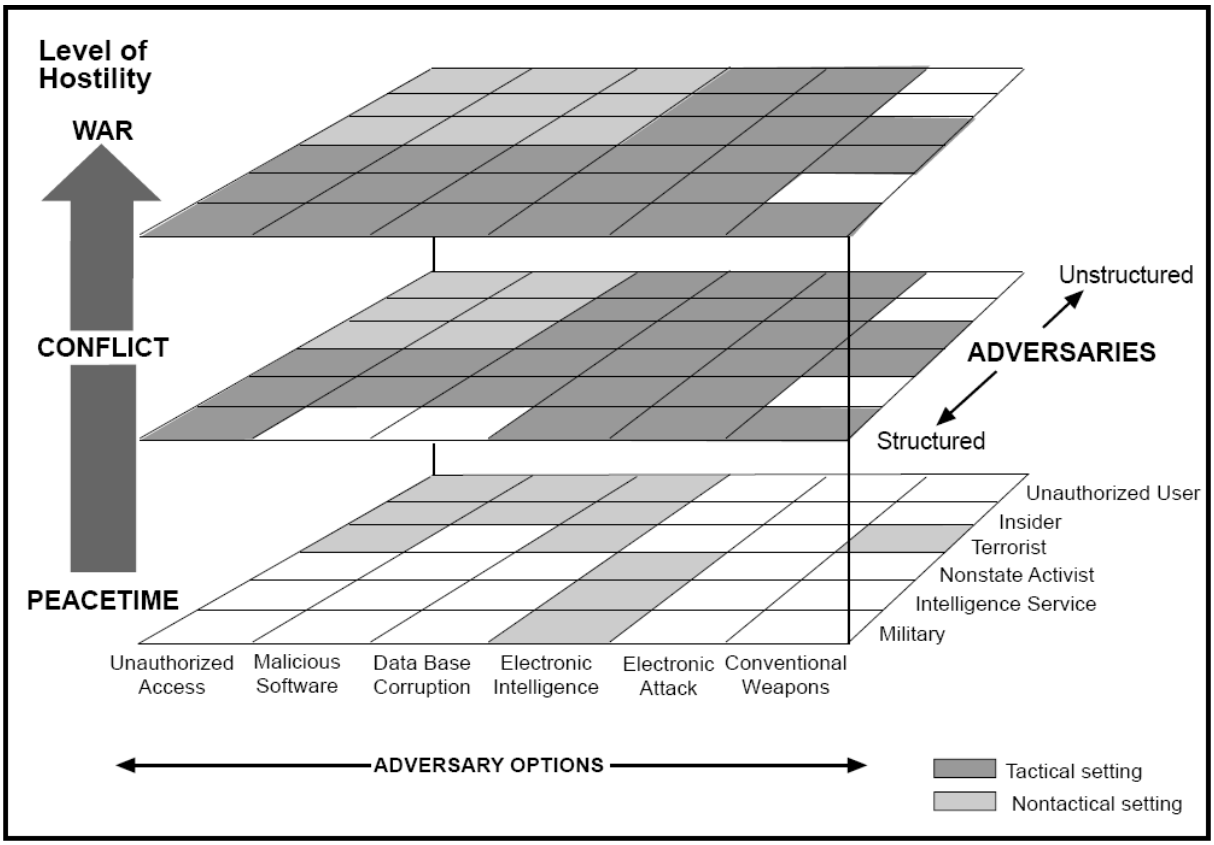


Abbildung 25: Bedrohungsbild gegenüber Informationstechnologie[231]

Die Strategen gehen also von möglichen neuen Bedrohungen auch im nicht-militärischen Bereich aus und sehen in der Folge daraus die Beherrschung des Informationsraumes als Antwort auf diese Herausforderungen. Diese ergibt sich als Informationsdominanz (Information Dominance) gemäß Definition wie folgt:

"The degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation "in operations short of war, while denying those capabilities to the adversary."[232]

Sie soll den Informationsvorteil in einen Wissensvorteil umsetzen, der Kommandanten in die Lage versetzt, situationsbezogen optimal führen zu können. Dieser als „*situational awareness*" bezeichneter Grundsatz wird uns später im Rahmen der NCW noch einmal begegnen.

Informationsoperationen sollen also für den entscheidenden Vorteil sorgen und werden in drei Teilbereiche unterteilt:

- *C2W-Operations*

  Diesen Teilbereich kann man am besten mit Kampf gegen die gegnerische Führung und Schutz der eigenen Führung umschreiben. Die Wurzeln liegen

[231] FM 100-6 Information Operations, Department of the Army, 1996, S 1-5
[232] FM 100-6 Information Operations, Department of the Army, 1996, S 1-9

hier in der AirLand Battle Doktrin, als man mit der Kombination von luft- und landgestützten Operationen Tiefe und Synchronisation zu erreichen versuchte. Daraus resultierte 1993 das Konzept der *deep-operations*, in dem feindliche Führungseinrichtungen zum Primärziel wurden.

"Today, C2W operations integrate and synchronize the capabilities of PSYOP, deception, OPSEC, and EW to facilitate the application of appropriate systems and forces to execute IO."[233]

Im FM 100-6 hat sich die Bandbreite der C2W also massiv erhöht, denn plötzlich spielen auch die psychologische Kriegsführung und die Elektronische Kriegsführung eine bedeutendere Rolle.

- *Civil Affairs Operations*

Der Globale Informationsraum ist integraler Bestandteil von Informationsoperationen. „*CA activities establish, maintain, influence, or exploit relations among military forces, civil authorities, and the civilian populace in an AO to facilitate military operations."*[234] Die Bedeutung der Operationen außerhalb des klassischen militärischen Spektrums für die Dominanz des Informationsraumes mag auf den ersten Blick nicht ganz klar erscheinen, vor allem aber in Konflikten abseits kriegerischen Auseinandersetzungen kommt diesen eine entscheidende Rolle zu. In diesem Zusammenhang sind auch Kooperationen zwischen NGOs, zivilen Autoritäten und anderen Organisationen in Konfliktgebieten zu sehen.

- *Public Affairs Operations*

„Der präzise Einsatz von Information ist genauso wichtig, wie die präzise Zieleinstellung bei Waffen, und die neuen Medien bieten hier nie da gewesene Möglichkeiten."[235]
Dieser Teil der Informationsoperationen beschäftigt sich mit dem Umgang und Einsatz der Medien und dem Einfluss auf die öffentliche Meinung im Rahmen militärischer Operationen. Die Bedeutung der Medien in der Kriegsführung ist gerade in den letzten Jahren massiv gestiegen, war in dieser Phase aber sicher noch nicht so ausgeprägt wie dies beispielsweise im Irakkrieg 2003 der Fall war, allerdings hat man zumindest das Potential von Operationen in diesem Bereich erkannt. Das FM 100-6 schreibt vor, dass Public Affairs integraler Teil von Planungsprozessen aller Ebenen sein müssen und sagt weiters: *„Providing accurate, timely news, information, and entertainment reduces distractions, rumors, fear, and confusion that could cause stress and undermine efficient operations."*[236]

---

[233] vgl. FM 100-6 Information Operations, Department of the Army, 1996, S 2-4
[234] FM 100-6 Information Operations, Department of the Army, 1996, S 2-4;
AO = Area of Operation, CA = Civil Affairs
[235] Toffler, Alvin; Toffler, Heidi; Überleben im 21.Jhdt; Übersetzt aus dem Amerikanischen „War and Anti-War" von Helmut Dierlamm et al. Deutsche Verlags Anstalt, 1994, S242
[236] FM 100-6 Information Operations, Department of the Army, 1996, S 3-15;

Als Konsequenz ergeben sich neben dem Bedarf an C4I-Systemen, Führungsinformationssystemen und neuen Führungsfunktionen, wie z.B. dem Public Affairs Officer, auch Anforderungen an ein optimiertes Informationsmanagement und an die Führungsstruktur im Allgemeinen. Auffallend dabei ist auch das Verschwimmen der Grenzen zwischen dem Militär und dem zivilen Bereich und damit in weiterer Folge auch die unschärfere Abgrenzung von Konflikten im Allgemeinen.

Verantwortlich für die Durchführung von Informationsoperationen ist eine eigene Zelle im Stab eines Verbandes und, anders als das noch in Phase I bei der Elektronischen Kriegsführung der Fall war, sind Operationen dieser Art nicht mehr so dezidiert auf einzelne Führungsbereiche aufgeteilt. Die grundsätzliche Stabsstruktur einer solchen Zelle ergibt sich wie folgt:

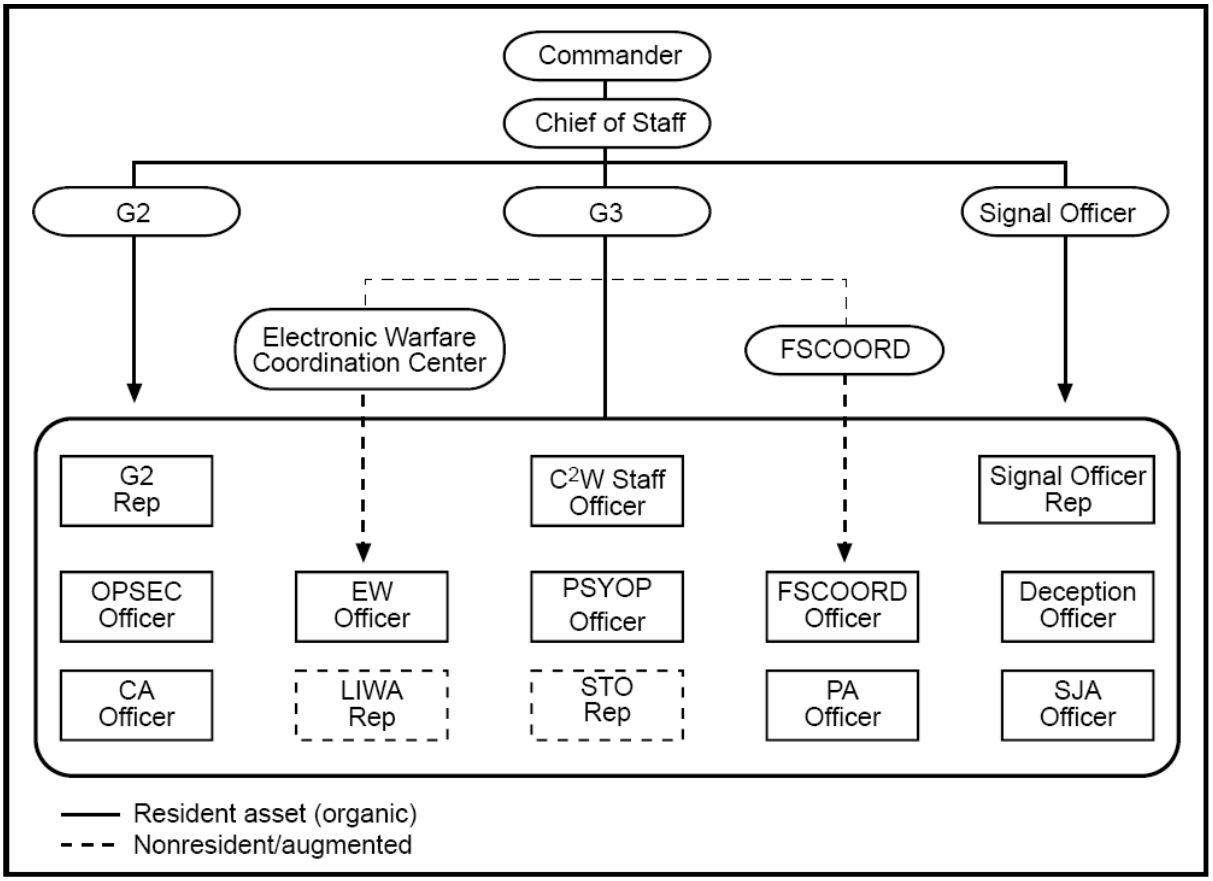


Abbildung 26: Stabsstruktur für Informationsoperationen[237]

Im Vergleich zu Phase I fällt uns hier auf, dass die Aufteilung der Elektronischen Kampfführung auf die verschiedenen Stabsbereiche zwar im Wesentlichen noch existiert, aber in der Zelle nun unter einem Kommando vereint ist und daher im Rahmen dieser Operationen homogen und aufeinander abgestimmt arbeiten kann.

Abschließend betrachtet können wir feststellen, dass das FM 100-6, sowohl an Libicki als auch an Arquilla/Ronfeldt gemessen, ganz eindeutig den Informationskrieg abbildet. Wir erkennen nicht nur alle relevanten Merkmale des Informationskrieges, sondern auch ein breites Spektrum operativer Grundsätze, die

[237] FM 100-6 Information Operations, Department of the Army, 1996, S D-1;

durch dieses Dokument abgedeckt werden, was wiederum auf eine homogene Gesamtsicht auf den Informationskrieg schließen lässt. Daher kann das FM 100-6 wohl als erste echte Informationskriegsdoktrin der US Army begriffen werden.

1.4.2.4. Network Centric Warfare

Parallel zur Joint Vision und dem FM 100-6 entwickelte, wie bereits erwähnt, Vice Admiral Arthur Cebrowski sein Konzept der Network Centric Warfare (NCW), das wir ja bereits in Abschnitt I detailliert vorgestellt haben. Wir wollen hier an dieser Stelle daher nur noch einmal die doktrinelle Bedeutung dieses Dokuments auf die zukünftige Streitkräfteentwicklung betonen und dieses Konzept natürlich ebenfalls als Informationskriegsdoktrin werten. In Phase III werden wir noch einmal auf die NCW zurückkommen und dort feststellen, was sie in unserer Analyse bedeutet.

1.4.2.5. Joint Vision 2020

Ebenfalls in diese Phase fällt noch die Joint Vision 2020, die im Jahr 2000 nur vier Jahre nach der Joint Vision 2010 veröffentlicht wurde und die die Vorstellungen für eine Streitkraft im Jahr 2020 propagierte. Wir werden sie in Phase III behandeln, da sie für unseren Untersuchungszeitraum in Phase II nicht relevant ist.

1.4.2.6. Streitkräfteorganisation

Wir haben in Phase I zunächst die Joint Chiefs of Staff kennen gelernt, und uns kurz mit dem USAISC beschäftigt. Es sei an dieser Stelle gesagt, dass diese beiden Organisationen auch weiterhin existieren, auch wenn sie an die Zeit angepasste Aufgaben haben. So stehen die JCS natürlich auch unter dem Einfluss geopolitischer Entwicklungen und die USAISC ist mit der Entwicklung neuer technologischer Systeme betraut. Wir wollen auf diese beiden Kommanden aber aus Relevanzgründen nicht näher eingehen. Allerdings sei an dieser Stelle noch die Schaffung des Joint Forces Commands (USJFCOM) erwähnt, das 1999 aus dem Atlantic Command hervorging. Seine Aufgabe war es, den Kampf der Verbundenen Kräfte weiterzuentwickeln und die Entwicklung der Joint Force zu unterstützen.

Viel interessanter für die Bewertung dieser Phase sind aber einerseits die Stärke der Streitkräfte sowie die Force XXI andererseits - beides wollen wir nun kurz untersuchen.

