Geiger, Gebhard

Research Report

Offensive Informationskriegführung: Die "Joint Doctrine for Information Operations" der US-Streitkräfte: sicherheitspolitische Perspektiven

SWP-Studie, No. S 2/2002

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Geiger, Gebhard (2002) : Offensive Informationskriegführung: Die "Joint Doctrine for Information Operations" der US-Streitkräfte: sicherheitspolitische Perspektiven, SWP-Studie, No. S 2/2002, Stiftung Wissenschaft und Politik (SWP), Berlin

This Version is available at:
https://hdl.handle.net/10419/252407

SWP-Studie
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale
Politik und Sicherheit

Gebhard Geiger

Offensive Informationskriegführung

Die »Joint Doctrine for Information Operations« der US-Streitkräfte: sicherheitspolitische Perspektiven

S 2
Februar 2002
Berlin

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

Gestaltungskonzept
Gorbach Büro für Gestaltung und Realisierung
Buchendorf

Inhalt

Offensive Informationskriegführung. Die *Joint Doctrine for Information Operations* der US-Streitkräfte: sicherheitspolitische Perspektiven

Mit der »Joint Doctrine for Information Operations« aus dem Jahre 1998 legt der US-Generalstab Richtlinien für den Einsatz militärischer Führungs- und Nachrichtensysteme bei gemeinsamen Operationen zweier oder mehrerer Teilstreitkräfte fest. Das Dokument dient dazu, die Operationen der US-Streitkräfte in umfassender Weise den Erfordernissen der informationselektronischen Revolution im modernen Militärwesen anzupassen. Darüber hinaus stellt es die Streitkräfteoperationen in den breiteren Kontext der US-Sicherheitspolitik im Informationszeitalter.

Zu den zentralen sicherheitspolitischen Herausforderungen zählt der US-Generalstab insbesondere die Bekämpfung des Terrorismus und der internationalen Kriminalität. Deren Problematik war zum Zeitpunkt der Veröffentlichung des Dokuments noch gar nicht im heutigen Ausmaß erkennbar, ist mit den Attentaten vom September 2001 jedoch in den Brennpunkt der internationalen Sicherheitspolitik gerückt.

Das Dokument ist zudem weit über seine militärischen Anwendungen hinaus von sicherheitspolitischem Interesse. Es wirft neuartige, bislang völlig ungeklärte Probleme der internationalen Sicherheit, der Geltung des Kriegsvölkerrechts sowie der Charta der Vereinten Nationen auf, desgleichen Fragen nach Art und Umfang künftiger internationaler Konflikte, möglicher Konfliktlösungsstrategien sowie der Rüstung und Rüstungskontrolle im Informationszeitalter.

Die Studie beschäftigt sich im wesentlichen mit den Richtlinien der offensiven Informationskriegführung in Kapitel II des Dokuments. Die sicherheitspolitische Problematik des offensiven Informationskriegs ergibt sich im wesentlichen aus den technischen Möglichkeiten der Computerspionage und -sabotage und des verdeckten elektronischen Netzangriffs, die sich neben militärischen Zielen auch auf die (Zer-)Störung ziviler öffentlicher IuK-Systeme sowie informationsabhängiger Infrastrukturen richten können.

Ihrer äußersten Zielsetzung nach ist der Einsatz von Informationskriegsmitteln dem militärischen Waffeneinsatz vergleichbar, ohne allerdings an herkömmliche politische und rechtliche Regelungen des Kriegszustands effektiv gebunden zu sein. Sie können anonym und ohne Frühwarnung über die weltweit

und öffentlich zugänglichen Informationsnetze erfolgen und bieten dem angegriffenen Staat oder Militärbündnis kaum eine Chance, den Angreifer zu ermitteln. Ihr Einsatz ist an keine Mobilmachung der Streitkräfte und schon gar nicht an eine Kriegserklärung gebunden. Kaum kontrollierbar – und in internationalen Krisen- und Konflikten effektiv kaum korrigierbar – ist die Verbreitung gezielter Falschinformationen durch die elektronischen Massenmedien. Kurz, offensiven informationsgestützten Operationen bietet sich ein weites Arsenal für verdeckte physische Gewaltanwendung und mediengesteuerte Agitation und Propaganda auf zentralen Gebieten der internationalen Politik und Sicherheit. Mit fortschreitender informationstechnischer Entwicklung entsteht auf diesen Gebieten ein zunehmend rechts- und herrschaftsfreier Raum, der sich bereits weit im Vorfeld akuter Konflikte zu überfallartigen Offensiv- und Präventivmaßnahmen nutzen läßt.

Auch wenn weite Teile der »Joint Doctrine for Information Operations« der Verteidigung im Informationskrieg gewidmet sind, ist sie doch in der klaren Absicht verfaßt, die Angriffsarten und -möglichkeiten, die der Informationskrieg heute und in absehbarer Zukunft bietet, umfassend zu nutzen.

Die Studie gelangt zu einer Reihe von Schlußfolgerungen für die internationale und die deutsche Sicherheitspolitik:

- Die amerikanische Regierung und die US-Streitkräfte bekennen sich zum offensiven Informationskrieg als einem Mittel der internationalen Politik, und zwar zu einer wie auch immer bedingten oder eingeschränkten Anwendung dieses Mittels im Frieden wie im militärischen Konflikt.
- Dieser Sachverhalt ist insofern von beträchtlicher sicherheitspolitischer Tragweite, als bisher alle einschlägigen US-Regierungsdokumente in dieser Frage eine rein defensive Haltung eingenommen haben. Möglicherweise wird das neue, offensive amerikanische Beispiel international Schule machen. Bei Interessenkonflikten mit den USA können sich zudem andere Staaten durch die amerikanische Bereitschaft zum offensiven Informationskrieg bedroht sehen, konfliktträchtige internationale Beziehungen durch diese Bereitschaft zusätzlich destabilisiert werden.
- Wahrscheinlich wird der offensive Informationskrieg künftig in internationalen Konflikten zunehmend als Routinemittel gegen zivile und militärische Ziele eingesetzt.
- Aus informationstechnischen Gründen ist es unmöglich, zur Verhinderung von Computernetzangriffen wirksame internationale politische und rechtliche Kontrollen, Beschränkungen und Verbote zu errichten. Eine »Rüstungskontrolle im cyber space« wird es daher auch in Zukunft nicht geben.

Auf der Basis dieser Schlußfolgerungen lassen sich auch einige generelle Empfehlungen für den Schutz der Bundesrepublik Deutschland und ihrer Informationsinfrastrukturen aussprechen:

- Die sicherheitspolitische Hauptaufgabe besteht in einer möglichst umfassenden Schadensprävention durch Schaffung robuster politisch-gesellschaftlicher Infrastrukturen, die nach Organisation und technischer Ausstattung in der Lage sind, auch unter Bedingungen eines elektronischen Angriffs die Öffentlichkeit mit Informationsdienstleistungen zu versorgen.
- Angesichts der (militärischen, technischen, wirtschaftlichen) Dimensionen einer offensiven Informationskriegführung bedürfen sicherheitspolitische Entscheidungen einer umfassenden Aufklärung und systematischen Daten- und Lageanalyse internationaler Aktivitäten und aktueller Entwicklungen auf dem Gebiet der Computernetzangriffe.
- Herkömmliche Formen zwischenbehördlicher Zusammenarbeit mit periodischem Datenaustausch reichen nicht aus. Eine Zentralbehörde (Information Warfare Center), nach dem Vorbild amerikanischer Einrichtungen (Critical Infrastructure Assurance Office [CIOA], National Infrastructure Protection Center [NISP]) und mit den notwendigen Kompetenzen ausgestattet, ist den Herausforderungen des offensiven Informationskriegs angemessen. Eine solche Behörde hätte nicht nur zu koordinieren, sondern die Aktivitäten von Verteidigung, innerer Sicherheit, Bundesamt für Sicherheit in der Informationstechnik, Justiz und Wirtschaft ressortübergreifend ebenso zu organisieren wie die Zusammenarbeit zwischen der Bundesrepublik Deutschland und ihren europäischen und atlantischen Verbündeten.

Die Sicherung kritischer Infrastrukturen der Informationsgesellschaft umfaßt nicht zuletzt Aufgaben der Forschung und Entwicklung auf dem Gebiet der Systemanalyse, Unternehmensforschung und des Risikomanagements. Aus einem verstärkten deutschen (personellen, finanziellen) Beitrag zu den bestehenden europäischen Initiativen auf dem Gebiet der sicherheitswissenschaftlichen Systemforschung können Sicherheit und Sicherheitspolitik der Bundesrepublik erheblichen Nutzen ziehen.

Offensiver Informationskrieg

Die elektronische Revolution in der modernen militärischen Kommunikation und Informationsverarbeitung kann nicht einfach als rein technischer Innovationsprozeß mit den üblichen Auswirkungen auf militärische Waffen-, Nachrichten- und Aufklärungssysteme verstanden werden. Es handelt sich vielmehr um eine Umwälzung des gesamten Militärwesens auf allen Ebenen der Rüstung, Organisation und Streitkräfteplanung, Strategie, Taktik und militärischen Operation bis hin zur internationalen Sicherheitspolitik. Golfkrieg (1991) und Kosovo-Einsatz der NATO (1999) haben gezeigt, in welchem Ausmaß die Informations- und Kommunikationstechnik (IuK) sowie die Fähigkeit zur elektronischen Kampfführung, über die moderne Streitkräfte heute verfügen, die Lösung internationaler Konflikte zu beherrschen beginnen.

Am weitesten durchdacht, geplant und im Ansatz realisiert ist das Konzept einer »Revolution in Military Affairs« (RMA) in den US-Streitkräften.[1] Ziel der amerikanischen Rüstungsplaner und Militärstrategen ist es, unterschiedliche militärische Fähigkeiten zu einem IuK-gestützten »System der Systeme« zusammenzuführen, das bei totaler Überlegenheit (full spectrum dominance) über den Gegner (across the range of military operations) ein koordiniertes Gefecht aller Teilstreitkräfte (TSK) und Waffensysteme (joint capabilities) ermöglicht.[2]

Im Zuge der informationstechnischen Entwicklung wird sich auch das Erscheinungsbild bewaffneter Konflikte in seinen Grundzügen wandeln, das heißt zunehmend vom Einsatz intelligenter, unbemannter, distanzfähiger, nahezu perfekt getarnter Präzisionswaffen und Waffensysteme geprägt sein.[3] Der Generalstab der US-Streitkräfte hat dieser Entwicklung durch seine »Joint Doctrine for Information Operations« (Oktober 1998) Rechnung getragen.[4] Über die bestehenden speziellen Richtlinien für sogenannte »Information Operations« (IO) der Teilstreitkräfte[5] hinaus legt das Dokument vom Herbst 1998 allgemeine Grundsätze für IuK-gestützte – und gegen feindliche IuK-Systeme gerichtete – TSK-übergreifende Maßnahmen fest, und zwar für den gesamten Bereich militärischer Operationen.

Grundlegende militärische Bedeutung besitzt das Dokument zunächst aufgrund seiner Eigenschaft als »doctrine«, das heißt als allgemeine, verbindliche Richtlinie und Anweisung des Generalstabs an die militärischen Befehlshaber zur Führung von Truppen und militärischen Operationen. Darin sind die »doctrines« der amerikanischen Streitkräfte in groben Zügen den Führungsgrundsätzen und zentralen Dienstvorschriften der Bundeswehr vergleichbar. Seine aktuelle Bedeutung erhält das Dokument durch die Stellung der Informationstechnik im militärischen Führungs- und Aufklärungswesen, bei TSK-übergreifenden Operationen sowie bei der weitgehenden Vernetzung militärischer und ziviler Aufgabenbereiche.[6]

Darüber hinaus ist das Dokument aufgrund seines umfassenden Anspruchs weit über seine militärischen, strategischen und operativen Anwendungen hinaus von sicherheitspolitischem Interesse. Es wirft neuartige, bislang völlig ungeklärte Fragen der internationalen Sicherheit, der Geltung des Kriegsvölkerrechts sowie der Charta der Vereinten Nationen (VN) auf, desgleichen Fragen nach Art und Umfang künftiger internationaler Konflikte, nach möglichen Kon-

1 John M. *Shalikashvili* (Hg.), Joint Vision 2010, Washington, D.C. 1996; Henry H. *Shelton* (Hg.), Joint Vision 2020, Washington, D.C. 2000.

2 Vgl. die Planungsdokumente des Generalstabs der US-Streitkräfte, herausgegeben von den Generalstabschefs *Shalikashvili*, Joint Vision 2010, und *Shelton*, Joint Vision 2020, sowie H. H. *Shelton* (Hg.), Joint Doctrine for Information Operations, Washington, D.C. 1998; *Computer Science and Telecommunications Board*/*National Research Council USA*, Realizing the Potentials of C^4I: Fundamental Challenges, Washington, D.C. 1999.

3 John *Arquilla*/David F. *Ronfeldt* (Hg.), In Athena's Camp. Preparing for Conflict in the Information Age, Santa Monica, Cal. 1997; Edward *Waltz*, Information Warfare. Principles and Operations, Boston 1998; James *Adams*, The Next World War, New York 1998; Zalmay M. *Khalilzad*/John P. *White* (Hg.), The Changing Role of Information in Warfare, Santa Monica, Cal. 1999.

4 Zur Unterscheidung von anderen »Joint Doctrines« der US-Streitkräfte wird hierfür im folgenden der Kurztitel »Joint Doctrine IO« verwendet. Einen Überblick über andere »Joint Doctrines« enthält »Joint Doctrine IO«, Appendix D.

5 Zum Verhältnis der Richtlinien für die Teilstreitkräfte zur »Joint Doctrine IO« siehe Richard H. *Wright*, The Evolution of Info Ops Doctrine, in: Military Review, 81 (2001) 2, S. 30–32.

6 Joint Doctrine IO, S. vii.

fliktlösungsstrategien sowie nach Rüstung und Rüstungskontrolle im Informationszeitalter.

