Olivier Minkwitz

Ohne Hemmungen in den Krieg?

Cyberwar und die Folgen

HSFK-Report 10/2003

Hessische
Stiftung
Friedens- und
Konfliktforschung

Für diese Studie wurden Titel der von der Deutschen Forschungsgemeinschaft geförderten Spezialsammlung „Außenpolitik der USA“ genutzt.

Adresse des Autors:

HSFK • Leimenrode 29 • 60322 Frankfurt
Telefon: +49(0)69/959104-0 • Fax: +49(0)69/558481
Email: minkwitz@hsfk.de
Internet: http://www.hsfk.de

ISBN: 3-933293-84-7

Euro 6,--

Zusammenfassung

Neue Militärtechnologien und Militärstrategien unterlaufen die demokratietypischen Hemmungen gegen die Anwendung militärischer Gewalt auf mehrfache Art und Weise. Sie senken materielle Kosten und politische Risiken der Kriegsführung. Demokratien, die an der Spitze dieser Entwicklung stehen, sind damit in der Lage, bewaffnete Konflikte zu führen, die nahezu risikolos für ihre Gesellschaften und Entscheidungsträger geworden sind. Die Hemmschwelle, das Militär als außenpolitisches Instrument einzusetzen, kann dadurch sinken. Mit Hilfe neuer Militärtechnologie wird das Einsatzrisiko heute für Soldaten demokratischer Streitkräfte reduziert. Mittels moderner Waffentechnologie wird der Gegner aus der Distanz bekämpft. Nicht nur das Risiko für die Streitkräfte nimmt ab, auch das gesellschaftliche, wirtschaftliche und politische Risiko sinkt, wenn Kriege kurz und erfolgreich geführt werden können. Gleichzeitig erhöht sich die Feuerkraft, Präzision und Geschwindigkeit der Streitkräfte enorm. Demokratische Gesellschaften und ihre Regierungen scheinen von den direkten Auswirkungen solcher Militäreinsätze verschont zu bleiben.

Neben dieser paradoxen Verwerfung, die der demokratietypische Wunsch nach Vermeidung von eigenen und fremden Opfern hervorbringt, lassen sich fünf kritische Entwicklungen identifizieren. Sie alle entspringen dem Wunsch nach Opfervermeidung und tragen erstens dazu bei, dass institutionelle Schranken fallen, die Demokratien die Entscheidung über Krieg und Frieden bislang erschwerten. Neue Militärtechnologien und Strategien, in der Form von Computernetzwerkangriffen führen zweitens zur Auflösung der Grenze zwischen Krieg und Frieden. Diese Grenze weicht einem militärisch-operativen Graubereich. Drittens machen es neue Technologien und Strategien möglich, dass moralische und völkerrechtliche Hemmungen bei der „präzisen" Zielplanung entfallen. Paradoxerweise entsteht die Möglichkeit, dass zivile Objekte angegriffen werden, weil dies vermeintlich präzise und ohne nennenswerte „Kollateralschäden" möglich ist. Viertens bringt die Vernetzung und Digitalisierung moderner Streitkräfte einen Verlust an politischer Kontrolle von Militäroperationen mit sich. Fünftens kann die klassische Rüstungskontrollpolitik die neuen militärischen Innovationen und die daraus folgenden neuen Rüstungsdynamiken nicht mehr einhegen. Nicht Waffensysteme sind der Kern der neuen Dynamik, sondern die „Strategie" der Vernetzung von Systemen und das Konzept der Transformation der Streitkräfte. Wenn aber Rüstungskontrolle als kooperativer Teil der Sicherheitspolitik entfällt, laufen Demokratien Gefahr, ihren Nimbus als rüstungskontrollorientierte und friedliebende Staaten zu verlieren.

Mit den neuen Möglichkeiten der Militärtechnologien geht andererseits der Versuch einher, Militäroperationen und ihre Verläufe noch weiter politisch-militärisch zu steuern. Sie sollen es möglich machen, eine noch nie dagewesene Übersichtlichkeit und Transparenz des Schlachtfeldes herzustellen. Der von Clausewitz beschriebene „Nebel des Krieges" soll damit gelichtet werden. Auf Friktionen, Risiken und Unwägbarkeiten, wie sie bislang noch in allen Kriegen vorkamen, sollen technologische Antworten in der Form komplexer, automatisierter „C4ISR"-Angriffssysteme gefunden werden. Ultimatives Ziel dieser Anstrengungen ist die Kontrolle des Kriegs in allen Aspekten. Dabei wird verkannt,

dass die Quellen von Friktionen auf dem Schlachtfeld nicht nur technischer Art sind, sondern im dynamischen Wesen des Krieges selbst liegen. Da ein Krieg nach Clausewitz letztlich aus zwei widerstreitenden Willen besteht, kann der Gegner sein „Veto" auch gegen die beste Strategie, Planung und Technologie einlegen.

Die neuen Militär*technologien* sind nicht alleine für die neue Dynamik verantwortlich. Eine solche Sichtweise erliegt leichtfertig einem technologischen Determinismus. Erst in Kombination mit neuen Militär*strategien* tragen sie das Potenzial in sich, die politische Hemmschwelle in Demokratien gegenüber dem Einsatz militärischer Gewalt zu senken. Militärstrategien bestimmen die Art und Weise, wie die von Demokratien gewählte Militär*politik* umgesetzt und in Konflikten angewendet werden soll. Sie geben in der Folge der Technologieentwicklung auch eine Richtung vor. So ist die gegenwärtige „Revolution in militärischen Angelegenheiten" („RMA") nicht allein ein Produkt neuer Technologien, sondern Resultat der Anpassung des militärischen Instruments an politische Zwecke. Erst die Einbettung der Technologieentwicklung in neue Militärstrategien, Doktrinen, Taktiken und Institutionen der Streitkräfte ermöglicht es, die Vorteile des technologischen Vorsprungs zu nutzen. Die neuen Militärstrategien, Konzepte und Visionen setzen dabei auf „Informationskriegsführung", „netzwerk-zentrische Kriegsführung" oder „effektbasierte Operationen". Ausgangspunkt dieser neuen Strategiekonzepte ist die Annahme, dass die „Informationsrevolution" auch die Art und Weise der Kriegsführung umgestaltet. Der Begriff „RMA" wird als Konzept verwendet, um die Veränderungen und Trends in der Kriegsführung durch Technologie, Strategie und Organisation zu beschreiben. Es lässt sich noch nicht absehen, ob die Trends wirklich „umwälzend" sind und alle alten Erfahrungen von Problemen und Friktionen in der Kriegsführung zunichte machen, oder ob die Trends nicht eher inkremental die Kriegsführung „transformieren". Die „RMA" ist kein historisch oder technologisch determinierter, sondern ein sozialer Prozess. Als solcher wird sie von handelnden Akteuren voran getrieben. Mit dieser Sichtweise auf die „RMA" wird sie von der Politik wieder beeinflussbar und regulierbar. Ob diese „RMA" wirklich revolutionäre Auswirkungen hat oder nur eine Evolution der Kriegsführung darstellt, ist letztlich zweitrangig.

Die Zukunft des Krieges ist nicht unbedingt die eines hochtechnologischen Krieges. Die Mehrzahl der Kriege wird, eher von niedriger Intensität sein und viel wahrscheinlicher die Form von Bürgerkriegen haben. Dennoch dürften Computernetzwerkangriffe am High-Tech-Ende des Konfliktspektrums eine Realität werden. Es zeichnet sich ab, dass die Streitkräfte westlicher Demokratien, unabhängig von den Konfliktszenarien, in friedenserhaltenden Einsätzen wie auch in konventionell geführten Kriegen auf Digitalisierung, Vernetzung und Präzisierung ihrer Truppen angewiesen sein werden.

Aus diesen Gründen empfiehlt der Report eine neue Rüstungskontrollpolitik. Sie soll ein rüstungskontrollpolitisches Umfeld schaffen, das es ermöglicht, neue Militärtechnologien und Strategien zum Gegenstand von Rüstungskontrolle zu machen. Die Schwierigkeiten einer solchen Politik liegen auf der Hand, dennoch bieten sich die folgenden Optionen an:

- Eine *deklaratorische Politik* der Selbstbeschränkung in Bezug auf „Informationsoperationen" und „Computernetzwerkangriffe"

- Eine „*No-First-Use*“ *Doktrin* in Bezug auf „Informationsoperationen“ und „Computernetzwerkangriffe“
- Einen „*Verhaltenskodex / Code of Conduct*“ im Umgang mit „Informationsoperationen“ oder die Schaffung einer „*Informationskriegsordnung*“
- *Informationsaustausch* und *vertrauensbildende Maßnahmen* in internationalen Gremien oder in bilateralen Beziehungen in Bezug auf Militärstrategien und Militärdoktrinen die „Informationsoperationen“ zum Gegenstand haben
- Die Verstetigung und Verdichtung solcher „weichen“ Rüstungskontrollbemühungen zu einem internationalen „*Informationsoperationsregime*“

Inhalt

1. Warum neue Militärtechnologien und Militärstrategien die Demokratien unfriedlicher machen könnten[1]

Gegenwärtig ermöglichen neue Militärtechnologien und -strategien den technologisch entwickelten Industrieländern eine Steigerung ihres Zerstörungspotentials jenseits der militärischen Verteidigungsfähigkeit anderer Staaten. Triebkraft hinter dieser Entwicklung ist eine „Revolution in militärischen Angelegenheiten" („RMA"). Sie verspricht eine Umwälzung in der Art und Weise, wie Kriege geführt werden. Paradoxerweise wird diese neue Rüstungsdynamik, die „RMA", gerade von Demokratien angestoßen und vorangetrieben. Dies ist insofern paradox, als in Demokratien andere gesellschaftliche Ansprüche mit der Rüstung um knappe Haushaltsmittel konkurrieren und Demokratien, die „Erfinder" der Rüstungskontrolle, traditionell am offensten gegenüber kooperativen Sicherheitsbemühungen gewesen sind.

Die „RMA" eröffnet Demokratien die Möglichkeit, sich williger für Militäroperationen zu entscheiden, weil sie geringe Risiken mit sich bringt und Verluste minimieren kann.[2] Sie nährt die Illusion vom sauberen Krieg. Neue Technologien und Strategien relativieren damit demokratietypische Hemmungen, die bislang dem Einsatz von Streitkräften entgegenstanden. Bestimmte Strategien eröffnen sogar die Möglichkeit unentdeckter militärischer Operationen zwischen Demokratien. Da sich diese Entwicklung im Anfangsstadium befindet, bestehen Möglichkeiten, diese Tendenzen mit einer neuen Rüstungskontrollpolitik als politischer Antwort einzuhegen. Allerdings ist die militärtechnologische Entfaltung der Entwicklung von neuen Normen und Regeln in der Rüstungskontrollpolitik einen Schritt voraus.

Dieser Report untersucht fünf problematische Entwicklungen für Demokratien, die mit den „Strategien der Informationskriegsführung" entstehen können. Der Report beschränkt sich in der Sache auf „Strategien der Informationskriegsführung", die sich auf das Führen von Militäroperationen durch Staaten auswirken (Kapitel 2). Er behandelt „Informationsoperationen" (IO), wenn diese eine operative Relevanz haben, d.h. wenn sie

1 „Antinomien des demokratischen Friedens" ist der Titel des laufenden Forschungsprogramms der HSFK, in dessen Rahmen dieser Report entstanden ist. Es geht der These nach, dass die Eigendynamik der Außen- und Sicherheitspolitik der Demokratien das Risiko birgt, die weithin unterstellte Friedensfähigkeit demokratischer Gemeinwesen zu neutralisieren. Für Kritik und Anmerkungen danke ich Prof. Dr. Harald Müller, Una Becker, Andreas Hasenclever, Bernd Kubbig, Hajo Schmidt, Niklas Schörnig, sowie Ralf Bendrath, Wanja Naef, Georg Schöfbänker und Anneke Gerloff.

2 Vgl. Seyom Brown, The Illusion of Control: Force and Foreign Policy in the Twenty-First Century, Washington, D.C. (Brookings Institution Press), 2003. Michael Ignatieff, Virtueller Krieg. Kosovo und die Folgen, Hamburg (Rotbuch), 2001. Niklas Schörnig, Demokratischer Friede durch überlegene Feuerkraft?, HSFK Standpunkt Nr. 3, Frankfurt a.M. (Hessische Stiftung Friedens- und Konfliktforschung) 2001. Harald Müller/Niklas Schörnig, "Revolution in Military Affairs" – Abgesang kooperativer Sicherheitspolitik der Demokratien?, HSFK Report Nr. 8, Frankfurt am Main (Hessische Stiftung Friedens- und Konfliktforschung) 2001. Harald Müller/Niklas Schörnig, Mit Kant in den Krieg?, in: Friedenswarte, Jg. 77, Nr. 4, 2003, S. 353-374. Bradley A. Thayer, The Political Effects of Information Warfare: Why New Military Capabilities cause Old Political Dangers, in: Security Studies, Jg. 10, Nr. 1, 2000, S. 43-85. Vgl. auch das Projekt der HSFK „Militärische Innovation und die Senkung der Kriegsschwelle" unter http://www.hsfk.de/project.php?id=410 (7.07.2003)

sich auf das Führen von militärischen Operationen direkt auswirken. Sogenannte „Hackerkriege“ oder „Cyberterrorismsus“ können höchstens theoretisch eine solche direkte Wirkung haben. Nicht behandelt werden daher „Informationsoperationen“ von substaatlichen Gruppen oder defensive „Informationsoperationen“, z.B. der Schutz kritischer Infrastrukturen. Ebenfalls nicht diskutiert werden Strategien zur Beeinflussung der Bevölkerung von Demokratien, deren Zustimmung und Wahrnehmung von Konflikten Grundvoraussetzungen dafür sind, dass demokratische Regierungen Kriege und Interventionen führen können, die nicht unmittelbar der Selbstverteidigung oder dem Überleben des Landes dienen. Ebenso bleibt der „Netzkrieg“ („Netwar“) außen vor, den Arquilla und Ronfeldt als neue Ebene des Konfliktspektrums einführen: „Netwar (...) means trying to disrupt, or damage or modify what a target population „knows“ or thinks it knows (...).“[3]

Der Report behauptet nicht, dass neue Technologien und Strategien automatisch und „quasi-kausal“ dazu führen, dass Demokratien mehr Kriege führen werden. *Stattdessen liegt dem Report die Hypothese zugrunde, dass neue Technologien und Strategien es den Demokratien erleichtern werden, auf militärische Gewaltanwendung als Mittel der Politik zurückzugreifen.* Der Report identifiziert fünf Risiken für die Friedfertigkeit von Demokratien, die durch „Strategien der Informationskriegsführung“ entstehen können. Sie betreffen die Kriegsführung von Demokratien und die Zukunft ihrer Rüstungskontrollpolitik. Zunächst beschreibt der Report aktuelle Probleme, Entwicklungen und Trends der neuen Strategien und Technologien (Kapitel 2). Dabei werden die Definitionen und der Stand der gegenwärtigen Entwicklung diskutiert. Im Hauptteil werden die fünf problematischen Mechanismen, die durch „Strategien der Informationskriegsführung“ für Demokratien aufgeworfen werden, ausführlich behandelt (Kapitel 3).

- Erstens vermindern „Strategien der Informationskriegsführung“ ganz allgemein die materiellen und moralischen Risiken konventioneller Kriegsführung für die eigenen Streitkräfte und Gesellschaften. Sie versprechen die Schonung der gegnerischen Zivilbevölkerung und senken damit auch die moralische Hemmschwelle, die einer Entscheidung für die militärische Intervention im Wege steht (Kapitel 3.1).
- Zweitens verwischen sie, z.B. in der Form von Computernetzwerkangriffen die Grenze zwischen Krieg und Frieden. Damit fällt die in Demokratien hohe institutionelle Hürde der Entscheidung über Krieg und Frieden (Kapitel 3.2).
- Drittens geht der Unterschied zwischen offensiver und defensiver Kriegsführung und zwischen ziviler und militärischer Zielplanung verloren (Kapitel 3.3).

3 John Arquilla/David Ronfeldt, Cyberwar is Coming!, in: John Arquilla/David Ronfeldt (Hg.), In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica (RAND) 1997, S. 23-60. S.28. Vgl. aktuell dazu *108th U.S. Congress, Senate,* Committee on Foreign Relations, American Public Diplomacy and Islam, Washington, D.C.: 27.2.2003.

- Viertens kann es zum Verlust ziviler Kontrolle über Militäroperationen durch Automatisierung und Digitalisierung kommen. Außerdem kann durch den Einsatz von „C4ISR“4 die Zahl ziviler Opfer paradoxerweise wieder ansteigen (Kapitel 3.4).
- Fünftens unterminieren „Strategien der Informationskriegsführung“ die traditionelle Rüstungskontrollpolitik von Demokratien (Kapitel 3.5).

Diese Risiken sind beeinflußbar und lassen sich vermindern. Um diese für Demokratien problematischen Entwicklungen aufzufangen, schlägt daher der Report im Anschluss neue rüstungskontrollpolitische Maßnahmen vor (Kapitel 4).

1.1 Die Wirkung von neuen Technologien und Strategien auf Demokratien und die internationale Stabilität

Die verschiedenen „Strategien der Informationskriegsführung“ unterscheiden sich in ihren Wirkungen auf die Friedfertigkeit von Demokratien (vgl. Kapitel 3) und die internationale Stabilität. Weiterhin unterscheiden sie sich in ihrem Charakter. So sind Computernetzwerkangriffe ein neues Mittel der Kriegsführung. Hingegen ist die Automatisierung und Digitalisierung weniger ein neues Mittel als ein Resultat der neuen Möglichkeiten, die sich durch die informationstechnische Vernetzung („Information in War“) ergeben. Die Probleme für die Rüstungskontrolle ergeben sich für alle „Strategien der Informationskriegsführung“ gleichermaßen.

Die Steigerung der militärischen Letalität durch die neuen Technologien und Strategien steht theoretisch allen Streitkräften als Option zur Verfügung. Grundvoraussetzung ist zwar eine rudimentäre Informations- und Telekommunikationsinfrastruktur, um so wichtiger ist der militärpolitische Wille, die eigenen Streitkräfte zu digitalisieren und zu vernetzen und sie an die Bedingungen des Informationszeitalters anzupassen. Dies ist mit Hilfe von IT-Systemen des kommerziellen Marktes kostengünstig zu realisieren. Der „RMA“ wird daher eine hohe asymmetrische Effizienzsteigerung unterstellt, z.B. durch die Verbindung alter Plattformen mit neuen IT-Systemen.

Dabei ist es nicht die Technologie per se, die zu internationalen Instabilitäten oder neuen Rüstungswettläufen führt. Erst der Zweck und die Art und Weise („Force Employment“) wie die neuen Strategien in den Streitkräften umgesetzt werden, machen die „RMA“ zu einer Technologie, die die Offensive begünstigt.[5] Die Möglichkeit der Umsetzung der „RMA“ stellt sich heute vor allem den technologisch fortgeschrittenen Industriestaaten. Die Mehrzahl davon sind demokratische Staaten. Nur diese Staatengruppe ist gegenwärtig in der Lage die Transformation ihrer Streitkräfte vorzunehmen und militärisch relevante „Informationsoperationen“ durchzuführen. Die Interventionen und Kriege der letzten Dekade haben dies sichtbar gemacht. Unter den Demokratien besitzen die

4 C4ISR = Command, Control, Communication, Computer, Intelligence, Surveillance, Reconnaissance

5 Vgl. Stephen Biddle, Rebuilding the Foundations of Offense-Defense Theory, in: The Journal of Politics, Jg. 63, Nr. 3, 2001, S. 741-774.

USA eine Sonderposition. Sie haben die Systemführerschaft über die „RMA" inne. Sie sind führend bei der Entwicklung von Technologien und Strategien der Informationskriegsführung und Computernetzwerkangriffen. Viele Entwicklungen nehmen sie vorweg, die in anderen Demokratien nachgeholt werden. Bislang profitieren von der „RMA" vor allem Demokratien.