(a) Truppenstärken

Zehn Jahre nach dem Goldwater-Nichols Act und der Force 86 ergeben sich die Truppenstärken wie folgt[238]:

[238] The Military Balance 1996/97, International Institute for Strategic Studies, Oxford University Press, 1996, S.15-31

Landstreitkräfte:	**Luftstreitkräfte:**	**Seestreitkräfte**:
Stärke: 495.000 Mann	Stärke: 388.200 Mann	Stärke: 426.700 Mann US Navy + 176.900 Mann US Marine Corps
10 Divisionen, davon – 2 Panzerdivisionen – 4 Mechanisierte Infanteriedivisionen – 2 leichte Infanteriedivisionen – 1 Luftlandedivision – 1 Luftbewegliche Division	8 Strategische Raketenstaffeln 242 Fliegerstaffeln – 13 Strategische Bomberstaffeln – 52 Taktische Kampfstaffeln – 3 Strategische Aufklärungsstaffeln – 3 Taktische Aufklärungsstaffeln – 26 Transportstaffeln (15 Strategisch/11 Taktisch) – ca. 30 Sonderstaffeln (Kommunikation, AWACS, Search&Rescue…) – 21 Tankerstaffeln	Aus Relevanzgründen wollen wir auch hier die Navy nicht näher betrachten.
Gesamtstärke: Knapp 1,5 Mio Angehörige der Streitkräfte Zusätzlich dazu verfügen die Streitkräfte über Reserven der Nationalgarde und der Army, Air Force, Navy und Marine Reserve, die wir hier ebenfalls nicht näher behandeln wollen.		

Tabelle 4: Truppenstärken der US Streitkräfte 1996

Wir erkennen eine deutliche Reduktion der Truppenstärken in allen Bereichen, allerdings können wir diese nur bedingt für die Auswertung unserer Analyse verwenden. Der Wegfall des Feindbildes Kommunismus und das Ende des Kalten Krieges hat weltweit zu einer Neubewertung des Bedrohungsbildes und der Streitkräfteausrichtung geführt, so natürlich auch in den USA. In unserem Untersuchungszeitraum hat es alleine drei grundsätzliche Überprüfungen der Verteidigungspolitik gegeben: die Base Force Review (BFR) 1991, die Bottom-Up Review (BUR) 1993 und die Quadrennial Defense Review (QDR) 1997. Kern der Überlegungen waren aber in erster Linie nicht der Informationskrieg oder wie man die Streitkräfte auf diese Entwicklungen ausrichten kann, sondern natürlich die zu erwartenden strategischen Bedrohungen, auf die in Zukunft reagiert werden muss und budgetäre Erwägungen.[239] Die Reduktion der Streitkräfte ist daher in erster Linie auf die Clinton'sche Administration und die restriktive Budgetpolitik gegenüber dem Militär zurückzuführen, das den politischen Auftrag hatte, Truppenstärken zu reduzieren. Daher wäre es hier falsch, Schlüsse auf den Informationskrieg zu ziehen, vielmehr können wir die Stärke der Armee an dieser Stelle nicht in die Bewertung einfließen lassen.

[239] vgl. Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006", Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.148f

(b) Force XXI

Diese Truppe, in die die oben erwähnte EXFOR eingebettet war, hatte den Auftrag neue Technologien zu entwickeln, zu erproben und die Digitalisierung des Schlachtfeldes voranzutreiben.

Der Grundgedanke war, eine Art Test-Division für die zukünftige Streitkräfteentwicklung zu schaffen, in der man neue Konzepte testen und beurteilen konnte, ohne die gesamte Army in einen Strukturierungsprozess zu verwickeln. Die Force XXI nahm an zahlreichen Manövern teil und entwickelte erste Brigaden als *Interim Force*, die in ihrer Größe und Ausstattung von den regulären Brigaden differierten. Unter dem Kommando des US Army Training and Doctrin Command (TRADOC) wurden so zahlreiche Technologien wie beispielsweise das bereits erwähnte Land-Warrior Konzept entwickelt und erprobt.[240]

Die Charakteristiken, die sich dabei für die Force XXI ergaben, waren

- weitreichende Waffensysteme
- verzugslose Datenübermittlung
- modularer Aufbau und bedarfsorientierte Zusammensetzung der Kräfte
- Echtzeitaufklärung durch multiple Sensoren
- Einheitliches Informationsniveau aller Führungsebenen und Truppenteile
- Simultane Gefechtshandlungen höchster Präzision
- Überlegene Operationsführung durch schnelle Entschlüsse und Aktionen
- Intelligente Waffensysteme, die abstandsfähig sind, zwischen Feind und Freund unterscheiden und autonom Ziele bestimmen, auswählen und zerstören können[241]

Wir erkennen neben den Grundsätzen der AirLand Battle Doktrin und den bereits behandelten technologischen Zielen auch den Faktor der Modularität, ein Punkt der in Phase III noch wichtig werden wird.

Diese Division war damit so gesehen die erste operative Kraft, die, wenn auch nur zu Testzwecken, die moderne Kriegsführung im Sinne des Informationskrieges in vollem Umfang anwenden konnte.

1.4.3. Komplexitätsmanagement

Wir haben anfangs die Bedeutung des Begriffes Information unter anderem in Zusammenhang mit dem Informationsfluss gebracht. Die Erfahrungen aus dem Golfkrieg 1990/91 zeigten, dass mit der hohen Anzahl an Führungsinformations- und Waffensystemen künstlich Problemfelder und Hindernisse geschaffen wurden. Die Teilstreitkräfte hatten mit der Entwicklung eigener C3I-Systeme begonnen, diese

[240] vgl: Artikel *Force XXI* In: globalsecurity.org, URL: http://www.globalsecurity.org/military/agency/army/force-xxi.htm, (Abgerufen: 17.09.2008)
[241] vgl. Weigl, Ludwig, Strategische Einsatzplanung der NATO, Dissertation an der Univeristät der Bundeswehr München, Fakultät für Sozialwissenschaften, 2005, S.253

sollten nun als Konsequenz in ein „System der Systeme“, also ein übergeordnetes C3I-System integriert werden. Der technologische Fortschritt und die damit verbundene hohe Informationsdichte, machte es Kommandanten immer schwerer, Entscheidungen zu treffen. Expertensysteme sollten daher Informationen filtern und aufbereiten, Entwicklungen am Schlachtfeld antizipieren und Entscheidungen und Operationspläne weitgehend vorbereiten. Eines dieser Systeme war der *AirLand Battle Manager*, der auf Korpsebene die Führungsverfahren der Stabsoffiziere unterstützen sollte.[242] Als primäres Einsatzsystem diente das *Joint Global Command and Control Systems* (GCCS), das an das *Army Global Command and Control System* (AGCCS) anknüpfte. Weiters finden wir das *Army Battle Command System* (ABCS) und das *Army Tactical Command and Control System* (ATCCS).
Weitere Konzepte wurden im Rahmen der Überlegungen zur Network-Centric Warfare und zur Vernetzung der Truppen angedacht und von der Force XXI erprobt, die das *Force XXI Battle Command Brigade and Below System* (FBCB2) im Einsatz hatte. Ziel war es, ein homogenes System der Systeme zu schaffen, bestehend aus Applikationen und einer Art „taktischem Internet“.[243]

Neben den elektronischen Führungsinformationssystemen hat sich aber auch die Führungsorganisation als direkte Folge des Informationskrieges verändert. Wie bereits oben dargelegt, wurde im Stab des Verbandes die Zelle für die Durchführung von Informationsoperationen geschaffen. Diese Zelle integriert eigentlich alle Bereiche des Informationskrieges, soweit sie für einen operativen oder taktischen Verband relevant sind, und hat wesentlichen Einfluss auf die Elektronische Kampfführung als Teil des Informationskriegs, da sie so wesentlich übergreifender und vernetzter zum Einsatz gebracht werden kann.

Aus diesen Punkten lassen sich also wieder die Vernetzung der Truppen über C3I-Systeme, in weiterer Folge die Notwendigkeit von Informationsaufbereitung und -management für Kommandanten, sowie der Einfluss des Informationskrieges auf die Organisation im Stab und damit auf die Führungsstruktur eines operativen oder taktischen Verbandes ableiten.

1.4.4. Konfliktbeispiel

Wenn wir uns die Konflikte in dieser Phase ansehen, so fällt es schwer, einen Referenzkonflikt für unsere Untersuchung zu finden. Die USA intervenierten seit dem Ende des Irakkrieges in vielen kleineren Konflikten, aber auch immer mit begrenzten politischen und strategischen Zielen. Die Befreiung eines besetzten Staates, Okkupation oder die Herbeiführung eines Führungswechsels finden sich in keinem Konflikt als Ziel. Selbst der Schlag der NATO-Truppen gegen die damalige Bundesrepublik Jugoslawien nach den gescheiterten Verhandlungen von Rambouillet zur Lösung des Kosovo-Konflikts, den man eventuell noch heranziehen könnte, wurde als reiner Luftkrieg geführt, der Einmarsch der Bodentruppen erfolgte nach Beendigung der Kampfhandlungen im Grunde friedlich und ohne nennenswerte Zwischenfälle. Wir finden in dieser Phase keinen Konflikt, in dem das gesamte operative Spektrum ausgenutzt wurde und alle Teilstreitkräfte auch gemeinsam zum

[242] vlg. Bendrath, Ralph, Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Peter Bittner, Jens Woinowski (Hrsg.): Mensch - Informatisierung - Gesellschaft, Münster: Lit Verlag, 1999, S. 145
[243] vgl FM 100-6 Information Operations, Department of the Army, 1996, S 5-3;

Einsatz kamen. Eine sinnvolle Auswertung und ein Vergleich zum Golfkrieg 1990/91 erscheint daher an dieser Stelle nicht möglich.

1.4.5. Zwischenfazit

Seit Ende des Kalten Krieges und katalysiert durch den Golfkrieg 90/91 hat der Informationskrieg eine erstaunliche Entwicklung durchgemacht. Innerhalb von wenigen Jahren haben die Streitkräfte der USA das Potential dieser neuen Art der Kriegsführung erkannt und begonnen, es konsequent nutzbar zu machen. Natürlich war dies aufgrund von internen Widerständen, organisatorischen Problemen und politischen Vorgaben nicht immer leicht, allerdings haben wir dargelegt, dass sich der Informationskrieg von einer Idee zu einem umfassenden Leitbild entwickeln konnte.

Die Streitkräfte der USA versuchten dabei, die Entwicklung auf allen Ebenen massiv voranzutreiben. Der Einsatz von Hochtechnologie und die Einrichtung eigener Truppenteile zur Entwicklung und Erprobung lassen den Willen und den Ehrgeiz zum Ausbau der Vormachtstellung auf diesem Sektor erkennen. Kleinere, effizientere Einheiten sollten die großen schweren Verbände ablösen und Initiative und Mobilität garantieren. Allerdings können die reduzierten Truppenstärken nicht als Indikator für den Informationskrieg angesehen werden, da ihr Ursprung nicht eindeutig auf diese Entwicklungen zurückgeführt werden kann. Mit der Force XXI treffen wir allerdings erstmals auf eine Truppe, die bereits operative Fähigkeiten im Sinne der neuen Kriegsführung entwickelt hat und deren Manövererfahrungen für die weitere Streitkräfteentwicklung wichtig waren.

Zentrale doktrinelle Dokumente wie die Joint Vision 2010 oder die ersten Konzepte zur Network Centric Warfare lassen erahnen, in welche Richtung der Fortschritt gehen sollte und zeigen, dass die Notwendigkeit der vollen Vernetzung der Truppen bereits früh erkannt und deren Umsetzung massiv vorangetrieben wurde. Mit dem FM 100-6 hat der Informationskrieg weiters eine neue Dimension erreicht, da er erstmals in einer neuen Form der Operationsführung abgebildet wurde und damit nicht nur bestehende Konzepte und Doktrinen beeinflusste, sondern sogar eine neue hervorbrachte.
Im Rahmen des Komplexitätsmanagement erkennen wir ebenfalls erste Auswirkungen auf die Führungsstruktur der Verbände, die mit neuen Funktionen und Zellen den Anforderungen gerecht zu werden versuchen.

In Summe stellen wir also fest, dass sich der Informationskrieg in dieser Phase zu jenem systemimmanenten Gesamtkonstrukt entwickelt hat, wie wir es in Abschnitt I kennen gelernt haben. Im Vergleich zu Phase I können wir Doktrinen eindeutig als Teil des Informationskrieges identifizieren, Änderungen der Führungsstrukturen erkennen, die Vernetzung der Truppen feststellen und als Grundlage für technologische Entwicklungen den Informationskrieg identifizieren. Gegen Ende dieser Phase hat der Informationskrieg also nicht nur den Kern militärischer Organisationsstrukturen erreicht, er hat vielmehr das militärische Denken geprägt und ist in weitestem Sinne zu einer Art militärischem Bewusstsein erwachsen.

1.5. Phase III – Eine neue Dimension in einem neuen Jahrtausend

Die Abgrenzung zwischen Phase II und Phase III scheint an dieser Stelle etwas willkürlich gezogen zu sein und tatsächlich dürfte der Übergang an dieser Stelle eher fließend sein, wie allein die Datierungen der vorhandenen doktrinellen Dokumente implizieren. Plakativ gesehen wäre auch der Anschlag auf das World Trade Center im September 2001 und die damit auftretende neue Bedrohung durch den internationalen Terrorismus als geopolitische Abgrenzung der Phasen ähnlich dem Übergang zwischen Phase I und II auf den ersten Blick in Betracht gekommen. Allerdings erscheint der Amtsantritt des 43.Präsidenten der USA, George Bush Jr., wesentlich prägender, da Bush eine völlig andere Militärpolitik verfolgte als sein Vorgänger Bill Clinton und sich somit ja die gesamtgesellschaftliche Sicht[244] auf die militärische Kriegsführung verschoben hat. Daher wollen wir an dieser Stelle genau diesen Machtwechsel und die damit verbundene Richtungsänderung der amerikanischen Regierung als Grenze zwischen diesen beiden Phasen ziehen.

1.5.1. Einsatz von Technologie

Kommen wir an dieser Stelle wieder auf das Haushaltsbudget der Streitkräfte zurück. Als Bush im Januar 2001 sein Amt antrat, hatte sich im Militär ein Rückstau an Instandsetzungs- und Modernisierungsbedarf gebildet, der eine massive Erhöhung des Budgets erforderte. Für Bush Grund genug für einen Paradigmenwechsel: „*Yet, in our broader effort, we must put strategy first, then spending. Our defense vision will drive our defense budget; not the other way around. "*[245]

Damit war der Weg für eine umfassende Modernisierung scheinbar frei, allerdings waren die ersten Erhöhungen des Budgets unter Bush noch von der Clinton-Administration verabschiedet worden. Später kamen dann die kostenintensiven Konflikte in Afghanistan und dem Irak als Konsequenz der Anschläge vom 11.September 2001 dazu, was eine eindeutige Beurteilung der Motivation hinter dem Budgetanstieg zwar unmöglich scheinen lässt. Faktisch gab es unter Bush aber nicht nur eine deutliche Erhöhung des Verteidigungshaushalts, sondern auch ein klares Bekenntnis zu Technologie und Modernisierung. Erst dadurch wurde die Transformation überhaupt umfassend möglich.