Wie im folgenden dargestellt wird, beruht die sicherheitspolitische Problematik des Dokuments im wesentlichen auf Kapitel II, das die Richtlinien einer offensiven IuK-gestützten Kriegführung festlegt. Dabei liegt die besondere sicherheitspolitische Problematik des Dokuments weder darin, daß es militärische Offensivmaßnahmen gegen politische, militärische, ökonomische usw. Informationsinfrastrukturen des Konfliktgegners vorsieht, noch daß es den Einsatz der jeweils modernsten elektronischen Aufklärungs- und Kampfmittel verlangt. Der Offensiv- wie der High-Tech-Charakter militärischer Maßnahmen und Kampfmittel versteht sich für jede rationale (wirkungsoptimale) Strategie und operative Planung von selbst. Er ist weder neu noch ungewöhnlich.

Neuartig und problematisch am offensiven Informationskrieg (Information Warfare, IW) sind vielmehr die spezifischen Möglichkeiten der Computerspionage und -sabotage und des verdeckten elektronischen Netzangriffs, die sich neben militärischen Zielen auch auf die (Zer-)Störung ziviler öffentlicher IuK-Systeme sowie informationsabhängiger Infrastrukturen (Verwaltung, Wirtschaft, Transport und Verkehr, Energieversorgung, Nachrichtenwesen eines Landes) richten können.[7] Ihrer äußersten Zielsetzung nach sind Maßnahmen vom Typ des Informationskriegs dem militärischen Waffeneinsatz vergleichbar, ohne allerdings an herkömmliche politische und rechtliche Regelungen für den Kriegszustand effektiv gebunden zu sein. Sie können anonym und ohne Frühwarnung über die weltweit und öffentlich zugänglichen Informationsnetze vorgetragen werden und bieten dem angegriffenen Staat oder Militärbündnis kaum eine Chance, den Angreifer zu ermitteln. Ihr Einsatz ist an keine Mobilmachung der Streitkräfte und schon gar nicht an eine Kriegserklärung gebunden. Die erforderliche Soft- und Hardware ist handelsübliche Massenware, die nicht einmal einer Umrüstung für spezielle militärische Anwendungen bedarf. Kaum kontrollierbar – und in internationalen Krisen und Konflikten effektiv kaum korrigierbar – ist die Verbreitung gezielter Falschinformationen durch die elektronischen Massenmedien. Kurz, offensiven informationsgestützten Operationen militärischer wie ziviler Akteure bietet sich ein weites Feld der verdeckten physischen Gewaltanwendung und mediengesteuerten Agitation und Propaganda auf zentralen Gebieten der internationalen Politik und Sicherheit. Mit fortschreitender informationstechnischer Entwicklung entsteht auf diesen Gebieten ein zunehmend rechts- und herrschaftsfreier Raum, der sich bereits weit im Vorfeld akuter Konflikte zu überfallartigen Offensiv- und Präventivmaßnahmen nutzen läßt.

Auch wenn die IO-Doktrin vom Oktober 1998 in Kapitel III und weiteren Teilen Fragen defensiver IO behandelt, läßt das Dokument doch die klare Absicht erkennen, die Angriffsarten und -möglichkeiten, die der Informationskrieg heute und in absehbarer Zukunft bietet, umfassend zu nutzen. Diese Studie untersucht daher die Abschnitte über offensive IO im weiteren Kontext internationaler und sicherheitspolitischer Probleme des Informationskriegs. Dabei sollen im wesentlichen die beiden folgenden Arbeitshypothesen geklärt werden:

- *Bekenntnis zum offensiven Informationskrieg*: Während sich herkömmliche sicherheitspolitische Analysen und Programme (ob nun im Auftrag der US-Regierung oder nicht) in aller Regel auf IW-Schutz- und -Abwehrmaßnahmen konzentrieren, bietet die Doktrin das erste offenkundige Beispiel planmäßiger Vorbereitungen und einer unverhohlenen – wie auch immer bedingten oder eingeschränkten – Bereitschaft zur offensiven Informationskriegführung.
- *Unkontrollierbarkeitsthese*: Für offensive IW-Anwendungen, wie sie die Doktrin vorsieht, gibt es keine wirksamen internationalen, diplomatischen, rechtlichen und erst recht keine rüstungskontrollpolitischen Hürden oder Beschränkungen. Es kann und wird sie auch in absehbarer Zukunft nicht geben. Eine »Hegung« des offensiven Informationskriegs im Sinne des Kriegsvölkerrechts ist aus technischen Gründen grundsätzlich schwierig, in wesentlichen Elementen sogar völlig unmöglich.

Im nächsten Abschnitt werden die heute bestehenden bzw. absehbaren Bedingungen und Konsequenzen des Informationskriegs zusammengestellt und kurz erläutert. Die Unterscheidung zwischen defensivem und offensivem Informationskrieg wird hervorgehoben sowie auf die Eignung der Offensivmaßnahmen zur »asymmetrischen« Kriegführung hingewiesen. Es folgt ein Abriß der wesentlichen Begriffsbestimmungen und Richtlinien des Dokuments, sofern sie sich

7 Eine explizite Definition der »offensive information operations« folgt weiter unten in Anlehnung an den Sprachgebrauch der »Joint Doctrine IO«. Der Begriff des offensiven Informationskriegs wird hingegen immer im (weiteren) Sinne von computergestützten Störungs- und Zerstörungsakten der erwähnten Art verstanden.

auf IO mit offensivem Charakter beziehen. Dabei werden thematisch verwandte Dokumente des US-Streitkräfte mitberücksichtigt. Der folgende Abschnitt enthält eine sicherheitspolitische Analyse des Dokuments im Hinblick auf die skizzierten generellen Bedingungen und Konsequenzen des Informationskriegs, geht insbesondere aber auch auf Aspekte des internationalen Rechts ein. Der letzte Abschnitt qualifiziert die beiden Arbeitshypothesen im Lichte der sicherheitspolitischen Analyse und zieht Schlußfolgerungen für die deutsche Sicherheitspolitik.

Gefährdungen, Bedingungen und Konsequenzen des Informationskriegs

Spätestens seit dem Golfkrieg ist an den amerikanischen IO-Doktrinen eine kontinuierliche Entwicklung mit dem Ziel der operativen Vernetzung aller Teilstreitkräfte festzustellen.[8] Gleichzeitig läßt sich aber auch eine immer umfassendere Einbeziehung der kriegswichtigen gegnerischen Aufklärungs-, Führungs- und Versorgungssysteme in das Spektrum möglicher Angriffsziele der IO erkennen. Dabei gilt: Erstens, auch die (Zer-)Störung ziviler, aber dennoch kriegswichtiger Informationsinfrastrukturen zählt zu den strategischen Zielen eines bewaffneten Konflikts. Zweitens, aufgrund ihrer Informationsabhängigkeit sind diese Infrastrukturen verwundbar und mit den spezifischen Mitteln des Informationskriegs angreifbar. Und drittens, zur Informationskriegführung bietet sich ein breites Arsenal computer- und netzgestützter Mittel und Methoden an, die sich nicht notwendig auf militärische Waffengewalt zu stützen brauchen. Entsprechend müssen die offensiven Elemente der »Joint Doctrine IO« in einem breiten Kontext von Mitteln und Methoden, Bedingungen und Konsequenzen der Informationskriegführung verstanden und beurteilt werden.

Die elektronische Vernetzung von politisch-gesellschaftlichen Infrastrukturen hat die Hochtechnologieländer binnen weniger Jahre auf eine bislang unbekannte Weise verwundbar gemacht und weitreichenden Gefährdungen ausgesetzt.[9] Die neue sicherheitspolitische Lage ist dadurch gekennzeichnet, daß Handlungsfähigkeit und Überleben eines Staates oder Bündnisses in internationalen Krisen und Konflikten nicht mehr nur durch militärische Gewalt gefährdet sind, sondern zunehmend auch vom störungsfreien Betrieb staatlicher und internationaler IuK-Systeme abhängen.[10]

Zwar sind moderne gesellschaftliche Organisationen ganz allgemein auf die uneingeschränkte Verfügbarkeit ihrer technischen Betriebsmittel – darunter solche der Nachrichtenübertragung und Datenverarbeitung – angewiesen und bedürfen daher aufwendiger Maßnahmen zum Schutz gegen technische Störfälle, Naturkatastrophen und gezielte, planmäßige (Zer-)Störungsakte beispielsweise krimineller oder terroristischer Art. Doch hat sich die Gefährdungslage politisch-gesellschaftlicher Systeme mit dem Auf- und Ausbau internationaler digitaler Datenübertragungsnetze, Telekommunikationssysteme, Multimedia-Anwendungen und Online-Dienste auf vielfältige Weise rasant verändert und verschärft. Denn elektronische IuK-Netze sind in der Regel öffentlich und anonym zugänglich, weltweit verknüpft und gegen politisch oder kriminell motivierten Mißbrauch kaum ausreichend zu schützen.

Entsprechend haben die neuen IuK-Systeme auch neuartige Möglichkeiten der globalen, gesellschaftlichen Konfliktaustragung geschaffen. Elektronische Rechner, Datenspeicher, Netze und Software bieten aufgrund vielfältiger Schwachstellen zahlreiche Angriffspunkte für das unbefugte Mitlesen (Spionage) und die absichtliche, verdeckte Veränderung, Fälschung, Unterbrechung und Vernichtung elektronisch verbreiteter, gespeicherter und verarbeiteter Information. Staatliche Verwaltung, Wirtschaft, Verkehr, öffentliche Gesundheit oder Streitkräfte sind daher in dem Maße verwundbar, in dem sie sich auf öffentliche, weltweit vernetzte IuK-Systeme stützen.[11]

Die Verwundbarkeit oder – so der Titel der überhaupt ersten Studie zum Thema[12] – »Verletzlichkeit der Informationsgesellschaft« beruht auf zahlreichen komplexen Einflußfaktoren, die sich offensive IO zu-

8 *Wright*, Evolution.

9 Alexander *Roßnagel*/Peter *Wedde*/Volker *Hammer*/Ulrich *Pordesch*, Verletzlichkeit der ›Informationsgesellschaft‹, Opladen 1989; Gebhard *Geiger* (Hg.), Sicherheit der Informationsgesellschaft, Baden-Baden 2000.

10 Gebhard *Geiger*, Neue Strukturen und Herausforderungen der internationalen Sicherheit im Informationszeitalter, in: Aussenpolitik, 48 (1997) 4, S. 401–408; Gebhard *Geiger*, Internationale Sicherheit, in: *Geiger* (Hg.), Sicherheit, S. 145–199; Gebhard *Geiger*, Informationstechnischer Wandel und neue Risiken der internationalen Sicherheit, in: Jens *van Scherpenberg*/Peter *Schmidt* (Hg.), Stabilität und Kooperation: Aufgaben internationaler Ordnungspolitik, Baden-Baden 2000, S. 50–62.

11 *Roßnagel*/*Wedde*/*Hammer*/*Pordesch*, Verletzlichkeit; *Waltz*, Information Warfare; Dorothy E. *Denning*, Information Warfare and Security, Reading, Mass. 1999; *Geiger* (Hg.), Sicherheit.

12 *Roßnagel*/*Wedde*/*Hammer*/*Pordesch*, Verletzlichkeit.

nutze machen. Hierunter fallen zunächst die erwähnten Schwachstellen der IT-Systeme. Als solche gelten alle strukturellen, technischen und organisatorischen Sicherheitsmängel von Informationsinfrastrukturen, die potentiellen Angreifern einen Mißbrauch aussichtsreich erscheinen lassen. Typische Schwachstellen liegen in physischen Möglichkeiten des unberechtigten Zugriffs auf IT-Systeme und vertrauliche Informationen, in ungeklärten Zugriffs- und Nutzungsrechten, menschlichem Fehlverhalten einschließlich der Korruption des Betriebspersonals (»Innentäter«) und nicht zuletzt in Managementfehlern, etwa einer mangelnden Überwachung des sicherheitskonformen Systembetriebs. Im Unterschied zu herkömmlichen Formen gewaltsamer internationaler Konflikte gibt es bei IW-Angriffen auch kein geschütztes Staatsgebiet mehr, das an seinen Grenzen mit militärischen Mitteln erfolgreich zu verteidigen wäre.[13]

Verschärft wird die »Verletzlichkeit der Informationsgesellschaft« zudem durch eine bisher unbekannte Intensität und Komplexität der informationsgestützten sozialen Wechselwirkung. Die Folge ist, daß Störungen in einem gesellschaftlichen Funktionsbereich, etwa der Stromversorgung, unübersehbare und kaum mehr kontrollierbare Schadenfolgen in anderen Bereichen, beispielsweise der Telekommunikation, nach sich ziehen können.[14]

Zur elektronischen Vernetzung kommen die hohen IT-Innovationsraten hinzu, mit denen wissenschaftliche Technikfolgenanalyse, rechtliche Regelung und Sicherheitspolitik nicht Schritt halten können. In den internationalen Beziehungen, aber oft genug auch im Bereich der inneren Sicherheit, vollzieht sich der informationstechnische Wandel daher faktisch über weite Strecken in einem rechts- und herrschaftsfreien Raum (»Anarchie des Internets«).

Als Multimediasysteme sind elektronische Geräte und Netzwerke innerhalb einer großen Bandbreite möglicher Verwendungen multifunktional. Entsprechend schwierig ist es, die Nutzung, aber auch die Gefährdungen und politisch-gesellschaftlichen Herausforderungen der neuen Informationselektronik nach einzelnen Anwendungsbereichen, etwa als politisch oder wirtschaftlich, militärisch oder zivil, öffentlich oder privat, eindeutig zu klassifizieren. Der sogenannte »dual-use«-Charakter der militärischen wie zivilen Verwendbarkeit der Informationselektronik erscheint im Hinblick auf die offensiven Elemente der »Joint Doctrine IO« als besonders problematisch (s.u.).

Auch die internationalen Beziehungen und die politische Handlungsfähigkeit von Staaten und Bündnissystemen hängen zunehmend von technischen Fähigkeiten zur Informationsvermittlung und Systemsteuerung ab. Umgekehrt eröffnen die elektronischen Medien Möglichkeiten des kollektiven Handelns und der internationalen Organisation, die sich der politischen Kontrolle durch den Staat und seine Organe entziehen. Neue, nichtstaatliche Organisationen treten auf, die bestehende politische und militärische Machtstrukturen verändern können.[15] Das Spektrum herkömmlicher internationaler Konflikte wird sich erweitern, voraussichtlich sogar völlig verändern. Aufgrund der weltweiten elektronischen Vernetzung aller Lebensbereiche wird es immer schwieriger, zwischen kriminellen und militärischen Bedrohungspotentialen, politischen und geographischen Grenzen, innerer und äußerer Sicherheit von Staat und Gesellschaft zu unterscheiden.