Ob dieser Zustand von Dauer sein wird, ist fraglich. Es ist offen, welche Staaten mit ihren Streitkräften auf lange Sicht hin mit einer „RMA" ihre militärische Effektivität am meisten steigern werden.[6] Es ist mit unter nicht unwahrscheinlich, dass die Vernetzung von Streitkräften gerade aufstrebenden Regionalmächten hilft, ihre Streitkräfte in kurzer Zeit zu modernisieren. Dann würde die „RMA" ihre asymmetrischen Auswirkungen zeigen. Vorteile, die durch Hochtechnologien und Strategien in westlichen Staaten entstanden sind, würden relativiert werden. Die Informationstechnologien und neuen Militärstrategien sind kein exklusives Gut von westlichen Demokratien. Informationstechnologien verbreiten sich rasant und lassen sich nicht mehr als „Rüstungsgüter" kontrollieren. So ist es ein plausibles Szenario, dass andere Staaten schnelle Fortschritte bei der „RMA" machen können und mit Demokratien gleich ziehen oder sie gar überholen können. Zwar sind die USA und andere westliche Industriestaaten militärisch dominierend, aber auch diese militärische Dominanz zu Lande, zu Wasser, in der Luft und im Weltraum besteht nur eingeschränkt.[7]

Wenn sich der neue Typ der Kriegsführung weltweit ausbreitet, so ziehen dieselben Faktoren, die in Demokratien die Kriegs-Hemmschwelle senken, weitere negative Folge nach sich: vermeintlich geringere Risiken bei der Kriegsführung, die Verwischung der Grenze zwischen Krieg und Frieden, die Beseitigung der Differenz zwischen Offensive und Defensive, sowie der Verlust der politischen Kontrolle. Sie unterminieren allesamt die internationale Stabilität.

Um diese ungewissen Auswirkungen und Entwicklungen vorzubeugen, stellt eine neue konzipierte Rüstungskontrolle (vgl. Kapitel 4) ein Instrument dar, um die durch die neuen Rüstungsdynamiken ausgelösten Unsicherheiten und Instabilitäten aufzufangen und zu kanalisieren.

6 Vgl. Richard J. Harknett, The Risks of a Networked Military, in: Orbis, Jg. 44, Nr. 1, 2000, S. 127-144. Vgl. Thayer, a.a.O. (Anm. 2), S. 43-85. Thomas P.M. Barnett, The Seven Deadly Sins of Network-Centric Warfare, in: United States Naval Institute Proceedings, Jg. 125, Nr. 1, 1999, S. 36-39. Richard O. Hundley, Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us About Transforming the U.S. Military?, Santa Monica, CA (Rand), 1999.

7 Barry R. Posen, Command of the Commons: The Military Foundation of U.S. Hegemony, in: International Security, Jg. 28, Nr. 1, 2003, S. 5-46.

2. „Strategien der Informationskriegsführung“: Begriffe, Probleme und aktuelle Entwicklungen

„Strategien der Informationskriegsführung“ oder „informations-basierte Kriegsführung“ sind die Kernbestandteile, die der „RMA“ erst zum Durchbruch verhelfen. Unter „Informationskriegsführung“ („Information Warfare“) wird im Allgemeinen – eine einheitliche Taxonomie existiert bislang nicht – die Zentralität von „Informationen“ in jeglicher Form und ihre Verarbeitung in Militäroperationen verstanden. Damit kann die Zielführung satellitengesteuerter Bomben, die Kommunikation zwischen Truppen im Feld und ihren Hauptquartieren oder aber auch die Reduzierung der Zeit, die von der Entdeckung eines Zieles durch Sensoren über die Entscheidungsfindung bis zur Zerstörung gebraucht wird, gemeint sein („OODA“-Zyklus).[8] Sie kann die Vernetzung unterschiedlicher Systeme und Waffenplattformen bedeuten, die zu einer neuen Qualität der gesamten Architektur führen. Nicht zuletzt kann es sich auch um rein „virtuelle“ Kampfhandlungen („Cyberwarfare“ im eigentlichen Sinne) von Streitkräften im Cyberspace handeln. In einem solchen Falle findet der Angriff mittels Software und Hardware auf andere Computer- und Informationssysteme der gegnerischen Streitkräfte statt. Im Zentrum steht jedoch immer die Verarbeitung von *Daten*, *Informationen* und *Wissen*.[9]

In diesem Sinne ist der „Informationskrieg“ keine neue Form des „Krieges“, sondern eine neue strategische Dimension der Kriegsführung zur Erreichung bestimmter Ziele. Es ist eine neue Betrachtungsweise militärischer Gewalt, die zu neuen Strategien und Technologien führt. Dabei geht es weniger um neue Informationstechnologien, die in der Regel heute aus dem zivilen Bereich („Commercial-Off-the-Shelf“) stammen und nur auf militärische Bedürfnisse zugeschnitten werden.[10] Vielmehr geht es um die zielgerichtete Ausnutzung von Informationen und um ihre Verarbeitung zum eigenen Vorteil. Als Reaktion auf die steigende Bedeutung von Informationen und ihre schnelle Verarbeitung sowie als Antwort auf die höhere Komplexität von Militäroperationen entwickelt sich auch das strategische Denken in den Streitkräften weiter. Daher lösen neue Konzepte der „Informationsüberlegenheit“ und „Informationsdominanz“, die alten Planungsvoraussetzungen, wie z.B. die Powell-Doktrin der massiven quantitativen Überlegenheit auf dem

8 Der Entscheidungsablauf von der Entdeckung von Zielen bis hin zur verifizierten Zerstörung des Ziels in militärischen Handlungen, der sogenannte „OODA-Zyklus“ („Observe, Orient, Decide and Act“), ist schlechter Dings ohne Datenverarbeitung nicht mehr möglich. Der „OODA-Zyklus“ geht auf Col. John Boyd zurück. Einige Anhänger der Informationskriegsstrategien bezeichnen daher das Eindringen in den gegnerischen Entscheidungszyklus als das eigentliche Ziel von Informationsoperationen. Vgl. z.B. Edward Waltz, Information Warfare Principles and Operations, London (Artech House), 1998. S. 27f und 89f.

9 *Daten* bezeichnen in der einfachsten Form individuelle Beobachtungen und Messungen (Menschliche Kommunikation, Textnachrichten und technische Sensoren sind die wichtigsten Datenquellen), *Informationen* sind systematisch geordnete Daten, *Wissen* beschreibt analysierte und verstandene Informationen. Vgl. Waltz, a..a.O. (Anm. 8), S. 1-2.

10 Z.B. besteht das US-amerikanische Global Command and Control System (GCCS) aus einem Mix von Unix und kommerziellen PC Arbeitsstationen. Das NATO Command System „CRONOS“ basiert auf Microsoft NT Arbeitsstationen und Servern.

Schlachtfeld ab.[11] Demnach übersetzen sich Informationsüberlegenheit und Informationsdominanz während Kampfhandlungen in militärische Vorteile. Sie führen zur Dominanz im gesamten Konfliktspektrum zwischen Frieden und Krieg.[12]

„Informationsüberlegenheit" und „Informationsdominanz" führen letztlich dazu, dass zum Gewinnen von Schlachten nicht mehr „überwältigende Kräfte" („overwhelming force") notwendig sind, sondern dass als neuer Maßstab „überlegene Macht" („overmatching power") angelegt werden kann. Die Überlegenheit speist sich aus der Synergie von Wissen, Geschwindigkeit, Präzision und teilstreitkräfteübergreifenden Operationen.[13] Numerische Überlegenheit in der Masse wird mit Hilfe von Digitalisierung und Vernetzung durch teilstreitkraftübergreifende Operationen, Spezialkräfte, Geschwindigkeit und Flexibilität ersetzt, während die Schlagkraft auf dem Schlachtfeld noch erhöht wird. Die „überlegen verbundenen Kräfte" führen dazu, dass die Truppenzahl effektiv verringert werden kann. Die Diskussion und die Implementation von Informationskriegsführung in den Streitkräften und ihren Strategien spiegelt auch die gestiegene Bedeutung von Informationen in Gesellschaft und Wirtschaft wieder.[14]

Die „RMA" ist zunächst nichts weiter als ein handlungsleitendes Konzept bzw. ein zukunftsweisendes „Paradigma", das von vielen Streitkräften als richtungsweisend betrachtet, mittlerweile übernommen und akzeptiert wurde. Es leitet als „Kanon" die Technologie und Militärpolitik an.[15] Es bestimmt – ausgehend von den USA – das militärstrategische Denken und die organisatorische Umstrukturierung der Streitkräfte. Die „RMA" ist der Oberbegriff, mit dem die Entwicklungsrichtung der gegenwärtigen Militärpolitik und Technologie beschrieben und gedeutet wird. Der Begriff Informationskriegsführung („information war") ist enger gefasst und füllt die „RMA" konkret mit militärischen Handlungsoptionen. Er bezeichnet eine Reihe unterschiedlicher „Informationsoperationen", z.B. neuartige Angriffsmöglichkeiten wie „Computernetzwerkangriffe" (CNA), d.h. Attacken auf wichtige militärische Informationsinfrastrukturen mittels Com-

11 „Informationsüberlegenheit" wurde zum ersten Mal in der Joint Vision 2010 des US-Generalstabs formuliert. Vgl.: U.S. Department of Defense, Joint Chiefs of Staff, Joint Vision 2010, Washington, D.C. 1996.

12 Ebenda, S. 16.

13 Vgl. Vernon Loeb, Pentagon Credits Success in Iraq War to Joint Operations, Washington Post, 3.10.2003. S. A15. Allerdings warnen Kritiker dieser technologiefreundlichen Sichtweise daraus die falschen Konsequenzen für zukünftige Kriege zu ziehen. Vielmehr speiste sich z.B. die US-amerikanische Überlegenheit im Irak 2003 aus der Interaktion zwischen der US-amerikanischen Stärke und irakischen taktischen Schwächen und Fehlern. Nicht eine überlegene Technologie alleine war für den schnellen militärischen Sieg verantwortlich. Vgl. z.B. die ersten empirischen Ergebnisse von Stephen Biddle, Iraq and the Future of Warfare, Unveröffentlichte Folien, Carlisle: U.S. Army War College, Strategic Studies Institute 18.08.2003. („Jointness" = teilstreitkraftübergreifend)

14 Vgl. Manuel Castells, Das Informationszeitalter: Wirtschaft, Gesellschaft, Kultur. Bd. 1: Die Netzwerkgesellschaft, Opladen (Leske + Budrich), 2001. Alvin Toffler/Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century, London (Little, Brown and Company), 1993.

15 Vgl. U.S. Department of Defense, Joint Chiefs of Staff, Joint Vision 2010, Washington, D.C. 1996. U.S. Department of Defense, Joint Chiefs of Staff, Joint Vision 2020, Washington, D.C. 2000. Jede US-Teilstreitkraft hat darauf hin eigene „Visionen" für die Transformation formuliert.

putersystemen, Medienoperationen, aber auch Altbekanntes wie physische Angriffe auf Führungs- und Kommandoeinrichtungen von Streitkräften.

„Strategien der Informationskriegsführung" umfassen in der hier verwendeten Definition sowohl „Informationsoperationen", die in militärischen Operationen angewendet werden, als auch die formulierten Strategien und Doktrinen der Vernetzung, Automatisierung und Digitalisierung (z.B. netzwerk-zentrische Kriegsführung oder „effekt-basierte Operationen"), die zur Transformation der Streitkräfteorganisation und der Kriegsführung führen. Diese „Strategien der Informationskriegsführung" bezeichnen Arquilla und Ronfeldt als „Cyberwar": „Cyberwar refers to conducting, and preparing (...) military operations according to information-related principles. It means disrupting if not destroying the information and communication systems, broadly defined to include even military culture (...) cyberwar is not simply a set of measures based on technology. (...) Cyberwar may require major innovations in organizational design, in particular a shift from hierarchy to networks."[16]

Informationen und ihre Verarbeitung (z.B. in der Führung, Aufklärung und Nachrichtengewinnung) in Militäroperationen sind keine neuen Phänomene und haben auf den Schlachtfeldern schon immer eine Rolle gespielt.[17] Allerdings ist heute die Aufmerksamkeit, die der Rolle von Informations- und Datenverarbeitung zukommt, gestiegen. Dies ist auf die erweiterten militärischen Verwendungsmöglichkeiten zurückzuführen, die sich mit der Einführung des Computers, der Digitalisierung und der schnellen Datenübermittlung in den Streitkräften ergeben haben. Ebenfalls ist neu dabei, dass „Informationen" und ihr Verarbeitungsprozess selbst als militärische Ziele und als Mittel in Konflikten betrachtet werden. Der „virtuelle Raum" wird zur Zone von Kampfhandlungen. Hinzu kommt heute, dass militärische Entscheidungsabläufe („OODA"-Zyklus) ohne elektronische Datenverarbeitungssysteme nicht mehr möglich sind. Sie tragen zur Übersicht über das Schlachtfeld („Dominant Battlespace Knowledge") in der Form von komplexen „C4ISR"-Systemen bei. Diese Informationsüberlegenheit auf dem Schlachtfeld hat praktische Auswirkungen. Das illuminierte Schlachtfeld hilft, tödliche Verluste durch eigenes Feuer zu reduzieren, indem die Bewegungen der eigenen und feindlichen Streitkräfte elektronisch verfolgt werden.[18] Daher sind Computer und Informations- und Telekommunikationstechnologie nicht mehr aus modernen Streitkräften wegzudenken. Sie bilden die technologische Grundlage für die Durchführung militärischer Operationen. Computer und Informationstechnologie reduzieren die Komplexität bei der Führung von Streitkräften, und gleichzeitig erhöhen sie die Komplexität militärischer Operationen.

16 Vgl. Arquilla/Ronfeldt, a.a.O. (Anm. 3), S. 23-60. S. 30 u. 45.

17 Vgl. z.b. den historischen Überblick der Rolle von „Command, Control and Communication" (C3) bei Martin van Creveld, Command in War, Cambridge, Mass. (Harvard University Press), 1985.

18 Durch drahtlose Netzwerksysteme (z.B. FBCB2, das „taktische Internet" der US-Army), die kleinen Einheiten im Feld und Kommandeuren die Position der eigenen und feindlichen Truppen anzeigen, GPS-Daten und Aufklärungsdaten integrieren und gleichzeitig als Kommunikationsinterface funktioniert. Zu den Chancen und Grenzen von „DBK" siehe Martin C. Libicki, DBK and its Consequences, in: Stuart E. Johnson/Martin C. Libicki (Hg.), Dominant Battlespace Knowledge, Washington, D.C. (National Defense University) 1995, S. 27-58.

2.1 Was sind Informationsoperationen?

Der Begriff „Strategien der Informationskriegsführung“ bezeichnet alle „Informationsoperationen (IO), die in Krisenzeiten oder Konflikten (Kriege eingeschlossen) unternommen werden, um spezifische Ziele gegenüber einem spezifischen Gegner oder Gegnern zu erlangen oder zu unterstützen“.[19] Informationsoperationen (IO) liegen in einer weiten Spannbreite. Sie können sowohl kinetische Angriffe auf Kommunikations- und Führungseinrichtungen („Command and Control Warfare“) umfassen als auch „Medienoperationen“ wie Propaganda und Medienmanipulation (Flugblätter, Radio und TV), elektronische Kampfführung oder virtuelle Angriffe auf Computernetzwerke („Cyberwarfare“), die in der virtuellen Welt stattfinden, aber reale Auswirkungen auf Militäroperationen haben. So zählt Martin Libicki verschiedene Formen von Informationsoperationen auf, die er alle als zur Informationskriegsführung zugehörig rechnet:[20]

- „Command and Control Warfare“
- „Intelligence-based Warfare“
- „Electronic Warfare“
- „Psychological Warfare“
- „Hacker War“ (software-based attacks on information systems)
- „Information Economic Warfare“
- „Cyberwar“ (combat in the virtual realm)

Allgemein umfassen Informationsoperationen (IO) heute nach der weitverbreiteten Definition der „Joint Doctrine for Information Operation JP 3-13“: „Handlungen, die gegnerische Informationen und Informationssysteme beeinflussen, während die eigenen Informationen und Informationssysteme verteidigt werden.“[21] Die JP 3-13 ist eines der wichtigsten Dokumente des US-Generalstabes zum Informationskrieg. IO umfassen nach dieser Definition sowohl offensive als auch defensive militärische Handlungen. Ihre größte Wirkung entfalten IO allerdings zu Friedenszeiten. Informationsoperationen dienen in Friedenszeiten und an der Schwelle zu Krisenzeiten als Instrument der Abschreckung und beeinflussen als eine Form der „Soft Power“ die Perzeption und den Entscheidungsprozess potentieller Gegner.[22] Ebenso ist damit aber auch gemeint, dass Informationen über

19 „Information warfare (IW) is IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries.“ U.S. Department of Defense, Joint Chiefs of Staff, Joint Doctrine for Information Operations JP 3-13, Washington, D.C. 1998. S. I-1, I-11. (eigene Übersetzung) Vgl. auch die Analyse des Dokumentes Gebhard Geiger, Offensive Informationskriegsführung. Die "Joint Doctrine for Information Operations" der US-Streitkräfte: sicherheitspolitische Perspektiven, SWP Studie Nr. S 2, Berlin: Stiftung Wissenschaft und Politik 2002.

20 Martin C. Libicki, What Is Information Warfare?, Strategic Forum Nr. 28, Washington, D.C.: National Defense University 1995. http://www.ndu.edu/inss/strforum/forum28.html (26.05.2003)

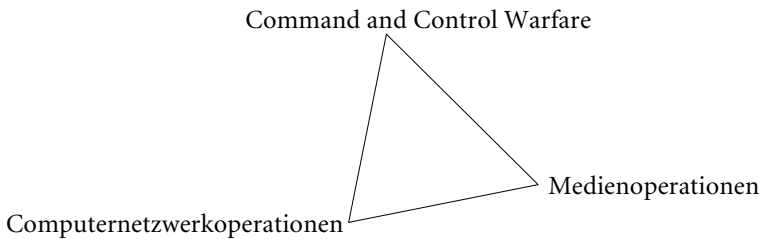
21 „IO involve actions taken to affect adversary information and information systems while defending one’s own information and information systems.” U.S. Department of Defense, Joint Chiefs of Staff, Joint Doctrine for Information Operations JP 3-13, Washington, D.C. 1998. S. I-1.

22 Ebenda, S.I-3. Vgl. auch Joseph S. Nye/William A. Owens, America's Information Edge, in: Foreign Affairs, Jg. 75, Nr. 2, 1996, S. 20-36.

gegnerische Computersysteme schon präventiv ausgespäht („NETINT", z.B. „Probing", „Network Mapping") werden müssen, um effektive Computerangriffe durchführen zu können.

Informationsoperationen lassen sich daher am besten als ein Kontinuum zwischen physischen Angriffen und virtuellen Angriffen vorstellen. Ziele, Mittel und Effekte variieren dabei. Nur das Militär als handelnder Akteur bleibt konstant. Dadurch lassen sich „Strategien des Informationskrieges" von Computerkriminalität („Cybercrime") oder „Cyberterrorismus" unterscheiden. Kriminelle Organisationen oder Terroristen besitzen nicht die Kapazitäten und Fähigkeiten wie staatliche Militärorganisationen, um Informationsoperationen des gesamten Spektrums effektiv auszuführen oder militärisch relevante Informationssysteme anzugreifen.[23] Da Terrororganisationen weder die Fähigkeiten noch einen großen Nutzen haben, sich der Computernetzwerkoperationen als Instrument zur Erreichung ihrer Ziele zu bedienen. „Cyberterrorismus" ist heute und in absehbarer Zukunft kein großes Risiko, das vorallem mit nicht-militärischen Mitteln, z.B. geeigneter Strafverfolgung bzw. Computersicherheit und Infrastrukturmaßnahmen, gelöst werden könnte.