Eines der zentralen technologischen Konzepte war und ist – und hier wollen wir unsere Grammatik auf die Gegenwart ändern – die Umsetzung der Network Centric Warfare sowie die Schaffung der technischen Infrastruktur für die in der Joint Vision 2020 festgelegten Ziele. Dazu gehört unter anderem das Global Information Grid, dem wir uns schon im Rahmen der NCW kurz gewidmet haben, aber auch beispielsweise die Schaffung des in der NSA angesiedelten Joint Functional Component Command for Network Warfare (JFCCNW), das Kräfte der CIA, NSA, FBI und der

[244] Sofern wir hier davon ausgehen wollen, dass das Wesen einer Gesellschaft auch durch ihre Regierung repräsentiert wird

[245] Bush Jr, George, *Remarks by the President to the Troops and Personnel,* Norfolk Naval Air Station, 2001, URL: http://www.whitehouse.gov/news/releases/20010213-1.html, (Abgerufen: 20.09.2008)
und vgl: Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006", Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.118

Militärgeheimdienste in sich vereint und damit ein zentrales Informationsbeschaffungselement bildet.[246]

Was wir erkennen können sind neben der massiven Aufwertung des Faktors Technologie hier auch wieder das Verschwimmen der Grenzen zwischen Militär und Zivilgesellschaft, ähnlich wie wir es bei den Informationsoperationen festgestellt haben. Das bedeutet, dass der Informationskrieg, am Faktor Technologie gemessen, eine höhere Ebene erreicht hat.

1.5.2. Organisation, Strategie, Dezentralisierung, Vernetzung

Wie wir bereits dargelegt haben, ist der Informationskrieg in der Zwischenzeit systemimmanent geworden, das heißt, er hat alle militärischen Bereiche erreicht und sogar darüber hinaus seine Fühler in die Zivilgesellschaft ausgestreckt. Das Militär versteht sich dabei immer mehr als System, was an Rüstung, Technologie, Doktrin und Führung neue Herausforderungen stellt.[247] Daraus folgte für die amerikanischen Streitkräfte, dass die trotz allem noch stark vom Kalten Krieg geprägte „AirLand Battle“ Doktrin[248] überholt war und neue Doktrinen für die zukünftigen Herausforderungen geschaffen werden mussten. Neue operative Ziele verdrängten den klassischen Abwehr- und Verteidigungsgedanken aus dem Kalten Krieg und prägen seitdem die amerikanische Verteidigungspolitik bis heute entscheidend. Im Quadrennial Defense Review Report 2001 definierte das Pentagon - ganz unter dem Eindruck der Anschläge vom 11.September desselben Jahres - diese Ziele wie folgt:

„Six critical operational goals provide the focus for DoD's transformation efforts:

- *Protecting critical bases of operations (U.S. homeland, forces abroad, allies, and friends) and defeating CBRNE[249] weapons and their means of delivery;*
- *Assuring information systems in the face of attack and conducting effective information operations;*
- *Projecting and sustaining U.S. forces in distant anti-access or area-denial environments and defeating anti-access and areadenial threats;*
- *Denying enemies sanctuary by providing persistent surveillance, tracking, and rapid engagement with high-volume precision strike, through a combination of complementary air and ground capabilities, against critical mobile and fixed targets at various ranges and in all weather and terrains;*
- *Enhancing the capability and survivability of space systems and supporting infrastructure; and*

[246] vgl: Blancke, Stephan, Information Warfare, in: Aus Politik und Zeitgeschichte 30-31/2005, Bundeszentrale für politische Bildung, S28, URL: http://www.bpb.de/publikationen/YAPI1Y,0,Information_Warfare.html, (Abgerufen: 20.09.2008)

[247] Vgl. Theile, Burkhard, Dr., Implikationen für die Heeresrüstung 1955-2005 – Bundeswehr wandelte sich zur Einsatzarmee, Das Profil, Zeitung des Rheinmetall-Konzerns 3/2005, S.10

[248] Vgl. Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006“, Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.149

[249] CBRNE: Chemical, Biological, Radiological/Nuclear, Explosive Incidents

- *Leveraging information technology and innovative concepts to develop an interoperable, joint C4ISR architecture and capability that includes a tailorable joint operational picture*."[250]

Die für uns relevanten Anforderungen an die Streitkräfte lassen sich wie folgt ableiten:

- Fähigkeit zur globalen Machtprojektion
- Sicherung von Informationssystemen und Einsatz effektiver Informationsoperationen
- Abstützung auf ein teilstreitkräftegemeinsames C4ISR-System und in weiterer Folge die
- Vernetzte Operationsführung

Für die amerikanischen Streitkräfte bedeutet dies eine stärkere Fokussierung auf die gegen Ende der Phase II erstellten doktrinellen Dokumente der *Joint Vision 2020* sowie der *Network Centric Warfare*, die beide an die Grundsätze der AirLand Battle Doktrin und der Joint Vision 2010 anknüpfen. Wir wollen hier wieder mit der Joint Vision 2020 beginnen.

1.5.2.1. Joint Vision 2020

Zunächst scheinen die operativen Grundsätze und Ziele der Joint Vision 2020 dieselben zu sein, wie wir sie bereits im Vorgängerdokument Joint Vision 2010 kennen gelernt haben. Auch über der Joint Vision 2020 steht als oberstes Ziel die *full spectrum dominance*, also die Beherrschung der gesamten Bandbreite militärischer Operationen, die durch die operativen Ziele *dominant maneuver, precision engagement, full-dimensional protection* und *focused logistics* unter Erlangung der *information superiority* erreicht werden soll.[251]

Allerdings beschreibt die Joint Vision die Notwendigkeit der Vorbereitung auf eine ungewisse Zukunft. Die nationalen Interessen der USA im Jahre 2020 seien breit gestreut und die sich bietenden Möglichkeiten und Herausforderungen würden Streitkräfte erfordern, die sowohl fähig sind, Kriege zu führen und zu gewinnen, als auch ihren Beitrag zum Frieden leisten können. So heißt es: *„The strategic concepts of decisive force, power projection, overseas presence, and strategic agility will continue to govern our efforts to fulfill those responsibilities and meet the challenges of the future. This document describes the operational concepts necessary to do so."* und weiter *" If our Armed Forces are to be faster, more lethal, and more precise in 2020 than they are today, we must continue to invest in and develop new military capabilities. This vision describes the ongoing transformation to those new capabilities".*[252]

---

[250]Shelton, Henry, Chairman of the Joint Chiefs of Staff, Quadrennial Defense Review Report, Department of Defense, 2001, S.30

[251] vgl. Shelton, Henry, General, Chairman of the Joint Chiefs of Staff, Joint Vision 2020, US Government Printing Office, 2000, S.6 und S.20-27 bzw.
vgl. Weigl, Ludwig, Strategische Einsatzplanung der NATO, Dissertation an der Univeristät der Bundeswehr München, Fakultät für Sozialwissenschaften, 2005, S.254f

[252] Shelton, Henry, General, Chairman of the Joint Chiefs of Staff, Joint Vision 2020, US Government Printing Office, 2000, S.1

Die Entwicklung neuer militärischer Kapazitäten ist dabei ein wesentlicher Faktor, der unter dem Schlagwort „Innovation“ vor allem in Zusammenhang mit der *full spectrum dominance* explizit betont wird und über den bloßen technologischen Aspekt hinausgeht. „*The ideas(…) in JV 2020 are, indeed, innovative and form a vision for integrating doctrine, tactics, training, supporting activities, and technology into new operational capabilities.“*[253]

Dabei ist der Gedanke der *joint force* ebenfalls wieder zentraler Punkt des Dokumentes. Hier werden der Entwicklung der Interoperabilität zwischen den Teilstreitkräften große Fortschritte attestiert, aber auch der Begriff der Interoperabilität selbst erweitert. Das Pentagon spricht nicht mehr nur von der Homogenisierung der Teilstreitkräfte, sondern nebst den Herausforderungen multinationaler Operationen vor allem auch von *interagency operations* und meint damit nichts anderes, als die koordinierte Zusammenarbeit zwischen dem Militär, Geheimdiensten, Regierungsorganisationen, aber auch NGOs, regionalen und internationalen Organisationen und privaten Organisationen. Dabei wird die Bedeutung der Information herausgestrichen, die solche Organisationen für die Beurteilung des *common relevant operational picture* beitragen können.[254]

Weiters wird die Bedeutung von Informationsoperationen und einer teilstreitkräftegemeinsamen Führung, der *Joint Command and Control*, der wir uns später kurz widmen wollen, hervorgehoben.

Es bietet sich uns also in diesem Dokument ein stark erweitertes Bild der bereits in der JV 2010 festgelegten Grundsätze. Wir können hier die Ausweitung des, um bei der amerikanischen Notation zu bleiben, militärischen Informationsraums und damit die steigende Unschärfe zwischen Militär und Zivilgesellschaft erkennen oder anders formuliert das Wachstum des Informationskrieges zu einem gesamtgesellschaftlichen Konstrukt, wie wir es bereits mehrmals festgestellt haben.

1.5.2.2. Network Centric Warfare

Eines der zentralen doktrinellen Dokumente der jüngsten Vergangenheit ist das Konzept der Network Centric Warfare, das wir ebenfalls schon kennen gelernt haben. Eine detaillierte Betrachtung dieser Doktrin liefert Kapitel 5 aus Abschnitt I, wir wollen uns an dieser Stelle der Bedeutung des Konzepts für den Informationskrieg bewusst werden. Wie bereits erwähnt, knüpft auch dieses Dokument an die Grundsätze der AirLand Battle an und greift auch die operativen Ziele der beiden Joint Vision Dokumente auf.

Wenn wir uns die Paradigmen und Grundprinzipien der NCW ansehen, so werden wir feststellen, dass nach Kenntnis der oben behandelten Doktrinen diese Elemente zumindest bekannt erscheinen. Wir wollen nun versuchen, diese Elemente gegenüberzustellen:

[253] Shelton, Henry, General, Chairman of the Joint Chiefs of Staff, Joint Vision 2020, US Government Printing Office, 2000, S.10f
[254] Shelton, Henry, General, Chairman of the Joint Chiefs of Staff, Joint Vision 2020, US Government Printing Office, 2000, S.18f

AirLand Battle Phase I	Joint Vision 2010 Phase II	NCW Phase III
	Information Superiority	Information Superiority
	Situational Awareness	Shared Awareness
Initiative, Überraschung	Decisive Speed	Speed of Command
Synchronisation	Synchronisation	Self-Synchronisation
Konzentration der Kräfte	Operational Dispersion	Dispersed Forces
	Operational dispersion	Demassification
Aufklärung, Intelligence	All-Source Intelligence	Deep Sensor Reach
		Alter Initial Conditions
		Compressed Operations

Tabelle 5: Vergleich doktrineller Elemente; Quelle: Eigene Darstellung

Damit lässt sich noch einmal veranschaulichen, dass Grundelemente der modernen Kriegsführung unserer Zeit bereits in der AirLand Battle Doktrin vorhanden waren. Weiterentwickelt und unter Fokussierung auf die *full-spectrum dominance* finden wir diese Elemente in der Joint Vision 2010 wieder. Interessant ist jetzt aber die NCW, die dieses Spektrum noch einmal erweitert und aus dem Ziel der Joint Vision 2010, nämlich besagter full spectrum dominance, Grundprinzipien zur Einsatzführung ableitet. Grundlage für alle Operationen ist nach wie vor die Informationsüberlegenheit, aber die in der JV 2010 im Rahmen der operativen Grundsätze zur Erreichung der full spectrum dominance noch als *situational awareness, synchronisation* und *operational dispersion* bezeichnete Faktoren, werden nun zu *shared awareness, self-synchronisation* und *dispersed forces bzw. demassification.*

Wir erkennen hier klar den hohen Vernetzungsgrad und den bereits in Abschnitt I angesprochenen Paradigmenwechsel hin zu einem horizontalen Führungssystem. Weiters stellen wir anhand der Demassifikation die Verkleinerung der Einheiten und deren großzügigere Verteilung im Operationsgebiet fest. Die NCW-Doktrin ist also nicht nur ein umfassendes neues Konzept für die vernetzte Operationsführung, was ja an sich schon ein sehr großer Fortschritt ist, sondern durch sie hat der Informationskrieg eine weitere, neue Dimension erreicht.

1.5.2.3. Streitkräfteorganisation

(a) Interim Force

Neue Doktrinen und neue Ziele benötigen auch neue Strukturen und Organisationsformen. Die Restrukturierungspläne unter Bush orientierten sich zunächst an der Army Vision 2010, also der Umsetzung der Joint Vision 2010 für die Army. Mit diesem von General Shinseki vorgelegten Dokument *„startete das*

amerikanische Heer einen umfassenden Prozess, in dem die Art der Landkriegführung transformiert werden und an deren Ende die ‚Revolutionierung der Fähigkeiten der Landstreitkräfte' stehen sollte."[255]

Die Transformation der Army läuft dabei in drei Stufen ab:

- *Legacy Force:* eine Aufwertung bestehender Systeme mit bestehender Technologie und C4I-Systemen
- *Interim Force:* Interim Brigade Combat Teams (IBCT) auf leichten gepanzerten Fahrzeugen als Überbrückung der Objective Force und der operativen Lücke zwischen schweren und leichten Verbänden
- *Objective Force*: Hochmoderne Zielstreitkraft im Jahre 2025, die das gesamte Spektrum militärischer Operationen abdecken können soll.

Noch in Phase II begann man mit der Umsetzung dieser Pläne. Wir wollen uns vor allem die Interim Force genauer ansehen, da sie auch die aktuelle Organisation der Streitkräfte darstellt. Wie bereits gesagt, soll diese Organisationsform die Lücke zwischen den schweren und leichten Verbänden schließen und dabei bereits im gesamten operativen Spektrum einsetzbar sein. Kleinere, mobilere Einheiten und erste modulare Elemente sollen dies gewährleisten, die so genannten Interim Brigade Combat Teams (IBCT). Der Verlust an Feuerkraft gegenüber schweren Verbänden sollte dabei durch die vernetzte Operationsführung wettgemacht werden. Die Forderung nach hoher Mobilität und geringem logistischen Aufwand führte zur Einführung neuer Fahrzeuge, konkret zum Radpanzer „Stryker", nach dem die IBCT auch in Stryker Brigade Combat Team (SBCT) umbenannt wurde.[256] Wir werden uns zunächst die Gliederung einer solchen Stryker Brigade ansehen und uns dann den Truppenstärken widmen.

(b) Stryker Brigade als Brigade Combat Team

Eine Stryker Brigade gliedert sich aktuell in ein Aufklärungsbataillon, drei Stryker-Infanterie Bataillone, ein Artilleriebataillon, ein Unterstützungsbataillon mit Sanitäts-, Berge- und Instandsetzungselementen und direkt von der Brigade geführten weiteren Kompanien für die Panzerabwehr, Pionierdienst, Network Support und Militärischer Aufklärung. Im Anhang findet sich ein Organigramm mit der Gliederung der Brigade.[257] Wichtig dabei ist die Standardisierung der Brigaden sowie die Modularisierung im Zuge der Army Modular Force Initiative.