Angesichts der zentralen Rolle der elektronischen Informationstechnologien dürften die von Konkurrenten und Gegnern genutzten Informationen und Kommunikationssysteme künftig als Angriffsziele auf den Märkten, aber auch bei internationalen Konflikten und organisierten Verbrechen dienen. Der Informationskrieg muß sich insofern nicht notwendig nur zwischen Staaten abspielen – er kann auch zwischen den »grenzenlosen«, weltweit operierenden Wirtschaftsunternehmen, Interessengruppen und nichtstaatlichen internationalen Organisationen einschließlich solchen des politischen Terrorismus unter Mitwirkung von Massenmedien und Nachrichtendiensten geführt werden. Zudem können IW-Angriffe gegen die Informationsinfrastruktur eines Staates militärische Gewaltanwendung sowohl unterstützen und ergänzen als auch um völlig neue Elemente erweitern, wenn nicht gar als Konfliktmittel ersetzen

13 Roger C. *Molander*/Andrew S. *Riddile*/Peter A. *Wilson*, Strategic Information Warfare, Santa Monica, Cal. 1996 (RAND).

14 *President's Commission on Critical Infrastructure Protection* (PCCIP), Critical Foundations. Protecting America's Infrastructures, Washington, D.C. 1997; Dietrich *Cerny*, Schutz kritischer Infrastrukturen in Wirtschaft und Verwaltung, in: *Geiger* (Hg.), Sicherheit, S. 21–42.

15 *Geiger*, Informationstechnischer Wandel, in: *van Scherpenberg*/*Schmidt* (Hg.), Stabilität; *Arquilla*/*Ronfeldt* (Hg.), Athena's Camp; R. E. *Hayes*/David S. *Alberts*, The Realm of Information Dominance: Beyond Information War, in: Gary F. *Wheatley*/Richard E. *Hayes*, Information Warfare and Deterrence, Washington, D.C. 1966, Anhang B.

oder ganz erübrigen.[16] Wie unten im einzelnen dargestellt wird, verlangt die »Joint Doctrine IO«, daß von solchen Möglichkeiten gegebenenfalls in vollem Umfang Gebrauch gemacht wird. Sie stützt sich dabei auf den Umstand, daß nicht einmal militärische IO an den Einsatz bewaffneter Streitkräfte gebunden sein müssen, um unter den technischen Bedingungen des Informationskriegs Zerstörungen strategischen Ausmaßes bewirken zu können. Das heißt, das Schadenausmaß kann dem angegriffenen Staat eine Verteidigung faktisch unmöglich machen, die technisch-organisatorischen Voraussetzungen seiner politischen Handlungsfähigkeit schlechthin zerstören.

Typen des offensiven Informationskriegs

Unter IO verstand man in den amerikanischen Streitkräften bis zum Golfkrieg im wesentlichen die klassischen Komponenten »Command, Control, Communications, Computers, Intelligence« (C^4I). Erst im Laufe des letzten Jahrzehnts trug man Schritt für Schritt den sich erweiternden Perspektiven des Informationskriegs Rechnung. So zählte 1996 das »Field Manual« FM 100-6 der Armee auch die gezielte Manipulation ziviler, öffentlicher Einrichtungen, psychologischer Einflußfaktoren (PSYOP) sowie elektronischer Informationssysteme (INFOSYS) zu den IO-Aufgaben.[17] Eine Klassifikation verschiedener Typen des offensiven Informationskriegs, die den IO der »Joint Doctrine IO« entsprechen, umfaßt im wesentlichen:

- C^4I und elektronische Kampfführung (Electronic Warfare, EW) auf dem Gefechtsfeld. IO dieser Art gehören zum Kernbestand der Offensivmaßnahmen, die die »Joint Doctrine IO« vorsieht.
- Psychologische Manipulation der Öffentlichkeit mit Mitteln der elektronischen Massenkommunikation. In der »Joint Doctrine IO« räumt der US-Generalstab der Propaganda und Manipulation der öffentlichen Meinung in Friedens- wie Konfliktzeiten Vorrang ein. Er nimmt in diesem Punkt Bezug auf die »Doctrine for Joint Psychological Operations« vom Juli 1996 sowie auf zahlreiche andere Richtlinien.[18]
- »Hacker Warfare« und die Verbreitung von Programmen mit Schadenfunktion (Computer-Viren). Die für einen entsprechenden Angriff auf elektronisch gespeicherte Daten, Nachrichtennetze und Rechneranlagen durch Computerhacker benutzten Techniken bieten sich auch für den militärischen und geheimdienstlichen Gebrauch an.
- »Business Information Warfare« in Form von Diebstahl, Mißbrauch, Fälschung oder Zerstörung wirtschaftlich genutzter, in Computern und öffentlichen Netzen verarbeiteter, verbreiteter und gespeicherter Information. IW-Angriffe dieses Typs können zur wirtschaftlichen Schwächung des Gegners in bewaffneten wie unbewaffneten Konflikten eingesetzt werden.
- »Cyber War«,[19] also Mißbrauch und (Zer-)Störung öffentlicher elektronischer IuK-Systeme sowie IT-abhängiger nationaler und internationaler Infrastrukturen. Nach Zielsetzung, Aufwand und Methoden reicht diese IW-Variante sehr viel weiter und ist umfassender als etwa die Wirtschaftskriminalität im Internet oder das »Spiel« der Computerhacker.[20]

Eines der sicherheitspolitischen Hauptprobleme liegt darin, daß die Bedrohungspotentiale des Informationskriegs vergleichsweise unscharf sind – begrifflich wie in der praktischen, sicherheitspolitischen und militärischen Beurteilung. Zum einen hängt dieser Sachverhalt mit dem erwähnten »dual-use«-Charakter der IT-Systeme zusammen, zum anderen mit den – ebenfalls technisch bedingten – Schwierigkeiten auf seiten des Opfers, eine Bedrohung, ja selbst einen IW-Angriff zu erkennen, bevor er Schaden angerichtet hat. IT-gestützte Angriffe können in unvergleichlich hohem Maße aus der Distanz in Territorien und (ungeschützte) Infrastrukturen eindringen, und sie sind nahezu perfekt getarnt – im ungünstigsten Fall erkennen die zuständigen Organe erst, daß ein Staat Ziel eines Informationskrieges ist, wenn dessen Infrastrukturen bereits in ihren wesentlichen Komponenten lahmgelegt sind.

Ganz anders stellen sich die Verhältnisse in bezug auf IW-Schutz und -Abwehr sowie defensive IW-Maßnahmen dar.[21] Sicherheitspolitisch betrachtet fehlt der IW-Abwehr nämlich, von Ausnahmefällen[22] abge-

16 *Arquilla/Ronfeldt* (Hg.), Athena's Camp; *Khalilzad/White* (Hg.), Changing Role; *Adams*, Next World War.

17 *Wright*, Evolution.

18 Eine »Doctrine for Joint Civil Affairs« JP 3-57 befindet sich laut Defense Technical Information Center des US-Verteidigungsministeriums derzeit noch in Vorbereitung.

19 In Anlehnung an die »cyber space«-Metapher für elektronische IuK-Netze.

20 David S. *Alberts*/John J. *Garstka*/Frederick P. *Stein*, Network Centric Warfare: Developing and Leveraging Information Superiority, 2. Aufl., Washington, D.C. 1999.

21 Vgl. die Darstellung von Schutz- und Abwehrtechnologien bei *Denning*, Information Warfare, sowie jene der sicherheitspolitischen Aspekte bei *Geiger*, Internationale Sicherheit.

22 Etwa Strategien der »Informationsdominanz« (s.u.).

sehen, die Fähigkeit, einen Angriff gezielt mit Gegengewalt zu beantworten. Die Ursache hierfür liegt im wesentlichen darin, daß Abschreckung und Vergeltung und ähnliche Defensivmaßnahmen mit »eingebauter« Gegendrohung im Informationskrieg wenig wirksam sind, da der Urheber elektronisch gesteuerter Angriffe schwer zu identifizieren ist. Die Quelle unberechtigter Eindringversuche in fremde Systeme kann kurzfristig beziehungsweise in Echtzeit kaum, langfristig bestenfalls mit erheblichem Aufwand und, sofern die Angriffe aus dem Ausland erfolgen, höchstens durch internationale Zusammenarbeit aufgeklärt werden. Unter Gegnern in internationalen Konflikten entfällt jedoch diese Möglichkeit. Eine wirksame IW-Defensive kann sich daher auf Abschreckung und Vergeltung nicht verlassen. Sie muß vielmehr auf Prävention, Schutz, Abwehr und einer Überwachung des sicherheitskonformen Systembetriebs aufbauen. Einige Berichte und Dokumente aus dem amerikanischen Verteidigungsministerium geben einer solchen rein passiven Abwehr den Vorzug,[23] während die »Joint Doctrine IO« unter den defensiven IO auch »attack-response«-Maßnahmen vorsieht, das heißt nicht strikt zwischen offensivem und defensivem Informationskrieg trennt (s.u.).

Informationsdominanz

Unter die sicherheitspolitischen Bedrohungspotentiale des IW fällt insbesondere die sogenannte Informationsdominanz. Sie umfaßt sämtliche informationstechnischen Voraussetzungen und Fähigkeiten eines Landes zu überlegenem militärischem und nichtmilitärischem Konflikthandeln. Mit anderen Worten, Informationsdominanz ist die Fähigkeit, über das ganze Spektrum kooperativer und gegnerschaftlicher internationaler Beziehungen hinweg eigene Interessen durchzusetzen.[24] Überlegene Fähigkeiten dieser Art beruhen auf unterschiedlichen Faktoren und deren wirksamer Koordination: technische Überlegenheit, ein immer aktuelles, möglichst genaues und vollständiges Lagebild, die Fähigkeit, einem Gegner ein solches Bild vorzuenthalten (Täuschen, Fälschen oder Vernichten von Information, Blockieren der gegnerischen Sensorik, Stören oder Zerstören gegnerischer IuK-Systeme), sowie nicht zuletzt die IT-gestützte Beherrschung und Manipulation der öffentlichen Berichterstattung und Meinung zum Konfliktgeschehen.

Zwar ist das Streben nach Informationsdominanz als rationale Konfliktstrategie weder mit der modernen Informationselektronik erst entstanden, noch liegen mögliche Anwendungen dieser Strategie ausschließlich auf dem Gebiet sicherheitspolitischer Konflikte. Dennoch hat die elektronische Vernetzung alten wie neuen Akteuren der internationalen Politik neue Handlungsspielräume mit neuen Chancen für die erfolgreiche Durchsetzung ihrer Interessen eröffnet. Nach Maßgabe der »Joint Doctrine IO« versucht die amerikanische Sicherheitspolitik nichts anderes, als diese Chancen im vollen Umfang der technischen, militärischen und zivilen Möglichkeiten der USA zu nutzen.

Asymmetrische Strategien

Wirtschaftlich-technisch-militärische Großmächte sind im Informationszeitalter in ihrer politisch-gesellschaftlichen Handlungsfähigkeit in dem Maße gefährdet, in dem ihre Infrastrukturen IT-gesteuert und auf elektronischem Wege angreifbar sind. Gerade die am weitesten fortgeschrittenen Hochtechnologieländer sind mit einer völlig neuartigen Sicherheitsproblematik konfrontiert, die selbst für eine Großmacht wie die USA mit militärischen Mitteln allein nicht zu lösen ist. Militärisch überlegene Konfliktgegner sind der Bedrohung »asymmetrischer« Kriegführung in Form eines IT-Angriffs auf ihre technisch-wirtschaftliche Infrastruktur ausgesetzt.[25]

Die Asymmetrie beruht auf einem Ungleichgewicht zwischen IW-Angriffs- und -Verteidigungsaufwand sowie zwischen Aufwand und Ertrag für den Angreifer.[26] Die Wahl von Angriffsart, -ziel und -zeitpunkt ist bei IW-Angriffen ganz in das Ermessen des Angreifers gestellt, während der Verteidiger seine gesamte IT-Infrastruktur unablässig schützen muß. Elektronische Angriffe sind daher »preisgünstiger« und erfordern

23 *Computer Science and Telecommunications Board/National Research Council USA*, Realizing the Potentials, S. 143–144.
24 Joseph S. *Nye*, Jr./William A. *Owens*, America's Information Edge, in: Foreign Affairs, 75 (1996) 2, S. 20–36; *Shalikashvili* (Hg.), Joint Vision 2010; *Shelton* (Hg.), Joint Vision 2020.

25 Insbesondere die Planungsperspektiven von »Joint Vision 2020« konzentrieren sich auf diesen Punkt – ebenso wie auf die Absicherung der amerikanischen Informationsdominanz. Sie werden dabei ausdrücklich als Weiterentwicklung und Ergänzung der »Joint Doctrine IO« von »Joint Vision 2010« aufgefaßt (s.u.).
26 *Computer Science and Telecommunications Board/National Research Council USA*, Realizing the Potentials, S. 139.

technisch und organisatorisch einen wesentlich geringeren Aufwand als ihre Prävention und Abwehr. Noch drastischer fällt das Bilanzungleichgewicht bei erfolgreichen Angriffen aus, weil hier das Schadenausmaß durch Ausbreitung der Schäden aufgrund von Vernetzungseffekten enorm sein kann. Dieser Fall wird durch die so simple Verbreitung des E-mail-Virus »I love you« illustriert, der weltweit Schäden in zweistelliger Milliardenhöhe verursacht hat. Schließlich muß auf seiten des Verteidigers jede sicherheitstechnische Verbesserung erst einmal entwickelt und in die IT-Systeme eingebaut werden (IT-security update), was Zeit und Aufwand kostet. In internationalen Krisen und Konflikten kann ein Zeitverzug beim IT-Sicherheits-update ein entscheidender Nachteil gegenüber den Operationsbedingungen des Angreifers sein.