Abb.1: Strategien der Informationskriegsführung



Als drei der anschaulichsten Beispiele von Informationsoperationen, ausgeführt durch staatliche Akteure, gelten der Angriff auf Führungs- und Komandoeinrichtungen („Command and Control Warfare") an einem Ende des Spektrums, Medienoperationen[24] in der Mitte (z.B. Medienbeeinflussungen, gezielte PR-Kampagnen oder auch Öffentlich-

23 Dass Terrororganisationen neue Technologien zur internen wie externen Kommunikation nutzen läßt noch nicht darauf schliessen, dass sie auch in der Lage wären, militärische relevante Computersysteme elektronisch anzugreifen. Insofern beinhaltet der Begriff des „Cyberterrorismus" mehr Übertreibung als das er Realitätsgehalt besitzt. Insofern ist es besser von „*Cyberplanning*" um den Nutzen neuer Technologien für Terrororganisationen zu beschreiben. Vgl. Timothy Thomas, Al Qaeda and the Internet: The Danger of "Cyberplanning", in: Parameters, Jg. 33, Nr. 1, 2003, S. 112-123. Dorothy E. Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, in: John Arquilla/David Ronfeldt (Hg.), Networks and Netwars, Santa Monica (Rand) 2001, S. 239-288.

24 Sie werden neuerdings als „Influence Operations" bezeichnet. Siehe zur Rolle von solchen Handlungen in Konflikten und während Krisen z.b. U.S. Department of Defense, Joint Chiefs of Staff, Doctrine for Joint Psychological Operations JP 3-53, Washington, D.C. 2003. Thomas Rid, Die Öffentlichkeitsarbeit der USA im Mittleren Osten: Amerikanische "Public Diplomacy" als Waffe in Kriegszeiten?, SWP Aktuell Nr. 16, Berlin: Stiftung Wissenschaft und Politik 2003.

keitsarbeit) und Computernetzwerkoperationen (CNO) am anderen Ende des Spektrums. „Command and Control Warfare" hat seine Wurzeln in der „AirLand Battle"-Strategie der NATO aus den 70er Jahren. Ziel dieser Strategie ist es, die feindlichen Streitkräfte im Feld von der Kommunikation mit ihrer Führung abzuscheiden und sie dadurch „unbeweglich" zu machen. Medienoperationen tragen nach der derzeitigen US-amerikanischen Doktrin dazu bei, die „Informationsumwelt" nach den Zielen der militärischen Regionalkommandos zu gestalten.[25] Computernetzwerkoperationen sind dagegen Operationen, die im virtuellen Raum stattfinden und offensiver wie defensiver Natur sein können. Computernetzwerkangriffe (CNA) haben zum Ziel, „Informationen in Computersystemen und Netzwerken oder die Computer und Netzwerke selbst zu stören, zu verhindern, zu degradieren und zerstören."[26]

2.2 Gegenwärtiger Stand der Entwicklung: Zwischen Formulierung und Institutionalisierung der Strategien

Nicht alle Elemente der informationstechnologisch basierten Kriegsführung werden umsetzbar sein. Einige Elemente wie z.B. der „reine" digitale Krieg werden sicherlich Fiktion bleiben. So befinden sich die „Strategien der Informationskriegsführung" überwiegen noch in der Phase der Planung und der konkreten Ausformulierung. Die nächsten Schritte der Institutionalisierung und der organisatorischen Verortung der Doktrin in den Streitkräften und die Schaffung von Informationsoperationseinheiten zeichnen sich allerdings ab.[27] Die „Strategien des Informationskrieges" sind dabei längst nicht mehr alleiniges Gedankengut demokratischer Streitkräfte. Das Paradigma der Präzisierung, Digitalisierung und Vernetzung der Streitkräfte – die „Revolution in militärischen Angelegenheiten" – findet weltweit Nachahmer mit rüstungsdynamischen Auswirkungen. Die USA setzen dabei die Standards.

Aktuell sind die USA dabei, Informationsoperationen in die nationale Befehlskette einzubauen und interorganisatorische Konkurrenzen und Kompetenzen zu klären. Im August 2002 ließ US-Präsident George W. Bush Richtlinien zur offensiven Anwendung von CNOs ausarbeiten. Die „National Security Presidential Directive 16" (NSPD-16) legt Presseberichten zufolge die Autorisierungs- und Befehlsstränge dar, wie im Falle von „Informationsangriffen" ein Gegenangriff gestartet werden kann. Bislang hatten die un-

25 U.S. Department of Defense, Assistant Secretary for C3I, DoD Directive 3600.1 "Information Operations" Revision One, Washington, D.C. 2001. S. 2. Vgl. auch die ältere U.S. Department of Defense, Joint Chiefs of Staff, Doctrine for Public Affairs in Joint Operations JP 3-61, Washington, D.C. 1997. Vgl. auch Rid, a.a.O. (Anm. 24).

26 U.S. Department of Defense, Joint Chiefs of Staff, Joint Doctrine for Information Operations JP 3-13, Washington, D.C. 1998. S. I-9. U.S. Department of Defense, Assistant Secretary for C3I, DoD Directive 3600.1 "Information Operations" Revision One, Washington, D.C. 2001. S.6.

27 Eine organisatorische Übersicht für die USA bietet Ralf Bendrath, Informationskriegsabteilungen der US-Streitkräfte: Eine Zusammenstellung der mit offensive Cyberattacken befassten Einheiten der US-Streitkräfte, FoG:IS Arbeitspapier Nr. 3, Berlin (Forschungsgruppe Informationsgesellschaft und Internationale Sicherheitspolitik) 2001.

klaren Kompetenzen dazu geführt, dass das Potential von IO und CNOs in Militäroperationen nicht ausgeschöpft wurde.[28] Die Richtlinien legen den Umgang mit offensiven CNOs gegen feindliche Staaten und ihre Computernetzwerke fest. Diese Richtlinien sind nur ein kleiner, dennoch wichtiger Teil der umfassenden Bemühungen, die US-Streitkräfte zu „transformieren", wie die doktrinale, organisatorische und technologische Umsetzung der „RMA" im US-Verteidigungsministerium genannt wird. Diese „RMA"-Bemühungen wurden unter der Clinton-Administration begonnen und werden von der zweiten Bush-Regierung fortgesetzt.[29]

Seit dem ziehen sich diese Anstrengungen in den USA wie ein roter Faden durch die Formulierung und Umsetzung der „RMA". So bekräftigte US-Präsident Bush im Dezember 2001, dass die Transformation der US-Streitkräfte erste Priorität habe.[30] Denn im ersten Halbjahr seiner Amtszeit schien die Umsetzung der „RMA" ins Stocken zu geraten. Die große „transformative" Umgestaltung drohte am Widerstand der Teilstreitkräfte auf der einen Seite und wegen des Führungsstils von Verteidigungsminister Rumsfeld auf der anderen Seite zu scheitern. Rumsfeld versuchte mit Hilfe eines Expertengremiums und unter Umgehung des US-Kongress, die Reform der Streitkräfte gegen institutionelle Widerstände durchzusetzen. Am Ende wurden nur wenige Großprojekte eingestellt, andere lediglich als „transformativ" eingestuft, um ihre Position im US-Verteidigungshaushalt zu rechtfertigen. Das Wahlkampfversprechen von Bush, eine Generation von Waffensystemen „zu überspringen", wurde nicht eingelöst.[31]

Erst nach den Anschlägen vom 11. September 2001 erhielt die Transformation der Streitkräfte, und damit Strategien der Informationskriegsführung Aufwind. Sie hielten Einzug in wichtige nationale Planungsdokumente. Die US-Regierung unter Bush hat erst spät ihre „nationale Sicherheitsstrategie" vorgelegt und eine „nationale Militärstrategie" noch nicht präsentiert. In ersterer werden „Informationsoperationen" beiläufig erwähnt.[32] Dass die Strategien des Informationskrieges einen gewaltigen Sprung hin zu mehr Be-

28 Bradley Graham, Bush Orders Guidelines for Cyber-Warfare Rules for Attacking Enemy Computers Prepared as U.S. Weighs Iraq Options, Washington Post, 7.02.2003. S. 1. Dawn S. Onley, U.S. aims to make war on Iraq's networks, Government Computer News, 24.02.2003. http://www.gcn.com/22_4/news/21231-1.html (24.02.2003)

29 Zur Entstehung der RMA- und Transformationspolitik der zweiten Bush-Regierung siehe Nicholas Lemann, Dreaming About War: Someone in the Pentagon is Staging a Defense Revolution – And it's Not the Generals, New Yorker, 16.07.2001. Vgl. auch die ersten „Visionen" des US-Generalstabes unter Clinton: U.S. Department of Defense, Joint Chiefs of Staff, Joint Vision 2010, Washington, D.C. 1996. U.S. Department of Defense, Joint Chiefs of Staff, Joint Vision 2020, Washington, D.C. 2000.

30 George W. Bush, Remarks by the President at the Citadel, Charleston, South Carolina, 11.12.2001, Washington, D.C.: (Office of the Press Secretary, White House Press Release) 2001. http://www. whitehouse.gov/news/releases/2001/12/print/20011211-6.html (13.12.2001)

31 George W. Bush, A Period of Consequences (Presidential Candidate George W. Bush Speaks to the Corps of Cadets at the Citadel), Charleston, South Carolina: (1999. http://www.citadel.edu/pao/addresses/pres_bush.html (13.12.2001)

32 Dort heißt es an einer Stelle, IO betreffend: „This broad portfolio of military capabilities must also include the ability to defend the homeland, conduct *information operations*, ensure U.S. access to distant theaters, and protect critical U.S. infrastructure and assets in outer space." Bush, George W., The National Security Strategy of the United States of America, Washington, D.C. (The White House) 2002. S. 30. [Herv. OM]

deutung in der US-Verteidigungsstrategie erfahren, lässt sich an Hand von drei Verteidigungsdokumenten erkennen.

In der „Quadrennial Defense Review 2001" („QDR") der Bush-Regierung werden Informationsoperationen als eines von sechs operativen Zielen genannt: „Assuring information systems in the face of attack and conducting effective information operations; (...)."[33] Die QDR 2001 stellt insgesamt eine Neuausrichtung im „Denken" der US-Streitkräfte dar. Sie bricht mit der alten Strategieplanung, die sich an plausiblen Szenarien orientierte, die darlegten, welcher Gegner bekämpft oder in welcher Region mit hoher Wahrscheinlichkeit gekämpft werden („Threat-based") muss. Die neue QDR richtet die Strategie statt dessen an der möglichen Art und Weise wie ein Gegner kämpft („Capabilities-based") neu aus. Sie legt dar, wie unter diesen Umständen auch mittels Informationsoperationen ein Gegner abgeschreckt und besiegt werden kann.

Das zweite, 2002 teilweise an die Öffentlichkeit gelangte Dokument, die „Nuclear Posture Review" („NPR") betonte ebenfalls die steigende Bedeutung von Informationsoperationen. Sie sieht eine sinkende Rolle der „nuklearen Triade" auf den Schlachtfeldern der Zukunft voraus, die durch konventionelle High-Tech-Rüstung ausgeglichen und z.B. durch Informationsoperationen ersetzt werden kann.[34] Die „neue Triade" besteht aus nuklearen und nicht-nuklearen Elementen. „Strategien der Informationskriegsführung" nehmen dabei eine prominente Stellung ein. Sie tragen zum militärischen Abschreckungspotential bei: „The addition of non-nuclear strike forces – including conventional strike and *information operations* – means that the U.S. will be less dependent than it has been in the past on nuclear forces to provide its offensive deterrent capability."[35] Um die Schlagkraft der „neuen Triade" sicherzustellen, verlangt die NPR, dass weitere Anstrengungen unternommen werden, feindliche Computernetzwerke „auszubeuten" und „Strategien der Informationskriegsführung" in die nukleare Kriegsplanung zu integrieren.

Die „Defense Planning Guidance" („DPG"), ist das dritte wichtige Planungsdokument, das seit 2002 die Durchführung von „Informationsoperationen" als ein operatives Ziel erklärt. Es legt die nationale Sicherheitsstrategie und deren Umsetzung in den Teilstreitkräften fest. Die DPG sorgt dafür, dass die Ressourcen und Fähigkeiten für die Anforderungen, die sich aus der Strategie ergeben, angeglichen und geschaffen werden. Das

33 U.S. Department of Defense, Office of the Secretary of Defense, Quadrennial Defense Review Report, Washington, D.C. 30.09.2001. S.30.

34 U.S. Department of Defense, Secretary of Defense, Nuclear Posture Review Report (Excerpts), Washington, D.C. 8.01.2002. http://www.globalsecurity.org/wmd/library/policy/dod/npr.htm (16.03.2002) [Herv. OM] J.D. Crouch, J.D. Crouch, Assissant Secretary for International Security Policy, Special Briefing on the Nuclear Posture Review, 9.01.2002, Washington, D.C.: (U.S. Department of Defense, News Transcript) 2002. James Dao, Pentagon Study Urges Arms Shift, From Nuclear To High-Tech, New York Times, 9.01.2002. William M. Arkin, Secret Plan Outlines the Unthinkable: A secret policy review of the nation's nuclear policy puts forth chilling new contingencies for nuclear war, Los Angeles Times, 10.03.2002. Vgl. zu diesem Trend Harald Müller/Annette Schaper, US-Nuklearpolitik nach dem Kalten Krieg, HSFK Report Nr. 3, Frankfurt am Main (Hessische Stiftung Friedens- und Konfliktforschung) 2003.

35 U.S. Department of Defense, Secretary of Defense, Nuclear Posture Review Report (Excerpts), Washington, D.C. 8.01.2002. http://www.globalsecurity.org/wmd/library/policy/dod/npr.htm (16.03.2002)

nichtöffentliche Dokument hat Aufmerksamkeit erhalten, weil es die präemptive Ausrichtung der neuen US-amerikanischen Verteidigungsplanung widerspiegelt und die alte Verteidigungsformel, wonach die USA in der Lage sein müssten, zwei größere Kriege zu gewinnen, durch die „4-2-1" Formel ersetzt.[36] Das US-Militär soll sich in der DGP darauf vorbereiten, selbst „Informationsoperationen" als Kernkompetenz durchführen zu können, die Differenzen zwischen den Teilstreitkräften auszuräumen und die rechtlichen Probleme zu klären, die bislang Computernetzwerkangriffe erschweren.[37]

Neben der Formulierung und Ausarbeitung von Strategien und Doktrinen zeichnen sich schon die nächsten Schritte der Institutionalisierung der Strategien und die organisatorische Verortung der Anwendung der Technologien erkennbar ab. Der erste Schritt dazu war die Schaffung einer sogenannten „Information Operations Cell" – einer Planungszelle, die Informationskriegsspezialisten umfassen soll und für die Implementierung von Informationsoperationen in Krisen zuständig ist.[38] Die Ansiedlung des JTF-CNO beim USSTRATCOM (2002) ist der vorläufige Höhepunkt dieser Institutionalisierung. Gleichfalls ist die erstmalige Operationalisierung von Informationsüberlegenheit im neuen Handbuch des US-Heeres (FM 3-0) zu bewerten. Ebenso gibt Hinweise auf die Institutionalisierung von CNOs in Militäroperationen. Es zeichnet sich ein Wandel von defensiven Computernetzwerkoperationen (CND) hin zu Computernetzwerkangriffen (CNA) ab. Nach dem die allgemeinen Übertreibungen (z.B. die Rede vom „elektronischen Pearl Harbor", das bevorstünde) der Verwundbarkeit und Bedrohung von kritischen Infrastrukturen einer abgeklärten Analyse der Risiken gewichen ist, werden nun die offensiven Möglichkeiten ausgelotet. Der Auftrag der „Joint Task Force-Computer Network Defense" (JTF-CND) umfasste in der Vergangenheit nur die Koordination der Verteidigung militärischer Netzwerke unter dem US-Weltraumkommando (USSPACECOM). Diese Mission wurde 2000 um offensive Computernetzwerkattacken (CNA) erweitert. Seit der Neustrukturierung der US-amerikanischen Militärkommandostruktur im Jahr 2002 ist das „Strategische Kommando" (USSTRATCOM) der USA für die gesamten Computernetzwerkoperationen des JTF-CNO zuständig. Dieser neue Auftrag umfasst nun sowohl die Verteidigung der militärischen Netzwerke als auch den Angriff von Computernetze durch CNA. CNO untersteht nun dem gleichen Kommando wie die US-amerikanischen Nuklearwaffen. Trotz der Implementationsprobleme und der ungeklärten

36 Michael E. O'Hanlon, Rumsfeld Defense Vision, in: Survival, Jg. 44, Nr. 2, 2002, S. 103-107. Die US-Streitkräfte sollen ihre Fähigkeiten darauf ausrichten, gleichzeitig vier kleinere Einsätze durch zuführen, zwei mittlere Regionalkriege führen zu können und dabei in einem Falle einen schnellen entscheidenden Sieg zu erringen.

37 Senior Defense Official U.S. Department of Defense, News Transcript, Background Briefing on the Defense Planning Guidance, 10.05.2002, Washington, D.C.: (U.S. Department of Defense) 2002. William M. Arkin, The Best Defense, Los Angeles Times, 14.07.2002.

38 U.S. Department of Defense, Joint Chiefs of Staff, Joint Doctrine for Information Operations JP 3-13, Washington, D.C. 1998. S. IV-3.

rechtlichen Fragen haben Informationsoperationen in der US-amerikanischen Sichtweise mittlerweile eine strategische Bedeutung für die Kriegsführung erhalten.[39]

2.3 Proliferation der Strategien außerhalb der USA

Der Paradigmenwechsel bleibt nicht auf die US-amerikanischen Streitkräfte beschränkt. Das Denken in Begriffen wie der „Revolution in Militärischen Angelegenheiten“ oder „netzwerk-zentrischen Kriegsführung“ breitet sich unter den US-Alliierten und Streitkräften weltweit aus. Wie bei den US-Streitkräften in der Rolle der Vorreiter lassen sich Anzeichen einer beginnenden Institutionalisierung auch bei anderen Streitkräften ausmachen. Das bedeutet, dass die Umsetzung der Strategien, die Aufgabenverteilung, die Planung und die Durchführung von Manövern unter dem Zeichen des neuen Strategieparadigmas stattfinden. Möglicherweise zeichnet sich hier eine neue weltweite Rüstungsdynamik ab. Sie unterscheidet sich grundlegend von der Rüstungsspirale des Kalten Krieges. Die Dynamik besteht nicht nur aus dem quantitativen Wettstreit technologisch überlegener Waffenplattformen und Systeme, sondern auch aus der qualitativen Zusammenbindung von neuen Technologien und Strategien. Von den USA ausgehend, findet es im Konzept der „netzwerk-zentrischen Kriegsführung“ Eingang in die NATO, in die Bundeswehr („Vernetzte Operationsführung“) und in andere europäische Streitkräfte.[40] Eine Informationsoperationsdoktrin der Bundeswehr ist bislang nicht öffentlich.[41] In der NATO wurde 2003 das Hauptquartier SACLANT in Northfolk in „Allied Command for Transformation“ (ACT) umbenannt. Das ACT soll unter anderem den neuen NATO-Mitgliedern bei der Anpassung behilflich sein, aber auch als Transmissionsriemen für die Transformation der NATO-Streitkräfte nach US-Muster dienen. Seit 1997 arbeitet die NATO an einem Entwurf zu einer gemeinsamen IO-Doktrin. Bislang sind Bemühungen nicht über eine IO-Definition in der NATO-MC422 hinaus gekommen.[42] So haben

39 Vgl. Gregory J. Rattray, Strategic Warfare in Cyberspace, Cambridge (MIT Press), 2001. S. 330. Vgl. auch Zalmay M. Kahlilzad/John P. White (Hg.), Strategic Appraisal. The Changing Role of Information in Warfare, Santa Monica (Rand), 1999.