---

[255] Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006", Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.155

[256] Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006", Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.156f

[257] Artikel *Transformation of the United States Army.* In: Wikipedia, The Free Encyclopedia*,* 29 September 2008, 15:00 UTC, URL: http://en.wikipedia.org/w/index.php?title=Transformation_of_the_United_States_Army&oldid=241780624 (Abgerufen: 6. Oktober 2008, 02:28 UTC)

Die Organisation der Streitkräfte um diese Brigade Combat Teams[258] soll die Voraussetzungen schaffen, um die Herausforderungen des 21.Jahrhunderts zu meistern. Modularisierung bedeutet in diesem Zusammenhang, dass diese Brigaden im Prinzip wie kleine Divisionen agieren können und wesentliche Elemente der Kampf- und Einsatzunterstützung, die früher nur ab Divisionsebene verfügbar waren, bereits in ihrer Grundorganisation integriert haben. Damit erreichen sie eine höhere Autonomie und verbesserte Interoperabilität, aber auch effizientere Logistik und rasche Verlegbarkeit. Diese Neustrukturierung betrifft die gesamte Army und wird kontinuierlich umgesetzt, dabei kommen die Stryker Brigaden der vernetzten Streitkraft, die als langfristiges Ziel definiert wurde, am nächsten.[259]
Mit der Modularisierung sollen folgende Ziele erreicht werden:

- zumindest 30% Kampfwertsteigerung
- Eine Steigerung der einsatzbereiten Verbände um 50%[260]
- Kräfte, die im Einsatz stehen, sollen weniger Nachschub erfordern und damit die Notwendigkeit von ad-hoc Organisationen verringern
- Verlegbare, interoperable Kommanden sollen eingerichtet werden und die Interoperabilität aller Verbände erhöht werden
- Änderungen in der Organisation aufgrund von zukünftigen Entwicklungen der NCW sollen schnell umsetzbar sein
- Weniger Belastung für die Truppe durch besser vorhersagbare Missionszyklen im Sinne von 1:2 Jahren Einsatz und Dienst in der Heimatgarnison für reguläre Kräfte (und 1:4 Jahren für Reservekräfte)
- Schnellere Mobilmachung für Reservekräfte[261]

Damit werden die Brigaden zu den eigentlichen Drehscheiben der Einsatzführung, dies ist aber nur durch Selbst-Synchronisation und Vernetzter Operationsführung möglich. Effizienzsteigerung durch Dezentralisierung und Verkleinerung der Einheiten lassen uns den Einfluss des Informationskriegs klar erkennen.

(c) Truppenstärken

Abschließend betrachten wir wieder die Truppenstärken, als Referenz dienen die Daten aus dem Jahr 2006:

[258] Neben den Stryker Brigade Combat Teams gibt es noch die Heavy und die Infantery Brigade Combat Teams
[259] vgl. Rumsfeld, Donald, Annual Report to The President and Congress, Department of Defense, 2005, S.40f
[260] Nicht jede Brigade kann aufgrund von Instandsetzungen, Wartungstätigkeiten, Ausbildung und Training, Urlauben etc zu jedem Zeitpunkt gleich einsatzbereit sein. Ein Rotationsprinzip zwischen den Verbänden regelt Zeit und Dauer erhöhter Einsatzbereitschaft.
[261] vgl. Feickert, Andrew, US Army's Modular Redesign, Issues for Congress, Congressional Research Service, 2006, S.CRS-2

Landstreitkräfte:	**Luftstreitkräfte:**	**Seestreitkräfte**:
Stärke: 502.000 Mann	Stärke: 379.500 Mann	Stärke: 376.750 Mann US Navy + 175.350 Mann US Marine Corps
10 Divisionen, davon – 2 Panzerdivisionen – 4 Mechanisierte Infanteriedivisionen – 2 leichte Infanteriedivisionen – 1 Luftlandedivision – 1 Luftbewegliche Division	11 Strategische Raketenstaffeln 242 Fliegerstaffeln – 4 Strategische Bomberstaffeln – 11 Taktische Bomberstaffeln – 47 Taktische Kampfstaffeln – 1 Strategische Aufklärungsstaffeln (JSTARS) – 3 Taktische Aufklärungsstaffeln – 29 Transportstaffeln (12 Strategisch/9 Taktisch/8 Operations Support) – ca. 15 Sonderstaffeln (Kommunikation, AWACS, Search&Rescue…) – 22 Tankerstaffeln – 3 UAV Staffeln	Aus Relevanzgründen wollen wir auch hier die Navy nicht näher betrachten.
Gesamtstärke: Knapp 1,5 Mio Angehörige der Streitkräfte Zusätzlich dazu verfügen die Streitkräfte über Reserven der Nationalgarde und der Army, Air Force, Navy und Marine Reserve, die wir hier ebenfalls nicht näher behandeln wollen.		

Tabelle 6: Truppenstärken der US Streitkräfte 2006[262]

Interessanterweise haben sich die Truppenstärken der Streitkräfte seit dem letzten Vergleichszeitpunkt kaum verändert, obwohl sich von der Entwicklung und vom Verständnis des Informationskrieges eigentlich eine Reduktion hätte ergeben müssen. Dies ist mit ziemlicher Sicherheit auf die veränderte geopolitische Lage und die hohe Anzahl an Einsätzen der US Streitkräfte, sei es im Irak, in Afghanistan oder den anderen zahlreichen Interventionsschauplätzen zurückzuführen. Wir können also auch in dieser Phase die Truppenstärken nicht als Indikator für die Beurteilung der Auswirkungen des Informationskrieges werten.

1.5.3. Komplexitätsmanagement

In punkto Komplexitätsmanagement kommen wir zunächst noch einmal kurz auf die Joint Vision 2020 zurück. In dieser Doktrin werden, wie bereits oben erwähnt, auch die Anforderungen an die zukünftige Führung formuliert. Unter dem *Joint Command and Control* Grundsatz werden die zukünftigen Anforderungen an Kommandanten und Stäbe wie folgt definiert:

- Kommandanten brauchen ein breites Verständnis der neuen operativen Fähigkeiten

[262] vgl The Military Balance 2005/06, International Institute for Strategic Studies, Oxford University Press, 2006, S.20-29

- Der Stab muss organisiert und trainiert werden, um die neuen Kapazitäten nutzen zu können
- Führen muss auch bei technischem Ausfall möglich sein
- Kommandanten können ihre Absichten formulieren und verbreiten, basierend auf einem aktuellen Lagebild
- Übergeordnete, gemeinsame Kommanden sollen aufgeteilt sein und die Fähigkeit haben, verteilte Einheiten und Operationen zu führen. Untergeordnete Kommanden sollen dabei klein, agil, mobil und vernetzt sein
- Ein schnellerer Operationsverlauf und eine verbesserte Einsatzführung in Hinblick auf erhöhte Reichweiten und effektiveren Waffensystemen erfordern kontinuierliche, simultane Planung und Durchführung auf allen Ebenen
- Die Zusammenarbeit mit anderen Organisationen erfordert gemeinsame Planungskapazitäten, technische Kompatibilität und Mechanismen zum Informationsaustausch[263]

Um diese Ziele zu erreichen werden seit 2007 neue so genannte *Joint Command and Control Joint Task Force-capable Headquarters* als voll funktionsfähige, skalierbare Führungseinrichtungen gebildet. Planungsprozesse werden in den Streitkräften aufeinander abgestimmt und in vernetzten Umgebungen koordiniert, um den Gedanken der Adaptiven Planung umzusetzen, also einer Planung, die in der Lage ist innerhalb kurzer Zeit auf neue Anforderungen zu reagieren.[264]

Daraus ergeben sich natürlich hohe Anforderungen an das Komplexitätsmanagement. Dabei sind zwei Faktoren entscheidend, die technische Komponente und die kognitive Domäne, also der Bereich der Führung.

Die technischen Herausforderungen ergeben sich aus der Vernetzung der Truppen, der Schaffung neuer Kommunikationswege und -kapazitäten, der Steuerung des Informationsflusses, der Informationsbeschaffung und der Forderung nach Kompatibilität mit fremden Systemen im Sinne der internationalen Kooperation mit anderen Armeen und Organisationen. Die Grundlage für die Vernetzte Operationsführung oder Network-Centric Warfare soll, wie bereits erwähnt, der Global Information Grid bilden. Seine Bedeutung wird im QDR 2006 noch einmal dezidiert unterstrichen.[265]

Der zweite Faktor im Komplexitätsmanagement ist die Führung im Allgemeinen. Der ohnehin schon sehr komplexe Vorgang des Führens ist noch komplexer und schwieriger geworden, was in weiterer Folge auch Ausbildung und Training besondere Bedeutung beimisst. In nahezu allen Dokumenten wird die Bedeutung der Führung betont, so heißt es beispielsweise in der JV 2020: *„(…) leaders must understand the implications for decision-making processes, the training of decision makers at all levels, and organizational patterns and procedures. The potential for overcentralization of control and the capacity for relatively junior leaders to make*

[263] vgl. Shelton, Henry, General, Chairman of the Joint Chiefs of Staff, Joint Vision 2020, US Government Printing Office, 2000, S.32
[264] vgl. Pace, Peter, Chairman of the Joint Chiefs of Staff, Quadrennial Defense Review Report, Department of Defense, 2006, S.60f
[265] vgl. Pace, Peter, Chairman of the Joint Chiefs of Staff, Quadrennial Defense Review Report, Department of Defense, 2006, S.59

decisions with strategic impact are of particular importance.It has often been said that command is an art and control is a science – a basic truth that will remain true. Our thinking about command and control must be conceptually based, rather than focused on technology or materiel.“[266]

Die Bedeutung der Führung ist für die Umsetzung der Doktrinen entscheidend, dabei geht es sowohl um die Herausforderung an einzelne Kommandanten, als auch um die Änderung in der Führungsstruktur und den Übergang von einer hierarchischen in eine horizontale flexible Hierarchie. Der Übergang zu kleineren, flexibleren, hochmobilen und autonomen Verbänden wie den Stryker Brigaden bedeutet ja nichts anderes als eine Abkehr von der traditionellen top-down Organisation hin zu einer flacheren Hierarchie. Dabei ändert sich auch das Bild des Kommandanten „*vom "Leitwolf" zum echten "Teamleader" mit den entsprechenden Forderungen an Persönlichkeit und Kompetenzen*“[267].
Dies ist aber vor allem im operationellen Kontext zu sehen und bedeutet nicht völlige Handlungsfreiheit der Verbände. Die grobe Richtung, das operative Ziel und die Grenzen in denen sich eine solche Brigade bewegen darf, müssen klar definiert sein.

Neben der zunehmenden Bedeutung von Informationstechnologie, der Vernetzung der Truppen und der Dezentralisierung lässt sich hier also ebenfalls durch die Verflachung der Hierarchie eine grundlegende Änderung im Komplexitätsmanagement nachweisen. Wir stellen daher abschließend fest, dass der Informationskrieg sich auch in diesem Bereich in neuer Qualität manifestiert hat.

1.5.4. Konfliktbeispiel

Die Anschläge von 11.September 2001 auf das Pentagon und das World Trade Center haben nicht nur der gesamten Militärpolitik der USA eine Wendung gegeben, sie dienten auch - völlig wertfrei - als Begründung für zwei Konflikte, die die USA zu Beginn des 21.Jahrhunderts führten. Sowohl in Afghanistan 2001 als auch im Irak 2003 kamen dabei bereits vernetzte Truppen zum Einsatz, so dass wir uns hier kurz mit den operativen Erfahrungen in beiden Konflikten beschäftigen wollen.

1.5.4.1. Afghanistan

Der Afghanistan Konflikt ist vor allem für die Auswertung in punkto Einsatz präzisionsgesteuerter Waffen interessant, da die amerikanischen Streitkräfte eine groß angelegte Bodenoffensive vermieden. Die Strategie war es, durch massive Luftangriffe die oppositionelle afghanische Nordallianz zu unterstützen, die auch rasch das Land erobern konnte. Dies ist hier insofern von Bedeutung, da über sprachliche und kulturelle Grenzen hinweg die operationelle Zusammenarbeit mit den lokalen Führern und Truppen forciert werden musste. Das Aufmarschgebiet

[266] vgl. Shelton, Henry, General, Chairman of the Joint Chiefs of Staff, Joint Vision 2020, US Government Printing Office, 2000, S.32
[267] Artikel *Häufig gestellte Fragen zur Vernetzten Operationsführung*, URL: http://www.luftwaffe.de/portal/a/luftwaffe/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLNzKId_cJAclB2QH6kZiiXs5IokEpqfre-r4e-bmp-gH6BbmhEeWOjooAVm-y1A!!/delta/base64xml/L2dJQSEvUUt3QS80SVVFLzZfMjBfSDk3?yw_contentURL=/01DB060000000001/W26KYHBK713INFODE/content.jsp, (Abgerufen: 21.09.2008)

der USA befand sich dabei in Usbekistan, von wo aus Verbindungselemente und Spezialkräfte in das Operationsgebiet entsandt wurden, um so die Einsätze zu koordinieren. Erst später landeten amerikanische Truppen in Afghanistan selbst, wo sie heute immer noch im Einsatz stehen.[268]

Interessant ist allerdings die Art und Weise der geführten Luftschläge, denn im Vergleich zum Golfkrieg 1990/91 hat sich der Anteil der präzisionsgesteuerten Bomben auf 57% gesteigert. Dabei betrug die Anzahl der täglich geflogenen Einsätze nur mehr 200 im Vergleich zu knapp 3000 Einsätzen im Zweiten Golfkrieg, wobei ein Ziel nur mehr von zwei Flugzeugen bekämpft wurde. Dies ermöglichte eine wesentlich flexiblere Operationsführung, so wurde von 178 Zielen nur ein einziges vorab ausgewählt, alle anderen ergaben sich aus dem Operationsverlauf.[269]

Dies zeigt das Potential der neuen vernetzten Kriegsführung recht deutlich, allerdings fehlt hier an sich der Vergleich zu einem intensiveren Konflikt, in den alle Teilstreitkräfte von Beginn an involviert sind.

1.5.4.2. Irak

Einen solchen Konflikt finden wir zwei Jahre später im Dritten Golfkrieg. Die militärische Intervention hatte einen Regimewechsel im Irak zum Ziel und dieser konnte nur mit einem Angriffskrieg erreicht werden. 47 Nationen beteiligten sich an den von den USA geführten Operationen und anders als im Zweiten Golfkrieg begann der Bodenkrieg nahezu zeitgleich mit dem Luftkrieg. In der Nacht zuvor gab es bereits massive Luftschläge, ehe am 19.März 2003 britische und amerikanische Soldaten über die kuwaitische Grenze in den Irak invadierten.

Von Seiten der Luftkriegsführung gab es noch einmal eine Steigerung am Anteil von Präzisionswaffen gegenüber konventionellen Bomben auf ca. 68% (20000 zu 9200), wobei auch hier die priorisierten Ziele wieder Kommando- und Führungseinrichtungen, Regierungsgebäude[270] und militärische Anlagen wie RADAR- und Flugabwehrsysteme waren.

Die Bodenoffensive nahm einen ähnlich raschen Verlauf wie 1990/91, in nur zwei Tagen rückten die Truppen mehr als 200km in irakisches Territorium vor und wieder ergaben sich für die Iraker die gleichen Probleme. Die irakische Führung hielt weiter an ihrer starren Befehlstaktik fest und hatte nach wie vor keine Mittel, um Luftüberlegenheit herzustellen oder die Elektronische Kampfführung bzw. die Informationsoperationen der Amerikaner zu entschärfen. Besonders interessant ist an dieser Stelle das bereits in Abschnitt I angeführte Beispiel der Täuschung irakischer Truppen durch simulierten Funkverkehr.