Die »Joint Doctrine for Information Operations« der US-Streitkräfte

Das Dokument legt Richtlinien und personelle Verantwortung für alle TSK-übergreifenden informationsgestützten Operationen der amerikanischen Streitkräfte im Frieden wie im Kriegszustand fest. Mit diesem umfassenden Anspruch erstreckt es sich auf die strategische, taktische und – im engeren Sinne – operative Planung, Vorbereitung und Ausführung des Streitkräfteeinsatzes. Es sieht sowohl offensive als auch defensive IO vor, desgleichen Aufgaben der militärischen Aufklärung, Kommunikation und Datenanalyse, die koordinierte Führung der Teilstreitkräfte und ihrer Untergliederungen auf dem Gefechtsfeld, Ausbildung, militärische Übung sowie die IT-gestützte Kooperation mit allen zuständigen Regierungsbehörden und den Bündnispartnern der USA.

An dem Dokument sind die strategischen offensiven IO von grundsätzlichem sicherheitspolitischem Interesse. Denn erstens richten sie sich gegen die Fähigkeiten von Staaten, Militärbündnissen oder auch nichtstaatlichen (Freischärler-)Organisationen, einen bewaffneten Konflikt auszutragen (strategic level of war).[27] Zweitens haben sie ausdrücklich Bedrohungscharakter oder bergen zumindest ein Bedrohungspotential, selbst wenn keine manifeste Angriffshandlung vorliegt. Und drittens liefern sie der sicherheitspolitischen Analyse Fallbeispiele für alle nur denkbaren spezifischen Probleme der internationalen Politik und Sicherheit im Informationszeitalter. Entsprechend konzentriert sich die folgende Analyse im wesentlichen auf die offensiven IO.

Schauplätze des offensiven Informationskriegs

Unter offensiven IO werden in der »Joint Doctrine IO« alle Maßnahmen der US-Streitkräfte verstanden, die sich gegen Informationen und Informationssysteme möglicher oder tatsächlicher Gegner vor oder in kriegerischen Konflikten richten. Sie sehen den umfassenden, koordinierten Gebrauch aller nutzbaren Einsatz- und Unterstützungskräfte aller Waffengattungen, der Aufklärung und Nachrichtendienste vor.[28]

Die offensiven IO schließen zunächst den Gebrauch herkömmlicher elektronischer Kampfmittel (C^4I, EW) ein, des weiteren aber auch die Nutzung der gesamten IuK-gestützten Verteidigungsinfrastruktur der USA (Defense Information Infrastructure, DII) mit ihren strategisch wichtigen Computer-, Telekommunikations- und Satellitennetzen.[29] Entsprechend verweist die »Joint Doctrine IO« in diesen Punkten auch auf andere einschlägige Richtlinien des US-Generalstabs zu IO und C^4I.

Völlig neuartig ist die breite Anwendung der offensiven IO und ihre Stoßrichtung gegen alle politischen und zivilen Einrichtungen und Aktivitäten, die jemals für einen Gegner kriegswichtig werden könnten. Hier zeigen sich tatsächlich Bereitschaft und Entschlossenheit der USA, nicht nur die oben skizzierten universellen sicherheitspolitischen Herausforderungen des Informationskriegs anzunehmen, sondern auch potentielle Konfliktgegner mit diesen Herausforderungen nach allen Regeln der Kunst zu konfrontieren.

Bereits die Festsetzungen[30] für informationsabhängige Prozesse und IO sind terminologisch so gefaßt, daß sie eine uneingeschränkte Anwendung auf alle gegnerischen Ziele zulassen. »Informationsgestützte Prozesse können in jeder Facette einer militärischen Operation angetroffen werden, vom Gefecht über Unterstützungsmaßnahmen bis hin zum Nachschub über die gesamte Bandbreite militärischer Operationen ebenso wie in jedem anderen Element staatlicher Macht. [...] IO sind Handlungen mit dem Ziel, gegnerische Informationen und Informationssysteme zu treffen bei gleichzeitiger Verteidigung der eigenen Informationen und Informationssysteme [...] IO-Fähigkeiten umfassen im wesentlichen OPSEC [Operations Security], PSYOP [Psychological Operations], militärische Täuschung, EW, physische Attacke und Zerstörung, gegebenenfalls auch Computernetzangriffe (CNA). IO-bezogene Maßnahmen erstrecken sich [...]

27 Joint Doctrine IO, S. I-2, II-10, II-14.

28 Joint Doctrine IO, S. I-9, I-10, II-3.

29 Joint Doctrine IO, S. I-4, I-9, I-14, II-3, II-5, sowie die darin enthaltenen Verweise auf weitere Streitkräftedokumente der elektronischen und psychologischen Kampfführung.

30 Joint Doctrine IO, Abschn. I.3.

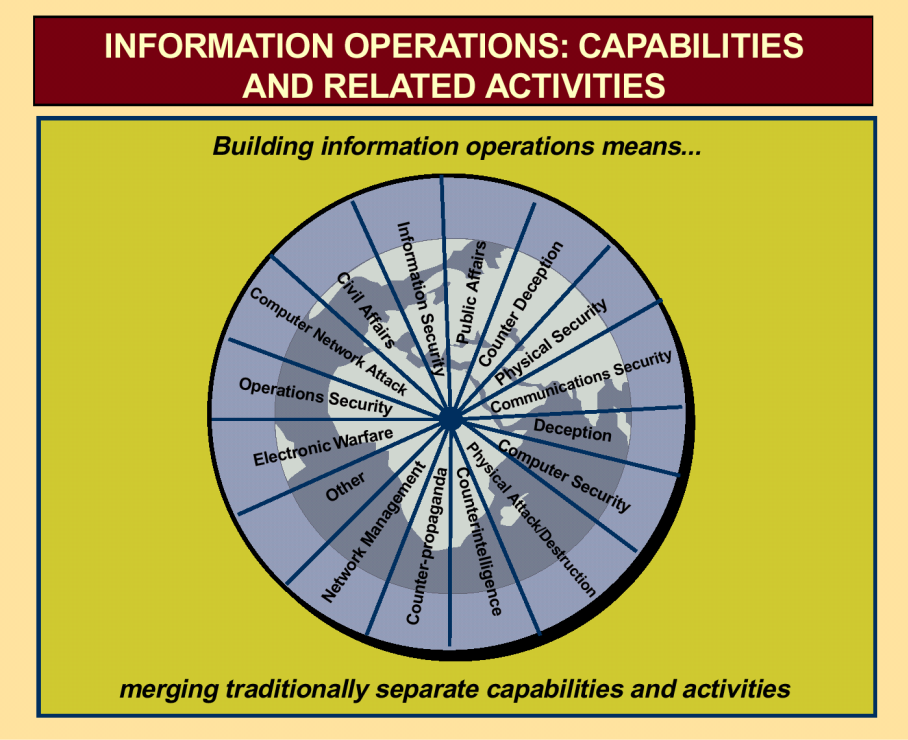

Abbildung 1
IO – sicherheitspolitische Aufgaben

Quelle: Joint Doctrine for Information Operations, S. I-10.

auf öffentliche und zivile Aufgabenbereiche.«[31] (Abbildung 1)

Eine wesentliche begriffliche Unterscheidung zwischen IO und IW wird nicht getroffen. Informationskrieg ist nichts anderes als die Gesamtheit aller informationsgestützten Maßnahmen, die sich in Krisen und Konflikten gegen den jeweiligen Gegner richten.[32] Der Oberkommandierende eines TSK-übergreifenden militärischen Verbandes (Joint Forces Commander, JFC) wird angewiesen, den Begriff des Gegners »breit« auszulegen, um alle Verbände, Gruppen und Entscheidungsträger zu erfassen, die US-Streitkräfte daran hindern könnten, ihren Auftrag zu erfüllen.[33] Ebenso werden alle Elemente der potentiellen beziehungsweise tatsächlichen gegnerischen Macht den strategischen Angriffszielen zugerechnet. Neben politischen und militärischen werden ausdrücklich ökonomische und informationstechnische Systeme mit aufgezählt.[34] »Special Operations Forces« (SOP) stehen bereit, in gegnerische Informationssysteme einzudringen, sie zu manipulieren, zu stören, zu hemmen und zu unterbrechen, ihren Gebrauch zu verhindern oder sie zu zerstören – im gesamten Bereich militärischer Operationen und auf allen Ebenen der Kriegführung.[35]

Der im Dokument immer wieder hervorgehobene Gesamtbereich aller militärischen Operationen schließt offensive IO in Friedenszeiten ausdrücklich ein. Es wird sogar unterstellt, daß solche Offensivmaßnahmen im Frieden ihre höchste Wirksamkeit entfalten. Sie fallen unter die sogenannten »Military Operations Other than War« (MOOTW), die ihrerseits die Androhung oder Anwendung von Gewalt nicht ausschließen. Neben politischen Aufgaben des Krisenmanagements werden ausdrücklich die Aufrechterhaltung des amerikanischen Einflusses in fremden Ländern und der Eingriff mit militärischen Kräften in Krisengebieten (power projection) als Ziele offensiver IO genannt.[36] Waffengewalt, unterstützt durch offensive IO, ist anzuwenden, wenn andere Mittel dabei versagen, die Ziele und Interessen der USA wirksam zu verfolgen.[37] In diesem Fall sind alle Elemente der

31 Joint Doctrine IO, S. I-9, 10. Vgl. hierzu auch die geheimdienstlichen IW-Aufgaben, z.B. Netzangriffe, S. I-8.
32 Joint Doctrine IO, S. I-4, I-11. Das Dokument war übrigens 1996 als »Joint Doctrine of Information Warfare« in Auftrag gegeben worden, der Titel wurde erst 1997 im Zuge der Fertigstellung in »Joint Doctrine for Information Operations« geändert. Vgl. hierzu *Defense Technical Information Center* (Hg.), Program Directives, Ft. Belvoir, VA o.J. (http://www.dtic.mil/doctrine/jel/pd/prog_dir.html).
33 Joint Doctrine IO, S. I-1.
34 Joint Doctrine IO, S. I-2, II-13.
35 Joint Doctrine IO, S. I-17.
36 Joint Doctrine IO, S. I-7, 8.
37 Joint Doctrine IO, S. I-7, 8.

gegnerischen Macht, militärische wie zivile, mit den Mitteln des Informationskriegs anzugreifen, die strategisch wichtigen Infrastrukturen des Gegners in aller Regel direkt (Beschädigung, Zerstörung).[38]

Die zentrale Rolle leistungsfähiger, überlegener IuK-Systeme für den Erfolg des modernen Streitkräfteeinsatzes wird nachdrücklich in den Planungsdokumenten des US-Generalstabs unterstrichen.[39] Informationsdominanz (information dominance, information superiority) gilt zunächst als operatives Ziel auf dem Gefechtsfeld, wird aber auch als wesentliche Bedingung einer erfolgreichen Kriegführung schlechthin angesehen, ebenso als militärisch-politisches Bedrohungs- und Abschreckungspotential, das den Waffeneinsatz gegebenenfalls erübrigt. Die »Joint Doctrine IO« trägt dieser strategischen Dimension offensiver IO Rechnung: »IO auf der operativen Ebene können in dem Maße zum Erreichen strategischer Ziele beitragen, in dem sie den Gegner unfähig machen, militärische Kräfte und Fähigkeiten zu organisieren, zu führen, zu verlegen und aufrechtzuerhalten.«[40] Zu diesem Zweck »nutzen IO die wachsende Raffinesse, Vernetzung und Abhängigkeit [von] der IT. Sie richten sich gegen Informationen sowie Informationssysteme, um IuK-gestützte Prozesse schlechthin zu treffen, seien diese personeller Art oder automatisiert. Solche IuK-abhängigen Prozesse umfassen die gesamte Bandbreite zwischen den höchsten politischen Entscheidungen und der automatisierten Steuerung lebenswichtiger kommerzieller Infrastrukturen, etwa der boden- und weltraumgestützten Telekommunikation und der elektrischen Stromversorgung.«[41]

Hervorgehoben wird weiterhin die Notwendigkeit, in eine umfassende offensive Informationskriegführung neben militärischen Kräften auch die zivilen Geheim- und Nachrichtendienste systematisch einzubeziehen. Die Aufgabengebiete, Institutionen und zuständigen Amtsträger werden benannt.[42] Die nachrichtendienstliche Aufklärung im Rahmen offensiver IO erstreckt sich auf die Nutzung aller möglichen geheimen und offenen Quellen, darunter das Internet, um alle gegnerischen militärischen wie zivilen Fähigkeiten, Systeme und Anlagen »gezielt auszubeuten«.[43]

Die »Doctrine for Joint Psychological Operations« (Juli 1996) sowie »Joint Vision 2020« (Juni 2000) assistieren mit Richtlinien für Streitkräfte, Nachrichtendienste und mediengesteuerte elektronische Kriegführung. PSYOP sind Streitkräfteoperationen – unterstützt durch geeignete Aktivitäten ziviler Behörden – mit dem Auftrag, die Öffentlichkeit im Ausland mit ausgewählten Informationen zu versorgen und Emotionen, Motive, aber auch das objektive Denken und schließlich das Verhalten fremder Regierungen, Organisationen, Gruppen und Individuen zu beeinflussen[44] – schlicht und ganz ohne Ironie auch als »truth projection«[45] bezeichnet. PSYOP sind im Krieg wie in nichtkriegerischen militärischen Operationen (MOOTW) anzuwenden. Zwar sind Waffeneinsatz und PSYOP auch Elemente der herkömmlichen Kriegführung, doch im Unterschied dazu zeichnet sich die von den US-Streitkräften angestrebte vollentwickelte offensive Informationskriegführung durch die systematische Verknüpfung von Waffeneinsatz, PSYOP und elektronischen Netzangriffen gegen die Infrastruktur des Gegners aus.[46]

Wenn zwei das gleiche tun …

Die Autoren des Dokuments sehen in modernen elektronischen Systemen und Kampfmitteln ein zweischneidiges Schwert: In demselben Maße, in dem die elektronische Vernetzung Informationsdominanz gewährt, schafft sie Abhängigkeit und Verwundbarkeit. Sie setzt die Informationsgesellschaft damit der Gefahr asymmetrischer IW-Angriffe aus, deren strategischem Umfeld (strategic environment) neben dem politischen Interessenkonflikt auch Motive, Ziele und Methoden von Hackern, Kriminellen, des organisierten Verbrechens, korrupter Innentäter, der Industrie- und Wirtschaftsspionage sowie »in einigen Fällen« auch diejenigen des Terrorismus zugerechnet werden.[47] Mehr noch als die »Joint Doctrine IO« ist »Joint Vision 2020« ausdrücklich als Antwort auf die Herausforderungen der asymmetrischen Informationskriegführung konzipiert.[48] Beide Dokumente geben Richtlinien vor, wie künftigen IW-Angriffen militä-

38 Joint Doctrine IO, S. I-8, I-14.
39 Joint Vision 2010; Joint Vision 2020, S. 28.
40 Joint Doctrine, S. I-3. Vgl. hierzu auch Joint Doctrine IO, S. I-10, I-15.
41 Joint Doctrine IO, S. I-11.
42 Joint Doctrine IO, S. I-8, I-17, 18 sowie Abschn. II.4.
43 Joint Doctrine IO, S. II-12.
44 C. W. *Fuller* (Hg.), Doctrine for Joint Psychological Operations, Washington, D.C. 1996, S. v.
45 Doctrine for Joint PSYOP, S. vi; Joint Doctrine IO, S. II-4; »truth projection« wird hier sogar als Mittel der militärischen Täuschung des Gegners verstanden!
46 Joint Doctrine IO, S. II-4; Joint Vision 2020, S. 28–30.
47 Joint Doctrine IO, S. II-11, 15, 16.
48 Joint Vision 2020, S. 4–5.

risch unterlegener Gegner auf informationsabhängige und insofern verwundbare Infrastrukturen der USA wirksam zu begegnen sei.

