FoG:IS

Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik

Texte

zur Sicherheitspolitik in der Informationsgesellschaft

1997-99

FoG:IS Arbeitspapier Nr. 1

November 1999

Inhalt

Grundlagen und Überblicksdarstellungen

Einzelaspekte

FoG:IS

Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik

"The computer offers us both
new models of mind and
a new medium on which to project
our ideas and fantasies."
Sherry Turkle

Der Übergang von der Industrie- zur Informationsgesellschaft bringt für gesellschaftliche Strukturen, Institutionen und Prozesse einen umfassenden Wandel mit sich, dessen Ausmaße noch nicht vollständig verstanden werden. Stichworte wie "flexible Netzwerkstrukturen", "Entmaterialisierung der Wertschöpfung" und "Beschleunigung" beschreiben zwar Trends, können aber noch nicht ausreichend Auskunft über die Gesellschaftsform der Zukunft geben. In Teilbereichen liegen aber empirische Studien vor, die zu soziologischen und politikwissenschaftlichen Theorieansätzen geführt haben. In die sicherheitspolitische Forschung haben diese Entwicklungen jedoch bisher nicht ausreichend Eingang gefunden.

Auch im Bereich der Sicherheitspolitik ist ein grundlegender Wandel zu beobachten. Elektronische Überwachungstechnologien, Präzisionswaffen, die Nutzung von kommerziellen Produkten, "Informationskriege" oder die "Revolution in Military Affairs" stellen den Kernbereich staatlicher Existenz, das Gewaltmonopol, in Frage. Die Grenzen zwischen innerer und äußerer Sicherheit, zwischen Krieg und Frieden (auch: zwischen Krieg und Kriminalität) sowie zwischen Militär, Polizei und Geheimdiensten werden unscharf. Im Gefolge der US-amerikanischen Diskussion wird seit kurzem auch in Deutschland darüber diskutiert, ob und wie neue Informationstechnologien Aufgaben, Strategien und Institutionen der Sicherheitspolitik verändern und wie darauf reagiert werden sollte.

Die Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik (FoG:IS) wurde im Sommer 1999 gegründet, um dieser Debatte ein solides Fundament zu geben. Bislang fehlt es an seriösen Studien, die nicht jede technische Innovation als militärischen Durchburch einschätzen oder als neues Sicherheitsrisiko bewerten, sondern fundierte Einschätzungen auf wissenschaftlicher Grundlage liefern. Die FoG:IS hat sich zum Ziel gesetzt, auf diesem Gebiet empirische Detailkenntnis mit theoretischer Reflexion zu verbinden. Dabei sollen neue Trends aufgespürt und abgeschätzt, implizite Grundannahmen der Diskussion auf ihre Ideologien abgeklopft sowie Alternativen zum militärisch dominierten Diskurs entwickelt werden.

Die FoG:IS arbeitet interdisziplinär als dezentraler Zusammenschluß von NachwuchswissenschaftlerInnen aus verschiedenen Fächern. Neben der inhaltlichen Arbeit leistet FoG:IS damit auch einen Beitrag zur wissenschaftlichen Nachwuchsförderung. Der Großteil der Arbeit wird vernetzt und projektbezogen

geleistet, daher kann die FoG:IS auf feste Strukturen oder einen großen Verwaltungsapparat verzichten.

Die FoG:IS ist

- *Ralf Bendrath*, Doktorand zum Thema “Das Militär in der Informations-gesellschaft”, FU Berlin; Listowner Infowar.de,
- *Elvi Claßen*, Doktorandin zum Thema “Krisen und Kriegskommunikation in der Informationsgesellschaft”; Lehrbeauftragte am Fachbereich Medienwissenschaft der Universität/GH Siegen,
- *Olivier Minkwitz*, Mitarbeiter der Arbeitsstelle Transatlantische Außen- und Sicherheitspolitik, FU Berlin; Mitherausgeber “antimilitarismus information” (ami),
- *Regina Passier*, freie Journalistin, Berlin.

Die FoG:IS bietet

- InterviewpartnerInnen und ReferentInnen
- Publikationen in Fachzeitschriften, der Presse oder in Online-Medien
- wissenschaftliche Gutachten als Technikfolgenabschätzungen, strategische Analysen oder Politikempfehlungen
- Konferenzen, Workshops und andere Veranstaltungen
- Kontakte zu thematisch verwandten Arbeitsgruppen und Initiativen
- die deutschsprachige Mailingliste Infowar.de
- eine Webseite mit Texten und einer systematischen Linksammlung (im Aufbau)
- Bearbeitung von individuellen Anfragen und Recherchewünschen.

Impressum

Die Arbeitspapiere der FoG:IS erscheinen unregelmäßig im Selbstverlag.

ViSdP für diese Ausgabe: Ralf Bendrath

Kontakt

Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik (FoG:IS)

Ralf Bendrath

Freie Universität Berlin

Otto Suhr-Institut für Politische Wissenschaft

Ihnestraße 22, D-14195 Berlin

Fon ++49-30-838-2299, Fax ++49-30-838-4160

Folgende Adressen sind in Kürze erreichbar:
Email: info@fogis.de
World Wide Web: http://www.fogis.de

Grundlagen und Überblicksdarstellungen

Elvi Claßen

Macht, Militär & Megabyte

Internet, Multimedia, Electronic Warfare und der Kampf um die Ressource 'Information'[1]

"Damit die im Wandel der Dinge
auftretenden Ungerechtigkeiten der Zustände
nicht zur Gewaltsamkeit führen,
muß eine friedliche Revision aller Verhältnisse
offengehalten werden."
Karl Jaspers, 1958

Noch ist das 'globale Dorf Internet' eine exklusive Enklave: Man geht davon aus, daß weltweit zwischen 30 und 70 Millionen Menschen einen Zugang zum 'Netz der Netze' haben; die Hälfte davon lebt in den USA. Und so hat man sich die Internet-Gemeinde größtenteils vorzustellen: "Zu fast zwei Dritteln handelt es sich um weiße, männliche Mittelstandsbürger zwischen 20 und 30 Jahren mit Universitätsausbildung aus den großen Industrieländern". In der "Zwei-Klassen-Informationsgesellschaft" bedingt die Kluft zwischen 'arm' und 'reich' auch die Zugangsmöglichkeiten zu Informations- und Kommunikationsmitteln; laut UNESCO gibt es z.B. in New York und Tokio mehr Telefonanschlüsse, als auf dem ganzen afrikanischen Kontinent.[2]

Technisch gesehen ist der "Information-Highway" zwar derzeit noch eine riesige desolate Baustelle, mit Umleitungen, Sackgassen und häufigen Massenstaus, in denen das "Surfen" jäh übergehen kann in - um im Bild zu bleiben - 'dümpeln in der Pfütze'. Trotzdem wird das Internet weltweit als das zukunftsträchtige Medium schlechthin bewertet, mit dem Texte, Töne, Bilder und Filme fast in Echtzeit verteilt und abgerufen werden können. Eine Einschätzung, die auch im politischen Bereich kontinuierlich an Boden gewinnt.

Die "Zivilisierung" und "Vergesellschaftung" des Internet seit den 60er Jahren

War das Internet ursprünglich eine Auftragsarbeit des US-Verteidigungsministeriums, das als dezentral organisierter Verbund regionaler Computernetze ein Funktionieren militärischer Kommunikation im Falle eines Krieges gewährleisten sollte, so 'zivilisierte' sich dieses Netzwerk seit den sechziger Jahren nach und nach: zunächst durch die Freigabe des Zugangs für Wissenschaftler, und, seit Computer und Programme für den Normalmenschen bezahl- und handhabbar sind, bis heute durch die immer schneller steigende Zahl derer, die dieses Medium beruflich oder auch privat für sich entdecken. Diese - mit den o.g. Einschränkungen des Nord-Süd-Gefälles - 'Vergesellschaftung' des Internet schafft aber nicht nur ein (fast) unerschöpfliches Informations- und Kommunikationsangebot für die Nutzer und einen zunehmend lukrativen Markt für die Privatwirtschaft. Das Internet als 'öffentlicher Raum' wird jetzt auch von Regierungen und Militärs 'wieder-entdeckt'.

1 Dieser Artikel erschien zuerst in ZivilCourage 1/1997, S. 6-9.

2 Vgl. hierzu auch C. German, Politische (Irr-)Wege in die globale Informationsgesellschaft. In: Aus Politik und Zeitgeschichte, B 32/96, S. 23.

Die US-Initiative für eine "globale Informationsstruktur"

In den USA postulierte Vizepräsident Al Gore erstmals im Wahlkampf 1992, daß der Ausbau des "Information Superhighway" (Gore), die flächendeckende Vernetzung der privaten US-Haushalte und öffentlichen Verwaltungen eines der Hauptziele der Regierung Clinton sein würde.[3] Unter dem Stichwort "National Information Infrastructure Initiative" (NII) sollen nun zur Erreichung dieses Ziels in den nächsten zehn Jahren 1,2 Mrd. Dollar investiert werden. Im Frühjahr 1995 brachten Clinton und Gore den Vorschlag einer "Global Information Infrastructure Initiative" (GII) in die Brüsseler G7-Konferenz ein. Seit dem gilt den sieben führenden Industrienationen die Schaffung einer "globalen Informations-Infrastruktur" ebenfalls als wichtiges gemeinsames Vorhaben.[4] Ein internationales Abkommen über die - für die Globalisierung der elektronischen Kommunikation als notwendig angesehene - Öffnung der Telekommunikationsmärkte kam allerdings bisher nicht zustande. Dieses Abkommen war u.a. Thema der GATT-Verhandlungen bis 1993 und wird dieser Tage im Rahmen der Nachfolgeorganisation World Trade Organisation neu und abschließend verhandelt.

Um die für "NII" und "GII" notwendige Erweiterung der Übertragungskapazitäten zu schaffen, sollen, so hieß es im Herbst 1996 in Presseerklärungen aus dem Weißen Haus und dem Pentagon, künftig die Nachrichtensatelliten des US-Militärs genutzt werden. Als Lieferant für die technische Ausstattung des sogenannten Projekts "Internet II" präsentiert sich auf seiner Internet-Homepage z.B. der US-Rüstungskonzern Hughes Electronics.

Die "Internet-Politik" in der Bundesrepublik

Auch die bundesrepublikanische Regierung entdeckte inzwischen die Notwendigkeit, sich mit den Entwicklungen im Bereich der Computerkommunikation zu beschäftigen. Hatte noch im März 1995 der "Zukunftsminister" Jürgen Rüttgers (CDU) in Interviews gefragt, "wo denn Nutzanwendungen für die Bereiche Multimedia und Infobahn lägen, die auch ihn überzeugen könnten"[5], so beeilte sich die Kohl-Regierung mit der im Dezember 1995 eingerichteten Enquete-Kommission "Zukunft der Medien in Wirtschaft und Gesellschaft. Deutschlands Weg in die Informationsgesellschaft" diese ihre Wissenslücke aufzufüllen. Ein Grund für die Betriebsamkeit war der am 1. Januar 1998 EU-weit anstehende Wegfall der Telekommunikations-Monopole. Hierfür galt es, gesetzliche Vorkehrungen zu treffen. Im Juni 1996 wurde deshalb im Bundestag das neue Telekommunikationsgesetz verabschiedet, das mit dem o.g. Termin in Kraft tritt. Die Freigabe des Telekommunikationsmarktes und die im Rahmen der G7 vereinbarte Beteiligung am Ausbau der "Global Information Infrastructure" signalisiert, daß die Bundesregierung bereit ist, die Clinton-Initiative "GII" zu unterstützen. Im Bundeshaushalt 1997 sind allein für die Multi-Media-Forschung 100 Millionen DM veranschlagt.[6]

3 Jahrbuch Telekommunikation und Gesellschaft, Bd. 2, Heidelberg 1994, S. 277ff.

4 J. Wilke, Multimedia - Strukturwandel durch neue Kommunikationstechnologien. In: Aus Politik und Zeitgeschichte, B 32/96, S. 6.

5 German, a.a.O., S. 17.

Der Gesetzestext selbst dokumentiert u.a. zwei Aspekte, die international für den staatlichen Umgang mit den neuen Kommunikationstechnologien charakteristisch sind: Zum einen wird nach Möglichkeiten gesucht, die faktische Unregulierbarkeit des Internets mit (noch) traditionellen rechtlichen Mitteln zu bewältigen bzw. zu 'verwalten' (vgl. z.B. zum Thema "Zensur im Internet" ZC 1/96, S 18: "Hiroshima goes Internet"). Zum anderen wird deutlich, daß keineswegs alle staatlichen Bereiche dem Internet-Boom hinterherhinken: Mit Art. 87 des Telekommunikationsgesetzes wird den bundesrepublikanischen Geheimdiensten und der Polizei z.B. ausdrücklich erlaubt, die Computernetz-Kommunikation jederzeit und umfassend "abzuhören".

Der "Information-Highway" als Aufmarschstrecke militaristischer Public Relations?

Ein weiterer staatlicher Bereich, der sich schon länger darauf versteht, die neuen Computertechnologien für seine Zwecke zu nutzen, ist das Militär. Die Bundeswehr ist dabei nicht nur mit ihren Kommunikations- und Simulationstechnologien oder in der Waffenelektronik auf dem neuesten Stand der Technik (vgl. ZC 6/95, S. 16: "Kriegsnah wie nie zuvor. Simulationstechnik in der Bundeswehr"). Es setzt sich auch die Erkenntnis durch, daß der 'öffentliche Raum Internet' mit seiner zunehmenden Bedeutung als Informationsquelle für "Normalmenschen" mehr und mehr zu einem relevanten Betätigungsfeld für die eigene Interessenpolitik wird. Die Bundeswehr optimierte in den vergangenen zwei Jahren ihre Werbe- und Informationsmöglichkeiten, indem sie die verschiedenen Print-, Rundfunk- und digitalen Medien in einem hochprofessionellen Gesamtkonzept (Bundeswehr-Terminus "Multi-Media-Mix") integriert: "Spots und Anzeigen für Wehrpflichtige, Anzeigen für Multiplikatoren, Info-Telefon, die Neugestaltung der Kommunikationsmittel und die Einführung eines neuen Logos sind Signale für die Beweglichkeit der Bundeswehr auf diesem Gebiet. ... Seit Anfang 1996 (ist die Bundeswehr) auch im Internet vertreten."[7] Dort bot sie die im kommerziellen Fernsehen gezeigten Spots der "Kampagne Wehrpflicht '96" als digitale Filmchen an, warb um Wehrdienstleistende, informierte über Berufsfelder innerhalb des Militärs usw. Die Zahl der Homepage-Besucher stieg von 44.000 im Juni 1996 auf über 165.000 nach Beginn der "Kampagne Wehrpflicht '96" im August. Zur Zeit findet der Interessierte auf der Bundeswehr-Homepage u.a. eine Adressenliste für das Angebot "Studentenbuden in Kasernen" und die schon obligatorischen Infos zum "Karriereberuf" Soldat. Die Resonanz auf den "Multi-Media-Mix" hat die Bundeswehrführung offenbar zufriedengestellt: "Strategie und Praxis der integrierten Unternehmenskommunikation der Bundeswehr haben in den letzten Jahren Erfolge gezeigt."[8] Die Multimedia-Offensive insgesamt und insbesondere die Selbstdarstellung im Internet läßt vermuten, daß Public Relations-Experten aus der Zivilwirtschaft hier Hand angelegt haben. Ähnlich wie im Bereich der Rüstungselektronik ist das Militär bei der Gestaltung seiner

6 D. Buchholtz, Total digital? Herausforderungen der Informationsgesellschaft. In: Information für die Truppe (IfdT), 12/96, S. 28.

7 IfdT, S. 31. Vgl. dazu auch: Informationsstelle Militarisierung (IMI) e.V.; T. Pflüger, Holen sich die Militärs das Internet zurück? (www.gaia.de/imi) und: Was wollen die Militärs im Internet? In: Zivil, Februar 1997.

8 Ebd.

multimedialen Öffentlichkeitsarbeit zunehmend auf die Kenntnisse ziviler Spezialisten (Kommunikationsdesigner, Filmemacher, Computerfachleute etc.) angewiesen. Das liegt nicht zuletzt an der Entwicklungsgeschwindigkeit der elektronischen Medien und den steigenden Ansprüchen der Adressaten an die Ästhetik und Dramaturgie der Informations-Präsentation.

Neben der "Nachwuchswerbung" bietet das Verteidigungsministerium, wie fast alle anderen westlichen Armeen (und auch die NATO), im Internet einen relativ aktuellen Informationsdienst an. Was hier vordergründig dem Bedürfnis des durchschnittlichen Netz-Benutzers nach authentischen 'Facts' mittels dokumentierter Pressekerklärungen, Vertragstexte, Fotos (z.B. "Rühe beim IFOR-Truppenbesuch"), "Hintergrundmaterialien" usw. entgegenkommt, ist in der Substanz ebenfalls nichts anderes als eine gänzlich ungebremste Selbstbejubelung. Aber so zeigt die Bundeswehr im für alle offenen Netz neben den anderen Informationsanbietern Präsenz. Und sie ist bereit, um das interessierte Publikum zu werben, das sich dort einloggt, wo es attraktive Angebote findet: "Die Qualität der Kommunikation entscheidet heute mehr denn je über die gesellschaftliche Akzeptanz und die Attraktivität des Unternehmens Bundeswehr."[9]

Welche politischen und gesellschaftlichen Folgen es haben wird, daß den Militärs im Kriegsfall künftig mit dem Internet erstmals ein Medium zur Verfügung steht, über das sie ihre eigene Sicht der Dinge einem weltweiten Publikum ohne den Filter mehr oder minder kritischer 'traditioneller' Zeitungs-, Radio- oder TV-Berichterstattung präsentieren können, läßt sich nicht absehen. Das US-Verteidigungsministerium beschäftigte übrigens schon 1993 über 1.000 Public-Relations-Mitarbeiter und hatte damit mehr Öffentlichkeitsarbeiter als die US-Fernsehnetworks ABC, CBS und NBC Journalisten.[10] Die Homepage "BosniaLINK", die das Pentagon zu Beginn des Einsatzes der US-Truppen auf dem Balkan einrichtete, galt eine ganze Zeit als "Geheimtip" unter jugendlichen Computerfreaks: Hier gab es "direkte Infos aus einem richtigen Krieg" und sogar die Möglichkeit, den Soldaten via E-Mail "Grüße und Ermutigungen" zu schicken.[11]

Das "globale Dorf Internet":
Schlachtfeld im Kampf um die Ressource Information?

Die Sichtweise, das Internet sei ein "freier Markt für Informationen" und demokratisch, weil alle (die dazu in der Lage sind) darin mittun dürfen, ist mehr als optimistisch. Die Kommerzialisierung des Internet z.B. durch Online-Dienste, die Diskussionen über Zensur, Datenschutz, Schutz der Urheberrechte und der Privatsphäre usw. "behindern" den freien Fluß der Informationen schon heute. In den USA versucht man - bisher erfolglos - per Gesetz den Einbau spezieller Computerchips gegen die Verschlüsselung von Nachrichten zu verfügen; in Frankreich ist die Codierung privater Nachrichten inzwischen verboten. Es ist abzusehen, daß sich mit den Entwicklungen im Multimedia-Bereich, z.B. der angelaufenen digitalen In-

9 Ebd.

10 P. Ludes, Auf dem Weg zu einer "fünften Gewalt". Die Auflösung von Öffentlichkeit in Public Relations. In: medium 1993, 23:2, S. 8.

11 Vgl. dazu auch M. Kemmerling, "Good Morning Bosni@", Friedensforum 6/96.

tegration von Printmedien, Radio, Fernsehen, Telefon und Netzcomputer, diese Probleme verschärfen und neue hinzukommen; und es liegt auf der Hand, daß die USA, die G7-Staaten und die EU nicht nur beabsichtigen, aus sozialem Engagement die digitale Vernetzung von Schulen, Krankenhäusern und bildungshungrigen Privatnutzern mittels "NII" und "GII" voranzutreiben: Vielmehr sollen alle anwenderspezifischen, logistischen, technischen und rechtlichen Hindernisse aus dem Weg geräumt werden, die der Etablierung eines digitalen Weltmarktes im Weg stehen.

Noch ist es kaum möglich, die mittel- und langfristigen politischen und sozialen Folgen dieser Prozesse einzuschätzen. Doch gerade diese Fragen beschäftigen natürlich auch die Industrie und - das Militär. So hatte die Bundeswehrakademie für Information und Kommunikation im September letzten Jahres 120 Experten aus Wissenschaft, Politik, Medienindustrie und Publizistik eingeladen, um auf dem "3. Strausberger Symposium" über die "Herausforderung Informationsgesellschaft" zu diskutieren. In einem Bericht über das Symposium in der Bundeswehr-Postille "Information für die Truppe" wird die Ansicht eines Vertreters der Firma "Electronic Data Systems" als besonders wichtig hervorgehoben, der davon überzeugt ist, daß in Zukunft "der Kampf um Rohstoffe wie Wasser und ™I ergänzt wird durch den Kampf um die Ressource Information".[12] Dieser Kampf hat bereits begonnen; mit welchen Mitteln er geführt wird, soll anhand folgender Beispiele aufgezeigt werden:

Der "Kampf um die Ressource Information" verschärft die Ausbeutung der Dritten Welt: Die weltweite Computervernetzung ermöglicht es westlichen Unternehmen, ihre Produktion in die Dritte Welt zu verlagern; Beispiel Indien: "Während mühsam darum gerungen wird, wenigstens ein normales Telefon in jedem Dorf des über 900 Millionen Einwohner zählenden Subkontinents zu installieren, verlagern internationale Computerfirmen wie Siemens ihre Softwareproduktion, Finanzinstitute wie die Deutsche Bank und Fluggesellschaften wie die Lufthansa ihre EDV-Dienstleistungen in die Großstädte Dehli, Bombay ... oder Madras. Hier verdient ein indischer Informatiker in einem Jahr soviel wie sein vergleichbar qualifizierter Kollege in Deutschland oder Nordamerika in einem Monat. ... Das Ergebnis seiner Arbeit wird via Standleitung oder Satellit in die Netze der Auftraggeber in Europa oder den USA geschickt."[13]

Der "Kampf um die Ressource Information" führt zu neuen technischen, ökonomischen und politischen Abhängigkeiten: Allgemein wird davon ausgegangen, daß "der Vorsprung an Technologie und Infrastruktur in den Industrieländern ... für die 'Informationshabenichtse' (in den unterentwickelten Ländern) nicht mehr aufholbar (ist)."[14] Klar, daß westliche Unternehmen auch diese Chance nutzen; der weitgehend unkontrollierte privatwirtschaftliche Technologie- und Wissenstransfer schafft neue Machtpotentiale, die sich jeglicher demokratischen Kontrolle entziehen; Beispiel China: Der Medien-Mogul Rupert Murdoch hat der chinesischen Regierung unlängst ein "Subskriptions-Managementsystem" für den Empfang ausländischer Satellitenprogramme angeboten. "Dem Regime wird ... mit der von Murdoch gleich

12 IfdT, S. 27.

13 German, a.a.O., S. 23.

14 Ebd., S. 25.

mitgelieferten Technologie ermöglicht, die ausgestrahlten Programme zunächst zu überprüfen und nur jene für die Zweitausstrahlung im eigenen Land zuzulassen, die politisch erwünscht sind. Auch den zuvor unkontrollierten Informationsaustausch mit dem Ausland von rund 100.000 Chinesen versucht die Regierung u.a. durch die polizeiliche Meldepflicht von Internet-Nutzern möglichst effektiv einzuschränken."[15]

Der "Kampf um die Ressource Information" stellt neue Anforderungen an die Kriegführung: Unter den Bedingungen einer globalen digitalen Informations-Infrastruktur wird auch die "Electronic Warfare" entsprechend ausgeweitet. Die bestehenden Telefon- und Satellitennetze werden dabei von den Militärs nicht nur zur "internen" Kommunikation genutzt. Sie werden zum 'digitalen Schlachtfeld', wenn die Waffen "Kommunikationsverhinderung" und "Desinformation" im Kampf gegen feindliche Truppen und Zivilbevölkerungen eingesetzt werden. So arbeiten die Propaganda-Spezialisten des US-Verteidigungsministeriums z.B. seit Mitte der 90er Jahre an einer neuen Waffe, die in kommenden Kriegen "so wichtig sein wird, wie ein Jet oder Bomber". Diese Waffe ist ein mit elf Informationsexperten und aufwendigem elektronischen Geräten ausgestattetes Transportflugzeug: "Modernste Übertragungstechnik, Faxgeräte, Computer, Radio- und Videogeräte erlauben der Crew, Radio und Fernsehen eines Landes zu unterbrechen und beliebige Frequenzen mit eigenen Berichten zu besetzen."[16]

Der "Kampf um die Ressource Information" führt zu neuen Militarisierungsschüben in der Zivilwirtschaft. Mit der wachsenden Bedeutung der High-Tech-Kommunikation im zivilen wie militärischen Bereich sind neue gesellschaftliche Militarisierungsschübe verbunden. Die technische Computerisierung der Waffen- und Kommunikationssysteme bedingt auch eine Modernisierung der digitalen Darstellungs- und Übermittlungsformen in der militärischen Informationsverarbeitung. Die Militärs setzen dabei auf die Innovationsfähigkeit und Kreativität ziviler Medienpraktiker und Computerspezialisten, die für sie z.B. wirklichkeitsnahe "Cyberspace"-Umwelten für Feuerleitsysteme entwickeln oder für die journalistische Professionalisierung der Informationsaufbereitung und -präsentation sorgen. Dies verstärkt die Interdependenzen zwischen Militär und ziviler "High-Tech-Avantgarde" und fördert eine 'schleichende Militarisierung' dieser für die "Informationsgesellschaften" so bedeutsamen Berufs- und Forschungsfelder. Nach Einschätzung des Forums InformatikerInnen für den Frieden (FIfF) ist z.B. die "militärische Einflußnahme auf die Informatik ein weltweites Problem. Die von militärischer Seite spezifizierten Anforderungen schlagen sich in den Forschungsthemen der weltweiten 'Scientific Community' nieder. Eine implizite Militarisierung ganzer Forschungsbereiche ist die Folge. Als politische Leitlinie für die Forschungsförderung setzt sich in Zeiten sinkender Mittel für das Militär auch in der Bundesrepublik Deutschland die Forderung nach 'Dual Use'-Gütern immer mehr durch. Dabei sollen gezielt solche zivilen Forschungen gefördert werden, die auch für die Militärs von Interesse sind. Über diese Hintergründe gilt es aufzuklären."[17]

15 Ebd., S. 23.

16 Th. Schuler, Gefälschte Reden und betrunkene Diktatoren, in: Süddeutsche Zeitung, 12.10.1995. Vgl. auch: M. Beham, Kriegstrommeln. Medien, Krieg und Politik. München 1996.