---

[268] vgl. Operation Enduring Freedom, The United States Army in Afghanistan, Center of Military History, 2003

[269] vgl. Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006“, Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.223f

[270] vgl. Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006“, Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007, S.225

Abseits der eigentlichen Kampfhandlungen, die nach den Gesichtspunkten der beschriebenen Doktrinen unter Einsatz der technologischen Systeme abliefen, ist dieser Konflikt aber aus zwei Gründen für uns interessant.

Erstens setzte dieser Krieg völlig neue Maßstäbe für Informationsoperationen und den Umgang mit Medien. Die Einbettung von Journalisten in die unmittelbare Kriegsführung vermittelte ein, wenn auch durch die Militärzensur eindimensionales, aber dennoch völlig neues Bild der Kampfhandlungen und bot eine große Oberfläche für die psychologische Kriegsführung. Die Institutionalisierung der Medien für militärische Zwecke sorgte für ein deutlich für die Amerikaner geprägtes Bild in der Öffentlichkeit, das einerseits den irakischen Kräften die Aussichtslosigkeit ihrer Lage vor Augen führte und andererseits bereits im Vorfeld beim amerikanischen Volk mit bewussten Falschmeldungen Akzeptanz für den Krieg zu schaffen versuchte.[271] Die gesamte Bandbreite von Informationsoperationen wurde damit erstmals in neuer Qualität angewandt und wir erkennen hier folgerichtig auch eine neue Qualität des Krieges.

Zweitens kam die erste Stryker Brigade zum Einsatz, die im Dezember zwar erst nach dem offiziellen Ende des Krieges im Mai in das Operationsgebiet verlegte, dort aber alles andere als ein befriedetes Gebiet vorfand. Diese Brigade bot optimale Voraussetzungen, um die Modularität und die Vernetzung der Truppen in einem realen Konflikt zu testen. Jedes einzelne Fahrzeug innerhalb der Brigade war in der Lage, sich mit dem Gesamtsystem zu vernetzen. Die Brigade zeichnete sich durch hohe operationelle Flexibilität, geringem Logistikaufwand und der raschen Einsatzfähigkeit in verschiedenartigen Missionen im ganzen Land aus und bestätigte damit die doktrinellen Ziele und Anforderungen an sie.[272]

Damit lässt sich dieser Krieg schon etwas eindeutiger als Informationskrieg klassifizieren, als dies noch 1990/91 der Fall war. Der höhere Anteil an Präzisionsmunition, die Aussparung ziviler Infrastruktur (soweit möglich) und das gemeinsame koordinierte Vorgehen der Teilstreitkräfte zeugen von einer neuen Qualität der Kampfhandlungen, die aber sicher noch nicht überall erreicht werden konnte. Gegen diese Klassifizierung spricht die Tatsache, dass immer noch knapp 30% der Waffen nicht präzisionsgelenkt und damit auf breite Vernichtung ausgerichtet waren. Ob diese Art der Waffen aber jemals ganz aus Konfliktszenarien verschwinden wird, bleibt zu hinterfragen. Weiters ist als Gegenargument anzuführen, dass die Organisation der Streitkräfte abseits der technologischen Vernetzung und des neuen Komplexitätsmanagement nicht für die vernetzte Operationsführung optimiert war und der Einsatz der Stryker Brigade als Referenzorganisation erst nach dem eigentlichen Krieg erfolgt ist. Damit bleibt wieder die Ungewissheit, wie dieser Konflikt einzuschätzen ist, was für unsere Untersuchung an dieser Stelle aber ohnehin nicht relevant ist und wir hier auch nicht beantworten wollen. Was wir aber durchaus erkennen können, sind wesentliche Elemente des Informationskrieges, die vielleicht dem Krieg im Gesamten selbst noch keine neue Qualität verleihen, ihn aber sicher entscheidend mitgeprägt haben.

---

[271] Artikel *Irakkrieg*. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 28. September 2008, 19:53 UTC. URL: http://de.wikipedia.org/w/index.php?title=Irakkrieg&oldid=51259753 (Abgerufen: 6. Oktober 2008, 02:17 UTC)

[272] vgl. Reardon, Marc; Charlston, Jeffery, From Transformation to Combat – The First Stryker Brigade at War, Center of Military History, Washington, 2007, S71f

1.5.5. Zwischenfazit

Fassen wir Phase III an dieser Stelle noch einmal kurz zusammen. Wir haben festgestellt, dass die Entwicklung der Streitkräfte unter Bush wieder forciert wurde, auch unter dem Eindruck der globalen Bedrohung durch den internationalen Terrorismus. Die Transformation der Streitkräfte hin zu einer Zielstreitkraft 2020 steht dabei im Zentrum der Entwicklungen.
Von technologischer Seite haben wir wieder die Vernetzung der Truppen und vor allem die Implementierung eines globalen Informationsnetzwerks, dem Global Information Grid, festgestellt sowie die Einbindung von Geheimdiensten und anderen staatlichen Organisationen in dieses System. Die daraus resultierende Unschärfe in der Abgrenzung zwischen Militär und Zivilgesellschaft ist uns auch später immer wieder begegnet.
Wir haben weiters die zentralen Doktrinen der Joint Vision 2020 und der NCW beleuchtet, die zwar ursprünglich an die AirLand Battle Doktrin anknüpfen, aber dennoch neue Maßstäbe setzen. Die Forderung nach globaler Machtprojektion und Vernetzter Operationsführung hat neben den technologischen C4I-Systemen auch klare organisatorische Auswirkungen und wir erkennen Dezentralisierung, Verkleinerung der Einheiten, Modularisierung, die Schaffung neuer Führungseinrichtungen, die Tendenz zu flacheren Hierarchien sowie die neue Dimension von Informationsoperationen auf einer breiten, zum Teil nicht-militärischen Basis. Auch hier verschwimmen wieder die Grenzen und die militärische Konfliktführung geht auf den zivilen Bereich über.
Wir haben auch die neuen Anforderungen an das Komplexitätsmanagement vor allem in Hinblick auf die Führung dargelegt, die ebenfalls eine neue Dimension erreicht. Die zukünftigen Herausforderungen an Kommandanten machen den Führungsvorgang als solches noch komplexer und fordern dem Menschen wesentlich mehr ab, als dies in der Vergangenheit der Fall war.
Abschließend haben wir kurz den Afghanistan- und Irakkonflikt beleuchtet und festgestellt, dass wir auch hier neue, in dieser Größenordnung bis dato unbekannte Elemente des Informationskrieges finden, auch wenn wir diese Kriege als solche nicht klassifizieren wollen.

In Summe präsentiert sich uns der Informationskrieg auf einer neuen, höheren Ebene, und wir können durchaus sagen, dass er eine neue, bisher unbekannte Dimension erreicht hat.

1.6. Schlussbetrachtung

Zusammenfassend haben wir mit dieser Untersuchung die Entwicklung des Informationskrieges in den letzten 30 Jahren verfolgt. Wir werden nun versuchen, die eingangs gestellten Forschungsfragen anhand der Ergebnisse der Analyse zu beantworten.

1.6.1. Wie haben sich Doktrinen bereits durch den Einfluss des Informationskrieges verändert?

Ausgehend von der AirLand Battle Doktrin, die wir als Ursprung des Informationskrieges identifiziert haben, haben wir dargelegt, dass die Entwicklung des Informationskrieges und sein Einfluss auf die Doktrinen im Verlauf der einzelnen Phasen deutlich zugenommen haben. Wir haben gezeigt, dass der Fortschritt vor allem in den 1990er Jahren viele doktrinelle Dokumente hervorgebracht hat, die das Wesen des Informationskrieges abgebildet und entscheidend weiterentwickelt haben. Mit der Joint Vision 2010, vor allem aber mit dem FM 100-6 Information Operations, hat der Informationskrieg bereits Mitte der 1990er Jahre eine neue Ebene erreicht und ist zu jenem systemimmanenten, homogenen Gesamtkonzept erwachsen, das fortan alle militärischen Entwicklungen entscheidend prägen sollte. Mit der Joint Vision 2020 und der NCW-Doktrin hat der Informationskrieg, wie wir ebenfalls dargelegt haben, eine neue Dimension erreicht, da er durch diese Dokumente ganz massiv und deutlich erkennbar Einfluss auf die Organisation der Streitkräfte und die hierarchische militärische Ordnung genommen hat. Die Vernetzung der Truppen, die Installation der operativ-taktischen Führung auf Brigadeebene, die Modularität der Truppen und die Verflachung des hierarchischen Systems sind hier als wesentlichste Punkte anzuführen. Die operativen Grundsätze der AirLand Battle, nämlich das mehrdimensionale Schlachtfeld, die Initiative, die Tiefe, die Synchronisation der Kräfte und die Beweglichkeit der Führung sind dabei im Kern bis heute erhalten geblieben und wurden durch neue Grundsätze wie der *full spectrum dominance* oder der *information superiority* ergänzt. Der operative Bewegungskrieg, der durch die AirLand Battle zu ihrer Zeit neu definiert wurde, hat also eine beeindruckende Entwicklung genommen und der Informationskrieg ist anhand der Doktrinen durchaus messbar geworden.

Allerdings bleibt kritisch anzumerken, dass noch nicht erwiesen ist, ob diese Art der Kriegsführung auch wirklich das hält, was sie verspricht. Die untersuchten Konflikte haben zwar jeweils entscheidende Elemente des Informationskrieges zu Tage gefördert und den Grad der „Informatisierung“ der Kriegsführung veranschaulicht, allerdings bleibt nach wie vor die Frage offen, wie sich ein solcher Konflikt entwickelt, wenn sich zwei Gegner mit nahezu gleichen Fähigkeiten und Kapazitäten gegenüberstehen. Weiters besteht durch die massive Abstützung auf Vernetzung, Digitalisierung und Informationssystemen die Gefahr, dass die Streitkräfte ihr ursprüngliches Handwerk verlernen und bei Ausfall dieser Technologien kampfunfähig werden.
Es ist immer noch der Soldat selbst, der den Schuss abfeuert und immer noch der Kommandant, der die Befehle dazu gibt. Daran wird auch die technologische Hochrüstung, Vernetzung der Truppen und Abflachung der Hierarchien zumindest in naher Zukunft nichts ändern. Die Virtualisierung des Krieges mag aber Kommandanten vergessen lassen, dass es Menschen sind, die sie auf ihren elektronischen Lagekarten verschieben. Dies im Bewusstsein zu halten wird eine der großen Herausforderungen abseits aller geopolitischen Entwicklungen an die Streitkräfte der Zukunft sein.

1.6.2. Wo ist der Informationskrieg im Militär bereits messbar?

Wir sind in unserer Untersuchung von der Beurteilung der Kriterien Technologie, Komplexitätsmanagement und Organisation, Strategie, Dezentralisierung etc. ausgegangen. Dabei haben wir dargelegt, dass gegen Ende unseres Untersuchungszeitraumes der Informationskrieg in all diesen Kriterien deutlich erkennbar wurde. Vor allem in den Doktrinen der Streitkräfte, aber auch im Komplexitätsmanagement und der Führung finden wir klare Elemente des Informationskrieges, die über den bloßen Einsatz von Technologie hinausgehen.

Der Informationskrieg hat sich im Militär also auf mannigfaltige Weise manifestiert. Wir haben festgestellt, dass wir ihn in allen Bereichen, von der operativen Einsatzführung bis hin zur Logistik, aber auch darüber hinaus in den fließenden Übergängen zur Zivilgesellschaft finden. Die Grenze, die Arquilla und Ronfeldt hier zwischen Netwar und Cyberwar ziehen und von der wir ebenfalls ausgegangen sind, scheint daher gar nicht so eindeutig zu sein und einmal mehr erkennen wir den Einfluss des Informationskrieges auf alle Bereiche der Gesellschaft.

1.6.3. Welche Kriterien könnte man für zukünftige Beurteilungen ableiten?

Ein allgemein gültiges Modell für zukünftige Beurteilungen der militärischen Kriegsführung zu erstellen, ist aufgrund der großen Bandbreite und der Unschärfe in der Abgrenzung zwischen militärischem und zivilem Bereich nur sehr schwer möglich. Abgeleitet aus unserer Untersuchung lassen sich aber durchaus Elemente definieren, die für weitere Untersuchungen hilfreich sein könnten. Diese wären:

- Grad der Vernetzung der Truppen
- Anteil an Informationsoperationen
- Einsatz von Führungsinformationssystemen
- Auswirkungen auf hierarchische Abläufe und Führungsstruktur
- Kampf gegen die Führung
- Kampf im Verbund
- Doktrinen und Strategiepapiere
- Größe der Verbände
- Organisation der Verbände
- Ebene der operationellen und taktischen Führung
- Grad der horizontalen Hierarchie
- Operative Grundsätze wie Informationsüberlegenheit und full spectrum dominance
- Selbstsynchronisation
- Dezentralisierung
- Hochmoderne voll integrierte Sensor- und Waffenplattformen

1.6.4. Wo finden wir bereits einen echten und umfassenden Informationskrieg?

Wie wir im Laufe der Untersuchung bereits dargelegt haben, finden wir bis dato keinen Konflikt, der sich eindeutig als Informationskrieg klassifizieren lässt. Die untersuchten Beispiele waren die größten Konflikte in den jeweiligen Phasen und natürlich ließen sich grundsätzlich Elemente des Informationskrieges finden. Der

Zweite Golfkrieg hatte zwar eine Katalysatorwirkung auf die Entwicklung des Informationskrieges, weil erstmals die neuen operativen Grundsätze mit fulminantem Erfolg zur Anwendung gebracht wurden, aber wir haben dargelegt, warum wir ihn nicht eindeutig klassifizieren können. Das zweite große Referenzbeispiel, der Dritte Golfkrieg, hat uns ein ähnliches Bild geboten. Wieder war die technische und operative Überlegenheit der Streitkräfte offensichtlich, aber dennoch hatte auch dieser Konflikt immer noch Elemente konventioneller Kriege, auch wenn wir hier das in Phase I fehlende Gesamtkonzept klar erkennen können. So scheint auch eine Klassifizierung dieses Konflikts nicht eindeutig möglich zu sein, vor allem auch weil wir uns ja die Frage nach dem umfassenden Informationskrieg gestellt haben. Daher ist eine Beantwortung dieser Frage nicht eindeutig möglich.

1.6.5. Sonstiges

Was wir aber ableiten können, ist die Geschwindigkeit der Entwicklungen und diese können wir durchaus auch in Zusammenhang mit den Konflikten bringen. Es ist nämlich auffallend, dass nach dem Krieg am Golf 1990/91, als die amerikanischen Streitkräfte in keinem größeren Konflikt mehr gebunden waren, die Entwicklung des Informationskrieges sehr rasant von statten ging. Innerhalb von nur wenigen Jahren ging man von der AirLand Battle zur Joint Vision 2010 und kurz darauf zur Joint Vision 2020 und der Network Centric Warfare über. Wenn wir dies nun in Zusammenhang mit den Ergebnissen der Untersuchung bringen, so stellen wir fest, dass es innerhalb von knapp zehn Jahren einen echten Quantensprung in der Entwicklung gab, in dem alle Elemente des Informationskrieges nach Libicki oder Arquilla/Ronfeldt in doktrinellen Konzepten zumindest angesprochen wurden. Der Vergleich zu Phase III zeigt uns, dass der Fortschritt hier wesentlich langsamer vor sich ging. Die Einführung neuer technischer Systeme hinkte dem Stand der Doktrinen nach, neue Organisationsformen wurden nur zögerlich eingenommen und Restrukturierungen für die Vernetzte Operationsführung, wie die Modularisierung der Brigaden, sind bis heute nicht vollständig umgesetzt. Dies liegt unter anderem auch daran, dass die Streitkräfte der USA sich in Afghanistan und im Irak in zwei nach wie vor sehr intensiven Konflikten befinden, die den Fortschritt in Richtung der voll vernetzten Streitkraft bremsen.