40 Stefan Krempl, Sturmlauf zum vernetzten Wissenskrieger, telepolis, 10.09.2003. http://www.heise.de/tp/special/info/15600/1.html (15.09.2003) Christiane Schulzki-Haddouti, Bundewehr richtet sich auf "Network Centric Warfare" aus, Heise News-Ticker) 2003. http://www.heise.de/ newsticker/data/wst-04.09.03-004/ (4.09.2003) Allerdings wird z.B. in Großbritannien der Begriff „network-enabled Capabilities“ verwendet, weil der US-amerikanische Begriff des „NCW“ sich zu sehr an Waffenplattformen ausrichtet und nicht an den Synergieeffekten, die durch die Vernetzung entstehen.

41 Wenn von „Informationskriegsfähigkeiten“ in der Bundeswehr gesprochen wird, ist in der Regel die hauseigene IT-Sicherheit gemeint. Allerdings verwischen sich die Grenzen zwischen offensiven und defensiven Fähigkeiten. Vgl. Ralf Bendrath, Die Bundeswehr auf dem Weg ins digitale Schlachtfeld, telepolis, 4.07.2000. http://www.heise.de/tp/deutsch/special/info/8326/1.html (5.4.2000)

42 Die in der NATO MC422 enthaltene „Information Operations Policy“, Anfang Januar 1999 von einer Arbeitsgruppe formuliert, definiert „Informationsoperationen“ als „Actions taken to influence decision makers in support of political and military objectives by affecting other's information, information based processes, C2 systems and CIS, while exploiting and protecting one's own information and/or information systems. There are two main categories of Info Ops: defensive Info Ops and Offensive Info Ops, depending upon the nature of the actions involved“.

die NATO-Alliierten in der Regel lediglich Arbeitsversionen von Informationskriegsdoktrinen für ihre nationalen Streitkräfte erstellt, aber gleichzeitig Institutionen und Organisationen geschaffen, die zwar gleiche, aber anders benannte Aufgaben wahrnehmen und entwickeln.[43]

Die Rezeption der „RMA", die Entwicklung von Informationskriegsstrategien und die organisatorischen Veränderungen sind nicht auf westliche Streitkräfte beschränkt. Die „RMA"-Debatte, Anfang der 90er Jahre in den USA angestoßen, hat sich innerhalb einer Dekade weltweit ausgebreitet. Zahlreiche Staaten ziehen militärpolitische Konsequenzen daraus. Seit jeher sind die russischen Streitkräfte an der konzeptionellen Entwicklung beteiligt, zumal die Vordenker der „RMA" aus dem sowjetischen Generalstab in der 70er Jahren stammen.[44] Die Streitkräfte der chinesischen Volksrepublik haben die „RMA"-Debatte rezipiert. Unter dem Eindruck des Golfkrieges von 1991 und des Kosovokrieges von 1999 wurden die Auswirkungen diskutiert.[45] Ähnlich sieht es in Taiwan, Israel, Indien und einer Reihe anderer Staaten aus.[46] Längst ist das Wissen um die „RMA" und ihre Auswirkungen auf die Kriegsführung allgemein verbreitet und entfaltet seine rüstungsdynamische Wirkung: „For the international community, the spread of the RMA image across states is but another way by which the era of post-Cold War democratic peace may be undermined."[47] Die Möglichkeit besteht, dass sich eine neuartige Rüstungsdynamik unter den Bedingungen des Informationszeitalters ankündigt. Sie ist neu, da sich bislang nur die Strategien und Doktrinen ausbreiten und weniger die Militärtechnologien und da die Dynamik nicht in einem direkten Wettlauf zwischen Akteuren stattfindet; vielmehr passt jeder Akteur die Strategien und Kapazitäten an seine Bedürfnisse an.[48]

43 Andrew Rathmell/Kevin O'Brien, Information Operations: An International Overview (Jane's Special Report), Couldson, Surrey (Jane's Information Group), 2001.

44 Nikolai A. Lomov (Hg.), Scientific-Technical Progress and The Revolution in Military Affairs (A Soviet View), Washington, D.C. (Moskau i.O.) (U.S. Government Printing Office), 1974. Mary C. FitzGerald, Marshal Ogarkov and the New Revolution in Soviet Military Affairs, in: Defense Analysis, Jg. 3, Nr. 1, 1987, S. 3-19. Timothy L. Thomas, Russian Views on Information Warfare, in: Airpower Journal (Special Edition), Jg. 10, Nr. 1, 1996, S. 25-35. Alexander I. Nikitin, From REF to EAR: Russian Concepts of "Seventh Generation War", Paper presented at Heinrich Böll Stiftung Conference on "Cyberwar and Arms Control", Berlin, 2001.

45 John Arquilla/Solomon M. Karmel, Welcome to the Revolution...in Chinese Military Affairs, in: Defense Analysis, Jg. 13, Nr. 3, 1997, S. 255-270. Shen Weiguang, Der Informationskrieg – eine Herausforderung, in: Christine Schöpf/Gerfried Stocker (Hg.), Infowar – information.macht.krieg (Ars Electronica), Wien (Springer) 1998, S. 67–91. James Mulvenon, The PLA and Information Warfare, in: James Mulvenon/Richard H. Yang (Hg.), The People's Liberation Army in the Information Age, Santa Monica (RAND) 1999, S. 175-186. Michael Pillsbury, Chinese Views of Future Warfare, Washington, D.C. (National Defense University) 2000.

46 Chris C. Demchak, The RMA in Developing States: Dilemmas of Image, Operations, and Democracy, in: National Security Studies Quarterly, Jg. 6, Nr. 4, 2000, S. 1-45. Ahmed S. Hashim, The Revolution in Military Affairs Outside the West, in: Journal of International Affairs, Jg. 51, Nr. 2, 1998, S. 432-445.

47 Demchak, a.a.O. (Anm. 46), S. 2.

48 Vgl. Arquilla/Karmel, a.a.O (Anm. 45).

3. Strategien der Informationskriegsführung und die Risiken für die Kriegsführung von Demokratien

3.1 Neue militärische Technologien und die Absenkung materieller und moralischer Kosten der Kriegsführung

Die neuen militärtechnologischen und militärstrategischen Tendenzen wirken auf die Hemmschwellen, die in Demokratien gegenüber der Anwendung militärischer Gewalt bestehen. Sie reduzieren die materiellen Kosten, Lasten und Hürden von Militäroperationen und senken deren politische und moralische Risiken.

Die neuen Technologien unterlaufen zunächst einen wichtigen Faktor im Verhältnis von Demokratie, Frieden und der Anwendung von militärischer Gewalt: die Abneigung der Wählerschaft gegenüber dem Krieg als Mittel der Politik, weil sie die *materiellen Kosten* eines bewaffneten Konfliktes scheuen oder gar um ihr eigenes Leben und Eigentum fürchten müssen.[49] Mit Hilfe neuer Militärtechnologie wird das Einsatzrisiko heute für Soldaten demokratischer Streitkräfte reduziert. Mittels moderner Waffentechnologie wird der Gegner aus der Distanz bekämpft. Eigene Verluste werden dadurch reduziert. Technologie und Feuerkraft substituiert die „Arbeitslast" und Zahl der Soldaten. Nicht nur das Risiko für die Streitkräfte nimmt dadurch ab, auch das wirtschaftliche, gesellschaftliche und politische Risiko sinkt für Demokratien, wenn Kriege aufgrund offensiver Überlegenheit kurz und erfolgreich geführt werden können. Gleichzeitig erhöht sich die Feuerkraft, Präzision und Geschwindigkeit der hochtechnisierten Streitkräfte enorm. Demokratische Gesellschaften und ihre Regierungen scheinen von den direkten Auswirkungen solcher Militäreinsätze verschont zu bleiben.[50]

Die neuen Militärtechnologien sollen es möglich machen, eine noch nie da gewesene Übersichtlichkeit und Transparenz des Schlachtfeldes herzustellen. Der von Clausewitz beschriebene „Nebel des Krieges" soll damit gelichtet werden.[51] Auf Friktionen, Risiken und Unwägbarkeiten, wie sie bislang noch in allen Kriegen vorkamen, sollen technologische Antworten in der Form komplexer, automatisierter „C4ISR"-Angriffssysteme gefunden werden. Ultimatives Ziel dieser Anstrengungen ist die Kontrolle des Kriegs in allen Aspekten. Dabei wird verkannt, dass die Quellen von Friktionen nicht nur technischer Art

49 Immanuel Kant, Zum ewigen Frieden: Ein philosophischer Entwurf [1781], Stuttgart (Reclam), 1984. S. 12f. Zur rationalistischen Begründung des Demokratischen Friedens vgl. Bruce Bueno de Mesquita/David Lalman, War and Reason: Domestic and International Imperatives, New Haven (Yale University Press), 1992. Bruce Bueno de Mesquita/James D. Morrow/Randolph Silverson/Alastair Smith, An Institutional Explanation of the Democratic Peace, in: American Political Science Review, Jg. 93, Nr. 4, 1999, S. 791-807. Vgl. auch Ernst-Otto Czempiel, Friedensstrategien: eine systematische Darstellung außenpolitischer Theorien von Machiavelli bis Madariaga, Opladen (Westdeutscher Verlag), 1998. Michael W. Doyle, Ways of War and Peace: Realism, Liberalism, and Socialism, New York (W.W. Norten & Company), 1997. (Kapitel 6,7)

50 Colin McInnes, Spectator-Sport War: the West and Contemporary Conflict, Boulder, Co (Lynne Rienner), 2002.

51 William A. Owens, Lifting the Fog of War, New York (Farrar, Straus, Giroux), 2000. William A. Owens, The Emerging System of Systems, in: Military Review, Nr. 3, 1995, S. 15-19.

sind, sondern im dynamischen Wesen des Krieges selbst liegen. Da ein Krieg nach Clausewitz letztlich aus zwei widerstreitenden Willen besteht, kann der Gegner immer ein „Veto" gegen die eigene Strategie und Planung einlegen.

Die Verbindung von neuen Technologien und Militärstrategien stellt Demokratien dabei nicht nur die Minimierung der *eigenen Verluste, sondern auch die Reduzierung von zivilen Opfern* auf Seiten des Gegners bei gleichzeitiger Steigerung der *„militärischen Effektivität"* in Aussicht. Die neuen Technologien und Strategien senken damit auch die politisch-moralischen Risiken von Militäroperationen. Der Einsatz militärischer Gewalt als Mittel der Außenpolitik muss von Demokratien normativ gerechtfertigt werden. Militärische Gewaltanwendung von Demokratien findet nicht mehr in der Form großer konventioneller Schlachten statt, sondern in der Form von begrenzten Kriegseinsätzen, Interventionen oder Einsätzen von Spezialeinheiten. Hohe eigene Verluste und zivile Opfer sind in solchen militärischen Einsätzen die Ausnahme und nicht mehr die Regel. Die Operationen selbst werden dabei mit dem Anspruch der Minimierung ziviler Opfer geführt und werden nur so den von Demokratien gesetzten Normen gerecht. „While no form of warfare is entirely antiseptic, avoiding all civilian injury or collateral destruction, information warfare may prove to be an effective means of coercion that is more adept at insulating civilians from the dangerous kinetic effects of war."[52] Mit den neuen Technologien und Strategien wird somit ein zweites demokratietypische Hindernis gegen die Kriegsführung unterlaufen: die *normative* Abneigung demokratischer Bürger gegenüber dem Krieg als Mittel der Politik.[53] So stellt das „Defense Science Board", ein wissenschaftliches Beratergremium des U.S.-Verteidigungsministeriums, in einem aktuellen Bericht die Notwendigkeit der Anpassung der Strategien und Technologien an einen neuen Kriegsführungsstil und neue Militäroperationen: „The need is driven by the nature of current military campaigns. A striking feature of these campaigns is tension among multiple strategic and operational objectives: cause regime change, destroy a terrorist organization, decapitate leadership, but preserve infrastructure, don't wage war on a people, do hold an international coalition together etc."[54]

Der Einsatz von militärischer Gewalt durch Demokratien in der gesamten Spannbreite der Operationen – von konventionellen Kriegen, militärischen Interventionen und friedenserhaltenden Maßnahmen unterhalb der Selbstverteidigung – rückt durch die neuen Militärstrategien und Technologien zu einer möglichen *Politikoption* auf. Diese Option verspricht, geringere materielle, politische und moralische Risiken zu verursachen als in

52 Brian T. O'Donnell/James C. Kraska, Humanitarian Law: Developing International Rules for the Digital Battlefield, in: Journal of Conlict and Security Law, Jg. 8, Nr. 1, 2003, S. 133-160. S. 134.

53 Zu den normativen Ursachen des „Demokratischen Friedens" vgl. Czempiel, a.a..O. (Anm. 49); vgl. Doyle, a.a.O. (49). Bruce Russett, Grasping the Democratic Peace: Principles for a Post-Cold War World, Princeton, NJ (Princeton University Press), 1993. Thomas Risse-Kappen, Democratic Peace – Warlike Democracies? A Social Constructivist Interpretation of the Liberal Argument, in: European Journal of International Relations, Jg. 1, Nr. 4, 1995, S. 491-517.

54 U.S. Department of Defense, Office of the Undersecretary of Defense For Acquisition, Technology, and Logistics, Defense Science Board, Report of the Defense Science Board Task Force of Discriminate Use of Force, Washington, D.C. Juli 2003. S. III.

der Vergangenheit. Militärische Gewalt wird wieder zu einem „brauchbaren" politischen Instrument. Neue Technologien und Strategien relativieren somit Faktoren, welche die Neigung von Demokratien zum Einsatz militärischer Gewalt hemmen. Die politischen und militärischen Risiken werden minimiert, und damit auch die innerdemokratischen Beschränkungen, Zwänge und Bedingungen für Militäroperationen die demokratischen Regierungen, durch ihre Gesellschaften auferlegt wurden.[55] Mehr noch, die Kriegsführung von Demokratien unterliegt heute genau dieser politisch-strategischen Beschränkung: Sie muss heute unter der Prämisse der Opfervermeidung und der „gezielten Gewaltanwendung" stattfinden. Diese Prämisse ist nicht nur abstrakt, sondern wird an der Schnittstelle von militärischen und politischen Entscheidern diskutiert und beeinflusst schon heute Technologieentwicklung, Operationspläne und die militärischen Operationen selbst.[56]

3.2 Das Ende der Grenze von Krieg und Frieden: Computernetzwerkangriffe

„Woher weiß man, ob man sich im Informationszeitalter im Krieg befindet?"[57] Diese Frage bringt ein weiteres Problem auf den Punkt, das „Strategien des Informationskrieges" für den Frieden darstellen. Sie verwischen die operative Grenze zwischen Krieg und Frieden. Sie eröffnen womöglich sogar für Konflikte *zwischen* Demokratien neue Möglichkeiten der Konfliktaustragung, weil sie sich unterhalb der Schwelle offener Gewalt befinden. Die Entscheidung über Krieg und Frieden stellte bislang in Demokratien eine hohe institutionelle Hürde da. Diese Grenze mag weiterhin existieren, nur tragen „Strategien der Informationskriegsführung" dazu bei, dass sich der operative Charakter von militärischen Handlungen derart ändert, dass die Grenze irrelevant werden kann. In der Folge werden institutionelle Schranken weniger greifen als bisher oder gar ganz versagen.

Paradoxerweise können gerade demokratische Normen, parlamentarische Restriktionen und die demokratische Öffentlichkeit Gründe dafür sein, die eine offene militärische Intervention durch eine demokratische Regierung in den „Untergrund" treiben. Diese verdeckten Operationen unterhalb der Schwelle offener und organisierter Gewaltaustragung liegen in der Grauzone zwischen direkter militärischer Aktion und indirekter geheimdienstlicher Unterstützung. Informationsoperationen sind ein ideales Instrument

55 Clifton T. Morgan/Sallly Howard Campbell, Domestic Structure, Decisional Constraints and War, in: Journal of Conflict Resolution, Jg. 35, Nr. 3, 1991, S. 187-211. Zur Rolle der Öffentlichen Meinung siehe Eric V. Larson, Casualties and Consensus: The Historical Role of Casualties in Domestic Support For U.S. Military Operations, Santa Monica, CA (RAND), 1996. Philip P. Everts/Pierangelo Isernia, Public Opinion and the International Use of Force, London (Routledge), 2001.

56 Ein eindruckvolles Dokument das diese Beschränkung diskutiert und nach einer technologischen Lösung sucht ist z.B. U.S. Department of Defense, Office of the Undersecretary of Defense For Acquisition, Technology, and Logistics, Defense Science Board, Report of the Defense Science Board Task Force of Discriminate Use of Force, Washington, D.C. Juli 2003. Zu den politischen Beschränkungen einer Kriegsführung siehe Ivo H. Daalder/Michael E. O'Hanlon, Winning Ugly: NATO's War to Save Kosovo, Washington, D.C. (Brookings Institution Press), 2000.

57 Richard W. Aldrich, How do You Know You Are at War in the Information Age?, in: Houston Journal of International Law, Jg. 22, 2000, S. 223.

für solche Handlungen. Sie sind schwer zu entdecken und hinterlassen wenig Spuren. Sie sind schwieriger politisch zu kontrollieren, da meistens nur ein kleines Gremium die Kontrolle von Geheimdiensten, Spezialkräften und verdeckten Operationen zur Aufgabe hat. Dieses Problem wird in den kommenden Jahren um so schwerer wiegen, da der „globale Krieg gegen den Terror" meist im Verborgenen, in der operativen Grauzone kleiner Einsätze oder Kommandoaktionen, geführt wird.[58]

In dieser Grauzone befinden sich Computernetzwerkoperationen (CNO), wenn sie von staatlichen Organisationen offensiv gegen andere ausgeführt werden.[59] Sie sind mithin das Paradebeispiel, wie neue Strategien und Technologien institutionelle Sperren unterlaufen können. Als eine besondere Form der offensiven Informationsoperationen verwischen sie die Grenze zwischen Krieg, Konflikten niedriger Intensität und Frieden. Als eine Art der militärischen Handlung ohne sichtbare physische „Gewaltanwendung" scheinen sie ferner das ideale militärpolitische Instrument zu sein, um Kriege ohne Opfer zu führen und keine Spuren zu hinterlassen. CNA eigenen sich daher als Instrument zur Erreichung von Zielen, wenn diese nicht entdeckt werden dürfen oder unter engen politischen Restriktionen umzusetzen sind. Institutionelle Schranken laufen bei solchen verdeckten Militäreinsätzen immer Gefahr, zu versagen.

3.2.1 Offensive Computernetzwerkoperationen: ein neues Element in Militäroperationen

Computernetzwerkoperationen sind eine Teilmenge von Informationsoperationen. Sie zerfallen wie diese in defensive Computernetzwerkoperationen und offensive Computernetzwerkangriffe (CNA). Offensive Computernetzwerkangriffe im militärischen Kontext, d.h. wenn sie von staatlichen Organisationen eingesetzt werden, sind definiert als „operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves."[60] Gemeint ist damit das Ein-

58 William M. Arkin, The Secret War: Frustrated by intelligence failures, the Defense Department is dramatically expanding its 'black world' of covert operations, Los Angeles Times, 27.10.2002. Ein weiterer Indikator dafür ist die Aufwertung des US Kommando für Spezaileinheiten in Florida (USSOCOM) von einem „supporting" zu einem „supported" Kommando. Das USSOCOM ist seit der Einrichtung Mitte der 80er Jahren unabhängiger als andere Kommandos und die Kontrolle durch den Senat ist geringer. Vgl. auch Dana Priest, The Mission: Waging War and Keeping Peace With America's Military, New York (W.W. Norton & Co.), 2003. Andrew Koch, USA Expands Special Operations' Role In 'War On Terrorism', Jane's Defence Weekly, 6.11.2002.

59 Von privaten Akteuren wie Hackern oder terroristischen Organisationen durchgeführte Informationsoperationen oder Computernetzwerkangriffen geht wegen Sicherheitslücken ein Risiko für die Infrastruktur eines Landes aus. Dennoch ist auch dieses Risiko minimal, da diesen Akteuren im Gegensatz zu staatlichen die Kapazitäten fehlen, um mehr als nur partielle Systeme und Dienstleistungen für eine Zeit zu unterbrechen. Dieses geringe Risiko sollte daher unter dem Problem von „Computerkriminalität", „Computersicherheit" oder Infrastruktursicherheit diskutiert werden. Dieser Report beschränkt sich daher nur auf „Strategien des Informationskrieges", die von staatlichen Akteuren und Organisationen durchgeführt werden könnten.