17 Vgl. eine Stellungnahme des AK "Ruin"/Rüstung und Informatik des FIfF (www.uni-paderborn.de/arbeitsgruppen/fiff)

Die Risiken erforschen und die Chancen nutzen

Niemand weiß, wie sich das Internet in den nächsten Jahren entwickeln wird. Der "Internet-Boom" dauert erst wenige Jahre; seit 1990 steigt die Zahl der ans weltweite Netz angeschlossenen Rechner um monatlich ca. 10 Prozent. Inzwischen nutzen viele, denen andere Medien kaum eine Öffentlichkeit bieten, die Chance, alternative Informationen zu "offiziellen Interpretationen" politischer oder sonstiger Geschehnisse in Sekundenschnelle weltweit zu verbreiten. Friedens-, Umwelt- oder Solidaritätsgruppen nutzen das Netz, um Mißstände anzuprangern und insbesondere in Krisensituationen, wie Kriegen, ökologischen Katastrophen oder auch bei Angriffen auf Demokratie und Menschenrechte, die offizielle Verlautbarungspolitik zu unterlaufen. Neben dem sich so entfaltenden demokratische Potential entstehen zugleich bisher nur im Ansatz erforschbare Probleme und Risiken. Die Multimedia-Technologie ist da, sie wird je nach Interessenlage genutzt, aber nicht jenseits bestehender Machtverhältnisse. Ob der 'öffentliche Raum Internet' mittel- und langfristig zu einem weltweit monopolisierten Austragungsort wirtschaftlicher und politischer Verteilungskämpfe mutiert, ist noch nicht abzusehen. Zumindest verfügen die Regierungen, Militärs und Wirtschaftsunternehmen über die Macht und die Moneten, die digitale Informationsstruktur ihren Interessen entsprechend zu gestalten. Grund genug, jetzt schon auf diese Zusammenhänge hinzuweisen und z.B. der Präsenz des Militärs im Internet ein internationales, aktuelles, qualifiziertes und attraktives friedenspolitisches Angebot entgegenzusetzen. Im Hinblick auf die skizzierten entwicklungspolitischen, sozialen und friedenspolitischen Problemfelder, die sich aus der zunehmenden gesellschaftlichen Bedeutung des Internet ergeben, wären darüber hinaus neue Gesprächszusammenhänge, z.B. mit Gewerkschaftern, Wissenschaftlern und Praktikern wünschenswert, die es ermöglichen, die entsprechenden Entwicklungen kritisch zu beobachten und gemeinsam Positionen für eine demokratische, zivile und gerechte Netzpolitik zu entwickeln.

Elvi Claßen

Information Warfare - Information als Ware oder: Wer bestimmt, was ‘wirklich’ ist?

“Precision-targeting information
is just as important as
precision-targeting weapons,
and the new media will make this
possible to an unprecedented degree.”
(Alvin & Heidi Toffler,
War And Antiwar, 1993, S. 201.)

Dem Fernsehen kommt aufgrund seines Verbreitungsgrads und der ihm zur Verfügung stehenden Darstellungsmöglichkeiten eine zentrale Rolle zu als 'Überbringer' von Beschreibungen und Erklärungen, was in der Welt geschieht und warum. Die spannendste Frage in diesem Zusammenhang, die JournalistInnen, PolitikerInnen, Militärs, ZuschauerInnen und alle anderen mehr oder minder beteiligten AkteurInnen gleichermaßen beschäftigen (sollte), ist, wessen Beschreibungen und Erklärungen präsentiert werden. Dies gilt nicht nur, aber in besonderem Maße für die aktuelle politische Berichterstattung. Und mögen sich seit der vom US-amerikanischen Network CBS ausgestrahlten, weltweit ersten täglich gesendeten Fernsehnachrichtensendung am 29. September 1947, die ökonomischen, strukturellen und technischen Bedingungen der Produktion und Rezeption auch noch so sehr verändert haben, Fernsehnachrichten waren und sind "the exercise of power over the interpretation of reality"[18].

Die Macht, das Fernsehen und die ‘Wahrheit’

Das Fernsehen entwickelte sich zum Leitmedium. Laut Umfragen hatten in den USA 1963 und in der Bundesrepublik 1970 die Fernsehnachrichten die Tageszeitungen und das Radio als wichtigste Informationsquelle überholt. Und je wichtiger das Medium wurde, desto stärker prägte sein Einfluß auch die Selbstwahrnehmung und Selbstdarstellung seiner Handlungsträger.

Bis in die 60er Jahre hinein waren dies in den US-Fernsehnachrichten fast ausschließlich Politiker und natürlich die von den Networks bewußt als “Medienstars” aufgebauten Journalisten, wie z.B. der CBS-Anchorman Walter Cronkite. In der Hauptausgabe der CBS Evening News vom 2. September 1963, die inzwischen als historisches Dokument gilt, sitzt Cronkite mit dem politischen “Star” John F. Kennedy in dessen Garten und plaudert über die US-amerikanische Außenpolitik; eine Schlüsselszene für eine Phase, in der sich die Journalisten als objektive, unangreifbare Beobachter "standing above politics" verstanden. Dieses Image der

Dieser Artikel erschien zuerst in antimilitarismus information (ami), 10/1998, S. 63-72. Der Text zitiert und aktualisiert z.T. Ergebnisse einer früheren Untersuchung der Autorin: Claßen, E.: Kriegsberichterstattung als Indikator gesamtgesellschaftlichen Wandels. Eine Untersuchung der Vietnam- und Golfkriegsberichterstattung in Fernsehnachrichtensendungen der Bundesrepublik Deutschland und der USA. In: Ludes, P.: Informationskontexte für Massenmedien. Opladen 1996, S. 264-316.

18 Schlesinger, Ph.: "The Sociology of Knowledge". Zit. nach Gans, H.J.: Deciding What's News. A Study of CBS Evening News, NBC Nightly News, Newsweek and Time. New York 1980, S. 81.

gleichberechtigten Akteure, die neben den politisch Mächtigen “über die Einhaltung der höheren Werte” wachen, wurde von den Politikern weitgehend toleriert und von den ZuschauerInnen verehrt; sie sprachen Journalisten wie Cronkite ein Höchstmaß an Glaubwürdigkeit und Integrität zu.

Ab Ende der 60er und in den 70er Jahre veränderte sich die Selbstwahrnehmung der US-amerikanischen Journalisten, Teil des Establishments zu sein. Einzelne mutige Reporter und Korrespondenten, die sich dem auch in den US-Medien dominierenden Hurra-Patriotismus und Chauvinismus widersetzten, machten die Verbrechen der USA in Vietnam weltweit bekannt, wie z.B. der damalige Washingtoner Reporter Seymour Hersh, der das Massaker von My Lai (16. März 1968) enthüllte. Die New York Times meldete am 17. März auf der Titelseite, My Lai sei Schauplatz einer US-“Offensive zur Aushebung feindlicher Nester” gewesen, bei der 128 nordvietnamesische Soldaten getötet worden seien. Hersh gelang es erst im November 1969, seine erste Story zu My Lai in die Presse zu bringen - über eine kleine Nachrichtenagentur. “Life” (u.a.) hatte eine Veröffentlichung abgelehnt. 1974 - ein weiteres bekanntes Beispiel - deckten Carl Bernstein und Bob Woodward, zwei Reporter der Washington Post, den “Watergate-Skandal” auf, was bekanntlich zum Rücktritt Richard Nixons führte. In der Pressearbeit sorgten solche Erfahrungen für neue Maßstäbe: "Journalists were becoming bolder about challenging political authority ... And more profoundly, the old model of 'objective journalism' was giving way to a more active, mediated, journalist-centered form of reporting."[19]

Nachrichtenmedien als Waffe

Aber auch die “Autoritäten” zogen in dieser Zeit Konsequenzen aus der scheinbar wachsenden Bereitschaft der Medien, die Dinge nach eigenem Ansehen zu interpretieren und die bis dahin weitgehend gültige ‘friedliche Koexistenz’ aufzukündigen. Aber es waren zunächst Militärs, die die neue Informationsstrategie Anfang der 80er Jahre etablierten. So forderte der Public Relations-Spezialist der US-Marine, Korvettenkapitän Arthur A. Humphries im Sommer 1983 in der "Naval War College Review", das Militär solle den Zugang zu den Kampfgebieten kontrollieren, da man, "um eine 'wohlwollende Objektivität' zu erreichen oder sichern zu helfen, imstande sein muß, bestimmte Korrespondenten vom Kampfgebiet fernzuhalten": "Wenn die Verwandten von Soldaten ihren Jungen oder jemanden, der ihr Junge sein könnte, durch die Bildübertragung in lebensechten Farben verwundet oder verstümmelt direkt vor sich sehen, so läßt das die Unterstützung für die Kriegsziele ihrer Regierung bei ihnen bröckeln. So war es im Vietnamkrieg. ... Was kann eine Regierung im Hinblick auf dieses Problem tun, wenn hochtechnisierte Kommunikationsmöglichkeiten bestehen und ein weltweites Publikum auf die Informationsfreiheit eingestimmt ist?" Humphries' Antwort auf die selbstgestellte Frage war jedoch nicht nur die Forderung nach umfassenden Kontroll- und Zensurmaßnahmen gegenüber den Kriegsberichterstattern, er schlug zudem auch eine gezielte Einbeziehung der Presse vor, um sie für die Unterstützung militärischer Operationen zu nutzen: "Die Nachrichtenmedien können in der psychologischen Kriegsführung ein nützliches Werkzeug, ja sogar eine Waffe sein, die den Soldaten den Einsatz ihrer schweren Waffen erspart."[20] Frühe Beispiele für die neue

19 Hallin, D.C. und Gitlin, T.: Agon and Ritual: The Gulf War as Popular Culture and Television Drama. In: Political Communication, Special Issue: The Media and the Gulf War. Chicago 1992, S. 18.

20 Zit. nach MacArthur, J.R.: Die Schlacht der Lügen. München 1992, S. 155ff.

Informationspolitik waren der Falklandkrieg 1982, in dem Großbritannien 29 Pressevertreter auf Kriegsschiffen mit in den Südatlantik nahm, sie in Pools zusammenfaßte und die Berichterstattung einer strengen Zensur unterwarf; die US-Invasion in Grenada im Oktober 1983, während der eine viertägige Nachrichtensperre über dem Kampfgebiet jegliche Medienberichterstattung verhinderte, und der Einmarsch von US-Truppen in Panama 1989, bei dem die wichtigste Phase der Intervention unter Ausschluß der Öffentlichkeit stattfand, weil die Journalisten des erstmals eingerichteten "National Media Pools" zwei Stunden vor Beginn der Kämpfe mit Militärmaschinen aus dem Kampfgebiet ausgeflogen und danach noch mehrere Stunden auf einem abgelegenen Militärstützpunkt festgehalten wurden.

Die Demontage politischen 'Heldentums'

Den politischen Autoritäten fehlten in den 80er Jahren noch die Strategien, mit der Omnipräsenz und der wachsenden Offensivität der Medien umzugehen: "Der politische Held wird vom Sockel gestoßen", konstatierte 1985 der US-amerikanische Kommunikationswissenschaftler Joshua Meyrowitz und wies auf eine sich - gegenüber den 60er/70er Jahren - tendenziell verändernde Präsentation von Politikern im Fernsehen hin: "Mystifikation und Ehrfurcht werden durch Distanz und begrenzten Zugang gestützt. Unsere neuen Medien entlarven zu oft zu viel, als daß die traditionellen Vorstellungen über politische Führungsfiguren weiter existieren können. Die Fernsehkamera dringt wie ein Spion in die Intimsphäre von Politikern ein. Sie beobachtet, wie sie schwitzen, belauert sie, wie sie bei ihren eigenen deplazierten Bemerkungen gequält ihr Gesicht verziehen."[21] Es war die Zeit, in der die Kommerzialisierung des Fernsehens in den USA den Konkurrenzkampf zwischen den Networks immer mehr zum dominierenden Kriterium der Programmgestaltung machte, ein Trend, der sich - zeitlich etwa um fünf bis zehn Jahre versetzt - ab der Einführung des dualen Systems auch für die Medien in der Bundesrepublik - nachweisen läßt und sich unmittelbar auf die Themenauswahl und -präsentation der Fernsehnachrichtensendungen auswirkte: "The character of the evening news has already changed substantially. Its pace has come to resemble more closely the pace of the rest of commercial television, with 10-second sound bites and tightly packaged stories. The agenda of news has changed, with fewer traditional political stories and more stories that 'tug at the heart strings'. And the pressure is far greater today for the stories to have high "production values", both narrative and visual: drama, emotion, and good video."[22] Und unter die traditionellen Nachrichtenbilder von wohlkomponierten PolitikerInnenauftritten an Stehpulten, beim Bad in der Menge oder am Konferenztisch mischten sich zunehmend Aufnahmen, die diese Inszenierungen konterkarierten: sie zeigten die kleinen Tricks, mit denen die "Mächtigen" sich vor der Öffentlichkeit in Szene setzen, z.B. den transparenten Teleprompter, von dem am Stehpult Texte abgelesen werden, der aber von vorn kaum zu sehen ist und so die Illusion des freien Vortrags erzeugt; und sie präsentierten - drama, emotion, and good video - weniger "Ambitioniertes" als eher "Spektakuläres": "The media are more reluctant to honor politicians' wishes about

21 Meyrowitz, J.: Die Fernsehgesellschaft. Wirklichkeit und Identität im Medienzeitalter. Weinheim u. Basel 1987, S. 183.

22 Hallin u. Gitlin, 1992, S. 21.

what will be publicized: Consider the networks' decision to broadcast tape of President Bush vomiting in the lap of the Japanese prime minister."[23]

Zweiter Golfkrieg:
Instrumentalisierung bzw. Selbstaufgabe des 'freien' Journalismus'

Als sich Ende der 80er/Anfang der 90er die bipolare Weltordnung auflöste, in der sich 45 Jahre lang die politische Kommunikation entwickelt hatte, entstand kurzzeitig ein Interpretationsvakuum. Der Wegfall spezifischer politischer Ordnungsfunktionen - der rapide internationale Machtverlust des sozialistischen Bündnissystems und der Verlust der auf den Ost-West-Gegensatz bezogenen ideologischen Freund-Feind-Schemata - betraf nicht nur die nationale und internationale Politik. Auch das journalistische Bezugssystem, in dem sich die Produktions-, Präsentations- und Rezeptionsweisen des Fernsehens entwickelt hatten, zerbrach. Und es sollte sich ganz schnell zeigen, wer über die nötigen ideologischen, strategischen und materiellen Ressourcen verfügte, um dieses Vakuum mit neuen Werten, Begriffen und politischen Orientierungen zu füllen. Mit zwei programmatischen Reden, vor der Generalversammlung der Vereinten Nationen am 1. Oktober 1990 und vor Beginn des Luftkrieges am Persischen Golf am 16. Januar 1991 (die von CNN weltweit live ausgestrahlt wurde) zur "new world order" hatte US-Präsident George Bush die politischen und militärischen Ziele der übriggebliebenen Weltmacht definiert. Zusammengefaßt ging es darum, das bisherige, europäisch orientierte Konzept der bipolaren nuklearen Abschreckung in eine neue, "primär konventionell instrumentalisierte und primär auf die Nord-Süd-Beziehungen"[24] ausgerichtete Abschreckungsbeziehung zu transformieren sowie um die pragmatische und ethische Neubestimmung der Legitimation des Militärs und des soldatischen Selbstverständnisses. So vermittelte der Zweite Golfkrieg, als erster elektronische High-Tech-Krieg 1991 nicht nur eine Ahnung, was künftig auf dem militärischen Sektor unter "Information Warefare" zu verstehen sein sollte; seine massenmediale Präsentation geriet zur ultimativen Entscheidungsschlacht um die "power over the interpretation of reality" in der "neuen Weltordnung". Die ZuschauerInnen wurden zum Objekt einer perfekt funktionierenden, politisch-militärisch-medialen Mobilisierungsstrategie, die ihnen mehr oder minder jede Möglichkeit nahm, den bis dahin, eben wegen seiner Authentizität und Aktualität als wichtigste Quelle geltenden Informationskanal zu nutzen: das Fernsehen. Und sie wurden ZeugInnen der Instrumentalisierung bzw. Selbstaufgabe des 'freien' Journalismus', der in dieser universalen Machtdemonstration öffentlich vorgeführt wurde. Der ZDF-Chefredakteur Klaus Bresser resümierte 1992: "Wir müssen nicht nur zugeben, daß wir als Propagandainstrument der Militärs mißbraucht wurden, sondern auch, daß wir uns haben mißbrauchen lassen. Wir wußten, daß wir nur einen weitgehend zensierten Ausschnitt aus der Realität des Krieges zeigen konnten und taten es trotzdem. ... Das Informationsbedürfnis der Zuschauer war ja so groß, die Einschaltquoten schnellten empor. ... Wer wird von seinen Zuschauern als erster verlangen, auf die spannenden ... Bilder von Luftangriffen, Panzergefechten und Raketenstarts zu verzichten? Er riskiert damit, sie an die Konkurrenz zu verlieren."[25] Und Dan Rather, Anchorman der CBS Evening News und Ex-Marineinfanterist, der in einer seiner

23 Ebd., S. 18.

24 Zellner, in: Blätter für deutsche und internationale Politik, 4/1993, S. 431.

25 Bresser, K.: Was nun? Über Fernsehen, Moral und Journalisten. Hamburg/Zürich 1992; S. 80.

Sendungen während des Golfkrieges den "jungen Männern und Frauen" am Golf einen militärischen Gruß via Bildschirm geschickt und salutiert hatte[26], räumte im Nachhinein ein, "Wir lassen uns immer weniger von Verantwortung und Anstand leiten, ... sondern immer mehr von Macht und Geld." Es habe den ReporterInnen während des Golfkrieges an Willen gefehlt “kein Blatt vor den Mund zu nehmen ... und mit seiner Meinung herauszurücken". Dies entspräche "einer allgemeinen Tendenz des amerikanischen Journalismus in den letzten fünf bis zehn Jahren ..., die sich ablesen läßt an der Berichterstattung über politische Kampagnen und über innenpolitische Fragen wie das Rassenproblem und die Wirtschaft ... Diese Tendenz geht dahin, die Mitte zu suchen und mit der Masse zu gehen, keinen Ärger zu machen, keine unangenehmen Fragen zu stellen, kein Risiko einzugehen ... Es ist in diesem Lande noch nicht allzu lange her, daß ein Reporter, um in den Augen seiner Kollegen, als dieser Bezeichnung würdig zu sein, unangenehme Fragen stellen mußte. Es ging dabei nicht um einen Popularitätswettstreit, sondern um eine Aufgabe, eine Verantwortung."[27]

Die Zeitenwende der politischen Öffentlichkeitsarbeit

Zwar ist es nicht neu, daß die Innovationsschübe in der zivilen Massenkommunikation mit den großen Kriegen dieses Jahrhunderts verknüpft sind. Die jeweils aktuellen Medien spielten in der Kommunikation im Krieg und über den Krieg eine zentrale Rolle - Beschreibungen wie "der erste mediatisierte Krieg der Geschichte"[28] für den Ersten Weltkrieg, "World War II had been a radio war"[29] für den Zweiten Weltkrieg, "der erste große Fernsehkrieg"[30] für den Vietnamkrieg - deuten dies an. Aber der Zweite Golfkrieg, der erste "Krieg in Echtzeit"[31], "der erste totale elektronische Krieg der Geschichte"[32] war deshalb so paradigmatisch, weil es der militärischen Öffentlichkeitsarbeit erstmals gelang, via Satellit eine weltweite “Fernsehgesellschaft” als Kriegspublikum zu integrieren. Den Kontext dafür lieferten die Medien selbst, die sich mehrheitlich politisch loyal der Selbstzensur unterwarfen und - auf der Jagd nach den schnellsten spektakulärsten Bildern - den journalistischen Anspruch der 'Aktualität' umdeuteten in eine Praxis der 'Live'-Berichterstattung[33], die statt journalistisch überprüfter Authentizität ein 'Augenzeugen'-Konzept anbot und damit die Interpretation der Nachrichten an die ZuschauerInnen delegierte. Die politisch-militärisch geschaffene "Informationsfront"

26 Zit. nach Ege, K.: Der Mythos von der vierten Gewalt. Medien und Demokratie in den USA. In: Gaus, G. u.a. (Hg.): Blätter für deutsche und internationale Politik, 11/1992, S. 1366-1374, hier S. 1372.

27 Zit. nach MacArthur, 1993, S. 234f.

28 Virilio, P.: Krieg und Kino. Frankfurt/M. 1991, S. 156.

29 Berg, R.: Covering Vietnam in an Age of Technology. In: Rowe, J.C. and Berg, R. (Hg.):The Vietnam War and American Culture. New York 1991, S. 118.

30 Sedat, P.: Zeitgeschichte im Fernsehen. 'Der Vietnamkrieg'. Buch und Regie: P. Sedat; Erstausstrahlung am 28.11.1974, NDR. Zit. nach Manuskript, abgedruckt in: Rundfunk und Fernsehen, 1991/2, S. 266.

31 Virilio, P.: Krieg und Fernsehen. München/Wien 1993, S. 41.

32 Ebd., S. 30.

33 ... die aber oft keine war: Zu Beginn des Krieges war es bei vielen Übertragungen - mangels ‘echter’ Live-Bilder vom Kriegsgeschehen - gängige Praxis, Live-Reportagen via Telefon mit archiviertem Filmmaterial zu illustrieren. Die ersten ‘echten’ Live-Bilder gab es erst ab 29. Januar.