Weiters war, für die Beurteilung nach den definierten Kriterien zwar nicht relevant, aber dennoch, die starke Betonung des Faktors „Mensch“ in den Strategiepapieren Joint Vision 2010 und Joint Vision 2020 auffallend. Immer wieder wurde in beiden Dokumenten auf die Bedeutung der Soldaten und der Angehörigen der Streitkräfte hingewiesen, sei es die Qualität der Kommandanten oder die Anforderungen an die Soldaten selbst. So heißt in der JV 2010 „*The courage and heart of our soldiers, sailors, airmen, and marines will remain the foundation of all that our Armed Forces must do.*“[273] und weiter in der JV 2020: „*The core of the joint force of 2020 will continue to be an All Volunteer Force composed of individuals of exceptional dedication and ability. Their quality will matter as never before as our Service members confront a diversity of missions and technological demands that call for adaptability, innovation, precise judgment, forward thinking, and multicultural understanding.*“[274] Dies ist insofern bemerkenswert, da sich hier auch der Kreis zu

[273] Joint Vision 2010, Department of Defense, 1996, S.28
[274] [274] Shelton, Henry, General, Chairman of the Joint Chiefs of Staff, Joint Vision 2020, US Government Printing Office, 2000, S.12f

Kapitel I/2 schließt, in dem wir unter anderem versucht haben, darzulegen, dass Führung mehr bedeutet als das Erteilen von Befehlen und wir hier weiters erkennen können, dass auch im Informationskrieg mit seiner Hochtechnologie und seinen modernen Waffensystemen, es immer noch der Mensch selbst ist, der die Basis der Kriegsführung darstellt.

2. Der Zusammenhang zwischen Führung, Doktrin und Technologie

Wir haben bereits in der Einleitung dieser Arbeit die Faktoren Führung, Doktrin und Technologie als wesentliche Elemente des Informationskrieges hervorgehoben und sind im Zuge der Arbeit immer wieder auf diese Aspekte gestoßen. In diesem Kapitel wollen wir nun den Zusammenhang zwischen diesen Elementen beleuchten und ein Modell zur Beschreibung des Verhältnisses zueinander finden. Zunächst wollen wir aber noch einmal kurz erörtern, warum der Faktor Führung in diesem Zusammenhang ebenfalls als gleichwertig zu betrachten ist.

2.1. Warum Führung?

Wie wir eingangs dieser Arbeit bereits festgestellt haben, geht die Militärwissenschaft grundsätzlich davon aus, dass Technologie und Doktrin in einem sehr engen Verhältnis zueinander stehen. Weiters haben wir die Definition der Schweizer Zeitschrift Air Revue aufgegriffen, die besagt, dass ein gemeinsamer Entwicklungsschritt beider Faktoren eine Revolution auslöst. Anhand des Beispiels des Blitzkrieges haben wir dann kurz begründet, warum die Führung ebenfalls in diese Gleichung einzubringen ist.

Diese Begründung mag für den Moment ausreichend gewesen sein, allerdings greift sie im Sinne der Thematik vielleicht ein wenig zu kurz. Führung ist einer der alltäglichen und zentralen Vorgänge im Militär und jede Maßnahme, die gesetzt, jeder Befehl der gegeben, jeder Auftrag der erteilt wird, ist grundsätzlich das Ergebnis eines Führungsverfahrens. Führung ist aber, wie gesagt, mehr als nur das Erteilen von Befehlen und Aufträgen und wie wir in Kapitel I/2.8 festgestellt haben, ist auch die Menschenführung wesentlicher Teil des Ganzen. Dies wird auch durch das Ergebnis unserer Untersuchung der Doktrinen in Kapitel II/1 durch die Betonung des Faktors Mensch untermauert. Führung ist aber auch Teil des Informationsmanagement sowie des Battle Management am Schlachtfeld und gerade hier zeigt sich, wie wichtig dieser Faktor eigentlich ist. Die angestrebte Informationsüberlegenheit dient vereinfacht formuliert eigentlich nur dazu, Führungsüberlegenheit zu erreichen, um in weiterer Folge Wirkungsüberlegenheit herzustellen. Wie wir bereits festgestellt haben bildet Führung also eine Grundlage im Informationskrieg, ähnlich einer Doktrin oder der Technologie.
Deshalb und vor allem auch weil wir den Krieg als solches nicht auf die reine technologische oder doktrinelle Ebene abstrahieren und damit eine „Entmenschlichung“ des Krieges in Kauf nehmen wollen, nehmen wir die Führung in diese Gleichung auf.

2.2. Wie sieht der Zusammenhang zwischen Führung, Doktrin und Technologie aus und wie lassen sich Entwicklungen in der Kriegsführung anhand eines Modells beschreiben?

Wie wir bereits zu Beginn der Arbeit erkannt haben, befinden sich die Faktoren Führung, Doktrin und Technologie in einer ständigen Wechselbeziehung. Diese Beziehung finden wir im Zusammenhang mit dem Informationskrieg immer wieder und sogar die von Arquilla/Ronfeld abgeleiteten und für unsere Untersuchung relevanten Punkte des „Cyberwar“ lassen sich auf diese drei Faktoren fokussieren, wie wir in Kapitel I/3.3 dargestellt haben.

Diese Wechselbeziehung dreier gleichberechtigter Elemente lässt sich am besten, wie wir ebenfalls schon zuvor angedeutet haben, als Dreiecksbeziehung beschreiben. Dieses Dreieck soll auch unser Modell für die weitere Behandlung dieses Themas sein.

2.3. Wo lässt sich aus diesem Zusammenhang ein Ansatz für eine Definition für Revolutionen in Militärischen Angelegenheiten finden?

Ausgehend vom Grundsatz, dass eine Revolution immer dann stattfindet, wenn Technologie und Doktrin einen gemeinsamen Entwicklungsschritt vollziehen, wollen wir dieses Prinzip nun um unsere Dreiecksbeziehung erweitern, indem wir die Hypothese aufstellen, dass ein gemeinsamer Entwicklungsschritt von zwei dieser drei Faktoren immer auch den dritten Faktor zu einer Entwicklung anregt. Diese Hypothese wollen wir anhand von drei Beispielen zu bestätigen versuchen und wir halten fest, dass die Hypothese nur dann als erfüllt gilt, wenn alle möglichen Kombinationen auch exemplarisch belegt werden können.

(1) Technologie und Führung schaffen Doktrin

Die erste Beziehung zwischen Technologie und Führung, die über einen gemeinsamen Schritt eine neue Doktrin impliziert, haben wir bereits in Kapitel I/2 in Zusammenhang mit dem Blitzkrieg behandelt. Wir haben unter Abstützung auf Frieser dargelegt, dass erst durch das flexible und für diese Zeit untypische Führungssystem mit seiner ausgeprägten Auftragstaktik und dem Einsatz neuer Technologie wie der Panzerwaffe an sich bzw. der Ausstattung derselben mit Funksystemen in jedem Fahrzeug die operativen Fähigkeiten soweit gesteigert werden konnten, dass der Blitzkrieg letztendlich zur Doktrin erhoben wurde. Wir können diese Bedingung daher als erfüllt ansehen.

(2) Technologie und Doktrin schaffen Führung

Auch diese Beziehung haben wir bereits kennen gelernt und zwar in Zusammenhang mit der Network Centric Warfare. Die Doktrin der Vernetzten Operationsführung und der Einsatz neuer Informationstechnologien haben eine Änderung im Führungssystem zur Folge, die sich unter anderem in der Ausprägung der Hierarchien niederschlägt. Der Übergang von einer vertikalen zu einer horizontalen Führungsstruktur und der damit verbundene Paradigmenwechsel ist an dieser Stelle als durch Doktrin und Technik erzwungener Entwicklungsschritt zu werten. Selbstsynchronisation und eine

extreme Flexibilisierung der Führungsverfahren sind weitere Indikatoren für die Richtigkeit dieser Beziehung.

(3) Doktrin und Führung schaffen Technologie

Für diese Beziehung wollen wir uns noch einmal kurz mit der AirLand Battle Doktrin auseinandersetzen. Die neuen operativen Grundsätze aus dieser Doktrin wie das mehrdimensionale Schlachtfeld und der Einsatz von Verbundoperationen in Kombination mit neuen, auf diese Grundsätze adaptierten und somit entwickeltem Führungsverfahren haben, katalysiert durch den Irakkrieg, einen technologischen Entwicklungsschub am Sektor der Führungsinformationssysteme ausgelöst. Das Ziel der Joint Operations erforderte neue Technologien, um das Informationsmanagement zu optimieren und Effizienzsteigerungen zu erreichen. Als weiteren Indikator können wir aber auch noch einmal das Beispiel der NCW bemühen. Die laufende Implementierung des Global Information Grid ist ebenfalls eine klare Folge aus der NCW-Doktrin und dem aktuellen, modernen Führungssystem der Streitkräfte.

Anhand dieser drei Beispiele, die übrigens zeitlich mit unserer Untersuchung aus Kapitel II/1 korrelieren, lässt sich die aufgestellte Hypothese anschaulich belegen. Das bedeutet, dass wir in diesem Sinne jede Entwicklung in der Kriegsführung anhand dieses Modells messen können und unsere Definition einer Revolution aus Kapitel I/3 für diese Arbeit Gültigkeit hat.

Allerdings wollen wir hier nicht in die vielschichtige Diskussion um Revolutionen in Militärischen Angelegenheiten einsteigen. Wir haben uns mit diesem Thema ja bereits in Abschnitt I befasst. Unsere Definition soll lediglich ein für diese Arbeit und für eventuelle zukünftige Untersuchungen gültiges Modell zeichnen, anhand dessen wir den Informationskrieg durchaus als Revolution verstehen können.

3. Fazit

Abschließend wollen wir noch einmal auf den Informationskrieg zurückkommen und ein Gesamturteil fällen.

Wir haben im Zuge dieser Arbeit die neuen Konzepte zur Kriegsführung kennen gelernt und festgestellt, dass Krieg und Frieden, Militär und Zivilgesellschaft längst nicht mehr so klar voneinander abzugrenzen sind. Mit der Entwicklung der Gesellschaft hin zu einer Informationsgesellschaft hält auch der Krieg in unser aller Leben Einzug und zukünftige Generationen werden sich auch die Frage nach Rüstungskontrolle und Beschränkungen in diesem Bereich stellen müssen. Zu Beginn des 21.Jahrhunderts präsentiert sich uns der Krieg in einer völlig neuen Gestalt und die Beherrschung dieser Gestalt wird eine der Herausforderungen an die Zukunft sein.

Der Informationskrieg manifestiert sich indes in sämtlichen aktuellen Doktrinen des Militärs. Er ist im Militär bereits systemimmanent geworden und bestimmt Denkmuster, Handlungsweisen und Organisation des Militärs. Er schlägt sich auf die militärische Führung nieder und bricht Hierarchien auf. Die laufende Anpassung im Sinne der Transformation der Streitkräfte trägt dabei dem hohen Tempo dieser Entwicklungen Rechnung und im Moment kann man nicht erkennen, wohin uns der Fortschritt noch führen wird.

Die möglichen Auswirkungen auf die militärische Operationsführung lassen viel erwarten und die Zeit der großen industrialisierten Schlachten, wie wir sie noch im Zweiten Weltkrieg und in den Planspielen des Kalten Krieges finden, dürfte endgültig vorbei sein. Mit dem Informationskrieg scheint eine Art der Konfliktführung möglich, die ein Mindestmaß an Letalität und Zerstörung aufweist und dennoch denselben Machtfaktor besitzt wie vergangene Kriege.

Die Visionen, die wir alle kennen, reichen dabei von chirurgischen Operationen ohne Kollateralschäden bis hin zur Automatisierung des Krieges und seiner Austragung durch Maschinen. Dass diese Visionen nicht real sind und insbesondere die Automatisierung des Krieges eine völlige Fehleinschätzung des Informationskrieges ist, wie bereits Arquilla/Ronfeld festgestellt haben, ist dabei wie ich meine das geringere Problem. Durch das Verschwimmen der Grenzen zwischen Krieg und Frieden sowie Militär und Zivilgesellschaft besteht die Gefahr, dass der Krieg allgegenwärtiger und immanenter Teil unserer Gesellschaft wird und damit auch die Hemmschwelle sinkt, Kriege zu führen.

Abseits aller Visionen und Möglichkeiten, die der Informationskrieg bietet und noch bieten wird, ist er immer noch ein Krieg, und damit die abzulehnende Anwendung von Gewalt in ihrer stärksten Form.