60 U.S. Department of Defense, Joint Chiefs of Staff, Joint Doctrine for Information Operations JP 3-13, Washington, D.C. 1998. S. I-9. U.S. Department of Defense, Joint Chiefs of Staff, Joint Doctrine for Electronic Warfare, Joint Publication 3-51, Washington, D.C. 2000. S. GL-5.

dringen, Manipulieren oder Zerstören von Informationen, die sich in Computernetzwerken befinden oder der Netzwerksysteme selbst. Beispiele für CNA sind der Einbruch in Computersysteme, die Zerstörung oder Manipulation von Daten, das Platzieren von Computerprogrammen wie logischen Bomben, Viren oder Würmern, die ein Netzwerk oder System zum Erliegen bringen können.

Computernetzwerke bilden das infrastrukturelle Rückgrat moderner Streitkräfte. Sie sind essentiell für das Führen von Militäroperationen geworden. Dies macht sie zu hochwertigen Zielen in einer militärischen Auseinandersetzung. Die Angriffe gegen solche System können physischer oder virtueller Art sein. Angriffe der ersten Art sind durch kinetische Zerstörung möglich. Letztere sind Angriffe über Datenströme und durch Programmcodes. Möglich gemacht werden solche Computernetzwerkangriffe durch eine Vielzahl von Werkzeugen und Sicherheitslücken, die einen Angriffsweg überhaupt erst eröffnen.[61] Mit Hilfe von Angriffswerkzeugen, den eigentlichen „Waffen" im Cyberspace, wird in Computersysteme eingebrochen und werden die Daten manipuliert oder das System von außen lahmgelegt. Ausgenutzt werden Sicherheitslücken in Computersystemen, die durch Programmierungs- oder Hardwarefehler verursacht werden. Früher boten Systeme vor allem durch Nachlässigkeit in der Konfiguration und Handhabung der Sicherheitsvorkehrung Angriffsflächen und „Zugangsmöglichkeiten". Die Angriffe waren meist noch manuell. Heute hat sich die offensive Seite weiterentwickelt, und es stehen halb- oder in Kürze auch vollautomatisierte Angriffswerkzeuge zur Verfügung.

Dennoch ist nicht jedes militärische Computersystem durch Computernetzwerkattacken verwundbar, und nicht jede kritische Infrastruktur ist von außen per Datenleitung zugänglich. Zum einen sind viele relevante Systeme nicht von außen einwählbar. Zum anderen gibt es abgeschottete Insellösungen, so dass in vielen Fällen nur ein System angriffen werden kann, nicht aber ein zweites. Ebenso erhöhen Redundanzen die Verfügbarkeit von kritischen elektronischen Dienstleistungen. Des weiteren ist auf der „defensiven" Seite die Entwicklung der Netzwerkverteidigung („Computer Network Defense") nicht stehen geblieben. Es wird an einer Vielzahl von „Intrusion Detection Systems" gearbeitet, die Einbrüche oder verdächtigen Netzwerkverkehr registrieren und Angriffe verhindern können. Ebenso werden Systeme durch sogenannte Red-Teams auf Angriffsmöglichkeiten getestet oder von anderen Organisationen auf Sicherheit geprüft und zertifiziert. Die größte Gefahr für kritische Systeme geht immer noch von „Insidern" aus, also Personen, die direkten Zugang zu sensitiven Systemen haben.[62] Allerdings werden auch im militärischen Bereich aus Kostengründen immer mehr „Commerical-Off-the-Shelf" Produkte verwendet, so dass militärische Systeme durch die gleichen Sicherheitslücken ver-

61 Vgl. z.B. Dorothy E. Denning, Information Warfare and Security, Reading, Ma. (Addison-Wesley), 1999. Edward Waltz, Information Warfare Principles and Operations, London (Artech House), 1998. S. 256-267. Zu Computerrisiken generell vgl. Peter G. Neumann, Computer-related Risks, Reading, Mass. (Addison-Wesley), 1995. (Solche z.T. freiverfügbare Werkzeuge sind Programme wie Scanner, Sniffer, Passwort-Crackprogramme oder Rootkits)

62 Vgl. U.S. General Accounting Office, Report to the Secretary of Defense, DoD Information Security, Serious Weaknesses Continue to Place Defense Operations at Risk, GAO/AIMD-99-107, Washington, D.C. August 1999.

wundbar sind wie zivile Systeme. Die Dynamik zwischen Angriff und Verteidigung, das heißt zwischen der Beseitigung von Sicherheitslücken und der Suche nach neuen Einbruchswegen bleibt allerdings auch in der Zukunft erhalten. Computernetzwerkangriffe und defensive Computernetzwerkoperationen unterliegen damit den alten rüstungstechnologischen Innovationen, die im nicht endenden Wettlauf abwechselnd die offensive oder die defensive Kriegsführung bevorteilen.

Die Vorteile von CNA liegen auf der Hand: Sollte es möglich sein, mit Hilfe von Computernetzwerkangriffen gegnerische „C4ISR" präemptiv in Krisen oder in heißen Phasen eines Konfliktes auszuschalten, werden immense militärische Vorteile geschaffen. Der Gegner würde, ähnlich wie bei anderen Militärstrategien (z.B. Enthauptungsschlägen), durch den Verlust seiner „C4ISR"-Fähigkeiten (z.B. Sensoren und Kommunikation) blind und handlungsunfähig sein, weil er sein elektronisches Nervensystem an Führungs-, Aufklärungs- und Reaktionsfähigkeiten verliert. CNA wären damit ein elegantes militärisches Instrument, das dazu beitragen kann, unter restriktiven politischen Bedingungen Kriegsführung wieder möglich zu machen und dabei eigene Opfer zu vermeiden.

Die Integration von CNA in die militärische Planung führt in langfristiger Konsequenz auch zur Anwendung in Krisen und Konflikten. Diese Integration ist nicht frei von Nachteilen. Durch CNA wird ein weiteres Problem aufgeworfen. Die Angriffsmethoden, wenn sie auf Sicherheitslücken zurückzuführen sind, existieren möglicherweise nur für eine kurze Zeit oder sind nicht wiederholbar. Die Abhängigkeit von Informationsinfrastrukturen moderner Streitkräfte macht diese in hohem Maße verwundbar und anderen Staaten bietet sich ein Anreiz, diese auszunutzen und in eigene Vorteile umzumünzen. Staaten, die konventionell-militärisch schwach sind, aber über eine wachsende Informationsinfrastruktur (z.B. China, Rußland, Taiwan, Indien, etc.) verfügen, könnten mit Hilfe von CNA ihre Schwäche ausgleichen. CNA wird somit zu einer militärischen Fähigkeit, die asymmetrische Effekte erzeugen kann. Die militärischen Vor- und Nachteile, die sich für Militäroperationen durch CNA ergeben, sind also heute noch ambivalent.[63]

3.2.2 „Operative Grauzone" – Militärische Handlungen in Friedenszeiten

CNA sind streng genommen nur in Kriegszeiten von Nutzen, wenn sie Militäroperationen unterstützen können. Ansonsten sind Computernetzwerkangriffe nur als geheimdienstliche Tätigkeit in der Form von Einbrüchen in Computersysteme oder zur Informationssammlung über die Informationsinfrastruktur, z.B. der sogenannten SCADA-Systeme, anderer Staaten und Akteure vorstellbar.[64] Sie stellen in diesem Sinne nur eine

63 Vgl. z.B. die illustrativen Auswirkungen der gestiegenen technologischen Komplexität durch Computernetzwerke im dritten Golfkrieg in Joshua Davis, "If We Run Out of Batteries, This War is Screwed." Wired 11.06, http://www.wired.com/wired/archive/11.06/battlefield.html (22.05.2003)

64 SCADA-Systeme („Supervisory Control and Data Acquisition") sind Soft- und Hardware, die eine Fernwartung und Steuerung von Großanlagen möglich machen. Unterschiedliche, zum Teil singuläre SCADA-Systeme werden in Kraftwerken, in der Öl- und Gas verarbeitenden Industrie, Telekommunikation, Transport und Verkehr, in der Energie- und Wasserversorgung und anderen Infrastrukturen verwendet. Allerdings wurde noch kein Kraftwerk oder Staudamm von außen durch einen Datenangriff manipuliert,

Form des „Auskundschaftens“ dar. Das Ausspähen von Netzwerken („NETINT“), ihres Aufbaus und ihrer Systemkomponenten lässt sich von manchen technischen Routinefunktionen, wie z.B. dem „Pingen“, von Servern nicht unterscheiden, womit festgestellt werden kann, ob bestimmte Rechner erreichbar sind und ein Netzwerkknotenpunkt existiert oder nicht. Die „operative Grauzone“ wird dadurch verstärkt, dass CNA sowohl geheimdienstlichen und aufgrund ihrer strategischen Auswirkung auch militärischen Charakter haben, sich jedoch von klassischen militärischen Handlungen unterscheiden.[65] Diese neue operative Grauzone ist von Demokratien noch wenig verregelt und daher schwer zu kontrollieren.

Den gängigen Militärdoktrinen zufolge werden Computernetzwerkangriffe wie Informationsoperationen generell jedoch in allen Phasen der Friedens-, Krisen- und Kriegszeiten angewendet. So heißt es in der US-amerikanischen Informationsoperationsdoktrin JP3-13: „Offensive IO-related plans with their capabilities may be employed in peacetime to promote peace, deter crisis, control crisis escalation, or project power.“[66] Das friedenspolitische Problem, das offensive Formen der „Strategien der Informationskriegsführung“ – hier die Computernetzwerkangriffe – darstellen, ist daher die Schaffung einer operativen Grauzone zwischen Krieg und Frieden. Die militärisch-operative Grauzone, die durch CNA und ihre Anwendung erst geschaffen wird, ist zu einem Teil der neuen Technik und zu einem weiteren Teil ihrem „strategischen Effekt“ geschuldet.

CNA müssen teilweise, um im Kriegsfalle von Nutzen sein zu können, schon vorher in „feindlichen“ Systemen technisch installiert werden. Bestimmte CNA-Aktivitäten finden daher schon in Friedenszeiten statt, um im Falle militärischer Auseinandersetzung als funktionierende Option der militärischen Führung zur Verfügung zu stehen. Bevor CNA ausgeführt werden können, müssen potentielle (zivile und militärische) Ziele auf ihre verwendete Technologie oder ihre Systemzusammensetzung hin aufgeklärt werden. Der militärisch-geheimdienstliche Aufwand geht, ähnlich wie bei der konventionellen Zielauswahl, der Planung voraus.[67] Allerdings unterscheidet sich diese Zielplanung von konventionellen Angriffen dadurch, dass sie einen Schritt weitergeht. Potentielle Ziele müssen schon in Friedenszeiten manipuliert werden, so dass der spätere Zugang sichergestellt ist. Ebenfalls dürfen sie nicht entdeckt werden. Somit müssen Computereinbrüche – in diesem Falle eine militärische Handlung – in einigen Systemen schon zu Friedenszeiten vorgenommen werden, wenn sie mehr als nur eine „theoretische“ Option für die militärische Führung im Krisenfalle sein sollten.

falls dies überhaupt möglich sein sollte. Ebenso kommt es immer wieder zur zeitweiligen Unterbrechung solcher Dienste, ohne das die nationale Sicherheit oder die Bevölkerung gefährdet wird.

65 Vgl. Rattray, a.a.O. (Anm. 39). Roger C. Molander/Andrew S. Riddle/Peter A. Wilson, Strategic Information Warfare: A New Face of War, Santa Monica (RAND), 1996.

66 U.S. Department of Defense, Joint Chiefs of Staff, Joint Doctrine for Information Operations JP 3-13, Washington, D.C. 1998. S. II-8.

67 Vgl. U.S. Joint Forces Staff College, Joint Command, Control and Information Warfare School, Joint Information Operations Planning Handbook, Norfolk (National Defense University) Juli 2002.

Es ist völkerrechtlich umstritten, ob Computernetzwerkangriffe mit einem physischen Angriff auf ein Land gleichzusetzen sind.[68] Bei reinen Computernetzwerkangriffen ohne physische Gewaltanwendung oder Auswirkungen stellt sich z.B. die Frage, was eine verhältnismäßige Reaktion auf einen solchen Angriff darstellen würde.[69] Ebenso ist es fraglich, ob Computernetzwerkangriffe in diesem Falle eine „Waffe" darstellen. Problematisch wird dieser Fall, wenn die Infrastruktur eines Landes angegriffen wird und weil meistens der Angreifer nicht zu identifizieren ist.[70] Das Völkerrecht hinkt der technologischen Entwicklung hinterher.

CNA verwischen die operative Grenze zwischen Krieg und Frieden. Diese neue Grauzone birgt für Demokratien unkontrollierbare Gefahren. Die Hemmschwelle für die militärische Gewaltanwendung schwindet, da sie scheinbar ein Instrument ohne sichtbare negative Konsequenzen darstellen. Die explizite, offene Entscheidung über kriegerische Handlungen ist der wesentliche Ort öffentlicher Kontrolle über die Exekutive. Dort findet die öffentliche Erörterung über das Für und Wider statt. Gibt es jedoch einen solchen Entscheidungspunkt gar nicht mehr, dann entziehen sich die Schritte zum Krieg vollends der demokratischen Prüfung.

Gleichzeitig ist jedoch das Eskalationspotential hoch. So könnte ein entdeckter digitaler „Zwischenfall" in einer heißen militärischen Auseinandersetzung münden. Sollten CNA zum Standardrepertoire für Militäroperationen werden, wird es in Zukunft schwieriger, technische Systemausfälle vom Beginn einer militärischen Offensive zu unterscheiden. Darüber hinaus nähren solche Optionen zusätzlich die Illusion einer sauberen digitalen, möglicherweise präemptiven Kriegsführung. Außer Acht gelassen wird bei solchen Vorstellungen zukünftiger Kriegsbilder, dass der reine „digitale Krieg" – der nur in und gegen Datennetzen geführt wird – auf absehbare Zeit nicht stattfinden wird. Vielmehr wird der digitale Krieg die klassische Gewaltanwendung in militärischen Disputen ergän-

68 Richard W. Aldrich, The International Legal Implications of Information Warfare, INSS Occasional Paper Nr. 9, Colorado: USAF Institute for National Security Studies 1996. Thorsten Stein/Thilo Marauhn, Völkerrechtliche Aspekte von Informationsoperationen, in: Zeitschrift für ausländisches öffentliches Recht und Völkerecht, Jg. 60, Nr. 1, 2000, S. 1-40. Michael N. Schmitt, Wired Warfare: Computer Network Attack and Jus in bello, in: International Review of the Red Cross, Jg. 84, Nr. 846, 2002, S. 365-399. Sie vertreten eine andere völkerrechtliche Position als z.B. David J. DiCenso, IW Cyberlaw: The Legal Issues of Information Warfare, in: Airpower Journal, Jg. 13, Nr. 2, 1999, S. 85-102. Vgl. die Beiträge in Michael N. Schmitt/Brian T. O'Donnell (Hg.), Computer Network Attack and International Law, Newport, R.I. (Naval War College), 2002.

69 Vorausgesetzt, der Angreifer läßt sich überhaupt identifizieren.

70 David Isenberg, An Electronic Pearl Harbor? Not Likely, in: Thomas E. Copeland (Hg.), The Information Revolution and National Security, Pennsylvania (Strategic Studies Institute) 2000, S. 92-102. Fälle von transnationaler Computerkriminalität stellen zwar ein Problem dar. Bislang dienen solche Szenarien der Übertreibung, denn der Sensibilisierung von Entscheidern für technische Lücke und politischen Handlungsbedarf. Wenn z.B. von Computereinbrüchen oder Hackerangriffen auf das Pentagon die Rede ist, dann bezieht sich das entweder auf die „theoretische Möglichkeit" und nicht die tatsächliche oder es sind nichtkritische, öffentliche Netzwerksysteme betroffen gewesen. Z.B. der Webserver des Presse- und Informationsdienstes der NATO während des Kosovokrieges. Allerdings ergibt sich eine „militärische" Achillesferse dadurch, dass geschätzte 80% der militärischen Kommunikation über zivile Netze laufen.

zend begleiten. Er wird sie aber nicht ersetzen.[71] Die Zukunft, der von Demokratien geführten Militäroperationen, liegt in der „digitalisierten Kriegsführung", bei der die Streitkräfte zumindest einer Seite digitalisiert und vernetzt sind.[72] In solchen Militäroperationen, vor allem in „klassischen" Militäroperationen gegen Staaten mit der entsprechenden Infrastruktur, können Computernetzwerkangriffe als komplementäres Mittel eingesetzt werden, um die militärische „Effektivität" der Streitkräfte zu erhöhen und die Zahl der Opfer zu senken. Dabei ist es irrelevant geworden, ob die technischen Fähigkeiten heute für die digitalen Angriffswege oder Verwundbarkeiten tatsächlich vorhanden sind oder nicht. Das Denken über (militärische) Computernetzwerkangriffe hat sich in den Strategien und Organisationen schon festgesetzt.

3.3 Die Wirkung von Computernetzwerkangriffen auf Normen der Kriegsführung

Durch Computernetzwerkoperationen wird die Kriegsführung immer präziser und maßgeschneidert. Andererseits geraten immer mehr zivile Infrastrukturen ins Visier, die bislang als tabu galten. Die „moralische" Hemmschwelle, zivile Ziele im Krieg anzugreifen, sinkt, da CNA scheinbar keinen physischen Schaden anrichten. Damit werden Regeln und Normen der Kriegsführung aufgeweicht, die bisher den Krieg einhegten.

Das Völkerrecht beschränkt rechtmäßige militärische Angriffe auf „legitime" militärische Ziele. Es unterscheidet zwischen Kombattanten und Nicht-Kombattanten sowie zwischen Angriff und Selbstverteidigung. Diese Unterscheidungen stehen vor der Auflösung und der Neudefinition, ausgelöst durch neue Technologien und Strategien. Die einst fixen Grenzen zwischen legitimen Zielen und Mitteln schwinden insbesondere bei Computernetzwerkangriffen wie auch bei Informationsoperationen im allgemeinen. Zivile und militärische legitime Ziele vermischen sich und werden vermischt. Die Ursachen dieser Verwischung der Grenzen legitimer Kriegsführung sind nur zu einem Teil dem technischen Charakter (komplexe Koppelung und Kaskadeneffekte) der Informationsinfrastruktur geschuldet. Zum anderen Teil sind sie das Resultat einer wohlüberlegten politischen Strategie in Militäroperationen, die den Druck auf den Gegner zu maximieren und dabei krude Feuerkraft zu ersetzen sucht. Paradoxerweise lösen CNA damit Normen des humanitären Völkerrechtes und moralische Hemmschwellen auf: zivile Ziele werden zu legitimen Ziele mit militärischem Wert.

Seit den 80er Jahren steigt der Einfluss von Militärjuristen auf die strategischen und taktischen Operationspläne im Pentagon.[73] Gleichzeitig können sie nicht verhindern, dass zivile Ziele, die unter dem Schutz der Genfer Konvention stehen, angegriffen werden und dabei Zivilisten getroffen werden. Der juristischen Einflusses wurde durch Dehnung, Fle-

71 Vgl. die Aktivitäten im Netz währen des Kosovokrieges, der Ostimor-Intervention und während US-amerikanisch-chinesischen Zwischenfalls wegen des EP-3 Orion Spionageflugzeuges.