(nach Virilio die "vierte Front", die "neben der Boden-, See- und Luftfront mehr und mehr zum wesentlichen Element zwischenstaatlicher Auseinandersetzungen" wird[34]), lieferte die Inhalte: Zensur und Desinformation sorgten dafür, daß das Kriegspublikum wochenlang überwiegend die vom Pentagon vorproduzierten Videoclips vermeintlich präziser Luftangriffe präsentiert bekam oder Fernsehkorrespondenten, die - hunderte Kilometer vom eigentlichen Kriegsgeschehen entfernt - Presseerklärungen des “U.S. Central Command’s Joint Information Bureau” in Dharan verlasen. Virilios Voraussage aus Januar 1991, man müsse nun via Fernsehen "blutigen und tödlichen Zerstörungen aller Art beiwohnen"[35] trat nicht ein. Und auch Klaus Bresser stellte im Nachhinein fest, es sei die Schuld der Medien, daß die Wahrheit, daß es ein Krieg war, "wie andere vorher, dreckig und blutig, mit vielen Tausend Toten und Verletzten, mit Leid und Tränen", nicht gezeigt wurde.[36] Das politisch-militärischen Kalkül, “to establish a new world order” ging auf: Verteidigungsminister Richard Cheney, bezeichnete den Sieg über die irakische Armee im Februar 1991 als "eine Zeitenwende für die amerikanische Politik und das amerikanische Militär" und erklärte das Vietnam-Trauma für überwunden.[37]

Die “öffentliche Meinung” - Zielgebiet für Public Relations-Fachleute

Die im Nachhinein bekanntgewordenen Kriegsverbrechen am Golf[38], die tatsächliche Zahl der zivilen Opfer, die dieser Krieg forderte, das Ausmaß der Zerstörungen in der Region, die Folgen der UNO-Sanktionen usw. interessierten nach dem Ende der Kampfhandlungen kaum noch jemanden. Und keinerlei - politische oder publizistische - Konsequenzen hatte auch die schrittweise Aufdeckung, mit welchen Mitteln die US-Regierung und ihre Verbündeten die Weltöffentlichkeit getäuscht und manipuliert hatten, um diesen Krieg zu beginnen, den politischen Widerstand dagegen zu diskreditieren und das Bild des Krieges in den Medien als ultima ratio gegen einen “irren Diktator” (Bush in seiner Rede am 16. Januar 1991) und als aseptischen, technisch präzisen Waffenspaziergang bis zum Schluß aufrechtzuerhalten. Die “politischen (und militärischen) Helden” hatten gelernt, sich selbst wieder auf den Sockel zu stellen. Sie hatten dafür auf die entsprechenden Fertigkeiten ziviler 'Medienmacher' (eine moderne Form des “dual use”) zurückgegriffen, die nicht nur die mediale Selbstdarstellung der “Autoritäten” fernsehgerecht professionalisierten: Die internationale Presse und insbesondere das “Live-Medium” Fernsehen wurden zum Instrument einer “Nachrichtenstrategie”, die die Kriegsberichterstattung und damit den weltweiten politischen Diskurs in einem Ausmaß beeinflußten, das bis zu diesem Zeitpunkt nicht möglich gewesen wäre: die technischen Bedingungen (portable Satellitentechnik, die die “Live”-Berichterstattung erst ermöglichten, elektronische TV-Bildgestaltung, mit der die Redaktionen das Kriegsdesign für den ‘Showdown in the Gulf’ erstellten und so den ersten “Video-Logo-Krieg”[39] kreierten), die journalistischen Dispositionen (s.o.) und das

34 Ebd., S. 61.

35 Virilio 1993, S. 43.

36 Bresser, S. 82.

37 Zit. nach: Der Spiegel 10/1991, S. 162.

38 Vgl. u.a. Clark, R.: Wüstensturm. US-Kriegsverbrechen am Golf. Göttingen 1995.

39 MacArthur, S. 93.

weltpolitische Interim nach Ende des Kalten Krieges, das es aus der Perspektive der US-Regierung und ihrer Verbündeten durch die neue Weltordnung zu ersetzen galt. So schlug die Stunde der Public Relations-Fachleute, die in den Monaten zwischen August 1990 und März 1991 an der neuen “vierten (Informations-)Front” als unsichtbare Streitmacht den Krieg vorbereiteten und seinen Ausgang maßgeblich mitentschieden. Und spätestens seit dem Zweiten Golfkrieg sollte auch klar sein, daß, wenn von “Information Warfare” die Rede ist, nicht nur die Verwendung elektronischer Hard- und Software in der Kriegstechnik eine qualitativ neue Bedrohung bedeutet, sondern daß die “öffentliche Meinung” immer mehr zum entscheidenden Zielgebiet immer perfekterer Informations- bzw. Desinformations-Bombardements wird.

Professionelle Desinformation

Schon 1991 beschäftigte das das US-Verteidigungsministerium mehr als 1.000 Public-Relations-MitarbeiterInnen[40], die zuvor als JournalistInnen oder Werbefachleute im zivilen Bereich tätig waren. Auch das “Outsourcing” der militärischen PR-Arbeit gewinnt zunehmend an Bedeutung. Als eines der bisher spektakulärsten Beispiele für das Engagement einer professionellen PR-Agentur gilt die von Hill & Knowlton (H&K) für die in den USA agierende Lobbyorganisation des kuwaitischen Königshauses “Citizens for a free Kuwait” erfundene “Brutkasten-Story”, die in den USA durch einen Kommentar John MacArthur’s in der "New York Times am 6.1.1992 aufgedeckt und in der BRD von Klaus Bednarz in der Sendung "Monitor" am 29.3.1992 mit weiteren Fakten belegt worden war. H&K hatten für die Kampagne, deren Ziel es war, in der US-Bevölkerung eine Mehrheit für den Waffengang am Golf zu schaffen, allein in den ersten 90 Tagen ab Anfang August 1990 5,64 Mio. Dollar kassiert. Die fingierte Greuelgeschichte über irakische Soldaten, die u.a. Brutkästen aus kuwaitischen Krankenhäusern stahlen und die darin liegenden Frühgeborenen auf dem Fußboden zurückließen, die am 27.11.1990 sogar vor den UNO vorgetragen wurde, hielt sich nicht nur bis Ende des Krieges in den Massenmedien, sondern wurden auch von den Regierungen der am Krieg beteiligten "Anti-Hussein-Koalition" immer wieder zur innenpolitischen Legitimation des Waffengangs gegen den Irak vorgebracht. Weitere Kunden von H&K sind z.B. die Regierungen Chinas, Indonesiens und der Türkei.[41] Im Balkankrieg hatte die kroatische Regierung am 12. August 1991 die ebenfalls US-amerikanische PR-Firma Ruder Finn engagiert, die u.a. im US-Kongreß mit Informationsmaterial über Bluttaten der serbischen “Aggressoren” für Unterstützung der Kriegspolitik Kroatiens warb. Von Ruder Finn produzierte Videoclips über serbische Kriegsverbrechen wurden weltweit von Fernsehstationen übernommen.[42]

Auch die Bundeswehr nimmt seit einigen Jahren übrigens die Hilfe von "Werbe-Profis" in Anspruch. Dies belegt z.B. ein Artikel des Werbeberaters und Geschäftsleitungsmitglieds der Werbeagentur Krakow-McCann in Düsseldorf, Karlheinz Hilsheimer in der Soldatenzeitschrift "Information für die Truppe"[43]. Die Agentur hatte schon 1988 zur Werbung von Zeitsoldaten für die Bundeswehr die

40 Ludes, P.: Auf dem Weg zu einer "fünften Gewalt". Die Auflösung von Öffentlichkeit in Public Relations. In: medium, 1993, 23:2, S. 8-11, hier S. 8.

41 Vgl. MacArthur, 2. Kap. “Wie die Babies verkauft wurden”, S. 46-90.

42 Vgl. z.B. Beham, M.: Kriegstrommeln. München 1996, S. 160ff.

43 Ausg. 9/1992, S. 29-33.

Kampagne "Eine starke Truppe" mit Anzeigen in Printmedien und Werbespots für Kino und Fernsehen durchgeführt. In dem Artikel heißt es: "Ziel war es, Akzeptanz und Ansehen der Bundeswehr zu verbessern und einen Dialog mit dem Bürger herzustellen. Wichtig war aber auch die angestrebte Binnenwirkung, den Soldaten den Rücken zu stärken. ... Professionelle Werbung ist darüber hinaus ein wichtiger Bestandteil im Gesamt-Kommunikationskonzept der Bundeswehr mit einer kritischen Öffentlichkeit - nicht mehr, aber auch nicht weniger." Für audiovisuelle Medienkonzepte sucht die Informations- und Medienzentrale der Bundeswehr inzwischen zivile Kompetenz (u.a.) bei der Gesellschaft für Mathematik und Datenverarbeitung, eine Kooperation “in der es um rechnergestützte Videoproduktionen, Telekooperation im Fernsehstudio sowie die Erprobung von Dreharbeiten in virtuellen Studios gehen soll - also anders ausgedrückt insbesondere um die Manipulation von Bewegtbildern.”[44]

Spin Doctors - Kommunikationsmanager in Krisen- oder Konfliktsituationen

Die ‘politische Konsensbildung’ professionellen Werbestrategen zu überlassen und eine willfährige Medienöffentlichkeit mit ‘künstlichen’ oder zumindest ‘verfälschten’ Nachrichten zu beliefern, hat in den USA inzwischen einen Namen: das “spin doctoring”. In der Bundesrepublik tauchte dieser Begriff im Zusammenhang mit dem aktuellen Bundestagswahlkampf mehrfach in der Presse auf, wenn es um die Kritik der “Amerikanisierung der politischen PR”[45] ging. Denn auch hier heben jetzt Profis die PolitikerInnen auf den Sockel: die Solinger Agentur ‘von Mannstein’ (u.a. für die Klosterfrau Melissengeist-Werbung verantwortlich) betreute im letzten Wahlkampf Helmut Kohl, KNSK/BBDO (Hamburg, sonst z.B. Lucky Strike, o.tel.o.) die SPD und die Düsseldorfer Agentur Schirner B90/Die Grünen.[46] Aber die Inszenierung mediengerechter Auftritte von PolitikerInnen ist wohl die weitgehend harmloseste Erscheinungsform dieser Liaison zwischen ‘Macht- und Marketing-Experten’. Von größerer Bedeutung ist die Funktion der spin doctors in ihrem Hauptaktionsfeld - dem Kommunikationsmanagement in Krisen- oder Konfliktsituationen. Neben militärischer und politischer PR verdeutlicht dies ein aktueller Auftrag, den die US-amerikanische Firma Burson-Marsteller (B&M), die mit 63 Büros in 32 Staaten als eine der weltweit größten Agenturen gilt, von einem internationalen Unternehmensbündnis aus dem Bereich der Gentechnologie erhielt: Aus einem Anfang 1998 Greenpeace/Hamburg zugespielten B&M-Strategiepapier geht hervor, daß man eine Millionen Dollar teure Kampagne vorbereitet, die in Westeuropa die Vorbehalte gegen insbesondere aus den USA eingeführte genmanipulierte Nahrungsmittel eliminieren soll.[47] So werden wir in den nächsten Monaten vielleicht zu AugenzeugInnen (oder Opfern?) der “möglicherweise größten und teuersten Propaganda-Schlacht, die je geführt wurde”.[48] B&M lieferte übrigens für die südkoreanische Regierung während der Olympischen Spiele das PR-Konzept gegen den Vorwurf von

44 Ansorge, P. und Streibl, R.: Schöner neuer Krieg. In: Krämer, J. u.a.: Schöne neue Arbeit. Mössingen-Talheim, 1997.

45 Kocks, K.: Welche Fäden spinnt denn diese neue Spezies? In FR, 15.7.1998.

46 Höher, S.: Wenn Werbeprofis Wähler werben. In: Kölner Stadtanzeiger, 9.7.1998.

47 Fuchs, U.: Propaganda Strategy of Gen-Multis leaked out. www.home.intekom.com/ tm_info/ rw80119.htm (24.1.1998), 27.9.98..

48 Ebd.

Menschenrechtsverletzungen im Land und stand u.a. auch beim rumänischen Diktator Ceaucescu unter Vertrag.[49]

Krieg unter Ausschluß der Öffentlichkeit

Das PR-Geschäft gilt inzwischen als eines der am schnellsten wachsenden Segmente der globalen Marktwirtschaft, Anfang der 90er Jahre gab es allein in den USA bereits ca. 150.000 PR-Praktiker gegenüber 130.000 Journalisten.[50] Und die Rahmenbedingungen in denen sich Public Relations konstituieren - öffentliche Aufmerksamkeit, öffentliche Bekanntheit und öffentliche Kommunikation[51] - sind im Zeitalter der elektronischen Massenmedien besser denn je und sie werden mit der wachsenden Verbreitung des Internet - im politischen, wirtschaftlichen und militärischen Bereich - weiter an Bedeutung gewinnen.

Und wenn es um die Frage geht, was wir bezüglich “Krieg und Frieden im 21. Jahrhundert” zu erwarten haben, so ist eines sicher: Der Kampf um die “power over the interpretation of reality” wird auch in Zukunft im Mittelpunkt aller Aktivitäten stehen. Wie er geführt wird, läßt sich angesichts der geschilderten Aspekte ahnen. Und wer dazu neigt, im Zusammenhang mit “Information Warefare” den diesbezüglichen PR-Finten, Wortschöpfungen und Szenarien auf den Leim zu gehen und zu glauben, die Kriege der Zukunft würden “am Computer entschieden - unblutig”[52] und bedeuteten ein “Farewell to Arms”[53] wird sich früher oder später mit der “real virtuality”[54] eines Krieges konfrontiert sehen, der alle - neuen und alten - Techniken der Kriegsführung integriert und für das weltweite Kriegspublikum so perfekte Trugbilder generiert, daß er zumindest für die, die ihn nicht direkt erleiden müssen, in seinen tatsächlichen Ursachen, Auswirkungen und Folgen kaum noch faßbar sein wird. Deshalb abschließend - eine Reminiszenz an den ersten offiziellen Testlauf für künftige “Cyberwars”: "Es ist ein grenzenloser Zynismus, vom Golfkrieg als virtuellem Krieg zu reden. ... Für diejenigen, die in Bagdad allnächtlich bombardiert werden oder die in Tel Aviv oder Jerusalem vor jeder Scud-Rakete in den Keller flüchten, ist der Krieg real, sind die Zerstörungen ihrer Städte, ist der Tod von Verwandten sehr direkt. Darüber zu spekulieren, ob 'der Tod als Bild nicht manipulierbar ist' (Baudrillard), ob also das, was wir sehen, nicht nur einer emotionalen Dramaturgie folgt, fiktional, wie ein Produkt Hollywoods, verdrängt, daß durch ein solches virtuelles Geschehen Tausende ... sterben."[55]

49 Ruiz, C.: Burson-Marsteller: PR for the New World Order. www.home.intekom.com/tm_info/ge_bm.htm, 27.09.98.

50 Vgl. Ruß-Mohl, S.: "Ferngelenkte Medienberichterstattung?" In: Aus Politik und Zeitgeschichte. 1991, Nr. 51, S. 23ff.

51 Ronneberger, F. und Rühl, M.: Theorie der Public Relations. 1992, S. 50/51.

52 Der Spiegel: Schweiß schnuppern. Ausg. 34/1995, S. 132.

53 Carlin, J.: A Farewell to Arms. In: Wired, Mai 1997, S. 5/1.

54 Castells, M.: The Rise of the Network Society. Vol. 1 of: The Information Age: Economy, Society and Culture. Blackwell Pub., 1996.

55 Hickethier, K.: Die ordinäre Realität. Eine Antwort auf P. Weibels Vision vom Medienkrieg. In: epd (1991) 12, S. 3-6, hier S. 5.

Ralf Bendrath

Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges[1]

“Soon there will be no such thing as ‚unknown territory‘ for the United States Military.”
Bruce Sterling[2]

“We are not in the business of killing.”
General Norman Schwarzkopf[3]

Auf dem Weg zum vernetzten Militär

Nach dem Golfkrieg 1991 hat vor allem in den USA eine intensive Debatte darüber eingesetzt, wie neue Computer- und Informationstechnologien die Natur des Krieges verändern.[1] Der Krieg gegen den Irak galt für viele Soldaten und Beobachter als erster einer neuen Generation von Kriegen, in denen nicht mehr physische Gewalt über den Sieg entscheidet, sondern die “Informationsüberlegenheit” oder allgemeiner die Fähigkeit, einen “Informationskrieg” zu gewinnen.[2] Diese Entwicklung hatte vor allem zwei Ursachen: Natürlich spiegelt sie zum einen den Boom der zivilen Computerindustrie wider, vor allem die Entwicklung vom einzelnen Rechner zum Datennetz. Bereits vorher liefen aber schon Projekte in den amerikanischen Streitkräften, die mit dem Vietnamkrieg begonnen worden waren. Der Golfkrieg bildete für viele der damals entworfenen Systeme den ersten Kriegseinsatz.

Die Diskussion über den “Informationskrieg” ist seitdem vor allem in den USA zu einem sicherheitspolitischen Thema ersten Ranges geworden. 1994 wurde an der *National Defense University* eine *School for Information Warfare and Strategy* gegründet, wo seitdem Offiziere für “Informationsoperationen” ausgebildet sowie militärisch-konzeptionelle Überlegungen zum Krieg im Informationszeitalter angestellt werden.[3] 1995 erreichte das Thema mit einer Titelgeschichte des *Time Magazine* die

1 Dieser Artikel erschien zuerst in Peter Bittner/Jens Woinowski (Hg.): Mensch – Informatisierung – Gesellschaft, Münster 1999. Eine gekürzte Fassung wurde dokumentiert unter dem Titel “Krieg im Cyberspace. Auf dem Weg zur vernetzten Armee” in der Frankfurter Rundschau vom 1.4.1999.

2 Bruce Sterling: War Is Virtual Hell, http://www.wired.com/wired/1.1/features/virthell.html.

3 Zit. nach Chris Hables Gray: Postmodern War. The New Politics of Conflict, London, New York 1997, S. 46.

1 Diese Diskussion ist bis heute sehr heterogen. An ihr sind neben Militärplanern, Sicherheitsstrategen, Poltikern und Fachjournalisten auch ungewohnte Akteure beteiligt, so etwa verschiedene Hacker-Magazine, Computerfirmen, Datenbankanbieter oder Lobbygruppen für die elektronische Privatsphäre, interessanterweise nur vereinzelte Friedensbewegte oder Friedensforscher.

2 Vgl. Joseph S. Nye jr./William A. Owens: America´s Information Edge, in: Foreign Affairs, 3./4. 1996, S. 20-36; Martin C. Libicki: Information Dominance, Strategic Forum, Nr. 132, Washington D.C., Dezember 1997. Zum Golfkrieg vgl. z.B. Alvin und Heidi Toffler: War and Anti-War. Survival at the Dawn of the 21st Century, New York etc. 1993; Gray, Postmodern War.

allgemeine Öffentlichkeit.[4] Die Vereinigten Stabschefs[5] formulierten im folgenden Jahr ihr Planungspapier "Joint Vision 2010", in dem das alte "Feuerkraft ist Macht" durch "Wissen ist Macht" ersetzt wurde.[6] Das *Field Manual 100-5 (Operations)* wurde im August 1996 durch das *FM 100-6 (Information Operations)* ergänzt.[7] Der "Sieg im Informationskrieg" ist heute eines der fünf Langzeitziele in den Modernisierungsplänen der US Army.[8] Computer wurden in der Vergangenheit vor allem dazu verwendet, Aufgaben wie Kommunikation, Zielerkennung oder Logistik zu verfeinern und zu effektivieren. Heute läßt sich allerdings beobachten, daß sich die Anwendungsbereiche verschoben haben. So geht es mittlerweile auch um die Abwehr von Eindringlingen in Computernetzwerke, elektronische Abhör- und Überwachungstechniken, die Entwicklung sogenannter "logischer Bomben" in Form von Software oder die Nutzung von Computerviren als "nicht-lethale Waffen"[9].

Die seit etwa drei Jahren auch in Deutschland anlaufende Debatte ist sehr deutlich von dem Vorbild USA geprägt.[10] Dabei wird oft der Fehler wiederholt, den die sicherheitspolitischen Eliten jenseits des Atlantiks begehen: Die Annahme, daß eine verbesserte Vernetzung der Streitkräfte lediglich die militärische Effizienz erhöht. Mit der derzeit laufenden Umstrukturierung der amerikanischen Streitkräfte sind jedoch weitreichende Probleme verbunden, die Grundfragen der Kontrolle staatlicher Gewalt aufwerfen.[11] Im Zuge der "militärisch-technischen Revolution"[12], so die Ansicht vieler Beobachter, "untergräbt die Informationstechnologie den Großteil des

3 Vgl. John I. Alger: Introduction to *Information Warfare*, 2nd Edition, in: Winn Schwartau (Hg.): Information Warfare. Cyberterrorism: Protecting your Personal Security in the Electronic Age, New York 1996, S. 8-14, hier S. 8.

4 Vgl. Waller, Onward Cyber Soldiers.

5 Joint Chiefs of Staff (JSOS).

6 Shalikashvili, Joint Vision 2010.

7 US Army Training and Doctrine Command: Field Manual 100-6, Information Operations, August 1996, http://www.fas.org/irp/doddir/army/fm100-6/.

8 Vgl. Arneson/Starry, FM 100-6: Information Operations, S. 3-15, S. 66-69, hier S. 4.

9 Vgl. John Arquilla/David Ronfeldt (Hg.): In Athena´s Camp. Preparing for Conflict in the Information Age, Santa Monica 1997; Martin Libicki: What is Information Warfare?, ACIS Paper Nr. 3, Washington D.C., August 1995, http://www.ndu.edu/ndu/inss/actpubs/act003/a003cont.html; Douglas Waller: Onward Cyber Soldiers, in: Time Magazine, 21.8.1995, http://pathfinder.com/@@evaibYEm5gAAQHJ5/time/magazine/domestic/1995/950821/950821.cover.html.

10 Vgl. z.B. Michael J. Inacker: Kriegführung im Computerzeitalter. Der technologische Vorsprung der USA, in: Internationale Politik, Nr. 9, 1997, S.43-47; ders.: Anschluß nicht verlieren, in: Europäische Sicherheit, Nr. 7, 1997, S. 10; Gebhard Geiger: "Cyberwar" und neue Strukturen der internationalen Sicherheit. Informationsdominanz als Faktor der internationalen Stabilität, SWP-IP 3015, Ebenhausen, April 1997.

11 Dieses Problem ist den Militärs in den USA oft bewußter als den Politikern, vgl. Dunlap, Charles J.: Melancholy Reunion. A Report from the Future o the Collapse of Civil-Military Relations in the United States, in: Airpower Journal, Winter 1996, S. 93-109.

12 Vgl. Eliot A. Cohen: A Revolution in Warfare, in: Foreign Affairs, Nr. 2, 1996, S. 37-54; Earl H. Tilford Jr.: The Revolution in Military Affairs: Prospects and Cautions, Carlisle Barracks 1995.

angesammelten Wissens der Welt über bewaffnete Konflikte”[13] - und damit auch über deren politischen Kontext.

Beschleunigung, Integration, Automatisierung

Die Vernetzung der Streitkräfte auch auf den unteren Ebenen wurde in den USA seit dem Vietnamkrieg vorangetrieben. Einen Schub erhielt sie jedoch erst, als die Reagan-Administration 1980 wieder größere Finanzmittel für Forschung, Entwicklung und Beschaffung im Rüstungsbereich zur Verfügung stellte.[1] Im August 1982 wurde ebenfalls die AirLand Battle-Doktrin (ALB) fertiggestellt[2], die die Trennung von Heer und Luftwaffe durch einen integrierten Boden- und Luftkampf im “erweiterten Gefechtsraum” ablöste. Der Kerngedanke von ALB war die Ablösung der Überlegenheit in Masse oder Raum durch “Zeitdominanz”, die durch höhere Operationsgeschwindigkeiten und Überraschungsangriffe erreicht werden sollte. Dafür wurden integrierte Gefechtsstände, Sensoren und Trägersysteme benötigt, die in der Lage waren, Gefechtsdaten in Echtzeit zu berechnen, zu übertragen und auszuwerten.[3] Diese Aufgabe sollten die sogannten CI-Systeme übernehmen[3].

Der Golfkrieg 1991 war die erste praktische Anwendung der ALB-Doktrin, deren Grundannahmen durch den überlegenen Sieg der USA für die Militärs als bestätigt galten.[4] Besonders gut funktionierten erstmals die integrierten Systeme, die durch Korrelation von Aufklärungsdaten mit inhaltlichen Datenbanken einen umfassenden Lageüberblick ermöglichten. Daraus erwuchsen weitergehende Überlegungen: Wenn die Erfassung und Analyse der Daten funktionieren, wird die Frage interessant, wie sie für die Entscheidungsfindung genutzt werden können. Damit hatte die “Informationsrevolution” den Kern der militärischen Organisationsformen erreicht. Das Leitbild dieser Debatte ist ein Bild des radikalen Wandels, die “Revolution in Military Affairs”[5]. Ein vorläufiges Ergebnis waren 1996 die bereits erwähnte “Joint

13 John Carlin, A Farewell to Arms, in: antimilitarismus information, Nr. 5, 1998, S. 77-86, hier S. 79.

1 Reagan gab der C^3I-Entwicklung im Oktober 1982 die höchste Priorität unter allen neuen Waffensystemen, vgl. Manfred Domke: Aufklärungs- und Führungssysteme, in: Joachim Bickenbach et al. (Hg.): Militarisierte Informatik, Marburg 1985, S. 99-109, hier S. 102.