Es stellt sich an diesem Punkt die Frage, ob und worin sich Hackerangriff und elektronische Wirtschaftskriminalität auf der einen Seite von offensiven Streitkräfte-IO auf der anderen Seite unterscheiden, wenn sie sich der gleichen IW-Mittel und -Methoden bedienen. Die »Joint Doctrine IO« gibt drei verschiedene Antworten auf diese Frage mit sicherheitspolitisch höchst unterschiedlichen Konsequenzen:

Die erste Antwort ergibt sich aus der Forderung, offensive IO einzusetzen, um die Informationsdominanz der US-Streitkräfte im Frieden wie im Konfliktfall zu gewährleisten.[49] Dabei wird unterstellt, daß der Gegner technisch hinreichend versiert, aber militärisch unterlegen ist. Als Herausforderer bedient er sich der gleichen offensiven IW-Mittel wie die US-Streitkräfte und -Nachrichtendienste – nur eben mit dem Ziel, die Überlegenheit der US-Militärmacht zu unterlaufen.[50] Die erste Antwort begnügt sich insofern damit, beim Einsatz offensiver IO eine Rollenverteilung festzustellen: Wenn zwei das gleiche tun, ist es noch längst nicht das gleiche, sofern sie dabei in unterschiedlichen Rollen (Vormacht, Herausforderer) auftreten.

Die zweite Antwort geht vom praktisch uneingeschränkten Vorrang der staatlichen Ziele und nationalen Interessen der USA aus.[51] Der Informationskrieg wird innerhalb oder auch jenseits des herkömmlichen Gefechtsfelds geführt, wann immer dies die Kriegsziele der USA erfordern.[52] Offensive IO sind anzuwenden, wenn sie der Generalstabschef für angemessen erachtet.[53] Die »Joint Doctrine IO« beurteilt Bedrohungen, die sich gegen die USA richten, als kriminell, korrupt oder terroristisch,[54] eigene amerikanische offensive IO jedoch lediglich danach, ob und inwieweit sie den US-Interessen dienen (»... on terms favorable to the United States«).[55] Die zahlreichen Beiträge amerikanischer Autoren zum Thema »Ethik und Informationskrieg«[56] spielen in den IW-Dokumenten des Generalstabs offensichtlich keine Rolle.

Die dritte Antwort schränkt die beiden vorhergehenden ein. Die »Joint Doctrine IO« wie auch »Joint Vision 2020« enthalten ein klares Bekenntnis zum Kriegsvölkerrecht, zu den internationalen Verträgen der USA und der VN-Charta, desgleichen zur amerikanischen Verantwortung gegenüber den Bündnispartnern und für den Weltfrieden.[57] Offensive IO unterliegen den rechtlichen Beschränkungen, denen kriegerische Angriffshandlungen unterworfen sind, und müssen im übrigen den Schutz der staatlichen Souveränität und Sicherheit, die Vertraulichkeit der Telekommunikation und Information sowie die Unverletzlichkeit des Nichtkombattanten respektieren. Rechtlich gesehen liegen in diesen Schutz- und Abwehrbestimmungen die wesentlichen Unterschiede offensiver Streitkräfte-IO zum kriminellen oder terroristischen IW-Angriff. In der politischen Praxis erweist sich allerdings, daß die internationalen sicherheitspolitischen und völkerrechtlichen Beschränkungen der offensiven Informationskriegführung kaum wirksam und anwendbar sind (s.u.). Insbesondere drängt sich die Frage auf, ob die ausdrückliche Verpflichtung der »Joint Doctrine IO« auf das Kriegsvölkerrecht nicht der klaren Erkenntnis folgt, daß dessen Regelungsgehalt im Kontext des offensiven Informationskrieges ohnehin gering ist und den, der sich ihr unterwirft, zu nichts verpflichtet.

49 Joint Doctrine IO, S. I-2, 15.
50 Joint Vision 2020, S. 4–5.
51 Joint Doctrine IO, S. II-8.
52 Joint Doctrine IO, S. I-4, 11.
53 Joint Doctrine IO, S. I-5.
54 Joint Doctrine IO, S. I-16.
55 Joint Doctrine IO, S. II-8.
56 Z.B. John *Arquilla*, Ethics and Information Warfare, in: *Khalilzad/White* (Hg.), Changing Role, S. 379–377; W. J. *Bayles*, The Ethics of Computer Network Attacks, in: Parameters, 31 (2001) 1, S. 44–58. Selbst der Begriff der Verantwortung, der in der »Joint Doctrine IO« häufig verwendet wird, hat eher eine (rein) politische denn eine wie auch immer verstandene ethische Konnotation. Die Verantwortung für die Sicherheit der Bündnispartner, für Demokratie, Weltfrieden, Menschenrechte usw. entspringt ausschließlich dem amerikanischen Interesse und den internationalen Verträgen der USA. Vgl. hierzu Joint Doctrine IO, S. I-1.
57 Joint Doctrine IO, S. I-1, 12, 13; Joint Vision 2020, S. 30.

Internationale Perspektiven

Sicherheitspolitik

In den vergangenen Jahren sind im Auftrag der amerikanischen Regierung mehrere umfangreiche Studien zur Verletzlichkeit und zum Schutz informationsabhängiger Infrastrukturen der USA publiziert worden.[58] Diese Studien haben über die amerikanische Debatte hinaus die internationale Fachöffentlichkeit überhaupt erst nachhaltig auf die Gefährdung kritischer Informationsinfrastrukturen aufmerksam gemacht. Die Empfehlungen der Gutachter an die amerikanische Bundesregierung konzentrierten sich ausschließlich auf IT-Sicherheits- und -Abwehrmaßnahmen. Entsprechende Überlegungen und Empfehlungen richten sich seither auch an Akteure, die international zum Schutz der globalen Daten-, Telekommunikations- und Satellitennetze kooperieren.[59] Offensiver Informationskrieg kommt nach Maßgabe dieser Untersuchungen und Empfehlungen als Mittel der internationalen Politik grundsätzlich nicht in Frage. Hierzu steht das Offensivprogramm der »Joint Doctrine IO« in offenkundigem Gegensatz, dessen Bedeutung für die internationale Sicherheit anhand von zwei Arbeitshypothesen geklärt werden soll.

Zwei Arbeitshypothesen

Die erste Hypothese besagt, daß mit dem Kapitel über die offensiven IO ein sicherheitspolitisches Tabu gebrochen wird. Zum ersten Mal wird das elektronische Nervensystem der gesamten modernen gesellschaftlichen Informationsverarbeitung und Systemsteuerung unverhohlen[60] als Angriffsziel verdeckter militärischer und nachrichtendienstlicher Abhörpraktiken und (Zer-)Störungsakte ins Visier genommen.

Der Wortlaut der »Joint Doctrine IO« läßt keinen Zweifel daran, daß der amerikanische Generalstab – und sicher nicht nur das Militär – den offensiven Informationskrieg als Mittel der politischen Interessendurchsetzung ansieht. Offensive IO bleiben jedoch an zwei Einschränkungen gebunden: Sie nehmen als Mittel der Politik denselben Rang ein wie andere, herkömmliche Anwendungen oder Androhungen militärischer Gewalt, einschließlich der sogenannten MOOTW. Zweitens stehen die Richtlinien der »Joint Doctrine IO« ausdrücklich unter den Vorbehalten des internationalen Kriegsrechts und aller Verträge, zu deren Einhaltung sich die USA verpflichtet haben. Allerdings lassen die oben dargestellten technischen Mittel, Methoden, Strategien und Schauplätze des Informationskriegs bereits vermuten, daß IW-Angriffe von den Organen der inneren und äußeren, nationalen und internationalen Sicherheit mit herkömmlichen politischen Mitteln nicht mehr wirksam zu kontrollieren sind.

Dies führt zu der zweiten Arbeitshypothese, nach der selbst dort, wo Sicherheitspolitik und internationales Recht dem offensiven Informationskrieg Grenzen setzen, diese restriktiven Bestimmungen derzeit und in absehbarer Zukunft wahrscheinlich wenig bewirken. Als kaum durchsetzbar dürften sich insbesondere (mögliche, zukünftige) Verbote offensiver IO, Rüstungs- und Proliferationskontrollen, Vertrauensbildung und Vertragsverfikation erweisen.

58 *Defense Science Board Task Force*, Report of the Defense Science Board Task Force on Information Warfare-Defense, Washington, D.C. 1996; *PCCIP*, Critical Foundations; *The White House*, National Plan for Information Systems Protection, Washington, D.C. 2000; *Defense Science Board Task Force*, Report on Defensive Information Operations, Vol. II, Washington, D.C. 2001; *President of the United States*, Report of the President of the United States on Federal Critical Infrastructures Protection Activities, Washington, D.C. 2001.

59 Gebhard *Geiger*, Internationale Ansätze und Kooperationen, in: Bernd *Holznagel*/Anika *Hanßmann*/Matthias *Sonntag* (Hg.), IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen, Münster 2000, S. 32–47.

60 Die Betonung liegt dabei auf dem öffentlichen Eingeständnis der USA, zur Informationskriegführung auf allen Ebenen (at all levels of war) bereit zu sein. Eine strikt geheime und nach außen stets geleugnete Informationskriegführung, die von militärischen und geheimdienstlichen Stellen ausgeht, gibt es ansonsten häufig und mit weltweit steigender Tendenz. US-Behörden schätzen, daß Netz- und Computerspionage und -sabotage von über 30 Staaten vorbereitet bzw. bereits routinemäßig ausgeführt werden. Vgl. hierzu James *Adams*, Virtual Defense, in: Foreign Affairs, 80 (2001) 3, S. 98–112.

SWP-Berlin
Offensive Informationskriegführung
Februar 2002

Offensiver Informationskrieg als Mittel der Politik

Mehr noch als die »Joint Doctrine IO« geht »Joint Vision 2020« davon aus, daß die technischen und militärischen Fähigkeiten vieler Staaten – aber auch nichtstaatlicher internationaler Organisationen –, offensive IO auszuführen, derzeit bereits beträchtlich sind und weiter wachsen werden. Die USA, die sich erklärtermaßen selbst an die Spitze dieser Entwicklung gestellt haben, müssen nun damit rechnen, daß sich alle anderen »interessierten« Parteien in ihrer Absicht bestärkt sehen, ebenfalls IW-Fähigkeiten auf- oder auszubauen und offensiv zu nutzen. Das amerikanische Beispiel ist nicht nur geeignet, Schule zu machen, sondern könnte tatsächlich einem Trend Vorschub leisten, den amerikanische Sicherheitsexperten unablässig beklagen, daß sich nämlich zunehmend »ehrgeizige Neulinge« in den Club der IW-bereiten Staaten drängen.[61]

Jedenfalls scheinen die USA mit dem Erlaß der »Joint Doctrine IO« die Auffassung zu bestätigen, bei der offensiven Informationskriegführung handele es sich um ein »anerkanntes« Mittel der internationalen Politik. Verstärkt wird dieser Eindruck womöglich dadurch, daß sich viele Staaten durch die USA automatisch bedroht fühlen müssen, sobald sich für sie ein Interessenkonflikt mit der Supermacht abzuzeichnen beginnt. Dabei muß der Konflikt durchaus nicht sicherheitspolitischen Ursprungs sein. Es genügt beispielsweise eine wirtschaftliche Konkurrenzsituation, die bei drohender elektronischer Wirtschaftsspionage zwangsläufig sicherheitspolitische Dimensionen annimmt. Man braucht nicht einmal an die klassischen Rivalen China und Rußland zu denken.[62] Selbst die Europäer sind als enge Verbündete der USA allem Anschein nach sowohl aus wirtschaftlichen wie aus sicherheitspolitischen Gründen der IT-gestützten Spionage, Überwachung und dem Abhören des Funk- und Telephonverkehrs durch die National Security Agency (NSA) ausgesetzt.[63]

US-Generalstab und -Verteidigungsministerium bemühen sich, den Verdacht zu zerstreuen, die »Joint Doctrine IO« werde den vielbeschworenen »cyber terrorism« politisch hoffähig machen. In einem Interview mit dem Pressedienst der amerikanischen Streitkräfte bestritt General Bruce A. Wright, im Generalstab zuständig für IO, daß die USA es darauf abgesehen hätten, unliebsame Konkurrenten mit den Mitteln des Informationskriegs in die Knie zu zwingen.[64] Das Offensivprogramm der »Joint Doctrine IO« stehe lediglich im Zusammenhang mit herkömmlichen C^4I-Gefechtsfeldoperationen und sei nicht mehr als eine evolutionäre Anpassung vorhandener Streitkräfte-Doktrinen an die Herausforderungen der neuen Informationstechnik.