72 Z.B. die 4. Infanterie Division in Fort Hood, Texas.

73 Esther Schrader, War, On Advice Of Counsel, Los Angeles Times, 15.02.2002.

xibilisierung und einer legalistischen Sichtweise auf das Völkerrecht erkauft. Das Protokoll I der Genfer Konvention definiert militärische Angriffsziele folgendermaßen: „Angriffe sind streng auf militärische Ziele zu beschränken. (...) nur solche Objekte, die auf Grund ihrer Beschaffenheit, ihres Standorts, ihrer Zweckbestimmung oder ihrer Verwendung *wirksam zu militärischen Handlungen beitragen* und deren gänzliche oder teilweise Zerstörung, deren Inbesitznahme oder Neutralisierung unter den in dem

Abb.2 Mögliche Ziele von Informationsoperationen[74]

betreffenden Zeitpunkt gegebenen Umständen einen *eindeutigen* („definite“) militärischen Vorteil darstellt.“[75] Die im April von den USA erlassene „Military Commission Order No.2“, die in Anlehnung an das Protokoll I „Militärische Ziele“ definiert, deutet auf den Trend der Dehnung und Flexibilisierung in bezug auf C3-Systeme hin. Weil in komplexen C3-Systemen auch zivile Komponenten enthalten sein können oder die Kriegsfähigkeit des gegnerischen Militärs unterstützen, heißt es in ihr nunmehr, dass militärische Ziele alle Objekte darstellen, die „are those potential targets *effectively* contribute to the opposing force’s war-fighting or war-sustaining capability, (...) and whose total or partial destruction constitute a military advantage to the attacker (...).“[76] Da in dieser Definition

74 U.S. Department of Defense, Joint Chiefs of Staff, Joint Doctrine for Information Operations JP 3-13, Washington, D.C. 1998. S. I-17.

75 Vgl. Art.52, Zusatzprotokoll zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffenter Konflikte (Protokol I) 8. Juni 1977, Satorius, Internationale Verträge und Europarecht, Band II, München, 1993. (Hervorhebung OM). In der Englischen Übersetzung heißt an dieser Stelle „those objects which (...) make *an effective contribution* to military action and whose total or partial destruction, (...) offers a *definite* advantage.“

76 MCI Nr. 2 zitiert nach Noëlle Quénivet, A US Version of What Constitutes a "Military Objective", BOFAXE Nr. 256E, Bochum: Institut für Humanitäres Völkerrecht 2003. http://www.ruhr-uni-bochum.de/ifhv/publications/bofaxe/x256E.pdf (19.08.2003) Vgl. auch Michael N. Schmitt, Wired Warfare: Com-

auch das Wort „definite“ fehlt, schließt Noëlle Quénivet, dass die US-Regierung damit sich die Option offen hält, auch Ziele anzugreifen, die bei einem Angriff nur das mögliche Potenzial für einen militärischen Vorteil in sich tragen.[77]

Die neue rechtliche Sichtweise auf das humanitäre Völkerrecht verhindert in mit modernen Mitteln geführten Kriegen nicht, dass die Zivilbevölkerung angegriffen wird. Im Gegenteil, sie legitimiert eine Zielplanung, die zunehmend zivile Objekte als militärische Ziele umdefiniert: „The United States and its Allies practice a new style of legal warfare (...) that hinges on precision-guided bombs, standardized targeting and accepted levels and types of collateral damage, and higher bomber flight altitudes.(...) Modern warfare has dramatically reduced the number of direct civilian deaths, *yet the law sanctions infrastructural campaigns that harm long-term public health and human rights.*“[78] Dieser Sachverhalt spiegelt, jenseits von juristischen Definitionen, die gestiegene Bedeutung von Informationsinfrastrukturen für die Kriegsführung wider.

Einerseits ermöglichen CNA nach der Meinung einiger Experten das gezielte Ausschalten von militärisch relevanten Systemen. Der Direktor der CIA unter der Clinton-Administration ließ sich zu der Aussage vor dem Senat hinreißen: „The electron is the ultimate precision guided weapon“.[79] Dem gegenüber steht die Aussage von Arthur Cebrowski, eines der Erfinder der “netzwerk-zentrierten Kriegsführung”, wonach CNA „not necessarily very precise instruments“ sind.[80] Diese Aussage ist auf die technische Unkontrollierbarkeit bestimmter CNA zurückzuführen: Angriffe auf ein vernetztes System können zwar präzise sein, aber ein Angriff auf ein eng gekoppeltes, komplexes System kann möglicherweise zu unkontrollierbaren Kaskadeneffekten in anderen Systemen führen. Der Angriff auf die militärische Informationsinfrastruktur kann Auswirkungen auf die zivile Informationsinfrastruktur haben. In einem solchen Falle wären dann ebenfalls zivile Systeme wie z.B. Energieversorgung, Telekommunikation und Bankensysteme von den Auswirkungen eines CNA betroffen. Darüber hinaus ergibt sich die Verwischung der Grenzen zwischen militärischen und zivilen Netzwerken aus der Konstruktion der Systemarchitektur und der Nutzung von Informationsinfrastrukturen. Es existieren zwar gesicherte und von öffentlichen Netzen getrennte militärische Netzwerke für die Daten- und Kommunikationsübermittlung (z.B. SIPRNET, das einen Teil der US-amerikanischen militärischen Führung- und Kommunikationssysteme vernetzt, und das eine hardwareseitige Verschlüsselung benutzt, deren Schlüssel z.T. stündlich wechseln). Selbst wenn eine systemische Trennung zwischen zivilen und militärischen Systemen besteht, gibt es auch eine militärische Nutzung ziviler Systeme. So werden zivile Netzwerke und

puter Network Attack and Jus in bello, in: International Review of the Red Cross, Jg. 84, Nr. 846, 2002, S. 365-399.

77 Ebenda.

78 Thomas W. Smith, The New Law of War: Legitimizing High-Tech and Infrastructural Violence, in: International Studies Quarterly, Jg. 46, Nr. 3, 2002, S. 351-357. S. 356. (Hervorhebung OM)

79 Bradley Graham, Authorities Struggle With Cyberwar Rules, Washington Post, 08.07.1998.

80 Zitiert nach J.N. Ager, Is There a Military Utility to Information Operations?, in: Defense Analysis, Jg. 16, Nr. 3, 2000, S. 277-298. S. 289

Infrastrukturen (z.B Telefonschaltzentralen, Glasfaserverbindungen, Kommunikations- und Wettersatelliten etc.) für die militärische Kommunikation gebraucht und genutzt. Das bedeutet im Umkehrschluss, dass solche (zivilen) Informationsinfrastrukturen als militärisch so relevant für das Gewinnen von Kriegen angesehen werden können, dass sie als militärisches Ziel eingestuft werden (Vgl. Abb.2). In der Konsequenz ist eine technische Unterscheidung zwischen zivilen und militärischen Zielen bei bestimmten CNA nicht mehr aufrecht zu halten.

Die paradoxe Folge von CNA ist auf eine zweite, nicht-technische Ursache zurückzuführen. Zivile Ziele können bei Computernetzwerkangriffen und anderen Informationsoperationen zu militärisch relevanten Zielen werden, in dem der militärischen Führung sie als solche deklariert.[81] Dies ist weniger eine technische Folge, als vielmehr das Resultat neuer Militärstrategien, (z.B. „effekt-basierter Operationen") und der eingeschränkten politischen Zielsetzung bestimmter Militäroperationen (Schonung der Infrastruktur, keine Bodentruppen, etc.). Diese Militärstrategien stellen nicht mehr die Zerstörung oder die territoriale Besetzung in den Vordergrund, sondern den Effekt bestimmter Waffeneinsätze auf die Ziele von Militäroperationen. Das Zerstören ziviler Ziele, z.B. öffentlicher Computernetzwerke, kann dann ein gewünschter Effekt sein, um Datenströme und Informationsflüsse zu unterbrechen. Wenn militärische Gewalt von Regierungen in Konflikten nur begrenzt sanktioniert ist, könnten Computernetzwerkangriffe ihre Schadenswirkung entfalten und ohne lange Aufmarschzeiten oder ohne die Stationierung von Bodentruppen politische Ziele erreichen.

Nichtkombattanten und zivile Infrastrukturen sind durch das Völkerrecht vor militärischen Angriffen geschützt, solange sie nicht direkt und effektiv an der Kriegsführung beteiligt sind. CNA stellen keinen physischen Angriff (im völkerrechtlichen Sinne) dar und Nichtkombattanten (und Kombattanten) kommen in der Regel nicht zu Schaden, wenn nur Computersysteme über die Datenleitungen angriffen werden. Gerade in diesen Fällen eröffnen CNA die Option, solche vom Völkerrecht geschützten zivilen Einrichtungen „legitimerweise" in Militäroperationen dennoch angreifen zu dürfen.[82] Zivile Ziele und Einrichtungen, die nicht kriegsrelevant sind, werden nun ein Faktor in militärischen Auseinandersetzungen. Darüber hinaus werden zivile Netze und Einrichtungen nicht nur technisch „bekämpfbar", sie werden zu einer militär-strategischen Notwendigkeit, um eine gegnerische Gesellschaft und ihre Regierung zu bezwingen. CNA ist daher ein ideales, komplementäres Instrument für Militäroperationen oder Krisen, in denen eine mit militärischer Gewalt abgesicherte Diplomatie („Coercive Diplomacy") theoretisch die Bevölkerung gegen ihre Regierung aufbringen soll. Die Auswirkungen sind allerdings paradox. So schreibt Michael Schmitt: „Civilians and civilian objects continue to enjoy protected status vis-à-vis those aspects of CNA that cause human suffering and physical damage. (...) Indeed, military commanders will in certain cases be obligated to employ their cyber

81 Vgl. Thomas W. Smith, The New Law of War: Legitimizing High-Tech and Infrastructural Violence, in: International Studies Quarterly, Jg. 46, Nr. 3, 2002, S. 351-357. Quénivet, a.a.O. (Anm. 76).

82 Z.B. wenn wie im Kosovo-Krieg die Telekommunikationseinrichtungen in einer Stadt angriffen wird, um die Führungs- und Kommandozentralen zu beeinträchtigen.

assets in lieu of kinetic weapons when collateral damage and incidental effects can be limited."[83]

3.4 Automatisierung und die politische Kontrolle von Militäroperationen

Der Einzug von Computersystemen, Digitalisierung und Vernetzung in die Kriegsführung von Demokratien hat eine weitere bedenkliche Auswirkung: den Verlust der politischen Kontrolle über Militäroperationen. Er entsteht durch die neuen technologischen Möglichkeiten (kürzere Reaktionszeiten) *und* die unbedachte freiwillige Abgabe der zivilen Kontrolle, um die schnelle Reaktionsfähigkeit in einen militärischen Vorteil umzumünzen.

Zunächst sieht es so aus, als ob Digitalisierung und Vernetzung die politische Kontrolle über Militäroperationen stärkt. Auf den Bildschirmen seiner vorgelagerten Zentrale in Qatar konnte der US-Oberbefehlshaber Tommy Franks im Irakkrieg 2003 die Aktionen und Position jedes Truppenteils live verfolgen.[84] Die Technologie der Vernetzung ermöglicht die politische Kontrolle bis hin zur taktischen Ebene. Fortschritte in der Datenkommunikation machen es theoretisch möglich, dass der zivile Oberbefehlshaber in Demokratien direkt in Echtzeit über das Geschehen auf Schlachtfeld informiert wird und lokal eingreifen kann, um etwa Operationen abzubrechen, weil z.B. zivile Opfer zu befürchten sind.[85] Die zivile und die militärische Führung gewinnen so einen besseren Überblick („God's View") über das Kriegsgeschehen. Während solche Systeme die zivilen Interventionen und die demokratische Kontrolle stärken, birgt die Einführung neuer Technologien auf dem Schlachtfeld die Gefahr des „Mikromanagement" in sich.[86] Die zivil-militärischen Beziehungen könnten aus der Balance geraten, wenn sich die zivile und die militärische Führung im Blick auf zu viele taktische Details verlieren, denn auch die Live-Übertragung von Drohnen zeigt nur einen kleinen „strohhalmartigen" Ausschnitt des dynamischen Geschehens auf dem Schlachtfeld. Die Frage stellt sich daher, wie die Technologien der Automatisierung und Digitalisierung von der politischen und militärischen Führung genutzt werden, damit die technischen Möglichkeiten nicht nur zu einer „Unterhaltungsshow" für die Divisionskommandeure werden.[87]

Die politischen Risiken der Automatisierung der Kriegsführung liegen indes anderswo. Die Automatisierung von Zielaufklärung und Zielbekämpfung durch „C4ISR"-Systeme, „Battle Management"-Systeme („BM/C2") und vernetzte Waffensysteme führt zu schrumpfenden Reaktionszeiten. Die Kriegsführung hat sich beschleunigt, und Geschwindigkeit wird zu einem kriegsentscheidenden Faktor. Die Automatisierung und

83 Michael N. Schmitt, Wired Warfare: Computer Network Attack and Jus in bello, in: International Review of the Red Cross, Jg. 84, Nr. 846, 2002, S. 365-399. S. 397.

84 Joseph L. Galloway, General Tommy Franks Discusses Conducting the War in Iraq, Knight Ridder Newspapers, 19.06.2003.

85 Thomas E. Ricks, Beaming The Battlefield Home, Washington Post, 26.03.2002. S. A01. Thomas E. Ricks, Target Approval Delays, Cost Air Force Key Hits, Washington Post, 18.11.2003. S. A01.

86 William M. Arkin, The Rules of Engagement, Los Angeles Times, 21.04.2002.

87 Thomas E. Ricks, Beaming The Battlefield Home, Washington Post, 26.03.2002. S. A01.

Vernetzung von Systemen („Systems of Systems") führt dazu, dass sich der Mensch als das langsamste Element in der Entscheidungsfindung herausstellt. Immer mehr verfügbare Sensoren und Aufklärungssysteme verdichten den clausewitzschen Schlachtennebel durch „Informationsüberflutung", weil der Kommandozentrale oder dem einzelnen Soldaten im Feld zu viele Informationen bereitgestellt werden, die nicht mehr verarbeitet werden können. In einem solchen Falle würde es nahe liegen, weitere menschliche Entscheidungen über Militäreinsätze mit Hilfe von Informationstechnologie, Computern und „Battle Management"-Systemen zu rationalisieren, zu automatisieren und zu optimieren. Der menschliche Entscheidungsspielraum wird dann reduziert mit dem Effekt, dass Menschen aus dem automatisierten und digitalisierten Entscheidungsablauf herausgehalten werden.

Die Wurzeln dieser Automatisierung der Kriegsführung stammen aus der Nuklearstrategie der 60er und 70er Jahre, als Computer zur Verarbeitung von Frühwarndaten bis hin zu Freigabeprozeduren benötigt wurden, um unter den Bedingungen verkürzter Vorwarnzeiten die nukleare Abschreckung aufrechtzuerhalten.[88] Die Automatisierung führt in der Konsequenz zu einer möglichen Entmenschlichung operativer und taktischer Kriegsentscheidungen.[89] Die informationstechnologische Vernetzung von Aufklärungs- und Waffensystemen wirft damit neue Fragen der demokratischen Kontrolle von Militäreinsätzen und der zivil-militärischen Beziehungen auf.

Die Zeitspanne, zwischen Zielaufklärung, Bekämpfung und der verifizierten Zerstörung des Ziels („sensor-to-shooter"), kann inzwischen in einigen Fällen auf wenige Minuten komprimiert werden.[90] In der „Operation Enduring Freedom", dem Krieg in Afghanistan, betrug diese Zeit durch die Vernetzung von JSTAR-Aufklärungsflugzeugen, Spezialeinheiten und in Warteschleife fliegenden B-52 Bombern nur mehr 10 Minuten. Beim Einsatz der unbemannten, bewaffneten Kampfdrohne („UCAV") Predator gegen einzelne Ziele in Afghanistan lag diese Zeit noch darunter.[91] Dort wurden erstmals verschiedene Waffensysteme, Plattformen und Spezialeinheiten so vernetzt, wie es die Strategie der „netzwerk-zentrischen Kriegsführung" vorsieht. In diesem Krieg konnten u.a. das AC-130 „Spectre" Flugzeug, eine Art fliegende Artillerie mit immenser Zerstörungskraft, mit Echtzeit-Videobildern aus Aufklärungsdrohnen versorgt werden.

88 Vgl. den wegweisenden Beitrag Holger Iburg, Abschreckung und Software. Computertechnologie als Instrument der amerikanischen Sicherheitspolitik, Frankfurt a.M. (Campus), 1991. Frank Barnaby, The Automated Battlefield, London (Sidgwick & Jackson), 1986.

89 Vgl. Thomas K. Adams, Future Warfare and the Decline of Human Decisionmaking, in: Parameters, Jg. 31, Nr. 4, 2001, S. 57-71.

90 „Find, Fix, Track, Target, Engage, Assess" Zyklus, von der US-Luftwaffe auch „Sensor to Shooter" oder „kill chain" genannt. Vgl. Adam J. Hebert, Compressing the Kill Chain, in: Air Force Magazine, Jg. 86, Nr. 3, 2003, S. 50-54.

91 Vernon Leob, U.S. Gains in Attacking Mobile Arms, Washington Post, 5.07.2002. S. A14. John H. Chushman, Pentagon's Urgent Search For Speed, New York Times, 1.12.2002. Usha Lee McFarling, The Eyes and Ears of War: Data streaming from satellites proved pivotal in Iraq, Los Angeles Times, 24.04.2003.

Die Anzahl und das Einsatzspektrum von Drohen nehmen ständig zu.[92] In den US-Streitkräften kommt ferner schon heute eine digitale Zielerfassung zum Einsatz, die Boden- und Luftstreitkräfte miteinander vernetzt. Ebenso verwenden die US-Streitkräfte „Battle Management"-Systeme, die verschiedene Informations- und Nachrichtenquellen automatisch auswerten und mit Waffensystemen zusammenführen. Gemeinsam ist diesen Systemen, dass sie den „OODA-Zyklus" erheblich verkürzen. Ähnlich der Telematik machen sie obendrein die Kriegsführung aus der Distanz möglich.[93] Diese Digitalisierung und Automatisierung werden noch ausgeweitet. Sie sollen u.a. zu weniger zivilen Opfern führen.[94] Eine Forschungsabteilung des US-amerikanischen Verteidigungsministeriums „DARPA" und andere Einrichtungen forschen an weiteren futuristischen Projekten wie z.B. automatischen und halbautomatischen Kampfrobotern und der Miniaturisierung von Waffensystemen, die z.B. ihre Ziele selbst suchen.[95] Das Ziel ist, den Entscheidungszyklus weiter zu automatisieren und die meisten Entscheidungen durch Maschinen ausführen zu lassen.[96] Der Mensch wird dann effektiv aus dem Entscheidungsablauf („taking the human out of the loop") herausgenommen.

Digitalisierung und Automatisierung ermöglichen ein so rasches Handeln, dass die in Demokratien notwendige wie zeitraubende politische Entscheidung und zivile Kontrolle als operativ hinderlich erscheint. Daher wird die Autorisierung von bestimmten Operationen nach unten in die Befehlskette delegiert oder auf Vorratsbeschluss gefasst. Dies trifft zum Beispiel auf die Kriegsführung in Afghanistan gegen einzelne Mitglieder der al Qaida und der Taliban-Regierung oder einzelne US-amerikanische Spezialoperationen (z.B. Jemen) im Rahmen des „globalen Krieg gegen den Terrorismus" zu.[97] Unter dem Druck der Notwendigkeit kurzer Reaktionsfähigkeiten bei militärischen Operationen gegen Terroristen wird politische Autorität über Kommando und Kontrolle von Streitkräfte auch in hochsensiblen Bereichen, wie der direkten Tötung von Gegnern, zurückgenommen. So berichtet die New York Times über den bewaffneten Aufklärungsdrohneneinsatz im Je-

92 Vgl. zu Einsatzmöglichkeiten und technischen Details: Sascha Lange, Flugroboter statt bemannter Militärflugzeuge, SWP Studie Nr. S 29, Berlin (Stiftung Wissenschaft und Politik) 2003.

93 Peter Pae, Ushering In the Warfare Information Age, Los Angeles Times, 16.03.2002. David A. Fulghum, Rumsfeld Pushes Network Warfare, Aviation Week & Space Technology, 11.11.2002. S. 32.