2 Sie reflektierte einerseits die Lehren aus dem Vietnamkrieg, andererseits die Erfahrungen des israelisch-arabischen Krieges von 1973. Das offizielle Dokument ist das Field Manual (FM) 100-5 (Operations) der US Army, vgl. Toffler/Toffler, S. 44-56.

3Im Planungspapier AirLand Battle 2000 wurden unter anderem das Anlegen von Datensammlungen, C^2-Unterstützung durch Computer, C^3I-Informationsaustausch, abgeschirmte Geräte sowie eine Verstärkung der elektronischen Kampfführung gefordert, vgl. AirLand Battle 2000, in: Militärpolitik Dokumentation, Nr. 34/35, Frankfurt/M. 1982, S. 74-93, nach Klischewski/Ruhmann, Ansatzpunkte, S. 83.

3 Command, Control, Communications und Intelligence, dt. Kommando, Kontrolle, Kommunikation und Aufklärung.

4 Die Einschätzung, daß der Sieg vor allem auf der Hochtechnologie basierte, ist bis heute umstritten, vgl. Stephen Biddle: Victory Misunderstood. What the Gulf War Tells Us about the Future of Conflict, in: International Security, Nr. 2, 1996, S. 139-179; Frankfurter Rundschau, 30.6.1997, ”Waffentechnik im Golfkrieg offenbar überschätzt”.

5 Der Begriff wurde ursprünglich in den achtziger Jahren in der UdSSR geprägt, konnte aber offenbar erst nach dem Ende der “sowjetischen Bedrohung” in den USA hoffähig werden.

Vision 2010" der *Joint Chiefs of Staff* und das Field Manual 100-6 (Information Operations).[6]

Ihnen gemeinsam ist eine stärkere Integration und Zentralisierung der Kommandostrukturen. Die Teilstreitkräfte hatten in der Vergangenheit bereits eigene CI-Systeme entwickelt oder in Auftrag gegeben.[3] Seit dem Golfkrieg wird nun ihre Integration zu einem Gesamtsystem verstärkt vorangetrieben. Das Ziel ist ein "System of Systems", also ein umfassendes C3I-System, das alle bisherigen Systeme umfaßt.[7] Zur besseren Umsetzung wurde auch die Form der Innovation verändert. Anstelle der Ausschreibung großer Systeme wurde eine Experimentaltruppe (EXFOR)[8] eingerichtet und mit den Doktrinenentwicklern, Beschaffungsbeamten, Programmoffizieren und den Firmen, die für die Systementwicklung zuständig waren, unter einem Dach versammelt.[9] Damit wurden Ressourcen und Verantwortung von den ministeriellen Entwicklungsabteilungen zu den Endnutzern verschoben.[10]

Die Vernetzung der CI-Systeme wird derzeit bis auf die unterste Ebene, den einzelen Soldaten, weitergeführt. Im Rahmen des Projektes "Land Warrior Generation II" werden die Soldaten mit tragbaren Computern ausgestattet, die an die Kommandosysteme angebunden werden. Zusätzlich können sie Sensordaten empfangen.[3] Durch computergesteuerte Präzisisionsmunition, die auch über weite Entfernungen treffen kann, sowie unterstützende Miniaturflugsysteme (Drohnen) für Aufklärung und Kommunikation[11] sollen die eigenen Verluste möglichst gering gehalten werden. Für diese Entwicklung war auch die öffentliche Meinung in den USA wichtig, die es seit dem Vietnamkrieg immer weniger zuläßt, daß amerikanische Soldaten größere Verluste erleiden. Der Einsatz von Menschen soll nun durch Hochtechnologie ersetzt werden - der Krieger vergangender Jahre wird gewissermaßen wegrationalisiert.[12] Sein Nachfolger ist ein Fachmann im Bedienen hochkomplexer technischer Systeme, der seine Gegner oft nur noch auf dem am Helm montierten Display sieht.[13] Ähnliche Projekte laufen bei der Luftwaffe, wo die zu

6 Auch das FM 100-5 (Operations) wurde überarbeitet, in der Fassung von 1993 wird "the end of industrial-age warfare and the beginning of information-age warfare" angekündigt, zit. nach Toffler/Toffler, War and Anti-War, S. 55f.

3 Bedeutend sind bei der Luftwaffe das Airborne Warning and Control System (AWACS), das Joint Surveillance Target Attack Radar System (JSTARS) und das Airborne Battlefield Command and Control Center (ABCCC III), beim Heer das Army Tactical Command and Control System (ATCCS).

7 Diese Idee stammt von dem damaligen stellvertretenden Vorsitzenden der Joint Chiefs of Staff, William A. Owens, vgl. ders: The Emerging System of Systems, in: Military Review, Nr. 3, Mai-Juni 1995, S. 15-19.

8 Hierzu wurde die 4. Infanteriedivision in Fort Hood bestimmt.

9 Dies war die Central Technical Support Facility in Fort Hood, dem Sitz der EXFOR.

10 Vgl. Stanley, Evolutionary Technology, S. 36-49.

3 Vgl. Cord Rather: Die Ausstattung des Soldaten im Wandel, in: Europäische Sicherheit, Nr. 2, 1998, S. 37-41; Klischwski/Ruhmann, Ansatzpunkte, S. 143.

11 Vgl. Mario R. Dederichs/Brian R. Wolff: Kein Mann an Bord, in: Konr@d, Nr. 1, 1998, S. 136-141.

12 Vgl. dazu auch Edward N. Luttwak: A Post-Heroic Military Policy, in: Foreign Affairs, Nr. 4, Juli/August 1996, S. 33-44.

13 Vgl. Bernhardt/Ruhmann, Der digitale Feldherrnhügel, S. 8f.

teuer gewordenen bemannten Flugzeuge durch unbemannte ferngesteuerte Systeme (*Remotely Patrolled Vehicles, RPVs*) ausgetauscht werden sollen. Der "Pilot" steuert seine Maschine dann nur noch über eine Computer von der Kommandozentrale aus.[14]

Die technische Beschleunigung des Krieges bei gleichzeitiger Erhöhung der Informationsdichte macht es den Kommandeuren immer schwerer, Entscheidungen zutreffen. Daher werden seit den achtziger Jahren große Mittel für die Entwicklung von Expertensystemen und künstlicher Intelligenz investiert. Der AirLand Battle Manager etwa soll für Führungsoffiziere auf Korpsebene und darunter Informationen vorstrukturieren, die Züge des Gegeners antizipieren, darauf reagieren und sogar Truppenbewegungen und logistische Entscheidungen vornehmen. Die ausgedruckten Befehle müssen nur noch unterschrieben werden.[15]

Da Computer aber nur Zeichen verarbeiten können und prinzipiell nicht in der Lage sind, deren Bedeutung zu "verstehen", wird das künstliche "Wissen" über Hilfskonstruktionen, etwa Wahrscheinlichkeitsabschätzungen, erzeugt.[16] Die Modelle, die dafür verwendet werden, reduzieren die vielfältige soziale Realität des Krieges auf wenige Variablen. Die militärischen Informationssysteme sind aber in aller Regel nicht für beschränkte Konfliktformen, sondern für größtmögliche militärische Effizienz ausgelegt. Die Infanteriesoldaten etwa, die nach dem Modell "Land Warrior Generation II" über vernetzte Helm-Displays verfügen werden, können sich nicht mehr auf die eigene Beobachtung verlassen, zumal sie auch Ziele bekämpfen sollen, die außerhalb des Blickfeldes liegen oder aufgrund von Umwelteinflüssen nicht zu erkennen sind. Durch den technisch gefilterten Blick wird so die komplexe Umwelt des Soldaten auf militärische Kategorien reduziert. Im Auftrag der US Army werden daher bereits Freund-Feind-Erkennungssysteme für einzelne Soldaten entwickelt. Die Luftverteidigungssysteme auf den Schiffen der US Navy zeigen Raketen, die im Operationsgebiet gestartet wurden, auf einem Bildschirm in konzentrischen Kreisen an - allerdings nicht nach Entfernung, sondern nach Gefährlichkeit geordnet. Dies soll dem Waffenoffizier bei intensiven Gefechten helfen, die Prioritäten der Raketenabwehr zu bestimmen.[17] Auf diese Weise ist den militärisch genutzten Informationssystemen die spezifische Wahrnehmungsweise der Militärs in Form von Software und Datenmodellen bereits eingebaut.

14 Das RPV X-36 wurde im Mai 1997 erfolgreich getestet. Auch die Navy entwickelt ein "Arsenal Ship", das nur mit 40 Mann Besatzung auskommt und dessen Waffensysteme ebenfalls von einer entfernten Kommandozentrale gesteuert werden, vgl. Martin Ebbing: Wortbeitrag [Joint Vision 2010], in: Streitkräfte und Strategien, NDR4 Radio, 28.11.1997, Manuskript, S. 12-16.

15 Vgl. Gray, Postmodern War, S. 58

16 Vgl. Klischewski/Ruhmann, Ansatzpunkte, S. 28f.

Das Laser/RF Soldier Identification (ID) System soll eine Freund-Feind-Erkennung über 2km ermöglichen und wird auf dem Gewehr bzw. an der Kleidung angebracht, vgl. http://www.dynetics.com/prod/lrfsid.cfm. Vgl. auch Office of Technology Assessment: Who Goes There: Friend or Foe?, Washington D.C. 1993, http://www.wws.princeton.edu:80/~ota/disk1/1993/9351_n.html.

17 Vgl. Gary Chapman: Making Sense Out Of Nonsense: Rescuing Reality from Virtual Reality, in: Gretchen Bender / Timothy Druckrey (Hg.): Culture on the Brink: Ideologies of Technology, Seattle 1994, S. 149-155, hier S. 150f.

Wenn die Wahrnehmungen der Soldaten immer stärker von computererzeugten Anzeigen geprägt werden, kann eine Simulation im Computer auch das Manöver ersetzen. Das US-Verteidigungsministerium richtet zu diesem Zweck derzeit ein *Joint Simulation System (JSIMS)* ein, das vernetzte taktische Simulationen aller Teilstreitkräfte ermöglichen wird.[18] In den Simulationssystemen wird allerdings die die Realität, die normalerweise über die Sensoren noch mit dem System gekoppelt ist, durch theoretische Vorannahmen über den Ablauf von Kriegen oder Gefechten ersetzt. Dies kann im Zweifelsfall zu einer "Überspezialisierung"[19] der Truppe führen. Dies bestätigt auch die *"Joint Vision 2010"*. Als Hauptzweck der Modernisierung wird dort die Fähigkeit genannt, konventionelle Kriege zu führen. Andere Einsatzformen, die seit einigen Jahren unter dem Titel *"Operations Other Than War"* diskutiert werden, etwa humanitäre Hilfe, Peace-Keeping-Maßnahmen oder die Bekämpfung von organisiertem Verbrechen und Drogenterrorismus, sind in den Plänen der Joint Chiefs of Staff diesem klassischen militärischen Ziel nachgeordnet.[20]

Politische Widerstände und Probleme

Die Entwicklungen waren zunächst in den Streitkräften sehr umstritten. Die Teilstreitkräfte wehrten sich zum einen gegen die Einschränkung ihrer Eigenständigkeit, die eine solche Vernetzung mit sich bringen sollte. Zum anderen widersprachen die Pläne dem militärischen Ethos, daß der Soldat direkt im Kampf beteiligt sein muß und nicht durch einen Datenverarbeiter ersetzt werden kann: "You can´t take out an enemy tank with just information."[1] Besonders die Idee einer Luftwaffe ohne Piloten galt als Unding.[2] Diesen Einwänden wurde in der "Joint Vision 2010" Rechnung getragen, indem der ursprünglich geplante revolutionäre Ansatz durch einen evolutionären ersetzt wurde. Die neuen Systeme und Methoden sollen schrittweise eingeführt werden[3], dazu wird eine frühzeitige Beteiligung der unteren Ebenen nach dem Vorbild der EXFOR vorgesehen.[4]

Jenseits dieser institutionellen Beharrlichkeiten ist mit der vollständigen Vernetzung aber auch eine grundsätzlich neue Abstimmung der Kommandostrukturen und damit auch der zivil-militärischen Beziehungen notwendig. Mit den neuen CI[42]-Systemen[5] verfügen die Kommandeure mittlerweile über eine bessere Lageübersicht (den

18 Vgl. Don Herskovitz: The Million Dollar Nintendo: the State of Simulation Software, in: Journal of Electronic Defense, August 1998, http://www.jedonline.com/jed/html/new/aug98/cover.html.

19 Davor warnen auch die Joint Chiefs of Staff, ohne allerdings Schlüsse daraus zu ziehen, vgl. Shalikashvili, Joint Vision 2010, S. 27.

20 Shalikashvili, Joint Vision 2010, S. 17.

1 General Howell M. Estes III., Kommandeur der Unified und Air Force Space Commands und des North American Aerospace Defense Command, zit. nach William B. Scott: Computer/IW Efforts Could Shortchange Aircraft Programs, in: Aviation Week&Space Technology, 19.1.1998, S. 59.

2 Der Schwerpunkt liegt heute bei Pilotenunterstützungssystemen, vgl. Klischewski/Ruhmann, S. 155.

3 Vgl. Ebbing, Wortbeitrag, S. 15f.

4 Dazu dienen seit 1994 die Advanced Concept Technology Demonstrations (ACDTs), vgl. Klischewski/Ruhmann, Ansatzpunkte, S. 54.

5 Command, Control, Communications, Computers, Intelligence and Interoperability. Diese neue Bezeichnung, die das alte "C^3I" abgelöst hat, findet sich seit Mitte der neunziger Jahre.

sogenannte *"God's Eye View"*) als die Soldaten vor Ort, die ihre Informationen nur nach dem "need to know"-Prinzip erhalten.[6] Damit ist eine direkte Kontrolle auch der untersten Einheiten und einzelnen Soldaten durch höhere Führungsebenen möglich. Auf oberster militärischer Ebene zeichnet sich eine entsprechende Zentralsierung der Entscheidungen bei den Joint Chiefs of Staff ab.[7]

> "[F]ew military leaders can resist the temptation to dabble in their subordinate´s business. The easier it is for them to find out what that business is, even though they are 10 000 miles away, the more likely they are to do so. Political leaders will have the same capability"[8]

Damit ändert sich auch das Verhältnis der Streitkräfte zur politischen Führung: Es ist abzusehen, daß sich hohe politische Entscheidungsträger in das militärische Mikromanagement einmischen werden. Im Golfkrieg 1991 mußten bereits einzelne Raketenangriffe vom Weißen Haus autorisiert werden. Die Folge ist ein Ende der klaren Trennung zwischen Politik und Militär und eine Vermischung politischer und militärischer Entscheidungsrationalität.

Diese Entwicklung wird noch verstärkt dadurch, daß die institutionelle Trennung zwischen Geheimdiensten und kämpfenden Truppen aufgehoben wird. Auf nationaler Ebene arbeiten in den USA mehr als zwanzig Behörden oder Agenturen im Bereich der Aufklärung (Intelligence).[9] Die technologische Entwicklung hat hier zu neuen Überlegungen geführt, die Fragmentierung des Aufklärungsapparates zu überwinden und einen besseren Informationsfluß anzustreben. Ein entscheidendes Ereignis dafür war ebenfalls der Golfkrieg 1991, in dem die technischen und sozialen Koordinationsprobleme zwischen Militär und Aufklärungseinheiten deutlich zutage traten.[10] So wären die Streitkräfte technisch in der Lage gewesen, die Kommunikation auf den stark gesicherten irakischen Erdkabeln abzuhören. Sie durften diese Möglichkeit auf taktischer Ebene aber nicht nutzen, weil die nationalen Geheimdienste ihnen zuvorgekommen waren.[11] Teilweise wurden diese Hindernisse umgangen, indem die Informationen über informelle Kanäle weitergegeben wurden. Das Grundproblem, die behördliche Trennung und Aufsplitterung der

6 Bedeutend sind hierfür neben dem bereits erwähnten JSTARS das All Source Analysis System (ASAS) und das auf dem Global Positioning System (GPS) basierende Enhanced Position Locating Reporting System (EPLRS). Mit JSTARS können im gesamten Kampfgebiet die gegnerischen Truppen lokalisiert und durch Radarsignaturen identifiziert werden. ASAS kann Daten von 35.000 gegnerischen Einheiten verfolgen, bewerten und mit JSTARS austauschen. EPLRS gibt einen vollständigen Überblick über die eigenen Truppen im Einsatzgebiet. Vgl. Klischewski/Ruhmann, Ansatzpunkte, S. 102-105; John R. Wood: Transition into the information age: Opportunities, Lessons Learned, and Challenges, in: Pfaltzgraff, Robert L. Jr./Richard H. Shultz Jr. (Hg.): War in the Information Age: New Challenges for U.S. Security, Washington/London 1997, S. 121-141.

7 Vgl. Roman/ Tarr, The Joint Chiefs of Staff.

8 Cohen, A Revolution in Warfare, S. 50.

9 Immer noch grundlegend, aber nicht mehr auf dem heutigen Stand ist Jeffrey T. Richelson: The U.S. Intelligence Community, Boulder etc. 1985; einen aktuellen Überblick liefert Sidney E. Dean: Die Geheimdienststruktur der USA, in: Europäische Sicherheit, Nr. 3, 1998, S. 45-48.

10 Vgl. Sheila Kerr: The Debate on US Post-Cold War Intelligence: One More New Botched Beginning?, in: Defense Analysis, Nr. 3, 1994, S. 323-350, hier S. 329.

11 Vgl. Fulghum, Cyberwar Plans.

Aufklärungsarbeit der USA, kam dadurch aber wieder auf die politische Tagesordnung.

Der Trend, der sich in den letzten Jahren abgezeichnet hat, entspricht der Entwicklung der Führungs- und Informationssysteme in den Streitkräften: Eine technische Zentralisierung wurde mit einer organisatorischen Zentralisierung verknüpft. In der *Defense Intelligence Agency (DIA)* wurden in mehreren Reformschritten verschiedene Abteilungen zentralisiert und die teilstreitkräfteübergreifende Koordination verstärkt,[12] darüber hinaus werden die ehemals 34 technischen Informationssysteme der Streitkräfte zu fünf Systemen zusammengefaßt.[13] Die Kartografie- und Fotoaufklärungsbehörden wurden in der *National Imagery and Mapping Agency (NIMA)* zusammengefaßt, und auch in den einzelnen Teilstreitkräften wurden verschiedene Aufklärungsabteilungen integriert.[14]

Der vieldiskutierte Wandel von der Industrie- zur Informationsgesellschaft und der gleichzeitige Boom des Internet brachten dabei auch zivile Informationsquellen verstärkt ins Gespräch. Die weltweiten offenen Datennetze sollten verstärkt genutzt werden, um Informationen zu sammeln. Dieser sogenannte *"Open Sources"*-Ansatz ist auch in den Streitkräften mit dem *All Source Analysis System (ASAS)* teilweise bereits umgesetzt.[15] Darüber hinaus sollen auch die Informationen der amerikanischen Geheimdienste verstärkt an andere Staaten weitergegeben werden. Der Grund dafür ist die Sorge, daß zukünftig wird vieles Wissen, das früher der Geheimhaltung unterzogen werden konnte, ohnehin auf dem freien Informationsmarkt verfügbar sein wird. Viele Datenbankanbieter suchen mittlerweile verstärkt Staaten als Kunden. Im März 1998 kamen in Washington bereits erstmals mehr als 500 Geheimdienstmitarbeiter aus aller Welt zu einer Konferenz zusammen, auf der die stärkere Privatisierung der Intelligence diskutiert wurde.[16] Der Handel von Aufklärungsdaten wird daher bereits als neues Problem der Rüstungsexportkontrolle diskutiert.[17] Besonders im Bereich der Satellitenaufklärung sind zunehmend private Bilder mit hohen Auflösungen verfügbar.

Die USA, so die Autoren eines einflußreichen Artikels in der Zeitschrift "Foreign Affairs"[18], müßten daher gezielt Abnehmer für ihr Wissen suchen, um sich politischen Einfluß bewahren zu können. Der atomare Schirm müsse durch einen "Informationsschirm" ersetzt werden. Diese Sichtweise ist mittlerweile in sicherheitspolitischen Kreisen und auch im Militär weit verbreitet. Martin Libicki von

12 Vgl. Kerr, The Debate on US Post-Cold War Intelligence, S. 330.

13 Vgl. John F. Stewart: Intelligence Strategy for the 21st Century, in: Military Review, September-Oktober 1995, S. 75-81, hier S. 81.

14 Vgl. Dean, Die Geheimdienststruktur der USA.

15 Vgl. Stewart, Intelligence Strategy, S. 78.

16 Vgl. International Spies And Analysts Define New Model For Intelligence: Global Intelligence Forum Brings Together Twenty-Three Countries Including Saudi-Arabia, Japan, Israel, PRNewswire, 23.5.1998, gesendet von infowar@aec.at in: infowar@aec.at.

17 Vgl. Klischewski/Ruhmann, Ansatzpunkte, S. 51.

Vgl. Vipin Gupta: New Satellite Images for Sale, in: International Security, Nr. 1, Sommer 1995, S. 94-125; Oliver Morton: Private Spy, in: Wired, August 1997, S. 114-119, 149-152.

18 Vgl. Nye/Owens, America's Information Edge.

der National Defense University hat die praktische Umsetzung dieser Idee für multinationale Kriegseinsätze so formuliert: “In effect, the United States can use remotely delivered bitstreams to form virtual coalitions”.[19] Diese Idee der informationszentrierten Militärkoalitionen liegt auch der neuen NATO-Kommandostruktur *Combined Joint Task Forces (CJTF)* zugrunde.[20]

Diese Entwicklungen zeigen, daß die bisher klaren Grenzen zwischen Politik und Militär oder zwischen Militär, Geheimdiensten und privaten Informationsdienstleistern in der Auflösung begriffen sind. Die USA werden weiterhin darauf setzen, ihre militärische Vormachtstellung auf Feuerkraft zu stützen. Gleichzeitig wird aber die Verfügung über Informationen immer mehr als neue Quelle der Macht begriffen. Damit sind grundlegende Fragen der Rüstungskontrolle, der Militärstrategie und -bündnispolitik sowie der politischen Kontrolle der Gewalt wieder auf dem Tisch - aber bisher ohne ausreichende Diskussion in der politischen Öffentlichkeit.

Information Warfare und die Auflösung des Krieges

Die elektronische Aufrüstung führte in den achtziger Jahren zu einem Rüstungswettlauf von *Electronic Countermeasures (ECM)* und *Electronic Counter-Countermeasures (ECCM)*.[1] Zunächst waren diese Maßnahmen darauf gerichtet, die Lenk- und Ortungssysteme von Waffen zu beeinflussen. Mit der zunehmenden Bedeutung der Computersysteme in den Kommandozentralen setzten die USA stärker darauf, in den Entscheidungsprozeß des Gegners direkt einzugreifen.[2] Der neue Name dafür war *“Command and Control Warfare” (C-Warfare)*. Im Golfkrieg 1991 wurde C^{22}-Warfare erstmals systematisch eingesetzt. Die ersten irakischen Ziele, die von den USA angegriffen wurden, waren Sendemasten, Telefonzentralen und Brücken, in denen Kommunikationskabel verliefen. Viele irakische Einheiten waren so von der Verbindung zu ihren Führungsebenen abgeschnitten und wurden handlungsunfähig. Darüber hinaus wurden gezielt irakische Kommandobunker angegriffen.[3]

Zu C-Warfare gehört daher immer noch die physische Zerstörung der gegnerischen Informationssysteme, das Konzept geht aber weit darüber hinaus. Das US-Verteidigungsministerium definiert C^{22}-Warfare als umfassende Beeinflussung der Wahrnehmungs- und Entscheidungssprozesse des Gegners.[4] Mit

19 Martin C. Libicki: Information & Nuclear RMAs Compared, Strategic Forum Nr. 82, Washington DC, Juli 1996,S. 3.

20 Vgl. Ralf Bendrath: Die postmoderne NATO. Fragmentierte Herrschaft und globalisierte Gewalt.

1 Vgl. Klischewski/Ruhmann, Ansatzpunkte, S. 116.

2 Dafür werden in der “Constant Web” Datenbank” alle verfügbaren Daten über C^3I-Systeme gesammelt, vgl. Klischewski/Ruhmann, Ansatzpunkte, S. 142.