Krieg muss daher auch in Zukunft nur das allerletzte Mittel zur Austragung von Differenzen bleiben und er muss auch in Zukunft Staaten vorbehalten sein. Dies kann nur durch ein entsprechendes Bewusstsein der Gesellschaft und entsprechende Maßnahmen zur Kontrolle erreicht werden. Dieses Bewusstsein zu schaffen, wird auch Aufgabe des Militärs selbst sein, liegt aber im Informationszeitalter genauso in der Eigenverantwortung jedes Einzelnen. Denn die eigentliche Gefahr, die der Informationskrieg darstellt, liegt nicht in den Möglichkeiten, die diese Art der Konfliktaustragung militärisch und zivil bietet, sondern im Menschen selbst, oder um es mit den Worten des Papstes Paul VI. auszudrücken: *"Frieden bedeutet, dass der Mensch aufhört, sich als Wolf seinen Mitmenschen gegenüber zu gebärden."*

Literaturverzeichnis

Buchquellen und Publikationen:

Arnett, Eric; Welcome to Hyperwar zit. nach Arquilla, John; Ronfeldt, David; „Der Cyberkrieg kommt“ in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork, 1998

Arquilla, John; Ronfeldt, David; „Der Cyberkrieg kommt“ in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork, 1998

Blieberger, Johann et.al., Informatik, Dritte Auflage, SpringerWienNewYork, 1996

Bell, Daniel, Die nachindustrielle Gesellschaft, Frankfurt, New York, 1975 zit. nach (Bühl, Achim; Die virtuelle Gesellschaft; Westdeutscher Verlag, 1997)

Bell, Daniel, Die dritte technologische Revolution und ihre möglichen sozialökonomischen Konsequenzen, in: Merkur, 44 (1990) zit. nach (Hohls, Rüdiger; „Über die Werkbank zur tertiären Zivilisation“ in Europa und die Europäer. Quellen und Essays zur modernen Europäischen Geschichte; Stuttgart; Franz Steiner Verlag; 2005)

Bellin, D., Chapman G.(Eds): Computer in Battle – Will they Work?, Hartcourt Brace Jovanovich, Boston 1987 zit. nach (Simeoni, Thomas; War der Golfkrieg der erste Informationskrieg?, Diplomarbeit; Wien, 1997)

Bendrath, Ralph, Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Peter Bittner, Jens Woinowski (Hg.): Mensch - Informatisierung - Gesellschaft, Münster: Lit Verlag, 1999

Bühl, Achim; Die virtuelle Gesellschaft; Westdeutscher Verlag, 1997;

Clausewitz, Carl von, Vom Kriege, Insel Verlag, 2005

Stowasser J.M. et al., Der kleine Stowasser, 3.Auflage, Verlag Hölder-Pichler-Tempsky, 1991

Dodel, Hans; Häupler Dieter; Satellitennavigation, Hütig – Telekommunikation, 2004

Dodel, Hans; Satellitenkommunikation, dpunkt Verlag, 1999

Eckert, Dirk; Kölner Arbeitspapiere zur internationalen Politik Nr1/2001; Theorie und Praxis der Information Warfare in den USA, 2001

Fey, P., Informationstheorie, Berlin, 1968, zit. nach (Fleissner, Peter, et.al.; Der Mensch lebt nicht vom Bit allein; Europäischer Verlag der Wissenschaften, 2.Auflage, 1997)

Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006“, Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007

Fleissner, Peter, et.al.; Der Mensch lebt nicht vom Bit allein; Europäischer Verlag der Wissenschaften, 2.Auflage, 1997

Frieser, Karl Heinz, Blitzkrieg-Legende, Der Westfeldzug 1940; R.Oldenburg Verlag München, 1995;

Grechenig, Dipl-Ing. Dr., Thomas, at al., Software Engineering, 2.Auflage, 2004

Heraklit, 500vChr

Hofmann, Hans (Hrsg.), Führungs- und Informationssysteme, Probleme, Erfahrungen und Technologien im militärischen Bereich, Oldenburg R. Verlag Gmbh, 1982

Libicki, Martin C.; What is IW?; National Defense University; Library of Congress Cataloging-in-Publication Data; 1995;

Meurers, Mag., Bernhard, Führungsverfahren auf Ebene Brigade und Bataillon, Truppendienst Taschenbuch Nr. 46, Reihe Ausbildung und Führung, Verlag AV + Astoria Druckzentrum GmbH, Wien, 2004

Meurers, Mag., Bernhard, Führungs- und Organisationslehre, Truppendienst Taschenbuch Nr. 36, Reihe Ausbildung und Führung, Herold Verlag, Wien, 1998

Olischer, Ing., Josef; Koisser, AR, Ing., Leopold; Truppendiensttaschenbuch Nr. 17A, Elektronische Kampfführung, AV-Druck, 2003

Operation Enduring Freedom, The United States Army in Afghanistan, Center of Military History, 2003

Reardon, Marc; Charlston, Jeffery, From Transformation to Combat – The First Stryker Brigade at War, Center of Military History, Washington, 2007

Schildt, Gerhard Helge, Impulstechnik Grundlagen und Anwendungen, LYK-Informatiktechnik Gmbh, 2006

Siebert, Jörg, Führungssysteme zwischen Stabilität und Wandel. Gabler Verlag, 2006

Simeoni, Thomas; War der Golfkrieg der erste Informationskrieg?, Diplomarbeit; Wien, 1997

Stocker, Gerfried (Hrsg.), „Information.Macht.Krieg“ in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork, 1998

Jim Sourter/Loren Thompson, Army Vision and the Transformation of Land Power in the Next Century, in: Strategic Review, Vol.25(1997) 3 zit. nach (Fitschen, Patrick, Die „Transformation der US-Streitkräfte - Die Neuausrichtung der Streitkräfte der Vereinigten Staaten zwischen 2001 und 2006“, Analysen zur Sicherheitspolitik Bd1, Peter Lang, Frankfurt/Main, 2007)

Sun Tsu, Die Kunst des Krieges, S.14

The Military Balance 2005/06, International Institute for Strategic Studies, Oxford University Press, 2006

Tilford Earl H Jr, The Revolution of Military Affairs: Prospects and Cautions, Carlisle, Pa., 1995 (zit. nach Bendrath, Ralph, Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Peter Bittner, Jens Woinowski (Hg.): Mensch - Informatisierung - Gesellschaft, Münster: Lit Verlag, 1999)

Toffler, Alvin; Toffler, Heidi; Überleben im 21.Jhdt; Übersetzt aus dem Amerikanischen „War and Anti-War“ von Helmut Dierlamm et al. Deutsche Verlags Anstalt, 1994

Weigl, Ludwig, Strategische Einsatzplanung der NATO, Dissertation an der Universität der Bundeswehr München, Fakultät für Sozialwissenschaften, 2005

Weiguang, Shen; Der Informationskrieg; in Information.Macht.Krieg, Buch zur Ars Electronica 98; SpringerWienNewYork, 1998

Weizenbaum, Joseph, Die Macht der Computer und die Ohnmacht der Vernunft, Frankfurt, 1978 zit. nach (Bernhardt, Ute; Ruhmann, Ingo, Informatik und Militär, in Friedrich, J. et al (Hrsg.), Informatik und Gesellschaft, Spektrum u.a., Heidelberg, 1995)

Wiener, Friedrich, Dr., Truppendienst Handbook Nr.3, The Armies of the NATO Nations, First English Edition, Herold Publishers Vienna, 1987

Wiener, Friedrich, Dr., Truppendienst Taschenbuch Nr.3, Fremde Heere: Die Armeen der NATO Staaten, 4.Auflage, Verlag Carl Ueberreuter, 1973

Wolf, Wolfgang, Der Golfkrieg, Bernard & Graefe Verlag, Bonn, 1992

Militärische Publikationen:

BMLV Merkblatt, Das taktische Führungsverfahren, BMLV, 2001

Cebrowksi, Arthur, Vice Admiral US Navy, Network Centric Warfare, It’s Origins and Future, US Naval Institute, 1998

Cebrowski Arthur, Vice Admiral US Navy, The Implementation of NCW, Office for Force Transformation, Secretary of Defense, 2005

Cohen, S., William, Secretary of Defense, Annual Report to The President and The Congress, Department of Defense, 1999

Cohen, S., William, Secretary of Defense, Annual Report to The President and The Congress, Department of Defense, 2001

Dienstvorschrift für das Bundesheer, Die FM-Truppe, FMTS, 1986

Dienstvorschrift für das Bundesheer, Führungsbegriffe, BMLV, 2005

Feickert, Andrew, US Army’s Modular Redesign, Issues for Congress, Congressional Research Service, 2006

Field Manual 100-5 Operations, Headquarter Department of the Army, Washington, DC, 1982

FM 100-6 Information Operations, Department of the Army, 1996
The Military Balance 1996/97, International Institute for Strategic Studies, Oxford University Press, 1996

Joint Vision 2010, Department of Defense, 1996

Landesverteidigungsakademie, Handakt/Taktik, LAVAk, 2001

Militärstrategisches Konzept des Österreichischen Bundesheeres, BMLV, 2006

Network Centric Warfare, Department of Defense, Report to Congress, 2001

Pace, Peter, Chairman of the Joint Chiefs of Staff, Quadrennial Defense Review Report, Department of Defense, 2006

Shelton, Henry, Chairman of the Joint Chiefs of Staff, Quadrennial Defense Review Report, Department of Defense, 2001

Shelton, Henry, General, Chairman of the Joint Chiefs of Staff, Joint Vision 2020, US Government Printing Office, 2000

Zeitschriften:

Zeitschrift „Europäische Sicherheit“ Heft 2/2004, Artikel „Forum 2003 der Clausewitz-Gesellschaft“

Artikel „Doktrin und Technologie: Zwillings- oder Halbschwestern“ in Zeitschrift Air Power Revue der Schweizer Armee Nr.3, Beilage zur Allgemeinen Schweizerischen Militärzeitschrift ASMZ 12/2004;

Krepinevitch, zit. nach Air Power Revue der Schweizer Armee Nr.3, Beilage zur Allgemeinen Schweizerischen Militärzeitschrift ASMZ 12/2004

Schätz, Alfred; Nachrichtendienste im Transformationsprozess in Österreichische Militärzeitschrift; Ausgabe 4/2007;

Lauring, Mag., Bernhard, Network Centric Warfare, Österreichische Militärische Zeitschrift 6/2003

Gunzenhäuser, Max zit. nach ÖMZ, Österreichische Militärzeitschrift, Ausgabe 04/2007, Verlagspostamt Wien

Kaufmann, Stefan, „Electronic Soldier“ – Der Infanterist der Zukunft In: Der Offizier Nr3/3006

Benz Friedrich, Vernetzte Operationsführung in Zeitschrift Wehrtechnik V/2005

Moschin Andreas, Obstlt i Gst, Network Enabled Operations, Land Power Revue der Schweizer Armee Nr 3, Blg. zur ASMZ 12/2005

Commenda, Othmar, GenMjrdG, „Erste Erfahrungen, Erkenntnisse und Lehren“ in Truppendienst 1/1992, „Golfkrieg 90/91“, Herold Druck und Verlagsges. mbH, Wien, 1992

Fritz, Friedrich, „C3I – Alte Tatsachen, neue Dimensionen“ in Österreichische Militärische Zeitschrift, Heft 2/1993, Offsetdruck Carl Ueberreuterges. mbH., Wien, 1993

Theile, Burkhard, Dr., Implikationen für die Heeresrüstung 1955-2005 – Bundeswehr wandelte sich zur Einsatzarmee, Das Profil, Zeitung des Rheinmetall-Konzerns 3/2005

Neuneck, Götz, Scheffran, Jürgen, Die Grenzen technischer Kriegsführung, Spektrum der Wissenschaft 01/2000

Cebrowski Arthue, Vice Admiral US Navy, Network Centric Warfare, An Emerging Military Response to the Information Age, Military Technology 5/2003

Internet:

Capurro, Rafael, *Einführung in den Informationsbegriff*, URL: http://www.capurro.de/infovorl-kap3.htm#6.%20Das%20Capurrosche, (Abgerufen: 22.07.2007)

Hofkirchner/Fleissner nach CAPURRO, URL: http://www.capurro.de/infovorl-kap3.htm#6.%20Das%20Capurrosche, (Abgerufen: 22.07.2007)

Artikel *Schlacht bei Tannenberg (1914).* In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 5. Oktober 2008, 04:11 UTC. URL: http://de.wikipedia.org/w/index.php?title=Schlacht_bei_Tannenberg_(1914)&oldid=51484791 (Abgerufen: 6. Oktober 2008, 02:05 UTC)

Dirks, Ekhardt, *Die Schlacht von Tannenberg,* URL: http://www.tannenberg1914.de/ (Abgerufen: 6. Oktober 2008)

Artikel *Informationskrieg*. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 24. Mai 2008, 13:50 UTC. URL: http://de.wikipedia.org/w/index.php?title=Informationskrieg&oldid=46438284 (Abgerufen: 6. Oktober 2008, 02:12 UTC)

Artikel *Global Positioning System.* In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 5. Oktober 2008, 21:24 UTC. URL: http://de.wikipedia.org/w/index.php?title=Global_Positioning_System&oldid=51517918 (Abgerufen: 6. Oktober 2008, 02:14 UTC)

Decker Julio, *Seminararbeit Network Centric Warfare. Ein neues Konzept der Kriegsführung*, 2003, URL: http://www.politik.uni-koeln.de/jaeger/downloads/decker_ha.pdf, (Abgerufen: 21.04.2008)

URL: http://www.emeraldinsight.com/fig/0730130501001.png, (Abgerufen: 04.05.2008)

URL: http://www.fas.org/irp/program/collect/docs/pax_auvsi_1-2/sld033.htm, (Abgerufen: 08.05.2008)

Van den Berghe, F., Wiesendahl, U., *Funktionsweise der Network Centric Warfare*, 2003, URL: www.armscontrol.de/publikationen/ws0203ncw.pdf: (Abgerufen: 08.05.2008),

Artikel *Wie das Internet entstand* In: Bundesamt für Sicherheit und Informationstechnik, URL: http://www.bsi-fuer-buerger.de/internet/01_02.htm, (Abgerufen : 20.08.2008)

URL: http://www.internet4jurists.at/intern1a.htm, (Abgerufen: 20.08.2008)

Bendrath, Ralph, *Krieger in den Datennetzen*, URL: http://www.heise.de/tp/r4/artikel/7/7892/1.html, 2001 (Abgerufen: 6. Oktober 2008)

Artikel *The Evolution of the AirLand Battle Concept*, In: Air University Review 1984, URL: http://www.airpower.maxwell.af.mil/airchronicles/aureview/1984/may-jun/romjue.html (Abgerufen: 6.Oktober 2008)

Artikel *History of ISEC,* In: US Army Information Systems Engineering Command, URL: http://www.hqisec.army.mil/isec/about/history.asp, (Abgerufen: 20.08.2008)

Pflüger, Thomas, *Neue Armeen für neue Aufgaben* In: Netzwerk Friedenskooperative, Friedensforum 1/1999, Kommission Zukunft der Bundeswehr, URL: http://www.friedenskooperative.de/ff/ff99/1-23.htm, (Abgerufen: 15.09.2008)

Artikel *Force XXI* In: globalsecurity.org, URL: http://www.globalsecurity.org/military/agency/army/force-xxi.htm, (Abgerufen: 17.09.2008)

Artikel *Transformation of the United States Army.* In: Wikipedia, The Free Encyclopaedia*,* 29 September 2008, 15:00 UTC, URL: http://en.wikipedia.org/w/index.php?title=Transformation_of_the_United_States_Army&oldid=241780624 (Abgerufen: 6. Oktober 2008, 02:28 UTC)

Artikel *United States Army.* In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 30. September 2008, 10:24 UTC. URL: http://de.wikipedia.org/w/index.php?title=United_States_Army&oldid=51315323 (Abgerufen: 6. Oktober 2008, 02:26 UTC)

Bush Jr, George, *Remarks by the President to the Troops and Pesonnel,* Norfolk Naval Air Station, 2001, URL: http://www.whitehouse.gov/news/releases/20010213-1.html, (Abgerufen: 20.09.2008)

Blancke, Stephan, *Information Warfare*, in: Aus Politik und Zeitgeschichte 30-31/2005, Bundeszentrale für politische Bildung, URL: http://www.bpb.de/publikationen/YAPI1Y,0,Information_Warfare.html, (Abgerufen: 20.09.2008)

Artikel *Häufig gestellte Fragen zur Vernetzten Operationsführung*, URL: http://www.luftwaffe.de/portal/a/luftwaffe/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLNzKId_cJAclB2QH6kZiiXs5IokEpqfre-r4e-bmp-gH6BbmhEeWOjooAVm-

y1A!!/delta/base64xml/L2dJQSEvUUt3QS80SVVFLzZfMjBfSDk3?yw_contentURL=/01DB060000000001/W26KYHBK713INFODE/content.jsp, (Abgerufen: 21.09.2008)

Artikel *Irakkrieg*. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 28. September 2008, 19:53 UTC. URL: http://de.wikipedia.org/w/index.php?title=Irakkrieg&oldid=51259753 (Abgerufen: 6. Oktober 2008, 02:17 UTC)