94 Gerry J. Gilmore, Military Works On Faster, All-Digital Targeting System, American Forces Press Service, 24.10.03. http://www.iwar.org.uk/news-archive/2003/10-24-3.htm (24.10.2003)

95 Jürgen Altmann, Military Uses of Microsystem Technologies: Dangers and Preventive Arms Control, Münster (Agenda), 2001. Gebhard Geiger, Rüstungspotentiale neuer Mikrotechnologien: Konsequenzen für internationale Sicherheit und Rüstungskontrolle, SWP Studie Nr. S 24, Berlin (Stiftung Wissenschaft und Politik) 2003.

96 Vgl. u.a. die Studie des US Joint Forces Command „Unmanned Effects: Taking the Human out of the Loop" zitiert in Ron Schafer, USJFCOM Press Release: Robotics to Play Major Role in Future Warfighting, Norfolk: (U.S. Joint Forces Command) 2003. http://www.jfcom.mil/newslink/storyarchive/2003pa 072903. htm (01.08.2003)

97 Chris Floyd, Global Eye – Into the Dark, Moscow Times, 1.11.2002. James Risen/David Johnston, Bush Has Widened Authority of C.I.A. to Kill Terrorists, New York Times, 15.12.2002. David Isenberg, 'P2OG' allows Pentagon to fight dirty, Asia Times, 05.11.02.

men, dass der US-Präsident die direkte Entscheidung darüber delegiert hatte.[98] Inzwischen existieren in den USA Pläne, die per Joystick vom Boden aus gesteuerten Kampfdrohnen nicht mehr nur durch Angehörige der Luftwaffen steuern zu lassen, sondern dafür zivile Subunternehmer einzusetzen.[99] Der militärische Befehlshaber würde dann zwar über die operative Kontrolle verfügen, aber dem Zivilisten nur noch „über die Schulter" schauen.[100]

Die Automatisierung der Kriegsführung hat – neben dem möglichen Verlust politischer Kontrolle – einen zweiten negativen Effekt. Bei der starken Kompression der Reaktionszeiten ist die Gefahr größer geworden, dass Zivilisten in die Schusslinie geraten oder versehentlich getroffen werden. Aufklärungsdaten können zwar schneller verarbeitet werden, sie werden aber dadurch nicht „besser". Automatisierung und Digitalisierung tragen zum Beschleunigen des militärischen Handlungszyklus bei. Jedoch haben solche „C4ISR"-Systeme, ihre technischen und sozialen Grenzen.[101] An die technischen Grenzen stoßen solche Sensoren und Aufklärungssysteme im komplexen Terrain wie Wäldern oder in Städten. Ebenso stoßen sie beim zu übertragenden Datenvolumen an ihre Grenzen. Die seit dem ersten Weltkrieg gültigen militärischen Prinzipien des Suchens von „Deckung", das „Verbergen", die „Täuschung" und das „Verteilen" haben sich selbst im Afghanistan-Krieg des 21. Jahrhunderts als effektiv gegen eine informationsüberlegene Streitmacht gezeigt.[102] Das Terrain in Afghanistan gab al Qaida- und Taliban-Kämpfern, die Möglichkeit von elektronischen Sensoren unentdeckt zu bleiben. So konnten Stellungen erst durch „Reconaissance by Fire" bestimmt werden.[103] Aufklärung aus der Distanz und die Digitalisierung stößt bei der Erfassung möglicher Ziele an ihre Grenzen. Hinzu kommt, dass die durch „C4ISR" verarbeiteten Informationen weder verhindern können, dass eigene Truppen getroffen werden, noch können sie in Bürgerkriegen mit fließenden Fronten zwischen Zivilisten und Kombattanten unterscheiden. Wenn die Informationen „falsch" sind, werden auch weiterhin Zivilisten getroffen. Der hohe Anspruch der zivilen Opfervermeidung wird auch künftig trotz „C4ISR" in den Konflikten mit niedriger Intensität leiden. So stieg in dem aus Florida und den US-Operationszentren in Saudi-Arabien ferngelenkten Krieg in Afghanistan, die zivile Opferzahl trotz des Einsatzes von

98 David E. Sanger/David Johnston, Yemen Killing Based on Rules Set Out by Bush, New York Times, 6.11.2002.

99 Butler, Amy, DOD considers Using Civilians To Pilot UAVs in Military Operations, Inside the Air Force, 01.11.2003. Butler, Amy, Air Force Chief Says Service „Vervous" About Civilians UAV Pilots, Inside the Air Force, 08.11.2003.

100 Ebenda.

101 Vgl. die gemischte Bewertung von Sensoren, Computern und Kommunikation in Michael E. O'Hanlon, Technological Change and the Future of Warfare, Washington, D.C. (Brookings Institution Press), 2000. S. 64-67.

102 Vgl. die empirische Untersuchung von Stephen Biddle, Afghanistan and the Future of Warfare: Implications for Army and Defense Policy, Carlisle, PA (U.S. Army War College, Strategic Studies Institute 2002). Sowie die „C4ISR" und „Battle Management" Auswertung von Anthony H. Cordesman, The Lessons of Afghanistan: War Fighting, Intelligence, and Force Transformation, Washington, D.C. (CSIS Press), 2002. S.100-101 u. 112-114.

103 Vgl. Biddle, a.a.O (Anm. 102). Cordesman, a.a.O. (Anm.102).

Präzisionsmunition („PGM“) und Aufklärung in Echtzeit wieder an.[104] Die hohe Zahl an zivilen Opfern in Afghanistan – trotz Automatisierung und Digitalisierung der Zielerfassung und Bekämpfung von Zielen mit Präzisionsmunition – ist nur ein Symptom dafür, dass es auch zu tragischen Katastrophen durch die Komplexität der Interaktion von Menschen und Maschinen kommen kann.

3.5 Rüstungskontrolle und Informationskriegsstrategien

Die „RMA“ führt zu einer neuen Rüstungsdynamik. Die Einführung von Informationstechnologien transformiert die Streitkräfte. Neue Doktrinen und Strategien werden entwickelt und finden Eingang in die Militärpläne. Damit wird erstens eine qualitative Dynamik in den Streitkräften ausgelöst – sie steigern die militärische Effektivität. Zweitens verursachen die „Strategien der Informationskriegsführung“ eine neue internationale Rüstungsdynamik: Andere Staaten übernehmen Strategien und Technologien der „RMA“ nicht mehr „eins zu eins“, sondern passen sie an ihre Erfordernisse und Fähigkeiten an.[105]

Damit steht die traditionelle Rüstungskontrolle vor einer neuen Herausforderung. Nicht mehr eine militärische Konfrontation zweier Machtblöcke oder regionale Rüstungswettläufe sind der Auslöser für die Rüstungsdynamik. Es geht heute auch nicht mehr um Stückzahlen von Waffensystemen oder das austarieren einer fragilen Balance. Die neue Rüstungsdynamik speist sich aus „harter“ technologischer Innovation und „weichen“ Elementen wie der Umorganisation der Streitkräfte und neuen Einsatzkonzepten. Sie verursacht einen qualitativen Sprung in der militärischen Effizienzsteigerung. Die Herausforderungen bei der Regulation qualitativer Rüstungsprozesse nehmen daher zu. Für die „Strategien der Informationskriegsführung“ existieren bislang weder Rüstungskontrollregime noch -konzepte.[106] Aufgrund ihres virtuellen Charakters sind die meisten Informationsoperationen mit traditionellen Rüstungskontrollinstrumenten nicht zu er-

104 Vgl. ebenso einige Vorfälle im Kosovo. Im Afghanistan-Krieg stieg nach inoffiziellen Schätzung die Zahl der zivilen Opfer beachtlich an – trotz der „Revolution in Military Affairs“ und dem Einsatz von Präzisionsmunition (PGM) von über 50% (Kosovo ca. 30%, Golfkieg 1991 <10%). Vgl. Carl Conetta, The "New Warfare" and the New American Calculus of War, Briefing Memo Nr. 26, Cambridge, MA: Commonwealth Institute, Project on Defense Alternatives 2002. http://www.comw.org/pda/0209 newwar.html (3.10.2002)

105 Vgl. Demchak, a.a.O. (Anm. 46). Hashim, a.a.O. (Anm. 46).

106 Mit einigen Ausnahmen, vgl. die ersten Überlegungen von Andrew Rathmell, Information Warfare: Implications for Arms Control, in: Bulletin of Arms Control, Jg. 29, 1998, S. 8-14. William Church, IO Treaty Development Language, Revision 1.0, 1999. Vgl. auch die fruchtlosen Versuche Rußlands 1999 und 2001 in der UNO einen solchen Vertrag anzustoßen, sowie zweier Fachkonferenzen, die sich des Themas in unterschiedlicher Weise näherten: Chemical and Biological Arms Control Institute (CBACI)/Directorate for Nuclear and Counterproliferation (AF/XON) U.S. Air Force, Cyberwarfare: What Role for Arms Control and International Negotiations? (Draft Workshop Report), Washington, D.C.: 2000. *Heinrich Böll Stiftung,* Rüstungskontrolle im Cyberspace: Perspektiven der Friedenspolitik im Zeitalter von Computerattacken, Dokumentation, Berlin: HBS 2001.

fassen und entziehen sich so möglichen Beschränkungen. Verstärkt werden diese Probleme dadurch, dass auch die bestehenden Rüstungskontrollregime in der Krise stecken.[107]

Die „RMA"-Entwicklung und ihre Dynamik lässt sich in drei Stufen beschreiben. Auf der ersten Stufe finden sich Staaten, die schon heute eine „RMA" umsetzen und führend in diesem Gebiet sind. Dazu gehören die USA, Großbritannien, Frankreich und Japan. Auf der zweiten Stufe finden sich die Staaten, die im Begriff sind, eine „RMA" umzusetzen: Deutschland, Israel, Russland, Schweden, Südkorea, u.a. Die dritte Stufe umfasst demokratische wie nichtdemokratischer Staaten, die mittel- bis langfristig das Potential besitzen, eine „RMA" durchzuführen oder andere Staaten an Fähigkeiten gar zu überholen. Dazu gehören: China, Brasilien, Südafrika, Indien, Pakistan u.a. Die Fähigkeiten und die Chancen der „RMA" sind daher nicht nur auf Demokratien mit entwickelten Infrastrukturen begrenzt. Die „RMA" kann von allen Staaten umgesetzt werden, die eine entsprechende Vernetzung, Digitalisierung und Neukonzeption ihrer Streitkräfte und Strategien vornehmen.

Für Demokratien ist die Transformation der Streitkräfte ein möglicher Weg, um die ihrer Kriegsführung auferlegten „normativen" Beschränkungen (Opfervermeidung auf beiden Seiten) auszuhebeln. Computernetzwerkangriffe oder die Vernetzung von Sensoren und Waffenplattformen sind „moralisch" weniger vorbelastet. Durch die „Strategien der Informationskriegsführung" entstehen neue Schwierigkeiten für die traditionelle Rüstungskontrolle, da eine scheinbar größere Vermeidung ziviler Opfer ein Nebeneffekt der „RMA" sein kann. Die Integration von „RMA"-Technologien in die Streitkräfte umgeht damit Anwendungstabus, wie sie z.B. bei Massenvernichtungswaffen existieren. Sie sind nicht mehr dazu da, unterschiedslos zu töten oder unnötiges Leid zu verursachen. Sie sollen im Gegenteil dazu führen, dass Kriege und Interventionen kürzer und präziser werden und die Zivilbevölkerung schonen. Unter diesen Prämissen besitzen Demokratien kaum ein „moralisches" Interesse, die als positiv gesehenen Nebenwirkungen von Informationsoperationen und der „RMA" zu ächten.

Selbst wenn es im nationale wie moralischem Interesse der Demokratien sein sollte, Technologien und Strategien einzudämmen, gilt es weitere Hindernisse zu überwinden. Die technologischen Innovationen im Bereich der Informations- und Telekommunikation oder der Softwareindustrie stammen aus der zivilen Industrie. Aus Kostengründen werden zivile Produkte zum Teil auf militärische Anwendungen und Bedürfnisse nur noch zugeschnitten. Die meisten Informations- und Telekommunikationstechnologien sind „Dual-Use"-Güter, die in beiden Bereichen Anwendung finden, was eine effektive Rüstungskontrolle erschwert. Die Demokratien haben mithin kaum ein „nationales" und „moralisches" Interesse daran, solche Technologien und Strategien zum Gegenstand von Rüstungskontrollvereinbarungen zu machen, solange sie eine Monopolstellung über eben diese Systeme und Konzepte besitzen.

107 Vgl. Joseph Cirincione (Hg.), Repairing the Regime: Preventing the Spread of Weapons of Mass Destruction, New York (Routledge), 2000.

Die Schwierigkeiten der klassischen Rüstungskontrolle im Umgang mit den neuen „Strategien der Informationskriegsführung“ sind auf die Kennzeichen der qualitativen Rüstungsdynamik und auf die Charakteristika der „Strategien der Informationskriegsführung“ zurück zuführen.

Erstens steht und fällt jede wirksame rüstungskontrollpolitische Vereinbarung mit ihrer Verifizierbarkeit, Sanktionierung und Durchsetzbarkeit. Die gegenwärtige Netzstruktur macht es schwer, wenn nicht gar unmöglich, die Urheber von Computernetzwerkangriffen eindeutig zu identifizieren. Zugleich wird es schwierig sein, einen groß angelegten Angriff auf die zivil-militärische Informationsinfrastruktur von System- oder Benutzerfehlern zu unterscheiden. Damit ist nahezu unmöglich, die Verletzung von Rüstungskontrollverträgen durch Vertragsteilnehmer festzustellen. Die allgemeine Erfassung von Kommunikation und Datenverkehr würde darüber hinaus individuelle Freiheitsrechte einschränken und wegen ihrer Kosten auch das Wachstum in der Informations- und Telekommunikationsbranche beeinträchtigen.

Selbst eine Rüstungskontrolle ohne Verifikationsmechanismen ist schwierig zu entwerfen. CNA-Softwaretools als „Waffen“ sind derzeit weder „quantifizierbar“ noch „definierbar“, so dass es hier keine klassischen Rüstungsobergrenzen geben kann. Software lässt sich leicht und schnell duplizieren. Angriffswerkzeuge in Form von Programmen haben „Dual-Use“-Charakter. So sind CNA-Werkzeuge teilweise frei im Internet erhältlich, oder sie werden zum defensiven Testens gegen die eigenen Systeme benötigt, um die Sicherheit, Zuverlässigkeit und Integrität zu erhöhen und Sicherheitslücken zu schließen. Somit entfällt auch die Unterscheidung zwischen offensiven und defensiven Computernetzwerkoperationen und ihren Werkzeugen. Hier könnte sich zwar ein Verbot für Streitkräfte durchsetzen, aber die „Proliferation“ der Angriffswerkzeuge lässt sich aufgrund des „Dual-Use“-Charakters nicht verhindern.

Zweitens kann die Rüstungskontrolle kaum das gesamte Spektrum der militärisch interessanten Informationsoperationen abdecken. Es ist zwar vorstellbar, psychologische Operationen zu verbieten. Da sie aber keine direkten physischen Auswirkungen haben, wird es schwer sein, sie international zu ächten. Im Falle von virtuellen Computernetzwerk-operationen ohne physische Schadenswirkung liegt der Fall ähnlich. Noch schwieriger wird es für die Rüstungskontrolle bei anderen „Strategien der Informationskriegsführung“ wie der Automatisierung und Vernetzung von Systemen, die nur mittelbare Auswirkungen auf die Kriegsführung haben, etwa die Reduzierung der Reaktionszeiten.

Drittens sind „Strategien der Informationskriegsführung“ in vielen Fällen bislang nur konzeptionelle Entwürfe oder Visionen. Diese Konzepte sind neben der Technik die treibenden Faktoren der Rüstungsdynamik. Die Proliferation von Konzepte, Strategien und Doktrinen lässt sich nur schwerlich zum Gegenstand der Rüstungskontrolle machen.

Selbst Rüstungskontrollvereinbarungen, die auf der Ebene der Transparenz und der Vertrauensbildung ansetzen, stoßen viertens bei den „Strategien der Informationskriegsführung“ an ihre Grenzen. Die Inspektionen und das Offenlegen von Waffenplattformen, Laboren, Systemen oder Softwarearchitekturen würden Sicherheitsprobleme erst

mit sich bringen oder gar verursachen. Wie bei anderen in die Krise geratenen Rüstungskontrollregimen wäre die Wirksamkeit von Rüstungskontrollverträge infrage gestellt, wenn der Staat mit dem größten Informationskriegspotential (derzeit die USA) nicht daran teilnimmt.

Einige Rüstungskontrollskeptiker streiten aus den genannten Gründen wenn nicht die Notwendigkeit, so doch die Möglichkeit erfolgreicher rüstungskontrollpolitischer Maßnahmen für die „RMA" ab. Sie verweisen darauf, dass das Gewalt- und Aggressionsverbot der VN-Charta jegliche Art von Waffen einschließt und die Definition von Waffen bewusst offenlässt.[108] Staaten verlieren auch bei Computernetzwerkangriffen nicht ihr Recht auf „verhältnismäßige" Selbstverteidigung.[109]

Unter den Bedingungen der gegenwärtigen rüstungskontrollpolitischen Krise und der offenkundigen Schwierigkeiten, einen Konsens darüber zu erlangen, welche Informationsoperationen verboten werden sollten und welche nicht, scheint ein solches rüstungskontrollpolitisches Unterfangen nicht praktikabel. Vielen Autoren und Experten sehen die „RMA" als unausweichlichen Prozess an, der sich nicht steuern lässt.

4. Fazit und Empfehlungen: Eine alternative Sichtweise auf die neuen Strategien, Technologien und die Zukunft der Rüstungskontrollpolitik

Die neuen Militärtechnologien und Strategien bringen in langfristiger Perspektive ein schleichendes Risiko für die Friedfertigkeit von Demokratien mit sich. Die sogenannte „RMA" senkt die materiellen, politischen und moralischen Kosten der Kriege. Die neuen Militärtechnologien und Strategien nähren das Bild eines sauberen, vollautomatisierten, präzisen Krieges, der die Opfer auf beiden Seiten minimiert. Kriege, Interventionen und alle anderen Arten von Militäroperationen werden damit für Demokratien „akzeptabler", weil die moralische Hemmschwelle des Einsatzes militärischer Mittel sinkt. Informationsoperationen unterminieren die Grenze zwischen Krieg und Frieden. Sie schaffen eine operative Grauzone, welche die für eine demokratische Kontrolle notwendige Entscheidungsschwelle beseitigt. Zivile Aufsicht und Kontrolle können hier am ehesten versagen. Andere „Strategien der Informationskriegsführung", wie die Automatisierung, Digitalisierung und Vernetzung können einen Verlust an ziviler Kontrolle über Militäroperationen nach sich ziehen und erhöhen paradoxerweise auch das Risiko ziviler Schäden. Von der Steigerung militärischer Effektivität profitieren (noch) vor allem Demokratien mit ihren

108 Vgl. Lawrence T. Greenberg/Seymour E. Goodman, Information Warfare and International Law, Washington, D.C. (National Defense University), 1998.

109 Dieses Recht und was genau als verhältnismäßiges Mittel als Antwort im Falle von Computernetzwerkangriffe auf die nationale Infrastruktur gewertet wird, wird von Staaten unterschiedlich interpretiert. Russland behält sich angeblich das Recht vor, auf eine solche Attacke auch mit Nuklearwaffen zurückzuschlagen. Vgl. Timothy L. Thomas, Russian Views on Information Warfare, in: Airpower Journal (Special Edition), Jg. 10, Nr. 1, 1996, S. 25-35.

modernen Streitkräften. Dies geschieht unter der Preisgabe rüstungskontrollpolitischer Maßnahmen. Erschwerend kommt hinzu, dass sich die „Strategien der Informationskriegsführung" der klassischen Rüstungskontrolle entziehen. Dennoch muss Rüstungskontrolle auch im Informationszeitalter der hochvernetzten und digitalisierten Streitkräften nicht an Bedeutung verlieren. Mit einem stärkeren Gewicht auf die normenorientierte statt interessen-orientierte Rüstungskontrolle eröffnen sich Möglichkeiten, die „RMA", „Strategien der Informationskriegsführung" und „Informationsoperationen" einzuhegen.