3 Vgl. Toffler/Toffler, War and Anti-War, S. 70f.

4 Das US-Verteidigungsministerium definiert “Command and Control Warfare” als “The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions.”, DoD Dictionary, http://www.dtic.mil/doctrine/jel/doddict/data/c/01289.html.

“Informationsdominanz” bzw. “Informationsüberlegenheit” wird nicht mehr nur die Beherrschung des elektromagnetischen Spektrums, sondern der gesamten “Informationssphäre” angestrebt. Aufgrund der hohen Bedeutung von Computern für die Wahrnehmungs- und Entscheidungsprozesse aller Streitkräfte werden auch Computernetze jetzt als Teil des Kampfraumes verstanden. Im Zuge dieser Entwicklung wurde der Begriff “Information Warfare” in den offiziellen Sprachgebrauch der US-Streitkräfte aufgenommen[5] und das bereits erwähnte Field Manual 100-6 (Information Operations) veröffentlicht[6].

Die Haupttechniken dieser Art von Informationskriegführung sind das gezielte Eindringen in fremde Computersysteme *(“hacking”)* zum Zwecke der Datenmanipulation oder -zerstörung sowie das Verseuchen derselben mit Computerviren, die durch elektronische Kommandos aktiviert werden können (“logische Bomben”). Seit den achtziger Jahren arbeiten verschiedene staatliche Stellen an der Erforschung dieser Methoden. Auch die Streitkräfte beteiligen sich an der Entwicklung von Computerviren, die auch als “nicht-lethale Waffen” bezeichnet werden. Die Befehlshaber der Regionalkommandos wurden mittlerweile aufgefordert, ihre Einsatzpläne daraufhin zu überprüfen, inwieweit diese Techniken konventionelle Waffen ersetzen können. Alle Vorhaben unterliegen höchster Geheimhaltung und wurden bisher im Kongreß nicht öffentlich diskutiert.[7] Angehörigen der Streitkräfte ist es verboten, den Begriff ”offensive computer operations” in öffentlichen Debatten zu verwenden.[8] Bisher ist bekannt, daß eine Handvoll solcher Systeme bereits getestet wurden, mindestens eines wurde im Krieg eingesetzt.[9]

Die Idee, einen Krieg auch in den Datennetzen, also im sogenannten Cyberspace zu führen, war für die Militärs zunächst sehr ungewohnt, da der Cyberspace ein grundlegend anderes Verständnis von Raum und Körperlichkeit erfordert. Der “Raum” im Cyberspace besteht nur aus Daten und Symbolen sowie deren Verknüpfungen. Weil lineare Entfernungen im Sinne des cartesischen physischen Raumes nicht existieren, gibt es keine definierbare “Front” mehr. Die Akteure im Cyberspace sind nicht mehr physisch anwesend, sondern werden durch Symbole repräsentiert. Diese Nicht-Körperlichkeit des Cyberspace klammert die Anwendung physischer Gewalt, die zum professionellen Selbstbild des Militärs gehört, aus. Eine naheliegende Reaktion der Streitkräfte wäre daher gewesen, diese Aufgaben an andere, nichtmilitärische Akteure zu verweisen. Dies wurde in Fachkreisen auch erwartet. “Sobald Dinge nach etwas anderem riechen als nach Leute umbringen und

5 Das US-Verteidigungsministerium definiert “Information Warfare” als “actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks”, DoD Dictionary, http://www.dtic.mil/doctrine/jel/doddict/data/i/02944. html.

6 US Army Training and Doctrine Command: Field Manual 100-6, Information Operations, August 1996, http://www.fas.org/irp/doddir/army/fm100-6/.

7 Bei einer Anhörung des Senates zur defensiven Seite der Informationskriegführung im Juni 1998 antwortete der CIA-Direktor George Tenent auf die Frage, ob offensive Fähigkeiten entwickelt würden, nur mit einem Satz: “We’re not asleep at the switch in this regard”, zit. nach Bradley Graham: In Cyberwar, A Quandry Over Rules And Strategy, in: International Herald Tribune, 9.7.1998.

8 Vgl. Fulghum, Cyberwar Plans, S. 53.

9 ebda., S. 54.

Dinge zerstören, fangen die Militärs an, auf andere zu zeigen", so ein Berater des Verteidigungsministeriums.[10]

Daß die Streitkräfte dennoch begannen, sich grundsätzlicher auf diese Formen des Konfliktaustrages vorzubereiten, lag an der Etablierung des Leitbildes "Information Warfare" zu Beginn der neunziger Jahre. Damit wurde die Wahrnehmung des Themas so vorstrukturiert, daß eine Zuständigkeit der Streitkräfte zwingend erschien. Als Wendepunkt kann dabei das Jahr 1994 gelten, als zwei bisher getrennte Diskussionsstränge konvergierten. Während "Information Warfare" zunächst aus militärischer Sicht Computersicherheit *im* Krieg meinte, wurde daraus im zivilen Sprachgebrauch nach und nach die Bedeutung von Computersicherheit *als* Krieg.[11]

> "'Password security' became 'computer security', then 'information systems security', 'information protection', and now 'information warfare'."[12]

Das Leitbild "Information Warfare" umfaßte seitdem sowohl zivile als auch militärische Kontexte von Angriffen auf Computersysteme. Neben der Unterstützung "normaler" Kriege wurden jetzt Konflikte damit gemeint, die nur noch in den Datennetzen stattfinden. Bereits 1995 war "Information Warfare" das Leitbild für alle Forschungs- und Entwicklungspläne der US-Streitkräfte[13], und 1996 wurde es in die *Joint Vision 2010* aufgenommen.[14] Das hat weitreichende Folgen für die Identität des Militärs und seine politische Kontrolle.

Neben den Geheimdiensten ist auch das FBI bei der Strafverfolgung mit dem Eindringen in fremde Computersysteme befaßt, das Militär hat für den "Informationskrieg" also keine exklusive Zuständigkeit mehr. Im US-Kongreß wurde bereits davor gewarnt, daß die Hacker der verschiedenen staatlichen Akteure sich bei ihren Aktivitäten gegenseitig im Weg stehen könnten.[15] Die staatlichen "Informationskrieger" beziehen bereits einen großen Teil der offensiv verwendbaren Software aus Hackerkreisen.[16] Im Datennetz selber kann überhaupt nicht mehr unterschieden werden, ob ein Eindringling ein Angehöriger der Streitkräfte, ein Krimineller mit Profitabsichten oder einfach ein jugendlicher Hacker ist. Beim "Informationskrieg" werden darüber hinaus die völkerrechtlichen Normen der Kriegführung außer Kraft gesetzt.[17] Diese basieren auf der Unterscheidung von legitimen staatlichen Kriegen und illegitimen nichtstaatlichen Kriegern: Der "Soldat kann sich verbergen, aber er darf nicht die Tatsache verbergen, daß er ein Soldat

10 John Arlin, Präsident des Arlington-Instituts, zit. nach Carlin,A Farewell to Arms, S. 82.

11 Bedeutend war hierfür der Info-War-Enthusiast Winn Schwartau, der eine umfangreiche Webseite (http://www.infowar.com) betreibt. Vgl. auch Schwartau, Winn (Hg.): Information Warfare. Cyberterrorism: Protecting your Personal Security in the Electronic Age, New York 1996.

12 Michael A. Dornheim: Bombs Still Beat Bytes, in: Aviation Week&Space Technology, 19.1.1998, S. 60.

13 Vgl. Klischewski/Ruhmann, S. vi.

14 Vgl. Shalikashvili, Joint Vision 2010, S. 16.

15 Vgl. Graham, In Cyberwar.

16 Vgl. Waller, Onwar Cyber Soldiers.

17 Vgl. zum Folgenden Richard W. Aldrich: The International Legal Implications of Information Warfare, in: Airpower Journal, Herbst 1996, S. 99-110.

ist."[18] Diese Unterscheidung in Kombattanten und Nicht-Kombattanten ist beim Krieg im Datennetz nicht mehr möglich. Kurz gesagt: Im Cyberkrieg sind Militär und Polizei, staatliche und nichtstaatliche Akteure gleich.

Zusätzlich verschwindet die klare Trennung zwischen Krieg und Frieden: Um Lücken in den gegnerischen Computersystemen zu finden, sind die "Informationskriegs"-Einheiten gerade darauf angewiesen, diese schon in Friedenszeiten anzugreifen. Ein erfolgreicher Angriff besteht sogar daraus, daß er nicht einmal bemerkt wird. Der Einsatz von Viren ist ein Beispiel für einen Informationskrieg, der von den Opfern gar nicht als solcher erkannt werden könnte - wer hat nicht schon einmal einen Computerausfall durch Viren erlebt, ohne dabei gleich an Krieg zu denken?

Die politische Kontrolle ist dabei kaum noch aufrechtzuerhalten, da die Aktivitäten für technische Laien überhaupt nicht und selbst für Experten nur bedingt nachvollziehbar sind. Das Recht des Kongresses, einen Krieg zu erklären, wird ausgehebelt. Auf neue Art erleben die USA hier das Problem wieder, das von verdeckten Einsätzen der Special Operations-Einheiten bereits bekannt ist.

> "Twenty years ago, it was special operations; now info ops are shifting our conflict paradigms. But how do we control it [IW], and who should control it? How do we do the [information operations] 'bomb damage assessment'?"[19]

Auch auf der defensiven Seite wird die infrastrukturelle Sicherheit von innen und außen neuerdings als gleichermaßen gefährdet angesehen. Spätestens 1991 wurde im sicherheitspolitischen Diskurs ein Begriff geprägt, der die technologisch bedingte Unsicherheit mit einem historischen Trauma der USA verband: Das "elektronische Pearl Harbor".[20] Dieser Begriff hat eine bemerkenswerte Karriere gemacht[21] und fand Eingang in den Bericht des Defense Science Board, das im Auftrag des Verteidigungsministeriums seit 1995 die defensiven Aspekte des "Informationskrieges" untersuchte.[22] Er beschreibt ein Szenario, das aus einem elektronischen Angriff auf wichtige Teile der amerikanischen Computersysteme besteht, etwa "eine Softwarebombe auf dem Aktienmarkt" oder "ein elektromagnetischer Impuls, der das Telefonnetz zusammenbrechen läßt."[23] Die Definitionen entscheiden daher auch über Zuständigkeiten: Wird das Problem als "Computerkriminalität" betrachtet, ist es Sache des FBI; ein "Informationskrieg" dagegen betrifft das Verteidigungsministerium. Das im Mai 1998 neu geschaffene

18 Sheldon M. Cohen: Arms and Judgement. Law, Morality and the Conduct of War in the Twentieth Century, Boulder etc. 1989, S. 154, zit. nach Daase, Theorie und Praxis, S. 116.

19 Colonel Parks Shaefer, Stabsleiter der US Air Force für das Global Engagement '97 Wargame, zit. nach: Scott, Computer/IW Efforts, S. 59.

20 Die erste mir bekannte Quelle ist der Computersicherheitsberater Winn Schwartau, der diesen Ausdruck im Juni 1991 in einer Anhörung des Kongresses benutzte, vgl. ders.: Winn Schwartau: Electronic Civil Defense, in: ders. (Hg.): Information Warfare, S. 43-48, hier S. 43.

21 Er wurde 1993 in dem bereits erwähnten Buch "War and Anti-War" der Tofflers übernommen, ist seitdem in vielen Planungspapieren der Militärakademien zu finden und wurde unter anderem von CIA-Direktor John Deutch wiederholt gegenüber der Presse benutzt. Vgl. George Smith: "Electronic Pearl Harbour", in: Crypt Newsletter, http://sun.soci.niu.edu/~crypt/other/ harbor.htm.

22 Office of the Under Secretary of Defense for Aquisition & Technology, Report of the Defense Science Board, S. A-9.

23 Carlin, A Farewell to Arms, S. 80.

Amt eines nationalen Koordinators für den Schutz der Infrastruktur zeigt deutlich den Auflösungsprozeß der bisher klaren Grenzen zwischen äußerer und innerer Sicherheit. Der nationale Koordinator, der dem FBI angehört, ist jetzt auch für die Bekämpfung der *ausländischen* Terroristen und der inneren Bedrohung durch *Massenvernichtungswaffen* zuständig - beides Bereiche, die ebenso die Kompetenzen des Militärs betreffen. Das ebenfalls neu gegründete *National Infrastructure Protection Center (NIPC)* untersteht normalerweise ebenfalls dem FBI, also dem Justizministerium. Bei Bedarf kann es aber auch dem Verteidigungsministerium oder den Geheimdiensten unterstellt werden. Die genaue Entwicklung dieser Politik ist noch unklar, da weitere Studien vorgesehen sind und die Gründung weiterer Büros und Arbeitsgruppen geplant wird.[24] Der Trend zur Verschmelzung innerer, äußerer und privater Sicherheit der elektronischen Infrastruktur wird aber schon heute deutlich.[25]

"Soft Power" und die die Militarisierung der Öffentlichkeit

"Information Warfare" geht aber noch weiter. Im Rahmen dieses Konzeptes wird auch die Öffentlichkeit immer mehr als ein Mittel der Kriegführung angesehen, indem durch gezielte Falschmeldungen das taktische Wissen des Gegners manipuliert werden kann. Die USA haben diese Methode im Golfkrieg gezielt genutzt, indem sie den Zugang zu den Kriegsgebieten streng kontrollierten, aber die Reporter mit Bildern und Nachrichten aus eigener Produktion belieferten.[1] So sorgten Verlautbarungen an die Presse dafür, daß niemals eingesetzte amerikanische Landungstruppen vor der kuwaitischen Küste das sechsfache an irakischen Kräften banden. Eine Meldung über einen angeblich von den USA eingeschleusten Computervirus in den irakischen CI-Systemen sollte das Vertrauen der irakischen Kommandeure in die Zuverlässigkeit ihrer Informationen untergraben.[3] Der damalige Vorsitzende der *Joint Chiefs of Staff*, General Colin Powell, faßte dies folgendermaßen zusammen:

> "Once you've got all the forces moving and everthing's being taken care of by the commanders, turn your attention to television because you can win the battle or lose the war if you don't handle the story right."[2]

Die US-Streitkräfte haben die Lehren aus dem Golfkrieg, aber auch aus anderen Einsätzen[3], systematisch ausgewertet. Dabei wurde die psychologische Kriegführung

24 White House, Office of the Press Secretary: Fact Sheet. Summary of Presidential Decision Directives 62 and 63, 22.5.1998, http://www.pub.witehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/5/22/6.text.1

25 Vgl. auch Roger C. Molander/Andrew S. Riddile/ Peter A. Wilson: Strategic Information Warfare. A New Face of War, Santa Monica 1996.

1 Vgl. Frank J. Stech: Winning CNN Wars, in: Parameters, Nr. 3, 1994, S. 37-56, http://carlisle-www.army. mil/usawc/Parameters/1994/stech.htm.

3 Vgl. Ingo Ruhmann: Netwar and Cyberwar. Kriegsführung in der Zukunft, in: FIFF - Kommunikation, Nr. 4, 1994, S. 39-42, hier S. 41.

2 Zit. nach: McKenzie Wark: Virtual Geography. Living with Global Media Events, Bloomington, Indianapolis 1994, S. 41.

3 Die Intervention in Somalia galt als gescheitert, weil die US-Streitkräfte die Medien nicht kontrollieren konnten.

("PsyOps") erstmals als integrierter Bestandteil in die allgemeinen Operationsplanungen einbezogen. Mit der Veröffentlichung des *Field Manual 100-6 (Information Operations)* im August 1996 wurden alle Informationsflüsse im Kontext eines Krieges als entscheidend für seinen Ausgang indentifiziert. Der "Sieg im Informationskrieg" ist heute eines der fünf Langzeitziele in den Modernisierungsplänen der US Army.[4] Militärische Einsätze finden nach diesem Verständnis in einer globalen Informationsumgebung statt, die für die Zwecke des Einsatzes beeinflußt werden muß. Die Informationsumgebung wird dabei als Teil des Schlachtfeldes angesehen:

> "IO [information operations] greatly expands the commander's battlespace, including interaction with the media, industry, joint forces, multinational forces and computer/satellite networks worldwide."[5]

Das kann im Einzelfall dazu führen, daß die Angehörigen der Streitkräfte selber zum Opfer der Falschmeldungen ihrer Kollegen werden. Die bereits erwähnte Nachricht über den angeblichen Virus im irakischen CI-System etwa wurde mittlerweile mehrfach widerlegt, wird aber auch von Offizieren immer noch als Beispiel für erfolgreiche Informationskriegführung angeführt.[3]

Neuere Überlegungen gehen noch einen Schritt weiter: Anstatt die Wahrnehmungs- oder Entscheidungsprozesse des Gegners zu beeinflussen, sollen seine Ziele, also der politische Zweck des Krieges, verändert werden. "The target of information warfare, then, is the human mind ", so George Stein, Professor am *Army War College*, in einem vielzitierten Artikel.[6] Auf dieser Basis wurden Konzepte für weitergehende Formen der Kriegführung entwickelt, die unter den Leitbildern *"Netwar"* oder *"Neocortical War"* zusammengefaßt werden. Sie beinhalten eine Ausweitung des Kriegsbegriffes auf alle Konfliktformen in der Gesellschaft, die kommunikativ ausgetragen werden.[7] Als erster *"Netwar"* gilt die Auseinandersetzung zwischen Peru und Equador Anfang 1995, als sich offizielle Stellen schon vor dem Beginn der eigentlichen Kampfhandlungen im Internet einen heftigen Disput lieferten.[8] Aber auch die kritische Arbeit von Nichtregierungsorganisationen, die versuchen, die Ideen der Gesellschaft zu verändern, wird als *"Netwar"* bezeichnet.[9] Dies läuft in Umkehrung des Clausewitzschen Diktums auf eine Fortsetzung des Krieges mit politischen Mitteln hinaus. Im theoretischen Denken über den Krieg kündigt sich damit ein weiterer Wandel an: Informationen und ihre Kontrolle sind nicht

4 Vgl. Arneson/Starry, FM 100-6: Information Operations, S. 3-15, S. 66-69, hier S. 4.

5 ebda., S. 5.

3 Vgl. Dornheim, Bombs Still Beat Bytes, S. 60; Winn Schwartau erzählt die Geschichte dieser Falschmeldung, die als Aprilscherz begann und dann von der Fiktion zu den Fakten transformiert wurde, in ders.: Information Warfare, S. 426-429, 435.

6 George J. Stein: Information Warfare, in: Airpower Journal, Nr. 1, 1995, S. 30-39, http://www.airpower. maxwell.af.mil/airchronicles/apj/stein.html.

7 Vgl. John Arquilla/David Ronfeld: The Advent of Netwar, in: dies. (Hg.): In Athena´s Camp. Preparing for Conflict in the Information Age, Santa Monica 1997, S. 275-293; Ruhmann, Netwar and Cyberwar; Richard Szafranski: Neocortical Warfare? The Acme of Skill, in: John Arquilla/David Ronfeld (Hg.): In Athena´s Camp. Preparing for Conflict in the Information Age, Santa Monica 1997, S. 395-416.

8 Vgl. Klischewski/Ruhmann, Ansatzpunkte, S. 141.

9 Vgl. Arquilla/Ronfeldt, The Advent of Netwar, S. 372-374.

mehr bloß notwendige Mittel, sondern der Zweck des Krieges. Dies enspricht dem Wandel des innerstaatlichen Gewaltmonopols, den Michel Foucault beobachtet hat: Nicht mehr der Körper des Verbrechers ist heute das Objekt des Strafvollzuges, sondern sein Willen.[10]

Das bedeutet das Ende des *"American Way of War"*. Das Kriegsbild der USA beruhte lange auf der Annahme, daß das Militär erst dann aktiv wird, wenn die Politik gescheitert ist. Diese Idee des ohne politische Einmischung geführten Krieges ähnelt im Grundsatz Ludendorffs Konzept des totalen Krieges. Sie wird nun zunehmend vom Clausewitzschen Modell des Krieges als Fortsetzung und Mittel der Politik abgelöst. Clausewitz selber nannte als Ziele des Krieges nicht nur den Sieg über die feindlichen Streitkräfte und die Inbesitznahme der nicht-militärischen Hilfsquellen des Feindes, sondern auch die Gewinnung der öffentlichen Meinung.[11] Dies entspricht dem neuen amerikanischen Konzept der *"Information Operations"*. Dabei werden die Streitkräfte in einem Verbund anderer Maßnahmen eingesetzt, und das Verhältnis politischer und militärischer Entscheidungskriterien ist jeweils im Einzelfall neu festzulegen. Die Idee des *"Netwar"*, deren Umsetzung noch nicht abzusehen ist, die aber an Einfluß gewinnen könnte, wäre in dieser Entwicklung ein noch weitergehender Schritt. Er entspräche der Übernahme des Kriegsmodells von Sun Tsu, der als höchstes Ziel des Krieges die Unterwerfung des Gegners ohne Anwendung von Gewalt genannt hat.[12]

Der Hintergrund dieser Entwicklungen ist ein neues Verständnis von Macht. Der Begriff *"Soft Power"*, der mittlerweile im politischen Establishment der USA etabliert ist, bezeichnet "weiche" Formen von Macht, etwa Medienkontrolle, kulturelle Dominanz oder Softwaremonopole. Diese Faktoren erhalten in der "Informationsgesellschaft" eine hohe Bedeutung. In dem bereits erwähnten Artikel der Zeitschrift "Foreign Affairs" wird daher eine strategische Nutzung der weltweiten amerikanischen Dominanz im Bereich der Medieninhalte gefordert. Mit "Informationskampagnen", sollten die Köpfe der Völker der Welt im Kampf um amerikanische Werte gewonnen werden. Die Autoren plädieren dabei unter anderem für eine intensive Koordination des Aktivitäten des Verteidigungsministeriums mit der *United States Information Agency (USIA)* oder der *Voice of America*.[13] Die Zivilisierung des Militärs, die mit der Ausweitung der soldatischen Tätigkeiten auf Bereiche jenseits der physischen Gewalt einhergeht, fällt so zusammen mit einer Militarisierung der Zivilgesellschaft, in der die Öffentlichkeit als Raum des Kampfes, nicht der Verständigung, angesehen wird. Ähnliches gibt es übrigens auch in der Linken, die bestimmte Formen öffentlicher Aktionen neuerdings als "Kommunikationsguerrilla" bezeichnet.[14]

10 Vgl. Michel Foucault: Überwachen und Strafen. Die Geburt des Gefängnisses, Frankfurt/M. 1977.

11 Vgl. Jehuda L. Wallach: Das Dogma der Vernichtungsschlacht. Die Lehren von Clausewitz und Schlieffen und ihre Wirkungen in zwei Weltkriegen, Frankfurt/M. 1967, S. 27f.

12 Vgl. Sun Tsu: Die Kunst des Krieges,

13 Vgl. Nye/Owens, America's Information Edge, S. 31f.

14 Vgl. autonome a.f.r.i.k.a.-gruppe/Sonja Brünzels/Luther Blissett: Handbuch der Kommunikationsguerrilla, Berlin, Göttingen, Hamburg 1997.