Eine rein evolutionäre Interpretation der »Joint Doctrine IO« ist jedoch nicht angemessen. Das Dokument hat zwar eine evolutionäre Entstehungsgeschichte,[65] aber ihr Ergebnis ist qualitativ neu. Alle einschlägigen Dokumente sehen die offensiven IO als notwendige Konsequenz der RMA. Selbst die milliardenschweren finanziellen und organisatorischen Aufwendungen für die Sicherheit der zivilen amerikanischen IT-Infrastruktur werden damit gerechtfertigt, daß mit dem offensiven Informationskrieg ein historisch unvergleichlicher, qualitativer Sprung in der modernen Kriegführung vollzogen wurde. Die offensiven IO-Richtlinien des Dokuments sind bis ins einzelne nachweisbar (s.o.) darauf angelegt, die neuartigen, revolutionären Möglichkeiten der Kriegführung zu nutzen statt blind an ihnen vorüberzugehen.

Andererseits drängt sich die Frage auf, warum der US-Generalstab seine Bereitschaft zur offensiven Informationskriegführung überhaupt so offen zum Ausdruck bringt, wenn sie sich sicherheitspolitisch als derart zweischneidig erweist. Abgesehen von der amerikanischen Tradition, auch mit sicherheitspolitisch sensiblen Unterlagen freizügig umzugehen, geben die »Joint Doctrine IO« und die »Doctrine for Joint Psychological Operations« selbst die Antwort. Eine unmißverständliche Demonstration der amerikanischen Entschlossenheit und Fähigkeit, auf allen

61 *Adams*, Virual Defense, S. 102.

62 Bruce D. *Berkowitz*, War Logs On, in: Foreign Affairs, 79 (2000) 3, S. 8–12; *Adams*, Virtual Defense.

63 *European Parliament, Directorate-General for Research, Scientific and Technological Options Assessment (STOA)* (Hg.), An Appraisal of the Technologies of Political Control (Report prepared by Steve Wright), Luxemburg 1998; Duncan *Campbell*, Interception Capabilities 2000. Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment programme office), Edinburgh 1999. Die beiden Berichte an das Europa-Parlament enthalten auch Hinweise auf elektronische Spionage und Überwachung auf seiten europäischer Länder. — Vgl. auch verschiedene Beiträge zur Überwachung der Telekommunikation in Deutschland durch amerikanische Geheimdienste in: Datenschutz und Datensicherheit, (1999) 12.

64 Jim *Garamone*, Joint Staff Releases Information Operations Doctrine (American Forces Information Service), Washington, D.C., 10.3.1999.

65 *Wright*, Evolution.

möglichen Konfliktfeldern – vom Weltraum bis zum Internet – Krieg mit überlegenen technischen Mitteln zu führen, ist erklärtermaßen eine der psychologischen Maßnahmen der Informationskriegführung:[66] PSYOP kombiniert mit der Demonstration von Informationsdominanz. Daß diese Kombination andere Staaten und nichtstaatliche internationale Organisationen eher anspornt als hemmt, die Überlegenheit der USA mit asymmetrischen IW-Strategien zu unterlaufen, wird dabei von den US-Militärplanern sozusagen mißbilligend in Kauf genommen.[67]

Internationale Kontrollen?

Als Hochtechnologieland mit der weltweit dichtesten elektronischen Vernetzung sind die USA auch gegenüber offensiven IO besonders verletzlich. Von wirksamen internationalen Abkommen zur Begrenzung oder zum Verbot offensiver IO hätten sie daher den größten Nutzen, ebenso von rüstungskontrollpolitischen Beschränkungen für IW-taugliche Soft- und Hardware. Das US-Verteidigungsministerium hält jedoch nicht das geringste von IW-Verboten und einer Rüstungskontrolle im »cyber space« auf internationaler vertraglicher Basis. Daher haben die USA bisher auch keinerlei diplomatische Bemühungen mit dem Ziel irgendeiner IW-Kontrolle unterstützt.[68]

Im einzelnen erklärt sich diese Haltung aus folgenden Sachverhalten: Soft- und Hardware sowie öffentliche IuK-Netze sind bis zur völligen Ununterscheidbarkeit sowohl militärisch als auch zivil nutzbar (dual use). Ihre Klassifikation als offensiv (mißbräuchlich) oder defensiv, legal oder kriminell ist in den meisten Fällen unmöglich. Der Gebrauch oder der – wie auch immer definierte, normierte oder sanktionierte – Mißbrauch der Informationstechnik kann völlig anonym und verdeckt erfolgen. Jeder (legislative, behördliche, diplomatische) Versuch, diese Anonymität oder das Datengeheimnis einzuschränken, steht von vornherein im Konflikt mit dem Datenschutz und der Vertraulichkeit der Kommunikation, zudem vor praktisch unüberwindlichen technischen Schwierigkeiten der Durchsetzung (z.B. starke Kryptographie).

Mit den gleichen Problemen haben alle Verfahren zu kämpfen, die der herkömmlichen Rüstungskontrolle, Nonproliferation von Rüstungsgütern, Vertrauensbildung und Vertragsverifikation entstammen.[69] Mehr als bei jedem anderen technischen Produkt oder Verfahren wird der offensive militärische, der defensive oder legale kommerzielle Charakter der Soft- und Hardware nicht durch technische Konstruktions-, Eignungs- und Leistungsmerkmale, sondern ausschließlich durch den Gebrauch bestimmt, den der Nutzer von ihr macht. Jede Art qualitativer Rüstungskontrolle, die IT-Systeme und -komponenten nach Eignungskriterien wie zum Beispiel IW-Tauglichkeit einstuft, muß spätestens an diesem Punkt scheitern. Ein typisches Beispiel ist der Versuch des amerikanischen Handelsministeriums, ein Softwareprogramm zur »harten« Datenverschlüsselung als »Kriegswaffe« einzustufen und seine Verbreitung (Ausfuhr) zu verhindern. Das Ministerium ist nicht nur mit dieser Interpretation vor Gericht gescheitert, das Programm wurde auch kurzerhand an den Behörden vorbei über das Internet millionenfach verbreitet.[70]

Selbst eine noch so gutgemeinte vertrauensbildende Maßnahme (Gewährung von Einblick in den elektronischen Datenverkehr, in militärische Netzwerke, in die benutzte Software usw.) muß ihr Ziel verfehlen, weil sie ebensogut zur Täuschung über verdeckte offensive IO genutzt werden kann. Umgekehrt müßten aussagekräftige Verifikationsmethoden sowie vertrauensbildende Maßnahmen auf dem Gebiet der Rüstungskontrolle und Nonproliferation im höchsten Grade eindringfähig (»intrusiv«) sein. Sie würden IuK-Systeme vollständig transparent machen, was sich auf die Systemsicherheit verheerend auswirken müßte. Im übrigen sind bisher noch alle internationalen Bemühungen der Kriminalitätsprävention und Strafverfolgung bei dem Versuch gescheitert, die Verbreitung von Software, Programmen und Inhalten mit Schadenswirkung im Internet einzudämmen.

Eine Zwischenlösung sucht die geplante Konvention des Europarats über die Internetkriminalität.[71] Sie versucht nicht, ein internationales Verbot des IuK-Mißbrauchs durchzusetzen, sondern die Gesetzgebung der einzelnen Staaten auf dem Gebiet der Computerkriminalität zu vereinheitlichen. Dieser Versuch wird mit Einschränkungen auch von einigen

66 Doctrine for Joint PSYOP, S. I-1; Joint Doctrine IO, S. II-7.
67 Joint Vision 2020, S. 4–5.
68 *US Department of Defense, Office of General Counsel*, An Assessment of International Legal Issues in Information Operations, Washington, D.C. 1999, Kap. IX, X.
69 Dorothy E. *Denning*, Reflections on Cyberweapons Controls, in: Computer Security Journal, 16 (2000) 4, S. 43–53.
70 Verschiedene Versionen sind unter den Namen »Snuffle« und »Unsnuffle« auf zahlreichen Internetseiten zu finden.
71 *Counsel of Europe, European Committee on Crime Problems*, Draft Convention on Cybercrime, Straßburg, Juni 2001.

nichteuropäischen Staaten (USA, Japan, Kanada, Südafrika) unterstützt, wäre aber bei seiner Übertragung auf offensive IO als Mittel der Politik in seiner internationalen Wirksamkeit äußerst begrenzt. Jeder Staat betrachtet einen gegen ihn gerichteten IW-Angriff auch ohne ein solches Abkommen als kriminell, was den Angreifer in aller Regel nicht von seinem illegalen Tun abbringt. Eine Ausdehnung des Abkommens auf offensive IO der Streitkräfte und Geheimdienste könnte die Gesetzgebung in den Mitgliedstaaten höchstens insofern harmonisieren, als das IW-Verbot fortan auf einer einheitlichen Rechtsgrundlage nicht funktioniert.

Ein weiterer Gesichtspunkt ergibt sich aus der Tatsache, daß das Abkommen nicht die »hacker tools« als solche verbietet; sie lassen sich ohnehin als scheinbar harmlose Software nach Belieben über das Internet verbreiten. Angestrebt wird vielmehr neben dem Verbot des Computermißbrauchs auch die Strafbarkeit der Mißbrauchsabsicht (Art. 6 »Draft Convention«). Der Mißbrauch von Soft- und Hardware zu Spionage- und Sabotagezwecken und erst recht die Mißbrauchsabsicht sind aber schon aus rein technischen Gründen extrem schwierig nachzuweisen (s.o.).

Ganz allgemein sind Rüstungskontrollen und Verbote militärischer Operationen eines bestimmten Typs sicherheitspolitisch nur sinnvoll, wenn sich Vertragsverletzungen mit einer gewissen Wahrscheinlichkeit entdecken lassen (Verifikation, Aufklärung) und wenn sie im »Ernstfall« mit wirksamen Gegendrohungen oder -maßnahmen sanktioniert werden können. Der Verzicht auf eine internationale Strafverfolgung der Computerkriminalität in der europäischen Konvention unterstreicht nur, wie gering die Erfolgschancen auch für ein internationales IW-Sanktionsregime wären. Hier wie da gilt der Rechtsgrundsatz, daß die Nürnberger keinen hängen, sie hätten ihn denn. Im Internet kennen sie ihn nicht einmal.

Internationales Recht

Das Pentagon hat 1999 die rechtliche Zulässigkeit offensiver IO in bezug auf die Charta der VN, das Kriegsvölkerrecht und die internationalen Verträge der USA prüfen lassen.[72] Experten der National Defense University in Washington hatten bereits ein Jahr zuvor eine vielzitierte Arbeit zu völkerrechtlichen Problemen des Informationskriegs veröffentlicht.[73] Inzwischen liegen auch zahlreiche Spezialstudien zu verschiedenen juristischen Teilaspekten des Informationskriegs (internationales Telekommunikations-, Weltraum-, See-, Handelsrecht) vor. Einige Ergebnisse dieser Analysen werden im folgenden zusammengefaßt und kritisch beleuchtet.

Ein generelles Gewaltverbot in den internationalen Beziehungen zwischen Staaten verhängt Artikel 2, Absatz 4 der VN-Charta. Andere Artikel der Charta sowie die Beschlüsse der Vollversammlung und des Sicherheitsrates der VN lassen Ausnahmen zu. Sie betreffen im wesentlichen die Selbstverteidigung eines Staates gegen einen bewaffneten Angriff (Art. 51) beziehungsweise solche Maßnahmen zur (bewaffneten) Sicherung oder Wiederherstellung des Friedens, die der VN-Sicherheitsrat beschließt (Art. 39, 41, 42).

Die Unterscheidung zwischen Gewalt im allgemeinen und kriegerischer (Waffen-)Gewalt im besonderen ist im Hinblick auf offensive IO von zentraler Bedeutung, da sich die »Joint Doctrine IO« nicht nur auf den Waffeneinsatz im letzteren Sinne bezieht. Andere IO-Anwendungen sind insbesondere die MOOTW, etwa die Zerstörung von zivil genutzter Software (z.B. Computerbetriebssysteme) und von Datenbeständen nach Art der Hackerangriffe. Auch wenn keine militärischen Waffen eingesetzt werden, sind Angriffe mit Zerstörungswirkung eindeutig als physische Gewalt aufzufassen. Als solche verletzen sie die VN-Charta, sofern sie nicht aus Gründen der Selbstverteidigung als zulässige Ausnahmen gelten.[74]

Andererseits fallen unter offensive IO im Sinne der »Joint Doctrine IO« auch solche IT-Angriffe, die zumindest nach herkömmlichem Begriffsverständnis nicht als Gewaltakte anzusehen sind oder deren Gewaltcharakter fraglich erscheint, da sie Daten, die Datenübertragung, Soft- und Hardware nicht (zer-)stören. Hierzu zählen Handlungen wie die Netz- und Computerspionage einschließlich des unbefugten Kopierens elektronisch gespeicherter oder verarbeiteter

72 *US Department of Defense, Office of General Counsel*, Assessment.

73 Lawrence T. *Greenberg*/Seymour E. *Goodman*/Kevin J. *Soo Hoo*, Information Warfare and International Law, Washington, D.C. 1998.

74 *US Department of Defense, Office of General Counsel*, Assessment, Kap. III. Es sei an dieser Stelle nochmals darauf hingewiesen, daß – abweichend vom herkömmlichen Kriegsbegriff – der Informationskrieg nicht notwendig den militärischen Waffengebrauch einschließt. Die Bezeichnung »Informationskrieg« ist durch die Tatsache gerechtfertigt, daß mit offensiven IO unter Umständen Zerstörungswirkungen erzielt werden, die der militärischen Waffenwirkung gleichkommen und strategisches Ausmaß erreichen.

Information sowie das Überwachen des elektronischen Daten- und des Funkverkehrs. Spionage, als solche natürlich weder neu noch IT-spezifisch, wird jedoch von allen Staaten als äußerste Bedrohung ihrer (politischen, militärischen, wirtschaftlichen usw.) Sicherheit angesehen. Die Schäden, die ein Staat durch sie erleiden kann, werden in ihrem Ausmaß durch den elektronischen Datendiebstahl noch erheblich gesteigert. Jedoch sind Spionageakte weder durch die VN-Charta noch nach irgendwelchen Bestimmungen des Kriegsvölkerrechts verboten, da sie nicht als bewaffnete Aggression oder überhaupt als Gewaltakte gelten.