Es existieren zwei Sichtweisen auf die „RMA" und die Relevanz der Rüstungskontrolle. Einige Autoren betrachten ihre Ursachen als eine technologische Eigendynamik, die nicht steuerbar ist.[110] Der „RMA" muss durch die Investition in die „richtigen" Technologien, mit der Neuorganisation der Streitkräfte und der Neuformulierung von Strategien durch eine „RMA"-freundliche Politik zum Durchbruch verholfen werden. Der Handlungsspielraum und die Relevanz von Rüstungskontrolle für diesen Prozess sind gleich null. Rüstungskontrolle wird hier nur als verlängerter Arm der Durchsetzung nationaler Interessen konzeptionalisiert. Dieser Logik folgend, sehen daher die Anhänger dieser Thesen auch keine Chancen, Informationsoperationen zum Gegenstand der Rüstungskontrolle zu machen.[111] Versteht man dagegen die „RMA" und ihre Strategien und Technologien nicht als technologisch determiniertes Ergebnis, sondern als ein soziales Konstrukt, eine Evolution oder als eine „Transformation", deren Entwicklung, Form und Ausgang offen sind, dann eröffnen sich neue Handlungsmöglichkeiten.[112] Die Ausgestaltung der „RMA" hängt in dieser Sichtweise von Akteuren (deren Wahrnehmung, Interessen und Orientierungen), Institutionen und sowie von in der Gegenwart getroffenen Politikentscheidungen ab. Auch die „neue" Rüstungsdynamik ist ein sozialer Prozess, der sich nur nach dem Inhalt und Gegenstand der Strategien und Technologien geändert hat.[113]

110 Vgl. u.a. Andrew F. Krepinevich, Cavalry to Computers, in: National Interest, Jg. 37, Nr. 3, 1994, S. 28-36. Mackubin Thomas Owens, Technology, the RMA, and the Future of War, in: Strategic Review, Nr. 2, 1998, S. 63-70. Vgl. Owens, a.a.O. (Anm. 51). James Adams, The Next World War: Computers Are the Weapons And the Front Line Is Everywhere, New York (Simon & Schuster), 1998. Bruce D. Berkowitz, The New Face of War: How War Will be Fought in the 21st Century, New York (Free Press), 2003.

111 Gebhard Geiger, Offensive Informationskriegsführung. Die "Joint Doctrine for Information Operations" der US-Streitkräfte: sicherheitspolitische Perspektiven, SWP Studie Nr. S 2, Berlin: Stiftung Wissenschaft und Politik 2002. S. 20. Vgl. die interessengeleite Diskussion und in der Summe ebenfalls negative Bewertung in Chemical and Biological Arms Control Institute (CBACI)/Directorate for Nuclear and Counterproliferation (AF/XON) U.S. Air Force, Cyberwarfare: What Role for Arms Control and International Negotiations? (Draft Workshop Report), Washington, D.C.: 2000.

112 Vgl. u.a. Stephen Biddle, The Past as a Prologue: Assessing Theories of Future Warfare, in: Security Studies, Jg. 8, Nr. 1, 1998, S. 1-74. Michael E. O'Hanlon, Beware the "RMA'nia!" Paper presented at National Defense University, Washington, D.C.: 1998. O'Hanlon, a.a.O. (Anm. 101). Earl H. Tilford, The Revolution in Military Affairs: Prospects and Cautions, Carlisle, PA: U.S. Army War College, Strategic Studies Institute 1995.

113 Vgl. Harald Müller, Technologie und Sicherheitspolitik: Der Einfluß von technischem Wandel auf Strategie und Rüstungskontrolle, in: Christian Hacke/Manfred Knapp (Hg.), Friedenssicherung und Rüstungskontrolle in Europa, (Wissenschaft und Politik) 1988, S. 173-209. Erwin Müller, Rüstungstechnologische Innovationen: Überzeitliche Prinzipien und Strukturkonstanten von Waffenentwicklung, Rüs-

Die Rüstungsdynamik, verstanden als sozialer Prozess, ist dann zu einem gewissen Grad steuerbar, und Handlungsspielräume eröffnen sich. Rüstungskontrolle wird hier nicht mehr nur macht- und interessenorientiert gesehen, sondern als ein an sozialen Normen orientiertes Instrument. Mittels Normen, z.B. Tabus, Regeln oder einer rüstungskontrollfreundlichen Kultur kann das Verhalten von Akteuren beeinflusst werden.[114] Internationale Organisationen wären hier die Arenen für einen rüstungskontrollpolitischen Dialog. So besteht die Aussicht, dass die risikoreiche Wirkung und Entwicklung von einigen Informationsoperationen doch reguliert und zum Gegenstand „weicher" Rüstungskontrolle werden kann.[115] Vor allem eröffnen sich die Perspektiven, durch eine präventive Rüstungskontrollpolitik die versucht, frühzeitig kritische Entwicklungen in Strategie und Technologie zu identifizieren.[116] Wichtigstes Instrument, um eine Rüstungskontrolle für Informationsoperationen in Gang zu setzen, ist eine „Kultur der militärischen Zurückhaltung".[117]

Die Rüstungskontrolle muss daher nicht unter den Bedingungen des Informationszeitalters versagen, sondern kann in einer Neukonzeption und Anpassung zu einem Instrument zur Einhegung der „RMA" und ihrer negativen Konsequenzen werden.[118] Dies ist um so dringender, als die unkontrollierte Anwendung und Ausweitung von Informationsoperationen letztlich auch den Kern von Sicherheit und Vertrauen in der Informationsgesellschaft betreffen. Wenn in Krisen- und Friedenszeiten das Vertrauen in und die Systemsicherheit von Informations- und Telekommunikation durch Informationsoperationen gezielt oder als nichtintendiertes Resultat eines Angriffes auf komplexe und interdependente Systeme geschädigt werden, wird dies langfristig die Errungenschaften moderner Kommunikationsmittel zerstören. Rüstungskontrolle im Informa-

tungsmodernisierung und Rüstungsdynamik, in: Erwin Müller/Götz Neuneck (Hg.), Rüstungsmodernisierung und Rüstungskontrolle: Neue Technologien, Rüstungsdynamik und Stabilität, Baden-Baden (Nomos) 1991, S. 15-43. Andrew L. Ross, The Dynamics of Military Technology, in: David B. Dewitt/David G. Haglund/John J. Kirton (Hg.), Building a New Global Order: Emerging Trends in International Security, Oxford (Oxford University Press) 1993, S. 106-140.

114 Keith R. Krause, Culture and Security. Multilateralism, Arms Control and Security Building, in: Contemporary Security Policy, Jg. 19, Nr. 1, 1998, S. 1-22.

115 So z.B. Andrew Rathmell, Information Warfare: Implications for Arms Control, in: Bulletin of Arms Control, Jg. 29, 1998, S. 8-14. Olivier Minkwitz/Georg Schöfbänker, Information Warfare: Die neue Herausforderung für die Rüstungskontrolle, in: Vierteljahresschrift für Sicherheit und Frieden (S+F), Jg. 18, Nr. 2, 2000, S. 150-163. Joel Sokolsky, The Revolution in Military Affairs and the Future of Arms Control and Verification, Ottawa: Department of Foreign Affairs and International Trade, International Security Bureau 2001.

116 Thomas Petermann/Martin Socher/Christine Wennrich, Präventive Rüstungskontrolle bei neuen Technologien: Utopie oder Notwendigkeit?, Berlin (Sigma), 1997.

117 Hans-Joachim Schmidt, Konventionelle Rüstungskontrolle: Lessons Learned?, in: Heinrich Böll Stiftung (Hg.), Rüstungskontrolle im Cyberspace: Perspektiven der Friedenspolitik im Zeitalter von Computerattacken, Berlin (HBS) 2001, S. 42-46. Harald Müller, Früherkennung von Rüstungsrisiken in der Ära der militärisch-technischen Revolution, HSFK Report Nr. 7, Frankfurt am Main (Hessische Stiftung Friedens- und Konfliktforschung) 2000.

118 Emily O. Goldman, Arms Control in the Information Age, in: Contemporary Security Policy, Jg. 18, Nr. 2, 1997, S. 25-50.

tionszeitalter findet daher in beiden Varianten zur Vermeidung einer außer Kontrolle geratener Rüstungsdynamik ihre Berechtigung: Sowohl aus interessen-orientierter Politik zur Konservierung sicherheitspolitischer Vorteile der Demokratien als auch aus der normen-orientierten Sichtweise auf die Rüstungskontrolle macht es Sinn, Informationsoperationen zum Gegenstand von Rüstungskontrolle zu machen.

Da die meisten traditionellen Rüstungskontrollinstrumente (quantitative Beschränkungen, Verifikation, etc.) aufgrund des Charakters von Informationsoperationen nicht greifen, bleibt vorerst als praktikable Lösung die Schaffung einer „Kultur der militärischen Zurückhaltung". Sie kann als Form der normen-orientierten Rüstungskontrolle durch „weiche" Instrumente unter Verzicht auf „harte" Verifikation geschaffen werden. Sie bleibt vorerst notwendigerweise schwach in der Sanktionierung und Aufdeckung von Verstößen. Diese Schwäche muss nicht von Dauer sein und darf nicht als Argument dafür dienen, in diesem Bereich gar keine Rüstungskontrolle zu versuchen. Aus der „Kultur der Zurückhaltung" können im Verlaufe der Zeit und mit wachsender Erfahrung ein „harter" Rüstungskontrollvertrag oder ein ganz neues Rüstungskontrollregime entstehen.

Im folgenden werden mögliche Schritte der Nutzbarmachung von „weichen" Rüstungskontrollinstrumenten aufgezeigt. Sie haben das primäre Ziel, für die Sensibilisierung für Probleme, die durch Informationsoperationen aufgeworfen werden, zu sorgen. Sie wirken primär über Normen und Tabus und weniger durch „harte" Rüstungskontrollbeschränkungen, die momentan im Bereich von Informationsoperationen (noch) nicht umsetzbar sind.

Der erste „machbare" Schritt ist eine Politik der „deklaratorischen Selbstbeschränkung, d.h. der öffentlich bekundeten Nichtanwendung und -entwicklung von offensiven Informationsoperationen gegen zivile Ziele. Auch wenn dies technisch nicht verifizierbar ist, so stellt dies einen ersten Schritt der Vertrauensbildung dar. Eine deklarierte Selbstbeschränkung schafft Anreize für andere Staaten, diesem Schritt zu folgen. Internationale Organisationen (VN, OSZE, NATO, EU, G8 oder der VN-Weltgipfel zur Informationsgesellschaft) können hier eine Hilfestellung bieten, um kooperative und vertrauensbildende Dialoge zu beginnen. Ebenfalls sind multi- oder bilaterale Gespräche zum Austausch über Informationsdoktrinen und Entwicklungen auf der Ebene der Streitkräfte zur Vertrauensbildung sinnvoll.

Ebenso ist es vorstellbar, dass die Staaten, die am meisten von der Informationsrevolution profitieren und die eine weit entwickelte Informationsinfrastruktur besitzen, ihre Computernetze zu „friedlichen Zonen" erklären. Die am stärksten vernetzten Staaten müssten ein originäres Interesse an der Sicherheit der Netze haben.

Auch wenn Verifikationsmaßnahmen bei einem solchen Schritt fehlen, bedeutet dies nicht, dass eine Politik der Deklaration „zahnlos" sein müßte. Auch ohne Sanktions- und Verifikationsmaßnahmen stehen Staaten in der kritischen Prüfung der öffentlichen Meinung. Sie haben durchaus ein Interesse, ihre Glaubwürdigkeit unter Beweis zu stellen und sich entsprechend ihrer Deklaration zu verhalten. Diese selbstverpflichtende Maßnahme kann durch konkrete Verbote „offensiver Informationsoperationen" verstärkt werden. Als weitere Maßnahme innerhalb der deklaratorischen Politik würde ferner die Formulierung

einer „No-First-Use"-Doktrin fallen. Eine „No-First-Use"-Deklaration könnte Computernetzwerkangriffe als Element der Kriegsführung einschließen. Sie können negative Folgen für zivile Systeme haben und sind darüber hinaus kein geeignetes Instrument, um in der Informationsgesellschaft für Sicherheit und Vertrauen zu sorgen. Eine solche „No-First-Use"-Politik ist um so nötiger, als inzwischen eine Reihe von Staaten im Begriff sind, offensive Informationsoperations-Doktrinen zu formulieren. Sollten diese erst formuliert sein, so würde die Schaffung von offensiven Fähigkeiten und die Institutionalisierung folgen. In einem solchen Stadium wäre es dann schwieriger, den Prozess umzukehren. Die Form der Deklaration ist daher geeignet, das Vertrauen, das durch eine „Kultur der militärischen Zurückhaltung" entsteht, zu verstärken. Eine „No-First-Use" Deklaration im Umgang mit offensiven Computerangriffen trägt dabei, wie das nukleare Pendant, zur Krisenstabilität bei. Auch der Zeitpunkt scheint noch günstig für eine solche deklarierte Politik der Selbstbeschränkung zu sein. Von Staaten wurden noch keine Computernetzwerkangriffe gegen andere Staaten bekannt. Eine Politik der Zurückhaltung kann diesen wünschenswerten Zustand verfestigen. Eine normen-orientierte Rüstungskontrolle kann damit heute die Regeln schaffen, die verhindern, dass es in Zukunft zu solchen Angriffen kommt.

Zweitens ist die Schaffung eines „Verhaltenskodex" oder einer „Informationskriegsordnung" möglich, die den Umgang mit „Informationswaffen" regeln würde.[119] Darin könnten der Schutz bestimmter Infrastrukturen als Tabuzonen definiert werden. Im Gegenzug würde der Kodex festschreiben, welche Handlungen oder Informationsoperationen „militärisch" erlaubt sind. Die Effektivität eines Kodex wird zunächst daran gemessen, ob es gelingt, die „Kultur der militärischen Zurückhaltung" zu fördern. Die Grauzonen, die durch Informationsoperationen entstehen, würden durch solche Maßnahmen geringer werden.

Drittens gehen die klassischen Instrumente der Ziel-orientierten und der Prozess-orientierten Rüstungskontrolle über die Schritte der Schaffung einer Vertrauenskultur durch Deklarationen und der Selbstbeschränkung hinaus. Sie können konkreter greifen, wenn eine „Kultur der Zurückhaltung" geschaffen wurde und wenn eine weitere rechtliche und normative Verdichtung eines „Informationsoperationsregimes" gewünscht wird:

- Die ziel-orientierte Rüstungskontrolle strebt dann die Kontrolle der „sichtbaren" Waffensysteme an. Sie greift zum Beispiel dann, wenn für Informationsoperationen „Waffenplattformen" oder stationäre Forschungslabore gebraucht werden. Sie kann auch bestimmte offensive Systeme oder Programme verbieten. Die Hardware der „Strategien der Informationskriegsführung" könnte damit zum Gegenstand der Rüstungskontrolle werden.
- Die prozess-orientierte Rüstungskontrolle reguliert die weichen Elemente der „Strategien der InformationsKriegsführung". Sie macht die „Intentionen" von Akteuren zum Gegenstand der Rüstungskontrolle. Sie verringert Grauzonen, wenn es um die Ver-

119 William Church, IO Treaty Development Language, Revision 1.0, 1999.

wendung von „Dual-Use"-Gütern geht. Maßgeblich ist hier die Intention, die ein Akteur im Umgang mit Informationsoperationen hegt und nicht die Technologie selbst. Der Besitz wäre erlaubt, aber die Anwendung oder Strategien, die eine Gefahr für den Weltfrieden darstellen, wären verboten. Auch könnte ein „Informationsoperationsregime", wenn es sich auf „Waffeneffekte" oder „Waffenwirkungen" konzentriert, mit anderen bereits existierenden Rüstungskontrollregimen verknüpft werden.[120] Ebenfalls können dann weitere maßgeschneiderte Rüstungskontrollmechanismen angewendet werden.[121]

Die neuen und klassischen Mittel der Rüstungskontrolle sind kein Allheilmittel und enthalten keine Garantie, dass sie eine neue Rüstungsdynamik verhindern oder verlangsamen können. Aber sie stellen Instrumente dar, die von Demokratien angewendet werden können. Gerade die technologisch fortgeschrittenen Demokratien sind die Verursacher der neuen Rüstungsdynamik. Sie stehen daher in der Pflicht, die rüstungskontrollpolitischen Instrumente zu nutzen, die sie zur Hand habe, solange noch Möglichkeiten der Einflussnahme vorhanden bestehen.

120 Harald Müller/Niklas Schörnig, RMA and Nuclear Weapons – A Calamitous Link for Arms Control, in: Disarmament Forum, Nr. 4, 2001, S. 17-26.

121 Z.B. geographische Maßnahmen, strukturelle Maßnahmen, operative Maßnahmen, Verifikationsmaßnahmen, deklaratorische Maßnahmen, technologiebezogenen Maßnahmen, einsatzbezogene Maßnahmen, akteursbezogene Maßnahmen, zielbezogenen Maßnahmen. Vgl. Christian Mölling/Götz Neuneck, Präventive Rüstungskontrolle und Information Warfare, in: Heinrich Böll Stiftung (Hg.), Rüstungskontrolle im Cyberspace: Perspektiven der Friedenspolitik im Zeitalter von Computerattacken, Berlin (HBS) 2001, S. 47-53. S.48.

Abkürzungen

ACT	Allied Command Transformation
BM/C2	Battle Management / Command and Control
C3	Command, Control and Communication (Führung, Kontrolle, Kommunikation)
C3I	Command, Control, Communication and Intelligence
C4ISR	Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance (Führung, Kontrolle, Kommunikation, Computer, Nachrichtengewinnung, Überwachung und Aufklärung)
CIA	Central Intelligence Agency
CNA	Computer Network Attack (Computernetzwerkangriff)
CND	Computer Network Defense (Computernetzwerkverteidigung)
CNO	Computernetzwerkoperationen
CONOPS	Concept of Operations
DARPA	Defense Advanced Research Projects Agency
DBK	Dominant Battlespace Knowledge
DoD	Department of Defense
DPG	Defense Planning Guidance
EBO	Effects-based Operations (Effekt-basierte Operationen)
F&E	Forschung & Entwicklung
FM	Field Manual
GCCS	Global Command and Control System (Globales Befehls- und Führungssystem)
IO	Informationsoperationen
IT	Informationstechnologie
IW	Information Warfare (Informationskrieg)
JTF-CNO	Joint Task Force - Computer Network Operations
JSTAR	Joint Surveillance and Target Attack Reconnaissance System
NCW	Network Centric Warfare (netzwerk-zentrische Kriegsführung)
NETINT	Network Intelligence (Netzwerkspionage)
NPR	Nuclear Posture Review
NSPD	National Security Presidential Directive
OODA	Orient, Observe, Decide and Act (Orientieren, Beobachten, Entscheiden und Handeln)
P2OG	Proactive, Preemptive Operations Group
PGM	Precision Guided Munition (Präzisionsmunition)
RDO	Rapid Decisive Operations
RMA	Revolution in Military Affairs (Revolution in Militärischen Angelegenheiten)
SACLANT	Supreme Allied Commander Atlantic
SCADA	Supervisory Control and Data Acquisition

SIPRNET	Secret Internet Protocol Router Network
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Aerial Vehicle
UCP	Unified Command Plan
USAF	U.S. Air Force (Luftwaffe der USA)
USJFCOM	U.S. Joint Forces Command
USSPACECOM	U.S. Space Command (Weltraumkommando der USA)
USSTRATCOM	U.S. Strategic Command (Strategisches Kommando der USA)
USSOCOM	U.S. Special Operations Command (Kommando der Spezialeinheiten)
VN	Vereinte Nationen
QDR	Quadrennial Defense Review