Literatur

AirLand Battle 2000, in: Militärpolitik Dokumentation, Nr. 34/35, Frankfurt/M. 1982, S. 74-93

Aldrich, Richard W.: The International Legal Implications of Information Warfare, in: Airpower Journal, Herbst 1996, S. 99-110

Alger, John I.: Introduction to *Information Warfare*, 2nd Edition, in: Winn Schwartau (Hg.): Information Warfare. Cyberterrorism: Protecting your Personal Security in the Electronic Age, New York 1996, S. 8-14

Arneson, Charles W./Michael D. Starry: FM 100-6: Information Operations, in: Military Review, Nr. 6, November-Dezember 1996, S. 3-15

Arquilla, John/David Ronfeld: The Advent of Netwar, in: dies. (Hg.): In Athena´s Camp. Preparing for Conflict in the Information Age, Santa Monica 1997, S. 275-293

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

autonome a.f.r.i.k.a.-gruppe/Sonja Brünzels/Luther Blissett: Handbuch der Kommunikationsguerrilla, Berlin, Göttingen, Hamburg 1997

Bendrath, Ralf: Die postmoderne NATO. Fragmentierte Herrschaft und globalisierte Gewalt; in: Zivilcourage, Nr. 4, August 1997, S. 6-9

Bernhardt, Ute/Ingo Ruhmann: Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle, Wissenschaft und Frieden, Dossier Nr. 24, 1997

Biddle, Stephen: Victory Misunderstood. What the Gulf War Tells Us about the Future of Conflict, in: International Security, Nr. 2, 1996, S. 139-179

Carlin, John: A Farewell to Arms. Die USA planen für den Informationskrieg, in: antimilitarismus information, Nr. 5, 1998, S. 77-86 (zuerst in: Wired, Mai 1997, S. 51-54, 220-231)

Chapman, Gary: Making Sense Out Of Nonsense: Rescuing Reality from Virtual Reality, in: Gretchen Bender / Timothy Druckrey (Hg.): Culture on the Brink: Ideologies of Technology, Seattle 1994, S. 149-155

Cohen, Eliot A.: A Revolution in Warfare, in: Foreign Affairs, Nr. 2, 1996, S. 37-54

Daase, Christopher: Theorie und Praxis des kleinen Krieges. Ein Beitrag zum Verständnis des Wandels der internationalen Beziehungen, Phil. Diss., Freie Universität Berlin, Fachbereich Politische Wissenschaft, 1995

Dean, Sidney E.: Die Geheimdienststruktur der USA, in: Europäische Sicherheit, Nr. 3, 1998, S. 45-48

Dederichs, Mario R./Brian R. Wolff: Kein Mann an Bord, in: Konr@d, Nr. 1, 1998, S. 136-141

DoD Dictionary of Military Terms, http://www.dtic.mil/doctrine/jel/doddict/

Domke, Manfred: Aufklärungs- und Führungssysteme, in: Joachim Bickenbach et al. (Hg.): Militarisierte Informatik, Marburg 1985, S. 99-109

Dornheim, Michael A.: Bombs Still Beat Bytes, in: Aviation Week&Space Technology, 19.1.1998, S. 60

Dunlap, Charles J.: Melancholy Reunion. A Report from the Future o the Collapse of Civil-Military Relations in the United States, in: Airpower Journal, Winter 1996, S. 93-109

Dynetics, Inc.: Laser/RF Soldier Identification System http://www.dynetics.com/prod/lrfsid.cfm

Ebbing, Martin: Wortbeitrag [Joint Vision 2010], in: Streitkräfte und Strategien, NDR4 Radio, 28.11.1997, Manuskript, S. 12-16

Foucault, Michel: Überwachen und Strafen. Die Geburt des Gefängnisses, Frankfurt/M. 1977

Frankfurter Rundschau, 30.6.1997, ”Waffentechnik im Golfkrieg offenbar überschätzt”

Fulghum, David A.: Cyberwar Plans Trigger Intelligence Controversy, in: Aviation Week&Space Technology, 19.1.1998, S. 52-54

Geiger, Gebhard: ”Cyberwar” und neue Strukturen der internationalen Sicherheit. Informationsdominanz als Faktor der internationalen Stabilität, SWP-IP 3015, Ebenhausen, April 1997

Graham, Bradley: In Cyberwar, A Quandry Over Rules And Strategy, in: International Herald Tribune, 9.7.1998

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

Gupta, Vipin: New Satellite Images for Sale, in: International Security, Nr. 1, Sommer 1995, S. 94-125

Herskovitz, Don: The Million Dollar Nintendo: the State of Simulation Software, in: Journal of Electronic Defense, August 1998, http://www.jedonline.com/ jed/html/new/aug98/ cover.html

Inacker, Michael J.: Anschluß nicht verlieren, in: Europäische Sicherheit, Nr. 7, 1997, S. 10

Inacker, Michael J.: Kriegführung im Computerzeitalter. Der technologische Vorsprung der USA, in: Internationale Politik, Nr. 9, 1997, S.43-47

International Spies And Analysts Define New Model For Intelligence, PRNewswire, 23.5.1998, gesendet von infowar@aec.at in: infowar@aec.at

Kerr, Sheila: The Debate on US Post-Cold War Intelligence: One More New Botched Beginning?, in: Defense Analysis, Nr. 3, 1994, S. 323-350

Klischewski, Ralf/Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie, Studie für das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bonn 1995

Libicki, Martin C.: Information & Nuclear RMAs Compared, Strategic Forum Nr. 82, Washington DC, Juli 1996

Libicki, Martin C.: Information Dominance, Strategic Forum, Nr. 132, Washington D.C., Dezember 1997

Luttwak, Edward N.: A Post-Heroic Military Policy, in: Foreign Affairs, Nr. 4, Juli/August 1996, S. 33-44

Martin Libicki: What is Information Warfare?, ACIS Paper Nr. 3, Washington D.C., August 1995, http://www.ndu.edu/ndu/inss/actpubs/act003/a003cont.html

Molander, Roger C./Andrew S. Riddile/ Peter A. Wilson: Strategic Information Warfare. A New Face of War, Santa Monica 1996

Morton, Oliver: Private Spy, in: Wired, August 1997, S. 114-119, 149-152

Nye, Joseph S. jr./William A. Owens: America´s Information Edge, in: Foreign Affairs, Nr. 3/4 1996, S. 20-36

Office of Technology Assessment: Who Goes There: Friend or Foe?, Washington D.C. 1993, http://www.wws.princeton.edu:80/~ota/disk1/1993/9351_n.html

Office of the Under Secretary of Defense for Aquisition & Technology: Report of the Defense Science Board on Information Warfare-Defense (IW-D), Washington D.C., November 1996, http://www.strassmann.com/ pubs/dsb-iwd.html

Owens, William A.: The Emerging System of Systems, in: Military Review, Nr. 3, Mai-Juni 1995, S. 15-19

Pfaltzgraff, Robert L. Jr./Richard H. Shultz Jr. (Hg.): War in the Information Age: New Challenges for U.S. Security, Washington/London 1997

Rather, Cord: Die Ausstattung des Soldaten im Wandel, in: Europäische Sicherheit, Nr. 2, 1998, S. 37-41

Richelson, Jeffrey T.: The U.S. Intelligence Community, Boulder etc. 1985

Roman, Peter J./David W. Tarr: The Joint Chiefs of Staff: From Service Parochialism to Jointness, in: Political Science Quarterly, Nr. 1, 1998, S. 91-111

Ruhmann, Ingo: Netwar and Cyberwar. Kriegsführung in der Zukunft, in: FIFF - Kommunikation, Nr. 4, 1994, S. 39-42

Schwartau, Winn (Hg.): Information Warfare. Cyberterrorism: Protecting your Personal Security in the Electronic Age, New York 1996

Schwartau, Winn: Electronic Civil Defense, in: ders. (Hg.): Information Warfare, S. 43-48

Scott, William B.: Computer/IW Efforts Could Shortchange Aircraft Programs, in: Aviation Week&Space Technology, 19.1.1998, S. 59

Shalikashvili, John M.: Joint Vision 2010, Joint Chiefs of Staff, Washington D.C. 1996, http://www.dtic.mil/ doctrine/jv2010/jv2010.pdf

Smith, George: “Electronic Pearl Harbour”, in: Crypt Newsletter, http://sun.soci.niu.edu/ ~crypt/other/harbor.htm

Stanley, Elizabeth A.: Evolutionary Technology in the Current Revolution in Military Affairs: The Army Tactical Command and Control System, Carlisle/Pa. 1998

Stech, Frank J.: Winning CNN Wars, in: Parameters, Nr. 3, 1994, S. 37-56

Stein, George J.: Information Warfare, in: Airpower Journal, Nr. 1, 1995, S. 30-39

Stewart, John F.: Intelligence Strategy for the 21st Century, in: Military Review, September-Oktober 1995, S. 75-81

Sunzi (Sun Tsu). Die Kunst des Krieges, München 1998

Szafranski, Richard: Neocortical Warfare? The Acme of Skill, in: Arquilla/Ronfeld (Hg.): In Athena´s Camp, Santa Monica 1997, S. 395-416

Tilford, Earl H. Jr.: The Revolution in Military Affairs: Prospects and Cautions, Carlisle/Pa. 1995

Toffler, Alvin und Heidi: War and Anti-War. Survival at the Dawn of the 21st Century, New York etc. 1993

US Army Training and Doctrine Command: Field Manual 100-6, Information Operations, August 1996, http://www.fas.org/irp/doddir/army/fm100-6/

Wallach, Jehuda L.: Das Dogma der Vernichtungsschlacht. Die Lehren von Clausewitz und Schlieffen und ihre Wirkungen in zwei Weltkriegen, Frankfurt/M. 1967

Waller, Douglas: Onward Cyber Soldiers, in: Time Magazine, 21.8.1995

Wark, McKenzie: Virtual Geography. Living with Global Media Events, Bloomington, Indianapolis 1994

White House, Office of the Press Secretary: Fact Sheet. Summary of Presidential Decision Directives 62 and 63, 22.5.1998

Wood, John R.: Transition into the information age: Opportunities, Lessons Learned, and Challenges, in: Pfaltzgraff/Shultz (Hg.): War in the Information Age, S. 121-141

Ralf Bendrath

Postmoderne Kriegsdiskurse

Die Informationsrevolution und ihre Rezeption im strategischen Denken der USA[1]

"We are not in the business of killing."
General Norman Schwarzkopf[2]

Fast unbemerkt hat die Postmoderne nun auch die Militärs erreicht. Obwohl bereits der Vietnamkrieg als der erste "postmoderne Krieg" bezeichnet wurde[3], finden erst seit kurzem postmoderne Theoreme ihren Eingang in militärische Planungspapiere und konservative Denkfabriken. Feste Hierarchien gelten plötzlich als überholt, die Grenzen zwischen Krieg und Frieden oder zwischen innerer und äußerer Sicherheit werden eingerissen, und der Krieg findet nicht mehr auf dem Schlachtfeld, sondern auf den Computerterminals der Kommandeure statt. Am Ende wird der Kämpfer arbeitslos, wegrationalisiert durch autonome Kampfroboter und Manager des Informationskrieges.

So oder ähnlich könnte man die in den letzten Jahren entstandene Diskussion im Umfeld der US-Streitkräfte zusammenfassen. Mit der Betonung der Informationstechnologien für die Zukunft des Krieges ist eine diskursive Entwertung der kämpfenden Truppen verbunden, die im Selbst- und Fremdbild der Streitkräfte immer identitätsstiftend waren. Nach der Delegitimierung des klassischen Kämpfers wird nun ein neues Bild des Krieges und damit auch der amerikanischen Machtpolitik konstruiert. Auch dieser Diskurs, der von "Präzisionsschlägen", "virtuellen Schlachtfeldern", "Medienoperationen" und ähnlichem lebt und eine Zivilisierung der Kriegführung suggeriert, hat seine dunkle Seite der Macht. Diese findet sich allerdings nicht mehr in den Bombenschächten der B-52, sondern in der Kontrolle strategischer Informationsflüsse.

Von der Geopolitik zur Technopolitik

Ausgangspunkt der Debatte, die inzwischen eine ganze Garagenindustrie von Analytikern, Visionären, Konferenzen und Webseiten hervorgebracht hat, sind die rasanten Entwicklungen im Bereich der Informations- und Kommunikationstechnologie. Die Rede von der "Informationsrevolution" hat dabei die zunächst unter Geopolitikern attraktive "neue Weltordung" verdrängt. Damit wird als treibende Kraft des internationalen Wandels nicht mehr die Weltlage nach dem Ende des Ostblocks identifiziert, schon gar nicht die Veränderungen der internationalen Klassenbeziehungen, sondern die Technologie.

Dieser Paradigmenwechsel im strategischen Denken stieß zunächst auf größeren Widerstand. Die kalten Krieger in den Planungsabteilungen und Denkfabriken bestanden auf ihren alten Weltbildern. Nach der bislang auch im akademischen

1 Dieser Artikel erschien zuerst online in telepolis (http://www.heise.de/tp), CHECK DATUM sowie in der Zeitschrift für Informations- und Kommunikationsökologie, (CHECK) Heft 2, Winter 1999.

2 Zit. nach Chris Hables Gray: Postmodern War. The New Politics of Conflict, London, New York 1997, S. 46

3 Vgl. ebda., S. 158.

Bereich dominanten Theorieschule des sogenannten “Realismus” spielen Staaten immer noch die zentrale Rolle in der internationalen Politik, die im Kern ein Nullsummenspiel um knappe Ressourcen und den relativen Vorteil ist. Ihre Bedrohungskonstruktionen sind entsprechend ganz um staatliche Waffenarsenale zentriert (so wurde davor gewarnt, daß Rußland wieder eine Supermacht werden könnte), und das Kriegsbild, das dieser Theorie folgt, ist der klassische Territorialkrieg mit Panzerverbänden und klaren Frontlinien.

Um dagegen eine andere Vision des Krieges durchzusetzen, mußte der strategische Diskurs um ein neues, sehr mächtiges Leitbild herum strukturiert werden. Dabei war es wichtig, daß dieses Bild einen radikalen Wandel des Denkens impliziert, aber gleichzeitig hinreichend deterministisch konstruiert wird, um jeden Widerstand als veraltet und sinnlos erscheinen zu lassen. Als Anknüpfungspunkt bot sich daher die informationstechnische “Revolution” an, von deren Übermacht spätestens mit dem Boom des Internet niemand mehr überzeugt werden mußte. Dieser Diskursstrang wurde verknüpft mit einer Revolutionstheorie der Militärgeschichte, nach der immer wieder neue Technologien die Kriegführung grundlegend verändert haben.[1] Daraus wurde eine Theorie der militärischen Revolutionen konstruiert. Zusammen mit der “Informationsrevolution” ergab dies das aktuelle soziotechnische Leitbild der “Revolution in Military Affairs” (RMA)[2]. Die These von “revolutionären”, also diskontinuierlichen Sprüngen in der Entwicklung der Kriegführung erfüllt mittlerweile als Theorem der Militärwissenschaft auch für empirische Studien zur Kriegsgeschichte eine leitende Funktion.

Angewandt auf die Gegenwart beschreibt das Bild der “Revolution in Military Affairs” aber nicht etwa eine tatsächlich stattfindende Entwicklung, sondern sorgt umgekehrt erst für ihr Entstehen. Indem Szenarien der Kriegführung im 21. Jahrhundert gemalt werden, die aus digital vernetzten Armeen, intelligenten Bomben, globaler Überwachung und “Computer Network Attacks” bestehen, wird die in der Vergangenheit kumulierte Erfahrung der Militärs für null und nichtig erklärt. Die informationstechnische Zukunft erscheint nunmehr so klar, so drohend und unausweichlich, daß die Vergangenheit mit ihren Fehlschlägen und gelernten Lektionen keine Chance mehr hat. Dies spiegelt einen gesellschaftlichen Trend wider, der sich auch in der hohen Beliebtheit von Science Fiction ausdrückt: “Die extrapolierte oder narrative Zukunft hat die geschichtliche Vergangenheit als unseren grundlegendsten und entscheidendsten Bezugspunkt verdrängt.”[3] Sobald erst einmal die im Pulverdampf vergangener Schlachtfelder zu “Helden” gewordenen Soldaten der kämpfenden Truppen auf diesem Wege symbolisch entwertet sind, ist der Weg frei für ein “post-heroisches Militär” (so der Titel eines vielzitierten Aufsatzes[4]). Die

1 Eines der beliebtesten Beispiele ist der “Blitzkrieg” der deutschen Wehrmacht 1939, der auf der systematischen Nutzung mechanisierter Panzerverbände und ihrer Kontrolle durch Radiowellen basierte.

2 Vgl. Norman C. Davis: An Information-Based Revolution in Military Affairs, in: John Arquilla/David Ronfeld (Hg.): In Athena´s Camp, Santa Monica 1997, S. 79-98.

3 Alan Shapiro: The Star trekking of Physics, in: Ctheory, Article 52, 9.10.1997. http://www.ctheory.com/a52.html (Übersetzung R.B.).

4Edward N. Luttwak: A Post-Heroic Military Policy, in: Foreign Affairs, Nr. 4, Juli/August 1996, S. 33-44.

“Helden” der Zukunft, sofern es noch welche gibt, sind Hacker und Informationsmanager.

Die Rationalisierung des Krieges

Der konservative Teil der Militärstrategen versucht das Neue mit dem Alten zu verbinden, indem die Informationsrevolution für konventionelle Kriegführung genutzt werden soll. In dem zentralen Planungspapier des US-Generalstabes, der “Joint Vision 2010”[5], wurde daher auch der revolutionäre Ansatz durch einen evolutionären ersetzt. Mit einem Verbund von weltweiten Sensoren, Datennetzen, Künstlicher Intelligenz und Waffenlenksystemen, dem sogenannten “System of Systems”, soll das Schlachtfeld so transparent gemacht werden wie die irakische Wüste zur Mittagszeit. Im Kern läßt sich dieser Ansatz als das klassische “Toys for the Boys” beschreiben. Informationstechnologien werden als “Force Multiplier” betrachtet, die ansonsten keine grundlegenden Änderungen des strategischen und taktischen Denkens erfordern.

Die Datenverarbeitung wird so zur zentralen Aufgabe der Streitkräfte. Die Ausgaben des Pentagon, die mit dem Erzeugen, Sammeln und Verteilen von Informationen verbunden sind, belaufen sich derzeit auf ca. 43 Milliarden US-Dollar[6] - das sind bereits mehr als 150% des deutschen Verteidigungshaushaltes. Allein die Navy wird in den nächsten sechs Jahren 10 Milliarden Dollar für “Informationskriegführung” ausgeben, entsprechend hohe Ausgaben sind auch bei den anderen Teilstreitkräften eingeplant. Um die Menge an Daten (täglich mehrere Terabytes allein im Pentagon) überhaupt noch verstehen zu können, arbeitet man bereits eng mit den Spezialisten für dreidimensionale Grafiken aus Hollywood zusammen. So hat sich die US-Army zu 51% an einem Joint Venture mit der *School of Cinema-Television* der *University of Southern California* beteiligt, in dem eine umfassende Gefechtsfeld-Simulation entwickelt werden soll.[7] Das Ziel ist es, den “Nebel des Krieges” zu lichten und in einem virtuellen Datenraum den Kommandeur zum organischen Teil des Systems zu machen. Die US-Strategen glauben dabei recht naiv an die neue Technologie und ihre Computermodelle der kriegerischen Wirklichkeit. Es gibt kaum noch einen Bereich, in dem nicht digital modernisiert wird, von der Logistik über das Beschaffungswesen bis zur Öffentlichkeitsarbeit. Bis hin zum einzelnen Soldaten wird die Vernetzung derzeit vorangetrieben, mit Laptops, digitalen Helmkameras und Satellitennavigation.[8]

Diese Ausweitung der Nutzungsbereiche von Computersystemen im Militär läßt sich als Versuch beschreiben, immer weitere Aspekte der komplexen Realität des Krieges kalkulierbar und damit planbar zu machen. In der Geschichte des militärstrategischen Denkens zeigt sich dieses Denken bereits mit dem Verschwinden der “Fortuna” seit Beginn der Moderne.[9] Mit den Verheißungen der schönen neuen Informationswelt

5 John M. Shalikashvili: Joint Vision 2010, Joint Chiefs of Staff, Washington D.C. 1996, http://www.dtic.mil/ doctrine/jv2010/jv2010.pdf

6Neil Munro: Inducting Information, in: National Journal, 27.3.1999.

7 Vgl. Michael Stroud: War Is Virtual Hell, Wired News, 19.8.1999, http://www.wired.com/news/news/email/explode-infobeat/technology/story/21329.html

8 Vgl. Cord Rather: Die Ausstattung des Soldaten im Wandel, in: Europäische Sicherheit, Nr. 2, 1998, S. 37-41.

wird diese unberechenbare Schicksalsgöttin nun auch noch aus dem letzten Winkel des Krieges herausgerechnet.

Schon Carl von Clausewitz hat aber das “Spiel von Möglichkeiten, Wahrscheinlichkeiten, Glück und Unglück (...), welches (...) den Krieg dem Kartenspiel am nächsten stellt”[10] als elementares Element jeder Strategie identifiziert und mit seinem Begriff der “Friktion” beschrieben. Kein Schlachtplan überlebt daher, so eine alte Feldherrenweisheit, die erste Feindberührung. Da der gesamte militärische Diskurs um die Kriege der Zukunft aber bereits auf der Grundannahme der rational geplanten und kalkulierbaren Kriegführung basiert, die mit den Computersystemen verbunden ist, folgt aus Fehlern und Defiziten in der Praxis regelmäßig eine immer weitere Verfeinerung der militärischen Hard- und Software. Dies erklärt, warum Technologisierungsschübe besonders in und nach Kriegen einsetzen. Die Technologie wird in diesem Prozeß zunehmend in neue, vorher nur sozial integrierte Bereiche eingeführt. Nach der Signalübertragung und der Objektidentifizierung werden Computersysteme mittlerweile dazu eingesetzt, automatisch Befehle zu generieren.[11] Letzte Entscheidungen über Leben und Tod werden so den Modellen der Simulationsprogramme überlassen.

Das mit Computern ausgestattete Militär zeigt damit, soziologisch gesprochen, typische Merkmale eines großtechnischen Systems[12], nämlich eine Tendenz zur Expansion (das Bestreben, die Umwelt nach Kriterien des Systems zu strukturieren) und zur Innovation (die Unmöglichkeit eines technischen Stillstandes). Damit dringt aber die militärische Computernutzung in soziale Bereiche vor, die traditionell nicht als militärischer Handlungskontext angesehen wurden.

Wissen ist Macht - auch militärische

Aus dem blutigen Krieg wird so ein “Informationskrieg”. Dieser Begriff hat seit Anfang der neunziger Jahre eine rasante Karriere gemacht, die nicht zufällig parallel zum Boom des Internet verlief. 1993 erschien eine vielbeachtete Studie des militärnahen Think-Tanks *RAND Corporation*, in dem die Autoren als neue Kriegsform den “Cyberwar” ankündigten.[13] Im gleichen Jahr veröffentlichten die Futorologen Alvin und Heidi Toffler ihr Buch “War and Anti-War”, in dem ebenfalls eine neue Form des Krieges vorhergesagt wurde, die auf der Beherrschung der Informationen basiert.

9 Vgl. R.B.J. Walker: *The Prince* and ”The Pauper”: Tradition, Modernity, and Practice in the Theory of International Relations, in: James Der Derian / Michael J. Shapiro (Hg.): International/Intertextual Relations. Postmodern Readings of World Politics, Lexington/Mass. 1989, S. 25-48.

10 Clausewitz, Carl von: Vom Kriege, eingeleitet von Ernst Engelberg und Otto Korfes, Berlin (DDR) 1957 [1832-34], S. 32.

11 Das Gefechtssystem *AirLand Battle Manager* soll für Führungsoffiziere auf Korpsebene und darunter Informationen vorstrukturieren, die Züge des Gegeners antizipieren, darauf reagieren und sogar Truppenbewegungen und logistische Entscheidungen vornehmen. Die ausgedruckten Befehle müssen nur noch unterschrieben werden - falls das System jemals funktionieren sollte.Vgl. Gray, Postmodern War, S. 58.

12 Vgl. Peter Weingart: ”Großtechnische Systeme” - ein Paradigma der Verknüpfung von Technikentwicklung und sozialem Wandel?, in: ders. (Hg.): Technik als sozialer Prozeß, Frankfurt/M. 1989, S. 174-196.

13Vgl. John Arquilla / David Ronfeldt: Cyberwar is Coming!, in: Comparative Strategy, Nr. 2, 1993, S. 141-165.

Das Buch wurde zum Bestseller in den US-Streitkräften und gehört mittlerweile zur Pflichtlektüre an den meisten Militärakademien der USA. Alvin Toffler selber ist seitdem Gastprofessor an den War Colleges der Army und Air Force.[14] Die Folge war die Gründung der *School for Information Warfare and Strategy* an der *National Defense University* in Washington im Jahr 1994.[15] Bereits ein Jahr später war "Information Warfare" das Leitbild für alle Forschungs- und Entwicklungspläne des Pentagon[16], und 1996 wurde es in die bereits erwähnte *Joint Vision 2010* aufgenommen. Die US-Streitkräfte verfügen heute über eigene *Field Manuals*, Einsatzzentralen und defensive wie offensive Doktrinen des Informationskrieges.