Internationale Abkommen zum Schutz der Vertraulichkeit der Telekommunikation und des ungestörten Datenverkehrs räumen den Mitgliedstaaten in der Regel einen großen Ermessensspielraum ein, der es ihnen erlaubt, ihre vertraglichen Verpflichtungen jederzeit und für eine beliebige Zeitdauer selbst zu suspendieren. Zwischen kriegführenden Parteien gilt das Bestreben sogar als mehr oder weniger selbstverständlich, dem Gegner die ungestörte, vertrauliche Telekommunikation in jeder Beziehung und mit allen Mitteln unmöglich zu machen. Entsprechend sehen sich die US-Streitkräfte durch das internationale Telekommunikationsrecht in keiner Weise bei der Ausführung offensiver IO eingeschränkt.[75]

Ein Großteil der Bestimmungen der Charta sowie der Beschlüsse der Vollversammlung der VN betrifft die Beziehungen zwischen Staaten. Entsprechend weist das internationale Recht auch breite Lücken in der Regelung des Gewaltverbots für nichtstaatliche internationale Organisationen auf. Ausnahmen ergeben sich lediglich aus einigen Formulierungen (z.B. Art. 39, 51) und Zusatzbestimmungen des VN-Rechts, die besondere Maßnahmen des Sicherheitsrates und der VN-Mitglieder gegen nichtstaatliche Organisationen zulassen. Für einen Staat, der mit offensiven IO gegen einen Konfliktgegner vorgehen, sich eine Verletzung des Völkerrechts aber nicht nachweisen lassen möchte, eröffnen sich hier viele neuartige Möglichkeiten. Er kann beispielsweise ein Privatunternehmen mit Netz- und Computersabotageakten beauftragen beziehungsweise selbst ein (Tarn-)Unternehmen für solche Zwecke gründen. Verschiedene Varianten des getarnten, von einem Staat oder auch einer nichtstaatlichen Organisation geförderten oder geduldeten Auftragsterrorismus (state-sponsored cyber terrorism) werden allem Anschein nach bereits praktiziert.[76] Sie machen sich die beiden erwähnten Tatsachen zunutze, daß die Informationstechnik neue Formen nichtstaatlicher internationaler Organisation ermöglicht, die sich zudem in einem weitgehend rechtsfreien Raum entfalten können. Eine offensive Nutzung nichtstaatlicher Organisationen, die im Regierungsauftrag tätig werden, bietet sich als asymmetrische IW-Strategie geradezu an und scheint als solche nicht nur im Konflikt mit technisch-militärischen Großmächten geeignet.

Mit den hier nur angedeuteten Möglichkeiten, das Gewaltverbot in den internationalen Beziehungen mit informationstechnischen Mitteln zu unterlaufen, sind die völkerrechtlichen Probleme der offensiven IO noch längst nicht erschöpft. Die zitierte rechtswissenschaftliche Stellungnahme des US-Verteidigungsministeriums (Office of General Counsel) gelangt zu folgendem generellem Schluß: »Es ist völlig ungeklärt, in welchem Umfang die Weltgemeinschaft Computernetzangriffe als ›Waffengewalt‹ und ›Gewaltanwendung‹ betrachtet und in welchem Sinne das Recht auf Selbstverteidigung und Gegenmaßnahmen [gegen bewaffnete Angriffe, Anm. d. Verf.] auf Computernetzangriffe anzuwenden ist. [...] Wenn die Staaten sich nicht entschließen können, Verhandlungen über einen Vertrag über Computernetzattacken aufzunehmen, was in naher Zukunft ganz und gar unwahrscheinlich ist, wird sich das internationale Recht auf diesem Gebiet durch die staatlichen Handlungsweisen und im Sinne jener Positionen entwickeln, die die Staaten jeweils zum Gang der Ereignisse in der Öffentlichkeit einnehmen werden.«[77] Noch deutlicher werden Greenberg, Goodman und Soo Hoo, drei Kriegsrechtsexperten der National Defense University in Washington, D.C., die in ihrer Analyse kurz und bündig feststellen, daß »die Unklarheit des internationalen Rechts in bezug auf den Informationskrieg den Vereinigten Staaten genügend Raum geben dürften, Maßnahmen vom Typ des Informationskriegs zu ergreifen.«[78]

Das Kriegsvölkerrecht unterscheidet zwischen der Berechtigung, einen Krieg zu führen (ius ad bellum), einerseits und der Zulässigkeit bestimmter Kampfmaßnahmen im Krieg (ius in bello) andererseits. Wie

75 *US Department of Defense, Office of General Counsel*, Assessment, S. 33.

76 John *Arquilla*/David F. *Ronfeldt*/M. *Zanini*, Networks, Netwar, and Information-Age Terrorism, in: *Khalilzad*/*White* (Hg.), Changing Role, S. 75–111.

77 *US Department of Defense, Office of General Counsel*, Assessment, S. 25.

78 *Greenberg*/*Goodman*/*Soo Hoo*, Information Warfare and International Law, Executive Summary.

die »Joint Doctrine IO« hervorhebt, bemißt sich die Zulässigkeit offensiver IO in der Hauptsache – aber nicht ausschließlich – nach der Haager Landkriegsordnung (1907) sowie den internationalen Verträgen, deren Mitglied die Vereinigten Staaten sind.[79] Das Kriegsvölkerrecht verlangt unter anderem den Schutz von Nichtkombattanten, die Begrenzung des Waffengebrauchs auf das militärisch Notwendige, die Verhältnismäßigkeit der militärischen Mittel und Maßnahmen sowie die Achtung der Unverletzlichkeit neutralen Territoriums. Es verbietet Heimtücke und vermeidbare Kollateralschäden des Waffeneinsatzes.

Das amerikanische Verteidigungsministerium erkennt denn auch an, daß den offensiven IO der US-Streitkräfte rechtliche Schranken gesetzt sind: »Es gibt neuartige Eigenschaften der IO, die Erweiterungen und Interpretationen herkömmlicher Grundsätze des Kriegsvölkerrechts notwendig machen. Jedoch erscheint das Ergebnis einer solchen Extrapolation im großen und ganzen absehbar. Das Kriegsvölkerrecht ist vermutlich das einzige Gebiet des internationalen Rechts, auf dem bestehende rechtliche Normen mit größter Gewißheit auf IO angewandt werden können.«[80]

Von einer direkten Anwendbarkeit des bestehenden Kriegsvölkerrechts auf die offensive Informationskriegführung auszugehen ist jedoch in vielen Punkten fragwürdig. Viele Bestimmungen des Kriegsvölkerrechts gehen nämlich von stillschweigenden Voraussetzungen aus, die im historischen Entstehungskontext dieser Rechtsnormen selbstverständlich waren (z.B. die Unterscheidbarkeit von Kombattanten und Nichtkombattanten anhand von Uniformen und Zivilkleidung), die aber im Informationszeitalter durch »dual-use«-Technik und die elektronische Vernetzung militärischer und ziviler Systeme hinfällig geworden sind. Das folgende Beispiel legt nahe, daß die Pentagon-Studie Regelungsgehalt und Geltung des Kriegsvölkerrechts in bezug auf zentrale Probleme der Informationskriegführung systematisch überschätzt.

»Wird ein Computernetzangriff aus großer Entfernung vom Ziel ausgeführt, ist es praktisch unerheblich, ob der ›Kombattant‹ eine Uniform trägt. Jedoch verlangt das Kriegsvölkerrecht, daß rechtmäßige Kombattanten in Übereinstimmung mit dem Kriegsvölkerrecht handeln, effektiv einer Disziplin unterworfen sind und von Offizieren befehligt werden, die für ihr Verhalten verantwortlich sind. Daher ist es notwendig, daß während internationaler bewaffneter Konflikte IO nur von Angehörigen der Streitkräfte als den Kombattanten ausgeführt werden dürfen. [...] Die große Entfernung und Anonymität von Computernetzangriffen mag deren Aufdeckung und Strafverfolgung unwahrscheinlich machen, aber es ist ein feststehender Grundsatz der Politik der Vereinigten Staaten, daß die US-Streitkräfte in voller Übereinstimmung mit dem Kriegsvölkerrecht kämpfen.«[81]

Ob die Streitkräfte bereit sind, das Kriegsvölkerrecht einzuhalten, ist rechtlich gesehen gar nicht die Frage – dazu sind Streitkräfte selbstverständlich immer verpflichtet. Fraglich ist vielmehr, ob das Kriegsvölkerrecht für offensive IO überhaupt gilt. Wie das Zitat selbst hervorhebt, hat die Problematik im wesentlichen drei Dimensionen:

- Die Begriffe des Kriegsvölkerrechts (Kombattant, Nichtkombattant, Waffe, Waffengewalt, Krieg, Nichtkrieg usw.) erfassen die Akteure, Mittel und Methoden des offensiven Informationskriegs nicht zureichend. In dem Maße, in dem die offensiven IO der »Joint Doctrine IO« nicht an einen Waffengebrauch gebunden sind, unterliegen sie auch nicht dem Recht bewaffneter Konflikte.
- Rechtsverletzungen durch offensive IO sind als solche (für den Gegner, einen neutralen Zeugen, ein Kriegsverbrechertribunal) grundsätzlich nicht erkennbar. Dies gilt in dem zitierten Beispiel sicherlich für den anonymen Konfliktgegner und ist im übrigen typisch für alle distanzfähigen, anonymen und verdeckten IO.
- Kombattanten und Nichtkombattanten sind in einem bewaffneten Konflikt, der mit offensiven IO geführt wird, für einen Beobachter nicht mehr zu unterscheiden. Die »Joint Doctrine IO« sieht die Mitwirkung nichtmilitärischer Behörden und Medien an den offensiven IO der Streitkräfte vor. Die Mitarbeiter dieser Organisationen sind aber definitionsgemäß keine Angehörigen der Streitkräfte und daher keine Kombattanten beziehungsweise ihr Kombattantenstatus ist nicht überprüfbar und schon gar nicht offen erkennbar.

Insgesamt lassen die zitierten rechtswissenschaftlichen Untersuchungen erkennen, wie schwach und fragwürdig die Bestimmungen des internationalen Rechts in bezug auf offensive IO sind. Deutlicher noch als die Autoren der Pentagon-Studie (Office of General

79 Joint Doctrine IO, S. I-1.

80 *US Department of Defense, Office of General Counsel*, Assessment, S. 11.

81 *US Department of Defense, Office of General Counsel*, Assessment, S. 8.

Counsel) gelangen Greenberg, Goodman und Soo Hoo zu der Auffassung, daß alle Staaten, einschließlich die USA,[82] über offensive IO nach Maßgabe der Opportunität und nicht des internationalen Rechts entscheiden: »Wahrscheinlich werden die Staaten am wenigsten bereit sein, sich dem Diktat des internationalen Rechts zu beugen, wenn dieses Diktat ihre fundamentalen Interessen gefährdet oder sie an der Verfolgung ihrer Interessen hindert.«[83]

82 *Greenberg/Goodman/Soo Hoo*, Information Warfare and International Law, Executive Summary.
83 Ebd., Introduction.

Schlußfolgerungen

Die »Joint Doctrine for Information Operations« wurde vom Generalstab der US-Streitkräfte mit dem Ziel entwickelt, herkömmliche operative Grundsätze für militärische Führungs- und Nachrichtensysteme an die Erfordernisse der informationselektronischen Revolution des modernen Militärwesens anzupassen.

Das Dokument ist weit über seine militärischen, strategischen und operativen Anwendungen hinaus von breitem sicherheitspolitischem Interesse. Es rückt die Informationsabhängigkeit und Verletzlichkeit gesellschaftlicher Infrastrukturen in den Mittelpunkt der Sicherheitspolitik und wirft damit völlig neuartige Fragen nach Art, Umfang und Lösung künftiger internationaler Konflikte auf.

Konzipiert als umfassende Richtlinie für moderne technologiegestützte militärische Operationen, berücksichtigt die »Joint Doctrine IO« gleichzeitig auch nichtmilitärische (asymmetrische) Alternativen zum Waffengebrauch als einem »traditionellen« internationalen Konfliktlösungsweg. Sie kennzeichnet den offensiven Informationskrieg als radikale Herausforderung sowohl für die Rüstungskontrolle wie für das internationale Recht.

Problematisch erscheint die »Joint Doctrine IO« in ihrem Bekenntnis zum offensiven Informationskrieg als einem Mittel der internationalen Politik. Offensive IO, die über rein militärische C^4I-Gefechtsfeldoperationen, die elektronische Aufklärung und den Lenkwaffeneinsatz hinausgingen, waren in den zahlreichen US-Regierungsdokumenten während der vergangenen Jahre niemals in Erwägung gezogen worden. Nun stellt sich die Frage, ob das amerikanische Beispiel nicht Schule machen wird. Ein zusätzlicher »Motivationsschub« zugunsten einer offensiven Informationskriegführung ist bei allen Staaten, Armeen und Geheimdiensten zu erwarten, die – nach amerikanischer Beobachtung – ebenfalls Computerspionage und -sabotage sowie »truth projection« über elektronische Massenmedien planen. Bisher sahen sich die Staaten immer genötigt, solche Pläne geheimzuhalten, und fühlten sich bei der Ausführung entsprechend gehemmt. Diese Hemmungen fallen nun weg.

Bei offiziellen Stellungnahmen zum offensiven Charakter der »Joint Doctrine IO« sind die Amerikaner bestrebt, den Eindruck eines sicherheitspolitischen Dammbruchs bei der aggressiven Nutzung der Informationstechnik zu vermeiden. Sie verweisen auf die lange Praxis der militärischen Informationskriegführung, die im Informationszeitalter natürlich nicht abbricht, auf die verbürgte Bereitschaft der US-Streitkräfte, in allen Konfliktlagen internationales Recht zu respektieren (Distanz zum »cyber terrorism«), die offensiven IW-Vorbereitungen anderer Staaten sowie die sicherheitspolitischen Herausforderungen asymmetrischer Strategien.