Fraunhofer Institut Intelligente Analyse und Informationssysteme, URL: http://www.iais.fraunhofer.de/ps.html (Abgerufen: 11.10.2008);

Linke, Peter, Artikel *Ungleichgewicht des Schreckens* In Freitag, 16.02.2001 URL: http://www.freitag.de/2001/08/01080901.htm (Abgerufen: 11.10.2008);

Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr, *German Improved Air Defence System (GIADS)*, URL: http://www.it-amtbw.de/portal/a/itamtbw/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLNzKKN_Sy8AFJgjlejoH6kQjhoJRUfV-P_NxUfW_9AP2C3IhyR0dFRQCzn0K2/delta/base64xml/L3dJdyEvd0ZNQUFzQUMvNElVRS82XzIyXzFKOEw! (Abgerufen: 11.10.2008)

EADS, *Flugabwehrführungssystem SAMROC*, URL: http://www.eads.net/1024/de/businet/defence/dcs/solutions/air_defence%20Copy/samoc%20Copy/samoc%20Copy.html (Abgerufen: 11.10.2008)

Artikel *CL 289*. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 28. September 2008, 13:38 UTC. URL: http://de.wikipedia.org/w/index.php?title=CL_289&oldid=51246563 (Abgerufen: 13. Oktober 2008, 01:15 UTC)

Abkürzungsverzeichnis

(D)ARPA	(Defense) Advanced Research Project Agency
ABCS	Army Battle Command System
AEGIS	Airborne Early Warning Ground Environment Integration System
ALB	AirLand Battle
AO	Area of Operation
ATCCS	Army Tactical Command Control System
BCT	Brigade Combat Teams
BFR	Base Force Review
BMLV	Bundesministerium für Landesverteidigung
BUR	Bottom-Up Review
C2W	Command and Control Warfare
C4ISR	Command, Control, Communication, Computer, Intelligence, Surveillance, Reconnaissance
CA(O)	Civil Affairs (Operation/Officer)
CBRNE	Chemical, Biological, Radiological/Nuclear, Explosive Incidents
CCIS	Command and Control Information System
CEC	Cooperative Engagement Capability
CEWI	Combat Electronic Warfare Intelligence
CIA	Central Intelligence Agency
COMMINT	Communication Intelligence
CSA	Chief of Staff of the Army
CW	Cyber Warfare
DOD	Department of Defense
ECCM	Electronic Counter Counter Measures
ECM	Electronic Counter Measures
EIW	Economic Information Warfare
ELINT	Electronic Intelligence
EloAufkl	Elektronische Aufklärung
EloKa	Elektronische Kampfführung
EloSM	Elektronische Schutzmaßnahmen
EloUM	Elektronische Unterstützungsmaßnahmen
EMP	Elektromagnetischer Puls
EPM	Electronic Protection Measures
ESM	Electronic Support Measures
EU	Europäische Union
EVSP	Europäische Verteidigungs- und Sicherheitspolitik
EW	Electronic Warfare
EXFOR	Experimental Force
FBCB2	Force XXI Battle Command Brigade and Below System
FBI	Federal Bureau of Investigation
FM	Field Manual
FM	Fernmelde
FMAufkl	Fernmeldeaufklärung
FMTS	Fernmeldetruppenschule
FORSCOM	US Army Forces Command
FSCOORD	Fire Support Coordination
GASP	Gemeinsame Aussen- und Sicherheitspolitik
GCCS	Global Command and Control System

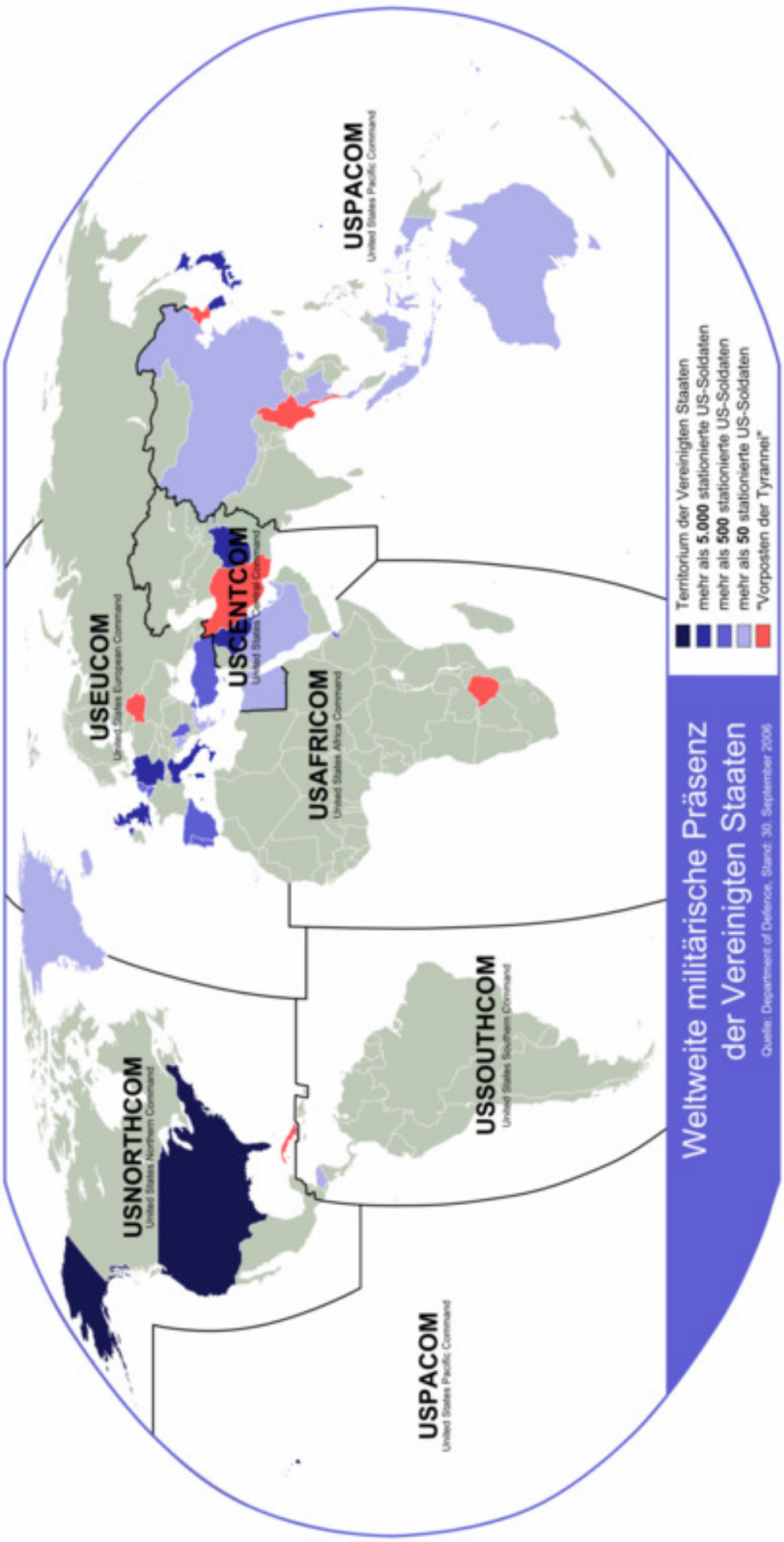
GenMjrdG	Generalmajor des Generalstabs
GIG	Global Information Grid
GPS	Global Positioning System
HIC	High Intensity Conflicts
HQDA	Headquarter Department of the Army
HUMINT	Human Intelligence
HW	Hacker Warfare
IBCT	Interim/Infantry Brigade Combat Teams
IBW	Intelligence Based Warfare
JCS	Joint Chiefs of Staff
JFCCNW	Joint Functional Component Command for Network Warfare
JSTARS	Joint Surveillance Target Attack Radar System
JV	Joint Vision
LAN	Local Area Network
LAVAk	Landesverteidigungsakademie
LEO	Low-Earth-Orbit
LIC	Low Intensity Conflicts
LIWA	Land Information Warfare Activity
MACOM	Major Command
MHV	Miniature-Homing-Vehicle
MIC	Mid Intensity Conflicts
MIPS	Military Intelligence Processing System
MIS	Management Information System
NATO	North Atlantic Treaty Organisation
NCA	National Command Authority
NCW	Network Centric Warfare
NEC	Network Enabled Capabilities
NGO	Non-Governmental Organisation
NSA	National Security Agency
ÖBH	Österreichisches Bundesheer
ONA	Office for Net Assessment
OODA	Observe, Orient, Decide, Act
OPSEC	Operations Security
PA(O)	Public Affairs (Operation/Officer)
PDA	Personal Data Assistant
PSYOP	Psychological Operations
PSYW	Psychological Warfare
QDR	Quadrennial Defense Report
RMA	Revolution in/of Military Affairs
ROE	Rules Of Engagement
SECARM	Secretary of the Army
SJA	Staff Judge Advocate
STO	Special Technical Operations
STRATCOM	Strategic Command
TECHINT	Technical Intelligence
TRADOC	Training and Doctrine Command
UAV	Unmanned Air Vehicle
UCAV	Unmanned Combat Air Vehicle
UCC	Unified Combatant Command
UGV	Unmanned Ground Vehicle
US	United States

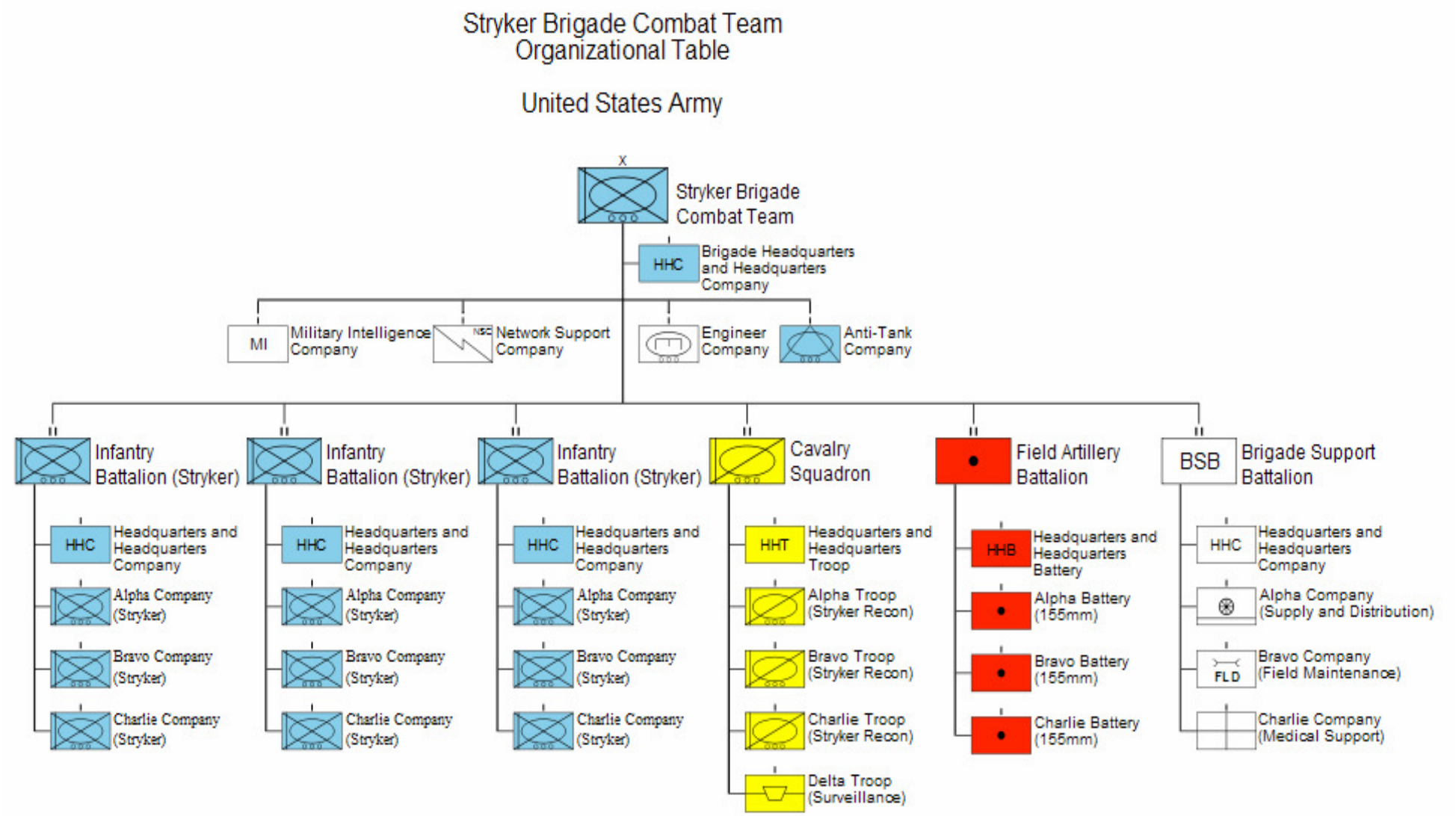
USAISC	US Army Information Systems Command
USCENTCOM	US Central Command
USEUCOM	US European Command
USJFCOM	US Joint Forces Command
USPACOM	US Pacific Command
USSOCOM	US Special Operations Command
USSOUTHCOM	US Southern Command
WAN	Wide Area Network

Abbildungsverzeichnis

Tabellen

ANHANG A


USPACOM
United States Pacific Command
USEUCOM
United States European Command
USCENTCOM
United States Central Command
USAFRICOM
United States Africa Command
USNORTHCOM
United States Northern Command
USSOUTHCOM
United States Southern Command
USPACOM
United States Pacific Command
Territorium der Vereinigten Staaten
mehr als 5.000 stationierte US-Soldaten
mehr als 500 stationierte US-Soldaten
mehr als 50 stationierte US-Soldaten
"Vorposten der Tyrannei"
Weltweite militärische Präsenz der Vereinigten Staaten
Quelle: Department of Defence, Stand: 30. September 2006


Stryker Brigade Combat Team
Organizational Table
United States Army
X
Stryker Brigade Combat Team
HHC
Brigade Headquarters and Headquarters Company
MI
Military Intelligence Company
NSC
Network Support Company
Engineer Company
Anti-Tank Company
Infantry Battalion (Stryker)
HHC
Headquarters and Headquarters Company
Alpha Company (Stryker)
Bravo Company (Stryker)
Charlie Company (Stryker)
Infantry Battalion (Stryker)
HHC
Headquarters and Headquarters Company
Alpha Company (Stryker)
Bravo Company (Stryker)
Charlie Company (Stryker)
Infantry Battalion (Stryker)
HHC
Headquarters and Headquarters Company
Alpha Company (Stryker)
Bravo Company (Stryker)
Charlie Company (Stryker)
Cavalry Squadron
HHT
Headquarters and Headquarters Troop
Alpha Troop (Stryker Recon)
Bravo Troop (Stryker Recon)
Charlie Troop (Stryker Recon)
Delta Troop (Surveillance)
Field Artillery Battalion
HHB
Headquarters and Headquarters Battery
Alpha Battery (155mm)
Bravo Battery (155mm)
Charlie Battery (155mm)
BSB
Brigade Support Battalion
HHC
Headquarters and Headquarters Company
Alpha Company (Supply and Distribution)
FLD
Bravo Company (Field Maintenance)
Charlie Company (Medical Support)