Der Begriff "Informationskrieg" ist sehr weit gefaßt. Er umfaßt das Stören von gegnerischen Kommunikationskanälen, physische Angriffe auf Kommandozentralen und Angriffe durch Computernetze ebenso wie psychologische Kriegführung und gezielte Öffentlichkeitsarbeit.[17] Während Teile davon, etwa ein Bombardement von Radarstellungen, nur in Verbindung mit einem "normalen" Krieg eingesetzt werden sollen, sind andere Maßnahmen - beschönigend "Informationsoperationen" genannt - auch in Friedenszeiten vorgesehen. Damit verschwimmt die klare Trennung zwischen Krieg und Frieden sowie zwischen militärischer und politischer Machtausübung.

Informationen gelten im politischen System der USA heute als strategische Ressource wie Militärarsenale und Wirtschaftspotentiale. Mit der Übernahme von Ansätzen aus der postmodernen Managementtheorie und der Netzwerkökonomie ändert sich aber der Umgang mit dieser Ressource. Im Gegensatz zu Kapital, Boden, Waffen oder Menschen sind Informationen mehr wert, wenn sie geteilt und nicht zurückgehalten werden. Für die Militärpolitik bedeutet dies, daß möglichst viele andere Staaten ihre Streitkräfte an das Informationssystem der USA anschließen sollen, die so zum "natürlichen Koalitionsführer" bei Militäreinsätzen werden. Der erste Einsatz nach diesem Modell war die IFOR/SFOR-Truppe in Bosnien. Auch die NATO-Kommandostruktur ist bereits darauf zugeschnitten worden; ihren Kern stellt seit 1996 das Modell der *Combined Joint Task Forces* dar, "projektbezogene" militärische Einheiten aus Truppenteilen verschiedener Staaten (Combined) und allen Teilstreitkräften (Joint), die für einen bestimmten begrenzten Einsatz gebildet und anschließend wieder aufgelöst werden (Task Force). Als Vorbild hat man sich hier unverkennbar an dem postmodernen Konzept der "virtuellen Unternehmen"

14 Vgl. R.L. DiNardo / Daniel J. Hughes: Some Cautionary Thoughts on Information Warfare, in: Airpower Journal, Nr. 4, 1995, S. 69-79, http://www.airpower.maxwell.af.mil/airchronicles/apj/dinardo.html.

15 Vgl. John I. Alger: Introduction to *Information Warfare*, 2nd Edition, in: Winn Schwartau (Hg.): Information Warfare, New York 1996, S. 8.

16 Vgl. Ralf Klischewski / Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie, Studie für das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bonn 1995, S. vi.

17 Joint Chiefs of Staff: Joint Doctrine for Information Operations, Joint Publication 3-13, 9.10.1999, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

Vgl. Ralf Bendrath: Die Postmoderne NATO. Fragmentierte Herrschaft und globalisierte Gewalt, in: Zivilcourage, Nr. 4, August 1997, S. 6-9.

orientiert.[18] Führende US-Strategen sprechen bereits von einem "Informationsschirm", der den atomaren Schirm ablösen wird.[19] Im Einzelfall kann das dazu führen, daß andere Armeen quasi in der Rolle von Subunternehmern die Drecksarbeit machen und die USA als "Systemführer" nur noch für die Datenverwaltung - Satellitenspionage, Zielerkennung oder Kommunikation - zuständig sind. Martin Libicki, ebenfalls RAND-Mitarbeiter und Vordenker des Informationskrieges, nennt dies passend "virtuelle Koalitionen".[20]

Zur Zeit wird in den USA eine "Nationale Informationsstrategie" vorbereitet, die solche militärischen Informationsflüsse mit ihren zivilen Entsprechungen zusammenführen soll. Wiederum beteiligt ist der Cyberwar-Vordenker John Arquilla, Professor an der *Naval Postgraduate School in Montery*.[21] Die mediale Repräsentation des Krieges ist in den letzten Jahren immer wichtiger geworden, sowohl für die Akzeptanz an der heimatlichen Fernsehfront als auch für die Manipulation der Wahrnehmung des Gegners. In den Streitkräften sind die Einheiten für psychologische Kriegführung, die traditionell immer eine Außenseiterrolle hatten, mit der Doktrin der "Informationsoperationen" nun ins Zentrum der strategischen und taktischen Überlegungen gerückt. Darüber hinaus wird eine stärkere Verzahnung der militärischen Informationseinheiten mit Einrichtungen wie der *Voice of America*, *Radio Free Europe* oder dem *US Information Service* vorgesehen.[22] Der damalige Vorsitzende der Vereinigten Stabschefs, General Colin Powell, brachte dies zur Zeit des Golfkrieges 1991 bereits auf den Punkt: "Wenn alle Truppen in Bewegung sind und die Kommandeure an alles gedacht haben, richte deine Aufmerksamkeit auf das Fernsehen, denn du kannst die Schlacht gewinnen oder den Krieg verlieren, wenn du mit der Story nicht richtig umgehst"[23]

Der neue Krieg um die Köpfe

An dieser Stelle setzen die selbsternannten Revolutionäre der Kriegstheorie an. Wenn das Entscheidende in den Kriegen der Zukunft nicht mehr die Feuerkraft, sondern die Informationsvorherrschaft ist, so die postmoderne Wende, dann zielt die Kriegsstrategie nicht mehr auf den Körper des Gegners, sondern auf seinen Geist. Die Selbst- und Umweltwahrnehmung des Gegners soll so strukturiert werden, daß er dem amerikanischen Willen folgt, ohne mit Gewalt gezwungen zu werden. Dies enspricht dem Wandel des innerstaatlichen Gewaltmonopols, den bereits Michel Foucault beobachtet hat: Nicht mehr der Körper des Verbrechers ist heute das Objekt des Strafvollzuges, sondern sein Willen.[24] Anstatt die Wahrnehmungs- oder

18 Vgl. William H. Davidow/ Michael S. Malone: The Virtual Corporation, New York 1992.

19 Joseph S. Nye, jr. / William A. Owens: America´s Information Edge, in: Foreign Affairs, Nr. 2, März/April 1996, S. 25.

20 Martin C. Libicki: Information & Nuclear RMAs Compared, Strategic Forum Nr. 82, Washington DC, Juli 1996, S. 3.

21 Vgl. Munro, Inducting Information.

22 Nye/Owens, America´s Information Edge, S. 31f.

23 Zit. nach: McKenzie Wark: Virtual Geography. Living with Global Media Events, Bloomington, Indianapolis 1994, S. 41, Übersetzung R.B.

24 Vgl. Michel Foucault: Überwachen und Strafen. Die Geburt des Gefängnisses, Frankfurt/M. 1977.

Entscheidungsprozesse des Gegners zu beeinflussen, sollen seine Ziele, also der politische Zweck des Krieges, verändert werden. “Das Angriffsziel des Informationskrieges ist dann das menschliche Denken, speziell das Denken derer, die die Schlüsselentscheidungen über Krieg und Frieden treffen”, so George Stein, Professor am *Army War College*, in einem vielzitierten Artikel.[25] Auf dieser Basis wurden Konzepte für weitergehende Formen der Kriegführung entwickelt, die unter den Leitbildern “Netwar” oder “Neocortical War” zusammengefaßt werden. Sie beinhalten eine Ausweitung des Kriegsbegriffes auf alle Konfliktformen in der Gesellschaft, die mit öffentlichen Mitteln ausgetragen werden.[26]

Informationen gelten dabei zunehmend als Waffen, so sprechen etwa die Tofflers von den amerikanischen “Medienhaubitzen” CNN und Hollywood.[27] Am Ende, so die Visionen aus den Denkfabriken, könnten “Special Media Forces” den Einsatz von richtigen Soldaten überflüssig machen[28]. Diese Position entspricht der postmodernen oder konstruktivistischen Wende in den Humanwissenschaften, mit der den ideellen, symbolischen Strukturen mehr Gewicht für menschliches Handeln zugemessen wird als den materiellen Bedingungen. Sie findet in den USA aber auch darüber hinaus eine hohe Akzeptanz, weil sie ein Bild vom unblutigen Krieg suggeriert. Daß diesen Krieg im Zweifelsfall andere führen, verschwindet unter den Bildern vom “Cybersoldaten”.

Der “Informationskrieg” ist aber mehr als nur eine beschönigende Darstellung des brutalen, blutigen Krieges durch gezieltes Informationsmanagement. Wäre es so - und so wollen es konservative Militärstrategen gerne behalten - , dann könnte man es mit dem alten Begriff der “Propaganda” beschreiben. Die postmoderne Variante der amerikanischen Informationsstrategie geht aber darüber hinaus: Ihre Vordenker hoffen ernsthaft, in der gezielten Zusammenarbeit mit Nichtregierungsorganisationen, Journalisten, Medienkonzernen und staatlichen Informationsstellen ein gewaltfreies Äquivalent für militärische Macht gefunden zu haben. Die weltweite Bereitstellung offener Kommunikationskanäle, so ihre These, führt automatisch zu offeneren Gesellschaften und freien Märkten. Überspitzt formuliert lautet ihre Lehre aus dem Vietnamkrieg: Den *American Way of Life* verbreitet man besser mit MTV und dem Internet als mit Bomben und Besatzungstruppen.[29]

Am Ende, so läßt sich auch diese “zivile” Variante der Informationsstrategie zusammenfassen, geht es also wieder um die weltweite Hegemonie eines spezifischen - liberal-kapitalistischen - Gesellschaftsmodells. Ob die Politik sich für Bomben oder Bytes als Mittel der Wahl entscheidet, wird dabei von den je spezifischen Umständen abhängen - von der Art des Gegners, der Stimmung in der

25 George J. Stein: Information Warfare, in: Airpower Journal, Nr. 1, 1995, S. 30-39, http://www.airpower. maxwell.af.mil/airchronicles/apj/stein.html.

26 Vgl. John Arquilla/David Ronfeld: The Advent of Netwar, in: dies. (Hg.): In Athena´s Camp, Santa Monica 1997, S. 275-293; Richard Szafranski: Neocortical Warfare? The Acme of Skill, in: John Arquilla/David Ronfeld (Hg.): In Athena´s Camp, Santa Monica 1997, S. 395-416.

27 Toffler, Alvin und Heidi: The New Intangibles, in: Arquilla/Ronfeldt (Hg.): In Athena's Camp, Santa Monica 1997, S. xvi.

28 John Arquilla / David Ronfeldt: The Emergence of Noopolitik. Towards an American Information Strategy, Santa Monica 1999, S. 50f.

29 Vgl. ebda, passim.

Bevölkerung oder den militärisch-strategischen Interessen. Die Öffentlichkeit ist dabei nur Mittel zum Zweck, und sie wird zunehmend als Raum des Kampfes, nicht der Verständigung angesehen. Die US-Strategen befinden sich dabei übrigens in interessanter Gesellschaft: Ähnliche Überlegungen werden seit einigen Jahren auch von postmodern geschulten Linken angestellt, die neue Formen öffentlicher Aktionen als “Kommunikationsguerrilla” bezeichnen.[30]

30 Vgl. autonome a.f.r.i.k.a.-gruppe / Sonja Brünzels / Luther Blissett: Handbuch der Kommunikationsguerrilla, Berlin, Göttingen, Hamburg 1997.

Einzelaspekte

Elvi Claßen

Infopeace im Cyberspace?

Hacker erklären Irak und China den Krieg[31]

Es war nur eine Frage der Zeit, bis eine Meldung wie diese die globale Internet-Gemeinde aufwühlen würde: “Hacker erklären Irak und China den Krieg”. Die Nachricht war am 29.12.1998 über “HNN”, das Hacker News Network, im Netz verbreitet worden. Auf einer Online-Pressekonferenz, so hieß es in der HNN-Mitteilung, hätten die “Legions of the Underground” (LoU) dazu aufgerufen, “die Computersysteme in beiden Ländern vollständig zu zerstören”. Nähere Einzelheiten zur Begründung ihrer “Kriegserklärung” lieferten die LoU in einem eigenen Statement: “In einer sehr hitzigen und emotionalen Diskussion erklärten die Legions of the Underground letzte Nacht den Cyber War gegen die Informations-Infrastruktur in China und im Irak. Sie verweisen auf gravierende Menschenrechtsverletzungen durch die Regierungen beider Staaten sowie auf das jüngste Todesurteil gegen zwei Bankräuber in China und die Produktion von Massenvernichtungswaffen im Irak als Begründung für ihren Angriff.” Und weiter heißt es: “Wir sind bereit loszuschlagen und - wenn das gewünscht wird - die elektronische Kriegsführung zu unterstützen.” Dem Aufruf vorausgegangen waren laut HNN mehrere Angriffe der Hacker auf eine am 26. Oktober 1998 neu ins Netz gestellte offizielle Informationsseite, mit der China “beabsichtige, sein angeschlagenes Image im Hinblick auf die Menschenrechte im Land aufzupolieren”. Am 27.10.98 hätten die LoU diese Seite “unkenntlich gemacht”, am 1.12. sei es einem LoU-Mitglied außerdem gelungen, die zentralen Schutzprogramme des chinesischen Computernetzes anzugreifen. Während sich Anfang des Jahres mehrere Hackergruppen als Unterstützer der “Kriegserklärung” meldeten, revidierte die LoU am 6. Januar ihre Stellungnahme und erklärte, man habe zu keiner Zeit destruktive Absichten verfolgt; die Medien trügen die Schuld, daß die Sache eskaliert sei.

Mit einer bisher beispiellosen Initiative antwortete ein Zusammenschluß von sieben der “wichtigsten Hackergruppen der Welt” (HNN) am 7. Januar auf die LoU-Aktion und verurteilte sie in einer gemeinsamen Erklärung scharf. Der Chaos Computer Club, einer ihrer Herausgeber, bietet den Text auf seiner Internet-Seite unter dem Titel “Infopeace: Antwort auf die ‘Kriegserklärung’ der LoU ...” an. Darin heißt es u.a.: “Wir widersetzen uns energisch jedem Versuch, die Macht des Hackens dazu zu benutzen, die Informations-Infrastruktur eines Landes zu bedrohen oder zu zerstören, aus welchem Grund auch immer. Einem Land den “Krieg” zu erklären, ist das Unverantwortlichste, das ein Hacker tun kann. ... Weltweit versuchen Regierungen den Cyberspace als neues Schlachtfeld ... zu vereinnahmen. ... Mit ihrer dramatischen Ankündigung spielen [die LoU] den Politikern in die Hände, die die uneingeschränkte Kontrolle über das Internet anstreben ... Wenn Hacker sich als paramilitärische Splittergruppen andienen, wird das Hacken bald allgemein als Kriegshandlung gesehen und die Hacker als legitimes Ziel kriegführender Staaten. ... Die Unterstützer dieser Erklärung bitten die Hacker, auf alle Aktionen zu verzichten, die die Informations-Infrastruktur eines Landes zerstören könnten. Unterstützt keine

31 Dieser Artikel erschien zuerst in ZivilCourage 1/1999, S. 14.

Art von “elektronischer Kriegführung”. Haltet die Kommunikationsnetze lebendig, sie sind das Nervensystem für menschlichen Fortschritt.”

Zwar erklärten die LoU am 13. Januar gegenüber dem Computermagazin Wired, die Pressekonferenz am 29.12.1998 sei ein Schwindel gewesen und niemand kann ihnen das Gegenteil beweisen. Aber die technischen Möglichkeiten für einen solchen Angriff sind gegeben, das bestätigt auch der Direktor für “Information Warfare Studies” am halbstaatlichen Washingtoner Center for Strategic and International Studies (CSIS): “Der Informationskrieg ist nicht mehr länger nur ein Thema für Science Fiction-Stories. In einer 1998 durchgeführten Übung der US-Armee bewies eine Gruppe von 35 Computerfachleuten, daß sie in der Lage wäre, Teile der Stromversorgung und des militärischen Abwehrsystems der USA lahmzulegen. Die Software dazu war auf Hackerseiten im Internet frei verfügbar.” Das Szenario eines solchen “strategischen Informationskriegs”, in dem “nichtstaatliche Akteure” die elektronische Infrastruktur eines Landes angreifen, liefert die Begründung für die o.g. Aufrüstungsmaßnahmen und Versuche, restriktive Beschränkungen für die Internetnutzung durchzusetzen.

Aber von diesen “Verteidigungsmaßnahmen” bis hin zu einem offensiven Gebrauch der Hackertechniken ist es offenbar auch auf staatlicher Ebene nicht mehr weit, wie folgende Beispiele zeigen: Im Herbst ’98 hatten serbische Hacker einen Internet-Anbieter in der Schweiz gezwungen, eine kosov@-albanische Zeitung aus dem Netz zu nehmen. Die FR schrieb am 17.10.98, serbische Geheimdienstkreise könnten für die Erpressung verantwortlich sein. Das Internet-Magazin Telepolis berichtet im Januar ’99, Unbekannte hätten in einer vernetzten Aktion (gleichzeitig 18 Angriffe von verschiedenen Kontinenten aus) die Seite einer Initiative für ein freies Osttimor angegriffen und unleserlich gemacht. Der Netzbetreiber bringt indirekt die indonesische Führung mit dem Anschlag in Verbindung: “Das wird die neue Form des Krieges sein. Man wird sehen, daß diese Taktiken zu einem Bestandteil der offiziellen Regierungspolitik und zu einer potentiellen Waffe werden.”

Der “Informationskrieg”, dezentral, international und mit unabsehbaren Risiken, ist bereits im Gange, wenn auch noch auf einem niedrigen Niveau. Die “Kriegserklärung” der LoU hat in dieser Situation unter den Hackern einen Diskussionsprozeß angestoßen, der längst überfällig war. Bisher genießt die politisch motivierte Hackerszene - auch über Hackerkreise hinaus - ein recht positives Image, nicht zuletzt, weil sie mit ihrem überragenden Knowhow insbesondere durch das Entlarven vermeintlich sicherer Computersysteme, durch Aktionen gegen rassistische oder militaristische Netzangebote usw. immer wieder Aufsehen erregt. Daß aber etwa eine Clique schlechtgelaunter Teenager aus den eigenen Reihen einen Angriff gegen Staaten in Erwägung ziehen könnte, bricht mit dem in der Szene bisher allgemein akzeptierten Ehrenkodex: “Viele Hackergruppen haben kein Problem damit, fremde Web-Seiten zu manipulieren, um so öffentlich auf Menschenrechtsverletzungen hinzuweisen. Aber wir reagieren sehr empfindlich auf Leute, die Computernetzwerke ... in repressiven Staaten oder anderswo zerstören wollen.” (Frank Rieger, Chaos Computer Club). Was können jedoch die “guten Hacker” wirklich dagegen tun, daß sich “Abweichler” für den Kriegsdienst im Netz rekrutieren lassen oder tatsächlich einmal die Sache “in die eigenen Hände nehmen”? Und wie können sie verhindern, daß die von ihnen im Internet

bereitgestellte Software nicht, wie oben beschrieben, auch von den “Bösen” benutzt wird? Ihr Appell “Unterstützt keine Art von “elektronischer Kriegführung” ist wichtig, kann aber nur ein erster Schritt sein, dem eine der Situation angemessene Auseinandersetzung über die eigene politische Rolle und weitere, über das Bekenntnis zur Gewaltfreiheit hinausgehende Aktivitäten folgen müssen.

Quellen

Amerikanische Cracker spielen Cyber-Rambos (7.1.99, www.heise.de/tp/deutsch/inhalt/te)

Bricht ein Goldenes Zeitalter des “Hacktivismus” aus? (11.11.98, www.heise.de/tp/deutsch/special)

Confusion Over 'Cyberwar' (12.1.99, www.wired.com)

Crackerangriff auf das virtuelle Osttimor (26.1.99, www.heise.de/tp/deutsch/special)

Crackers Call Off 'War' (8.1.99, www.wired.com)

Cybercrime... Cyberterrorism... Cyberwarfare... (10.12.98, www.csis.org/goc/taskinfo)

Cyber-Krieg, nein Danke! (13.1.99, www.spiegel.de/netzwelt/themen/hackerkrieg)

Cyberwar averted, but what now? (15.1.99, www.msnbc.com/news)

Cyberwar China s p l 0 i t (6.1.99, www.webking.com)

Hacker News Network. LoU China Iraq War (2.1.99, www.hackernews.com)

Hackers On Planet Earth Against Infowar (7.1.99, www.ccc.de)

Serbische Hacker erpreßten Internet-Abieter mit Computerabsturz (17.10.98, www.fr-aktuell.de/fr/spezial/kosovo)

Olivier Minkwitz

Atomwaffen und das Computer 2000 - Problem[32]

Das sogenannte Jahr 2000-Problem (Y2K) läßt viele Amerikaner unruhig schlafen. Denn jede Woche werden neue Problemfelder entdeckt, die davon betroffen sein könnten, wenn zum Jahresende die digitale Datumsangabe von 1999 auf 2000 springt. Von der Nahrungsmittelproduktion, der Flugverkehrskontrolle bis hin zu militärischen Frühwarnsystemen, funktioniert heute kein technologisches Großsystem ohne Computer. Doch auch das andere Extrem, die optimistische Sorglosigkeit und Nachlässigkeit insbesondere bei Atomwaffen, kann zum Problem werden. Zwar sind sich die Experten einig, daß ein alter Computerchip in einer Atombombe am Silvesterabend keine atomare Explosion auslösen wird. Dennoch ist auch bei den scheinbar sicheren Nuklearsprengköpfen erhöhte Aufmerksamkeit geboten. Atomraketen werden durch ein Kommando-, Kontroll- und Kommunikationssystem (Command, Control and Communication - C) eingesetzt. Genau dieses hochkomplexe System könnte auf Grund eines Softwarefehlers bei der Jahresumstellung jedoch versagen. Ebenfalls geht eine Gefahr vom russischen Frühwarnsystem aus, das nach Zeitungsberichten wegen Geldmangel langsam veraltert, zerfällt und funktionsuntüchtig wird.[3] Deshalb wird es höchste Zeit, daß noch vor Jahresende amerikanische und russische Atomraketen und Bomben in ihrem Alarmbereitschaftsstatus weiter herabgesetzt ("De-Alerting") oder ganz aus dem Betrieb genommen und abgerüstet werden. Bislang aber weigert sich die US-Regierung diesen Schritt zu tun. Als Antwort darauf sind auch die russischen Militärs nicht dazu bereit. Amerika steht mit dem Atomwaffen-Y2K-Problem nicht alleine da. Jedoch ist bisher von den anderen offiziellen Atommächten so gut wie gar nichts über ihr Y2K-Problem und Atomwaffensicherheit an die Öffentlichkeit gelangt.

Das Jahr 2000-Problem

Im Prinzip ist das Jahr 2000-Problem eine Glaubensfrage. Entweder man ist der Überzeugung, daß es ein wirkliches Problem ist, oder man hält es schlicht für einen technischen Hype, mit dem sich einige Softwarefirmen und Programmierer eine goldene Nase verdienen wollen. Trotzdem sollte dem Problem und seinen Auswirkungen auf Atomwaffen einige Aufmerksamkeit geschenkt werden, damit an Silvester wirklich nur mit Feuerwerksraketen geschossen wird.

Die ganze Aufregung und die Millionen an US-Dollar, die jetzt für die Überprüfung von kommerzieller und militärischer Computersoftware ausgegeben werden, rührt daher, daß man sich in den 70er Jahre wenig Gedanken über den Datumswechsel am Ende des Jahrtausends machte. Als Hardware noch teuer war, mußten Programmierer sparsam mit dem Speicherplatz umgehen. Jedes Byte und jede Programmzeile zählte. Infolge dessen ließ man die ersten zwei Stellen bei der Datumsangabe weg. Nun steht man vor dem Problem, daß einige Rechner das Jahr 2000 als das Jahr 1900 interpretieren und das moderne Computerzeitalter gleich zu

32 Dieser Artikel erschien zuerst online in telepolis (http://www.heise.de/tp) und in der antimilitarismus information, Nr. CHECK/1999.

3 Washington Post, 10.2.99.

Beginn des nächsten Jahrtausends in ein globales Chaos stürzen könnte.[33] Dabei wird es unmöglich sein, alle Computerbauteile und jeden Programmcode zu testen, um eine alte Programmzeile in einem unwichtigen Computerbauteil zu finden, die möglicherweise das Großsystem zum Abstürzen bringt.