Ungeachtet der sicherheitspolitischen Kritik, die solche Einwände herausfordern, bleiben zwei wesentliche Ergebnisse festzuhalten: Erstens, offensive IO sind – obgleich mit einigem Wenn und Aber – als Mittel der internationalen Politik öffentlich anerkannt –, und sei es nur von einem einzigen Staat, der aber immerhin derzeit alleinige Weltmacht ist. Zweitens, viele Staaten, die aus irgendeinem Grund, der nicht notwendig militärischer Natur zu sein braucht, mit den USA in einen Konflikt geraten, werden sich mit den Mitteln eines offensiven IT-gestützten »Konfliktmanagements« manipuliert und bedroht sehen. Entsprechende Befürchtungen werden sich auf die erklärte Absicht der USA stützen, die offensiven Maßnahmen der »Joint Doctrine IO« sorgfältig auf die IT-Schwachstellen ganzer gesellschaftlicher Infrastrukturbereiche auszurichten und gegebenenfalls bereits im Frieden und in latenten internationalen Konflikten als MOOTW zum Einsatz zu bringen.

Die Frage nach den Mitteln der internationalen Politik betrifft auch die denkbaren Kontrollen und vertraglichen Verbote der offensiven Informationskriegführung. Als solche kommen in erster Linie herkömmliche oder geeignet zu ergänzende Mechanismen der internationalen Rüstungs- und Proliferationskontrolle in Betracht, angewandt auf IW-taugliche Soft- und Hardware, ebenso ein aktualisiertes Gewaltverbot in den internationalen Beziehungen sowie geeignete Erweiterungen der rechtlichen Regelungen für bewaffnete Konflikte.

In bezug auf sicherheitspolitische und rechtliche Kontrollen der offensiven Informationskriegführung lassen sich im wesentlichen zwei Schwerpunkte der amerikanischen Argumentation und Politik ausmachen. Bereits die Regierung Präsident Clintons hat

zu erkennen gegeben, daß sie jeden Versuch des IW-Verbots und einer internationalen Rüstungskontrolle auf dem Gebiet der IW-tauglichen Hard- und Software für völlig unwirksam und daher rundum für verfehlt hält. Die neue Regierung Bush hat dieser Auffassung bislang nicht widersprochen und wird dies auch in Zukunft nicht tun. Eine »Rüstungskontrolle im cyber space« wird, soweit absehbar, keine amerikanische Unterstützung finden.

Stärker in die Pflicht genommen sehen sich die US-Streitkräfte durch das Recht der VN und das Kriegsvölkerrecht. Hier stellt sich allerdings das Problem, daß deren Bestimmungen viele technische Möglichkeiten des Informationskriegs grundsätzlich nicht erfassen (unzutreffende Rechtsbegriffe, nicht feststellbare rechtlich relevante Tatsachen usw.). Aus amerikanischer Sicht kann das Recht bewaffneter Konflikte bei der Wahl von Offensiv-, Defensiv- oder Vergeltungsmaßnahmen im Informationskrieg hilfreich sein, bietet aber keinen Ersatz für politische Entschlossenheit und militärische Bereitschaft.[84]

Nicht nur für die internationale Sicherheit, sondern speziell auch für die deutsche Sicherheitspolitik hat der Erlaß der »Joint Doctrine IO« Konsequenzen und gibt Anstoß zu folgenden Überlegungen:

- Versuche der militärischen und geheimdienstlichen Nutzung offensiver IO zu politischen und wirtschaftlichen Zwecken unternehmen angeblich viele Staaten. Die »Joint Doctrine IO« wird diese Aktivitäten eher verstärken denn hemmen. Auch die Bundesrepublik Deutschland muß damit rechnen, daß – ähnlich der Spionage oder der Agententätigkeit – offensive IO als Routinemittel der internationalen Politik eingesetzt werden.
- Ein systematischer Vergleich zwischen den IO der »Joint Doctrine IO« und solchen der Bundeswehr ist durchzuführen, dessen Befunde vor dem Hintergrund vergleichbarer beziehungsweise nicht vergleichbarer Streitkräfteaufgaben und Rahmenbedingungen sorgfältig analysiert werden müssen.
- Die Informationsabsicherung in der Bundeswehr wird zwar als Defensivmaßnahme zielstrebig vorangetrieben,[85] sie sichert aber nur eine notwendige Minimalbasis der deutschen Streitkräfteoperationen. Angesichts der (militärischen, technischen, wirtschaftlichen, medienabhängigen) Dimensionen offensiver IO ist eine umfassende Aufklärung und systematische Daten- und Lageanalyse internationaler IW-Aktivitäten und aktueller IW-Entwicklungen zur Bildung einer sicherheitspolitischen Entscheidungsgrundlage erforderlich.
- Die herkömmliche zwischenbehördliche Zusammenarbeit mit periodischem Datenaustausch reicht hierzu offenbar nicht mehr aus. Eine Zentralbehörde (IW-Kompetenzzentrum oder »Information Warfare Center«), nach dem Vorbild ähnlicher amerikanischer Einrichtungen (CIOA, NISP) und mit den notwendigen Kompetenzen ausgestattet, wäre den Herausforderungen des offensiven Informationskriegs angemessen.
- Eine solche Behörde muß nicht nur koordinieren, sondern die Aktivitäten zwischen Verteidigung, innerer Sicherheit, Bundesamt für Sicherheit in der Informationstechnik, Justiz und Wirtschaft ressortübergreifend organisieren, ebenso die Zusammenarbeit zwischen der Bundesrepublik Deutschland und ihren europäischen und atlantischen Verbündeten.
- Zum Aufbau einer wirksamen europäischen IW-Abwehr bedarf es unter dem Dach der EU oder neben (in Zusammenarbeit mit) bestehenden anderen Organisationen (NATO, International Telecommunication Union [ITU]) einer zwischenstaatlichen Behörde mit der Aufgabe, den internationalen Ausbau und Schutz öffentlich zugänglicher elektronischer Informationsnetze in allen technischen, wirtschaftlichen und rechtlichen Fragen zu fördern und zu koordinieren.
- Die Sicherheitspolitik darf nicht bei bloßen Reaktionen auf IW-Angriffe etwa nach dem Vorbild der Strafverfolgung in Fällen der Computerkriminalität stehenbleiben, das heißt erst reagieren, wenn das Kind in den Brunnen gefallen ist. Die Hauptaufgabe liegt in einer möglichst umfassenden Schadenprävention durch Schaffung robuster politisch-gesellschaftlicher Infrastrukturen, die nach Organisation und technischer Ausstattung in der Lage sind, auch unter den Bedingungen eines IW-Angriffs die Öffentlichkeit mit einem Mindestmaß an Informationsdienstleistungen zu versorgen.[86]

Die Sicherheit kritischer Infrastrukturen der Informationsgesellschaft umfaßt nicht zuletzt Forschung und Entwicklung auf den Gebieten Systemanalyse, Unternehmen und Risikomanagement.[87] Aus einem

84 *Greenberg/Goodman/Soo Hoo*, Information Warfare and International Law, Executive Summary.

85 Manfred *Cichos*, Informationsabsicherung – Die Sicht des Bedarfsdeckers, in: *Geiger* (Hg.), Sicherheit, S. 134–143.

86 *Geiger* (Hg.), Sicherheit.

87 Gebhard *Geiger*, Information und Infrastruktursicherheit –

verstärkten deutschen (personellen, finanziellen) Beitrag zu den bestehenden europäischen Initiativen auf dem Gebiet der sicherheitswissenschaftlichen Systemforschung[88] könnten Sicherheit und Sicherheitspolitik der Bundesrepublik erheblichen Nutzen ziehen.

Grundzüge eines sicherheits- und technologiepolitischen Forschungs- und Entwicklungsprogramms, unveröffentlichtes Arbeitspapier, Ebenhausen: Stiftung Wissenschaft und Politik, 2000.

88 *Geiger*, Internationale Ansätze und Kooperationen, in: *Holznagel/Hanßmann/Sonntag* (Hg.), IT-Sicherheit.

Literaturhinweise

Adams, James, The Next World War, New York 1998

— Virtual Defense, in: Foreign Affairs, 80 (2001) 3, S. 98–112

Alberts, David S./*Garstka*, John J./*Stein*, Frederick P., Network Centric Warfare: Developing and Leveraging Information Superiority, 2. Aufl., Washington, D.C. 1999

Arquilla, John, Ethics and Information Warfare, in: Zalmay M. *Khalilzad*/John P. *White* (Hg.), The Changing Role of Information in Warfare, Santa Monica, Ca. 1999, S. 379–377

Arquilla, John/*Ronfeldt*, David F. (Hg.), In Athena's Camp. Preparing for Conflict in the Information Age, Santa Monica, Ca. 1997

Arquilla, John/*Ronfeldt*, David F./*Zanini*, M., Networks, Netwar, and Information-Age Terrorism, in: Zalmay M. *Khalilzad*/John P. *White* (Hg.), The Changing Role of Information in Warfare, Santa Monica, Ca. 1999, S. 75–111

Bayles, W. J., The Ethics of Computer Network Attacks, in: Parameters, 31 (2001) 1, S. 44–58

Berkowitz, Bruce D., War Logs On, in: Foreign Affairs, 79 (2000) 3, S. 8–12

Campbell, Duncan, Interception Capabilities 2000. Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment programme office), Edinburgh 1999

Cerny, Dietrich, Schutz kritischer Infrastrukturen in Wirtschaft und Verwaltung, in: Gebhard *Geiger* (Hg.), Sicherheit der Informationsgesellschaft, Baden-Baden 2000, S. 21–42

Cichos, Manfred, Informationsabsicherung – Die Sicht des Bedarfsdeckers, in: Gebhard *Geiger* (Hg.), Sicherheit der Informationsgesellschaft, Baden-Baden 2000, S. 134–143

Computer Science and Telecommunications Board/*National Research Council USA*, Realizing the Potentials of C^4I: Fundamental Challenges, Washington, D.C. 1999

Counsel of Europe, European Committee on Crime Problems, Draft Convention on Cybercrime, Straßburg, Juni 2001

Defense Science Board Task Force, Report of the Defense Science Board Task Force on Information Warfare-Defense, Washington, D.C. 1996

— Report on Defensive Information Operations, Vol. II, Washington, D.C. 2001

Defense Technical Information Center (Hg.), Program Directives, Ft. Belvoir, VA o.J.

Denning, Dorothy E., Reflections on Cyberweapons Controls, in: Computer Security Journal, 16 (2000) 4, S. 43–53

— Information Warfare and Security, Reading, Mass. 1999

European Parliament, *Directorate-General for Research*, *Scientific and Technological Options Assessment (STOA)* (Hg.), An Appraisal of the Technologies of Political Control (Report prepared by Steve Wright), Luxemburg 1998

Fuller, C. W. (Hg.), Doctrine for Joint Psychological Operations, Washington, D.C. 1966

Geiger, Gebhard (Hg.), Sicherheit der Informationsgesellschaft, Baden-Baden 2000

— Information und Infrastruktursicherheit – Grundzüge eines sicherheits- und technologiepolitischen Forschungs- und Entwicklungsprogramms, unveröffentlichtes Arbeitspapier, Ebenhausen: Stiftung Wissenschaft und Politik, 2000

— Informationstechnischer Wandel und neue Risiken der internationalen Sicherheit, in: Jens *van Scherpenberg*/Peter *Schmidt* (Hg.), Stabilität und Kooperation: Aufgaben internationaler Ordnungspolitik, Baden-Baden 2000, S. 50–62

— Internationale Ansätze und Kooperationen, in: Bernd *Holznagel*/Anika *Hanßmann*/Matthias *Sonntag* (Hg.), IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen, Münster 2000, S. 32–47

— Internationale Sicherheit, in: Gebhard *Geiger* (Hg.), Sicherheit der Informationsgesellschaft, Baden-Baden 2000, S. 145–199

— Neue Strukturen und Herausforderungen der internationalen Sicherheit im Informationszeitalter, in: Aussenpolitik, 48 (1997) 4, S. 401–408

Greenberg, Lawrence T./*Goodman*, Seymour E./*Soo Hoo*, Kevin J., Information Warfare and International Law, Washington, D.C. 1998

Hayes, R. E./*Alberts*, D. S., The Realm of Information Dominance: Beyond Information War, in: Gary F.

SWP-Berlin
Offensive Informationskriegführung
Februar 2002

Wheatley/Richard E. *Hayes*, Information Warfare and Deterrence, Washington, D.C. 1966, Anhang B

Khalilzad, Zalmay M./*White*, John P. (Hg.), The Changing Role of Information in Warfare, Santa Monica, Cal. 1999

Molander, Roger C./*Riddile*, Andrew S./*Wilson*, Peter A., Strategic Information Warfare, Santa Monica, Cal.: RAND, 1996

Nye, Joseph S. Jr./*Owens*, William A., America's Information Edge, in: Foreign Affairs, 75 (1996) 2, S. 20–36

President of the United States, Report of the President of the United States on Federal Critical Infrastructures Protection Activities, Washington, D.C. 2001

President's Commission on Critical Infrastructure Protection (PCCIP), Critical Foundations. Protecting America's Infrastructures, Washington, D.C. 1997

Roßnagel, Alexander/*Wedde*, Peter/*Hammer*, Volker/*Pordesch*, Ulrich, Verletzlichkeit der ›Informationsgesellschaft‹, Opladen 1989

Shalikashvili, John M. (Hg.), Joint Vision 2010, Washington, D.C. 1996

Shelton, Henry H. (Hg.), Joint Vision 2020, Washington, D.C. 2000

US Department of Defense, *Office of General Counsel*, An Assessment of International Legal Issues in Information Operations, Washington, D.C. 1999

Waltz, Edward, Information Warfare. Principles and Operations, Boston 1998

The White House, National Plan for Information Systems Protection, Washington, D.C. 2000

Wright, Richard H., The Evolution of Info Ops Doctrine, in: Military Review, 81 (2001) 2, S. 30–32

Abkürzungen

C^4I	Command, Control, Communication, Computers, Information
CIAO	Critical Infrastructure Assurance Office
CNA	Computer Network Attack
DII	Defense Information Infrastructure
EW	Electronic Warfare
FM	Field Manual
INFOSYS	Information Systems
INTELSAT	International Telecommunications Satellite Organization
IO	Information Operations
IT	Informationstechnik
ITU	International Telecommunication Union
IuK	Information und Kommunikation
IW	Information Warfare
JFC	Joint Forces Commander
MOOTW	Military Operations Other Than War
NISP	National Infrastructure Protection Center
NSA	National Security Agency
OPSEC	Operations Security
PCCIP	President's Commission on Critical Infrastructure Protection
PSYOP	Psychological Operations
RMA	Revolution in Military Affairs
SOP	Special Operations Forces
TSK	Teilstreitkräfte