Die größte Gefahr, so befürchten Experten, geht von zivilen Großsystemen wie der Flugsicherung und besonders von Atomkraftwerken aus.[34] Atomwaffen und Interkontinentalraketen (ICBM) sind nicht im selben Maße vom Jahr 2000-Problem betroffen wie kommerzielle Großsysteme. Trotzdem legen die Militärs nicht alle Karten auf den Tisch und halten Informationen über mögliche Auswirkungen auf US-Atomwaffen zurück.[35] **Daß eine Atombombe gezündet oder eine Interkontinentalrakete durch einen Y2K-Fehler gestartet wird, ist nahezu unmöglich.[36]** Für das Militär und die nuklearen Streitkräfte ergeben sich jedoch indirekt erhebliche Probleme durch den digitalen Datumswechsel, die nicht vernachlässigt werden dürfen. Außerdem können Fehlfunktionen bei Atomraketen und Sprengköpfen zu anderen Unfällen führen, bei denen Radioaktivität freigesetzt werden kann. Außerdem sind Atomwaffen selbst nur ein Teil innerhalb eines System, das von den Atomwaffenlabors, die die Bomben entwickeln, bis hin zu Satelliten im All reicht, die einen Raketenabschuß melden. Solche "Makrosysteme" sind aufgrund ihrer Komplexität sehr anfällige Risikosysteme. Gefährlich wird dieses System dadurch, daß sich noch mehr als 4000 amerikanische und russische Atomraketen gegenüberstehen, die innerhalb von 30 Minuten bei einem nuklearen Schlagabtausch ins Ziel gebracht werden können. Ein kleiner Y2K Computerfehler oder eine Fehlinterpretation von Computerdaten durch einen Offizier, können in diesem schmalen Zeitfenster zu fatalen Folgen führen.

Mit was die C-Kommandoketten zum Jahreswechsel zu rechnen haben zeigte ein Test des nordamerikanischen Frühwarnsystems. Als das *North American Aerospace Defense Command (NORAD)*, das ein dichtes Netz von Satelliten, Radar und Kommunikationsnetzen zur Überwachung der Aktivitäten der russischen Nuklearstreitkräfte betreibt, für eine Simulation 1993 das Datum auf den 1. Januar 2000 stellte, schaltete sich das ganze System ab.[3]

33 Neben dem 31.12.1999 besteht noch eine weitere Serie von Datumsproblem: 29.2.2000 (Computer müssen das Schaltjahr mit 366 Tagen erkennen) 1.10.2000 (Oktober ist der erste zweistellige Monat) etc.. Darüber hinaus funktioniert das Global Positioning System (GPS), das z.B. die neuste Version der Tomahawk Cruise Missile in Ziel bringt, nicht nach dem Julinaischen Kalender, sondern nach einem internen Datum, das oftmals mit dem Baujahr beginnt. Vgl. Kraig, Michael. "January First is not the only Problem" In: Bulletin of the Atomic Scientists, March/April 1999, S. 40.

34 Expertenrunde während des "Nuclear Y2000 Symposium" am 8. März 1999 in Washington, DC. So könnte es zum Beispiel ein kalter Winter für die Bewohner Berlins werden, wenn ein alter russischer Rechner bei GAZPROM ausfällt, und die Erdgasversorgung zusammenbricht.

35 Der Bericht des Joint Chiefs of Staff und der STRATCOM über “Year 2000 Compliance on Nuclear Command and Control“ wurde bis jetzt nicht der Öffentlichkeit zugänglich gemacht.

36 Kraig, Michael. "Safe or sorry: The "Y2K" problem and nuclear weapons". In: Bulletin of the Atomic Scientists, March/April 1999, S.40.

3 Kraig, Michael. "The Bug in the Bomb. The Impact of the Year 2000 Problem on Nuclear Weapons." BASIC Research Report 98.0 Washington, DC/London 1998. S. 11.

Die Sicherheit von Atomsprengköpfen, abgeschaltete Interkontinentalraketen, menschliche Fehler und Y2K

Atomsprengköpfe sind durch zwei voneinander unabhängig funktionierende elektronische Sperren vor dem versehentlichen oder unerlaubten Zünden gesichert.[37] Ein Sensor *(Environmental Sensing Device)* verhindert, daß ein Sprengkopf durch gewaltsame Einflüsse von außen zur Explosion gebracht wird. Die zweite Sperre *(Permissive Action Links)* macht eine unauthorisierte Zündung unmöglich. Wird eine Sicherheitsmaßnahme umgangen, wird der Sprengkopf automatisch abgeschaltet und eine Explosion unmöglich gemacht. Eine nukleare Detonation durch Y2K ist deshalb so gut wie ausgeschlossen, auch wenn diese Sicherungssysteme selbst Y2K anfällig sein sollten.[38] Das Schlimmste, was passieren kann ist, daß sich sämtliche Atomsprengköpfe in der Silversternacht von alleine abschalten. Genau darin aber sieht das Strategic Command ein Problem für die Einsatzbereitschaft ihrer Waffen durch Y2K.

Nicht nur die Elektronik im Sprengkopf der Bombe ist Y2K anfällig. Eine andere Problemquelle ergibt sich aus den Trägersystemen. Atomraketen enthalten kleine Computer, die die monatliche Wartung überwachen. Wenn die Datumsanzeige auf "00" springt, könnten die Sicherheitschips und Wartungssysteme dies so interpretieren, als habe seit 1900 keine Wartung mehr stattgefunden und würden dann die Raketen bzw. Sprengköpfe automatisch abschalten. Alle weiteren Funktionen würden dadurch blockiert werden.[39] Damit wären die Nuklearstreitkräfte für einige Zeit außer Gefecht gesetzt.

Ebenso kann die Zielgenauigkeit der ICBMs durch ein nichtfunktionierendes Leitsystem, das während des Fluges die Zielkoordinaten übermittelt, abnehmen. Zum Beispiel ist in der Minuteman-III-Rakete eine elektronische Zielsteuerung eingebaut, die auf mathematischen Operationen basiert, die Datumsangaben enthalten *könnten*.[40] Dieses Phänomen könnte für den gegenwärtigen Kosovo-Krieg böse Folgen haben. Cruise Missiles werden durch das Globale Positions System (GPS) in das Ziel gesteuert, dessen Datumswechsel schon ein paar Monate vor dem Jahreswechsel von Experten erwartet wird.[41] Die interne GPS Uhr basiert auf einer relativen Datumsangabe, die sich von der absoluten Zeitangabe nach unserem Julianischen Kalender unterscheidet. Relative Datumsangaben können zum Beispiel mit dem Baujahr beginnen. GPS könnte in diesem Falle schon ab dem 22. August 1999 Cruise Missiles vom Kurs abbringen, auch wenn das Pentagon sagt die militärischen Anwendungen von GPS seien Y2K-tauglich.

Schließlich besteht noch die Gefahr, daß durch ein mangelhaftes Wartungs- und Sicherheitssystem ein Kurzschluß und ein Brand entstehen und dadurch Radioaktivität freigesetzt werden könnte. Der Brand des Treibstoffes einer Trident II Rakete kann Temperaturen von über 1000 Grad Celsius erreichen, denen die

37 Thomas B. Cochran, William M. Arkin, Robert S. Norris, Milton M. Hoenig. "Nuclear Weapons Databook Series Volume I: U.S. Nuclear Forces and Capabilities". S. 30-31.

38 Kraig, Michael: "Safe or sorry", S. 40.

39 Kraig, Michael. "The Bug in the Bomb", S. 12.

40 Ebenda S. 13.

41 vgl. Anm. 3.

Sprengkopfummantelung standhält. Dies kann zur Explosion des konventionellen Sprengsatzes in den W76 und W88 Sprengköpfen und zur Verseuchung weiterer Gebiete führen.

Ein weiteres Problem ergibt sich aus dem Zusammenspiel von Mensch und Maschine. Wenn ein Computer ausfällt und deshalb improvisiert werden muß, steigt die Gefahr, daß Fehler gemacht werden. Im Falle komplexer Systeme, wie Atomkraftwerken, Flugsicherung und Nuklearwaffen, kann dies unabsehbare Folgen haben.

Komplexität und Redundanzen

Atomwaffen werden von der Risiko-Fachterminologie als "ein System innerhalb eines Systems" bezeichnet.[42] Das bedeutet, daß Atomwaffen von der Makroperspektive aus gesehen nur ein System innerhalb des komplexen Systems von Nuklearwaffenlabors, Raketensilos und C-Frühwarnsystemen sind. Das Makrosystem wird zur Hochrisikotechnologie, wenn die Koppelung und die Interaktion zwischen den Einzelsystemen sehr eng bzw. hoch ist.[3] Unter Koppelung versteht die Risikotheorie Systeme, die in Folge voneinander, ähnlich wie Fließbänder, abhängen. Interaktion findet man in Systemen, die mit anderen Teilsystemen verzahnt sind oder mehrere Funktionen gleichzeitig ausführen. Zusätzliche Sicherheitssysteme (Redundanzen) bringen in solchen Systemen paradoxerweise keine zusätzliche Sicherheit, sondern machen Systeme noch komplexer und damit risikoanfälliger.

Genau diese prekäre Situation findet sich im Makrosystem der Nuklearwaffen wieder. Die Kommandostellen sind deshalb voneinander abhängig und eng verzahnt. Immer noch sind die amerikanischen Interkontinentalraketen in hoher Alarmbereitschaft *(Hair Trigger Alert)* und können innerhalb von einer Minute aktiviert werden. Die kurze Reaktionszeit kann so zum tödlichen Problem werden, wenn zum Jahreswechsel ein Softwarefehler fälschlicher Weise auf dem Radarschirm anfliegende Raketen zeigt und schnelles Handel gefordert ist. Da helfen auch nicht die voneinander unabhängigen Frühwarnsysteme am Boden (Radarstationen) und im All (Satelliten). Schon einmal interpretierte das russische Frühwarnsystem den Abschuß einer norwegischen Rakete zur Erforschung des Wetters als einen nuklearen Angriff.[43]

Löcher im Käse

Besonders Besorgnis erregend ist der Zustand des russischen Frühwarnsystems, der sich mit der anhaltenden ökonomischen Krise zunehmend verschlechtert. Zu Sowjetzeiten bestand das russische Überwachungssystem aus 9 geostationären und kreisenden Satelliten und einigen Radarstationen am Boden. Aufgrund der chronischen Finanzkrise wurden die alten Satelliten nicht mehr durch neue ersetzt, so daß mittlerweile nur noch drei funktionierende Satelliten einen Raketenabschuß

42 Perrow, Charles. "Normale Katastrophen: die unvermeidbaren Risiken der Großtechnik." Frankfurt a.M. 1989.

3 Ebenda.

43 Vgl. antimilitarismus information (ami), Nr. 3, 1995, S. 7f.

registrieren können.[44] Somit entstehen Überwachungslöcher im russischen Frühwarnsystem. Diese Lücken sind dazu noch größer geworden, da einige Bodenradars von Rußland nicht meht verwendet werden können, da sie sich in ehemaligen Sowjetrepubliken befanden. Den russischen Offizieren der Kommandostellen fehlen deshalb essentielle Informationen, mit denen ein Fehlalarm von einem wirklichen Angriff unterschieden werden kann. Y2K könnte hier die Situation verschlimmern, wenn noch weitere Systeme ausfallen, oder es zu Fehlanzeigen kommt.

Um diese Gefahr wenigstens etwas zu mildern, haben sich die USA bereit erklärt, den russischen Nuklearstreitkräften finanzielle und technische Hilfe zu leisten.[45] Im September gaben Jelzin und Clinton eine gemeinsame Erklärung über den Austausch von Informationen über Raketenstarts und Frühwarnung ab. Nun werden 190 Mio. US$ für ein gemeinsames Projekt zum Bau neuer Satelliten von den Amerikanern bereitgestellt. Den Russen wird ebenfalls erlaubt, neue Supercomputer und Sensortechnik zu kaufen. Ebenso wurde ein gemeinsames *“Center for Y2K and Strategic Stability”* in Colorado Springs, dem Sitz von NORAD und des *US Space Commands*, ins Leben gerufen, das den Informationsaustausch zwischen den Streitkräften sichern und somit vor einem versehentlichen Atomschlag schützen soll. Kritiker weisen jedoch darauf hin, daß der Datenaustausch nur schleppend in Gang kommt.

Silvesternacht - Wenn weltweit die Korken knallen

Y2K ist nicht nur auf die USA und Rußland beschränkt. Zwar sieht es derzeit ganz danach aus, weil die amerikanischen Medien dem Problem größere Aufmerksamkeit schenkten und Atomwaffengegner in Y2K die Chance zu weiterer nuklearer Abrüstung und zum *"De-Alerting"* sehen. Die Ungewißheit der Nuklearwaffensicherheit durch das Jahr-2000-Problem und das marode russische Frühwarnsystem sind Gründe genug, diesen Schritt, den auch Command und Control Experten schon lange fordern, endlich zu tun. Bislang sperrt sich das Pentagon vehement, die Alarmbereitschaft der Nuklearwaffen für den Jahreswechsel auszusetzen. Dahinter steht die Befürchtung des Militärs und des Nuklearwaffenkomplexes, daß Nuklearwaffen in ihrer sicherheitspolitischen Rolle herabgesetzt werden und an Bedeutung verlieren könnten, sobald einmal der Einsatzstatus der Waffen reduziert wurde.

Im Prinzip aber sind alle atomwaffenbesitzenden Staaten (China, Frankreich, Großbritannien, Israel, Indien und Pakistan) nicht vor dem Problem geschützt. Neueste Studien zeigen, daß den beiden neuen Nuklearstaaten, Indien und Pakistan, elementare Sicherheitssysteme wie die *Permissive Action Links* und C-Frühwarninstallationen, die die nukleare Stabilität zwischen den USA und Sowjetunion aufrecht erhielten, fehlen.[3] Die logische Konsequenz wäre ein

44 Washington Post, 10.2.1999.

45 Jane’s Defence Weekly, 29.3.1999.

3 Francois Heisbourg. The Prospects for Nuclear Stability between India and Pakistan. In: Survival, Jg. 40, Nr. 4 (Winter 1998/99). S. 85f.

weltweites *“De-Alerting”* und eine weltweite nukleare Abrüstung. Solange dies unmöglich ist, bleibt zu hoffen, daß an Silvester nur die Sektkorken knallen.

Links zum Thema:

Militär

Department of Defense Year 2000 Oversight and Contingency Planning Office
http://www.c3i.osd.mil/org/cio/y2k

Joint Staff Year 2000 Homepage http://www.dtic.mil/jcs/j6/j6v

US Strategic Command http://www.stratcom.af.mil

Army Y2K Web Site http://www.army.mil/army-y2k

Andere

Year 2000 Research Center http://www.cio.com/forums/y2k/index.html

Technology: The Millennium Bug, MSNBC
http://www.msnbc.com/news/TECHY2K_Front.asp

Year 2000 Ressources, Computerworld
http://www.computerworld.com/res/year_2000.html

Olivier Minkwitz

Clinton ließ Atomkoffer auf dem NATO-Gipfel zurück[46]

Bill Clinton ließ auf dem NATO-Gipfel Ende April in Washington den Offizier mit dem Koffer, der die nuklearen Optionen für einen Nuklearkrieg enthält, stehen.[47] Für 45 Minuten war der amerikanische Präsident und Oberbefehlshaber der Streitkräfte vom wichtigsten Gepäckstück der Welt getrennt. Der Präsident verließ das International Trade Center vorzeitig mit der Staatslimosine ohne den Begleiter, der den Koffer ständig bei sich trägt, mitzunehmen. Der Offizier, der sich immer in unmittelbarer Nähe des Präsidenten aufhält, wurde in der Hektik des Gipfels nach einer vorzeitig beendeten NATO-Konferenz zurückgelassen und mußte die 1,5 km zum Weißen Haus zu Fuß zurückgehen.

Die Aktentasche - die den militärischen Scherznamen "Fußball" trägt - enthält das Handbuch und eine Bedienungsanleitung für den Präsidenten. Mit Hilfe von Kartoons sind darin die verfügbaren nuklearen Optionen und die Auswirkungen für jedermann leicht verständlich dargestellt.[48]

Für die Sicherheit des Koffers und somit für die Kommunikation zwischen dem Präsidenten der Vereinigten Staaten und den Nuklearstreitkräften ist das Verbindungsbüro des Pentagon im Weißen Haus zuständig.

In der Regel wird jeder Präsident in die Handhabung des Koffers beim Amtsantritt eingewiesen. Seit den 80er Jahren geschah dies jedoch nicht immer nahtlos und nach Angaben eines ehemaligen Direktors der Verbindungsstelle im Weißen Haus, weiß der Präsident nicht einmal, wie der Koffer zu öffnen ist. "Sollte der Offizier, der den "Fußball" trägt, eine Herzattacke bekommen oder bei einem Attentat ums Leben kommen, dann müßte das verdammte Ding aufgesprengt werden", sagte der Direktor in einem Interview.[49]

Außer dem Präsidenten bekommen jeweils der Vizepräsident, der Verteidigungsminister, der Generalstab und die Oberbefehlshaber der nuklearen Teilstreitkräfte eine Version des Handbuches. Letztere geben in der Regel die Kommandoautorität nach unten ab, für den Fall, daß die militärische Elite bei einem nuklearen Angriff ausgeschaltet oder die Kommandostruktur unterbrochen wird.[50] Eine ganze Reihe anderer nichtmilitärischer Personen, die nach amerikanischem Gesetz als Nachfolger des Präsidenten in Frage kommen, so zum Beispiel der Sprecher des Repräsentantenhauses, der Sprecher des Senates und der Außenminister, werden nicht mit dem Handbuch versehen.

46 Dieser Artikel erschien zuerst online in telepolis (http://www.heise.de/tp) und in der antimilitarismus information (ami), Nr. CHECK 1999.

47 New York Times, 25.4.1999; Washington Times, 25.4.1999.

48 Stephen I. Schwartz ."The Football" in ders.(Hg.): "Atomic Audit. Cost and Consequences of US Nuclear Weapons since 1940". Brookings Institution Press: Washington, DC 1998. S. 222 (http://www.brook.edu/fp/projects/nucwcost/box3-4.htm).

49 Paul J. Bracken. "The Command and Control of Nuclear Forces". Yale University Press: London u. New Haven 1983.

50 Bruce G. Blair. "Strategic Command and Control". Brookings Institution Press: Washington, DC 1985.

Selbst der Vizepräsident Johnson wußte nach der Ermordung von John F. Kennedy 1963 zunächst nichts von der Existenz und dem Inhalt des Koffers, der während der Eisenhower-Administration in den 50er Jahren eingeführt wurde.

Im Gegensatz zum weithin verbreiteten Glaube enthält der Koffer nicht *den* Zündschlüssel oder Abschußknopf für die Atomraketen. Im Koffer sind neben dem *SIOP*-Handbuch wahrscheinlich auch die persönlichen Codes enthalten, die der Präsident braucht, um sich gegenüber den Kommandeuren der Nuklearstreitkräfte als Oberbefehlshaber zu identifizieren.[51] Nur so kann der Präsident den Einsatz der Waffen autorisieren. Die Autorisierungscodes werden vom Geheimdienst (National Security Agency - NSA) erstellt. Außer dem Präsidenten haben die nationalen Kommandostellen der nuklearen Teilstreitkräfte im Pentagon und über das Land verteilte Befehlsstellen die Autorisierungscodes. Das Pentagon hält sich somit technisch die Möglichkeit offen, die Raketen auch ohne die Autorisierung durch den Präsidenten zu zünden. Nachgeordnete Militärkommandeure brauchen die persönlichen Codes des Präsident nicht zur Aktivierung und Zündung der Raketen, falls sich dieser nicht identifizieren kann.

Ebenso wird auch der *"Single Integrated Operational Plan" (SIOP)*, der die einprogrammierten Ziele der Atomraketen enthält, fast jährlich überarbeitet.[52] Die Folge davon ist, daß nicht immer sicher gestellt ist, daß der Präsident oder sein legaler Nachfolger als Oberkommandeur der Nuklearstreitkräfte über die nuklearen Optionen im Bilde sind und die Atomwaffen im Notfall befehligen können.

Die Probleme mit der Sicherheit der Identifizierungscodes sind nicht neu. In der Vergangenheit wurden die Codes schon öfter verlegt. Nach einem Attentatversuch auf Ronald Reagan war der Koffer verschwunden und tauchte erst nach mehreren Stunden wieder auf.

Der Sprecher des Weißen Haus meinte zu der jüngsten Panne nur, "wir sind sicher".

51 Einige Präsidenten trugen diese Codes in der Hosentasche oder im Geldbeutel.

52 Hans M. Kristensen. "The Living SIOP" in ders.: "Nuclear Futures: Proliferation of Weapons of Mass Destruction and US Nuclear Strategy". BASIC Research Reports: Washington u. London 1998. S. 9f.

Ralf Bendrath

Der Kosovo-Krieg im Cyberspace[53]

"Es macht Spaß, zu sehen,
wie High-Tech an der Front eingesetzt wird."
Bill Gates bei den US-Marines[54]

Im Mai dieses Jahres schreckte das US-Nachrichtenmagazin Newsweek die Öffentlichkeit mit einer nach Science-Fiction klingenden Meldung auf: Hacker des US-Geheimdienstes CIA seien dabei, in die Computer ausländischer Banken einzubrechen und Milosevics Konten zu löschen. Autorisiert sei dieser Plan von US-Präsident Bill Clinton selber.[55] Sind damit die in Schundromanen[56] und Hollywoodproduktionen[57] schon seit einigen Jahren verbreiteten Visionen vom virtuellen Krieg Wirklichkeit geworden? In der Tat beschäftigen sich die US-Streitkräfte und Geheimdienste seit mehr als zehn Jahren mit dieser Art der Kriegführung, und auch in anderen Ländern werden Visionen vom Cyberkrieg entwickelt und futuristische Planungspapiere geschrieben. Der stellvertretende US-Verteidigungsminister John Hamre bezeichnete den Krieg gegen Jugoslawien bereits im April als den ersten Cyberkrieg, den die USA führen.[58]

Ein Blick hinter die Kulissen, soweit er möglich ist, relativiert dieses Bild in mehreren Richtungen: Für den Ausgang des Kosovo-Krieges waren die Cyberattacken relativ unbedeutend, und auch die Kriege der Zukunft werden nicht unblutig im Internet stattfinden. Neu ist allerdings, daß sich mit politisierten Hackergruppen bisher ungewohnte Kriegsparteien auf dem virtuellen Schlachtfeld tummelten. Dies zeigt, wie unkontrollierbar solche Pläne der staatlichen High-Tech-Eliten sind, wenn sie in die Realität umgesetzt werden. Zum übergreifenden amerikanischen Konzept des "Informationskrieges" gehört aber nicht nur die Manipulation von Bankkonten, sondern vor allem der Medien. Dies ist das eigentlich Entscheidende am Kosovo-Krieg: Wichtig ist nicht mehr der Sieg auf dem Schlachtfeld, das es in diesem Luftkrieg ohnehin nicht gab, sondern die Manipulation seiner medialen Repräsentation.

Elektronische Belagerung der NATO aus Jugoslawien

Kurz vor Ostern meldete die NATO einen jugoslawischen Angriff aus dem Cyberspace. Die "Attacke", die von einem Belgrader Computer ausging, war

53 Dieser Artikel erschien zuerst in der antimilitarismus information (ami), Heft 7/1999 und online in telepolis, 19.7.1999 (http://www.heise.de/tp). Er wurde gekürzt nachgedruckt in der Jungle World (Berlin) vom CHECK sowie in Megafon (Bern). Die vorliegende Fassung ist eine im November 1999 an einigen Stellen aktualisierte Version für die FifF-Kommunikation, Nr. CHECK.

54 FR, 18.11.1997

55 Gregory L. Vistica: "Cyberwar and Sabotage" in: Newsweek, 31.5.1999, S. 22

56 Zum Beispiel Tom Clancy / Steve R. Pieczenik: Netforce, Berkley Publishing Group, 1999

57 Zum Beispiel James Bond: Goldeneye

58 http://www.infowar.com/mil_c4i/99/mil_c4i_042399a_j.shtml

allerdings bei genauerem Nachlesen lediglich eine Massensendung von tausenden Emails, die das elektronische Postfach des Militärbündnisses für andere Besucher mehrere Tage lang unzugänglich machte. Frank Rieger, Sprecher des *Chaos Computer Club (CCC)*[59], hält es sogar für wahrscheinlicher, daß die NATO sich einen Computervirus wie "Melissa" eingefangen hat.[60] Dieser Virus, der die Adreßverzeichnisse von Email-Programmen benutzt, um sich selbsttätig zu verbreiten, hatte im März bereits im Pentagon sein Unwesen getrieben.[61]

Dennoch: Nach den veröffentlichten Informationen wurden die internen Datennetze der westlichen Militärinstitutionen, aber auch das öffentliche World Wide Web, von serbischer Seite ins virtuelle Visier genommen. Nach einem Bericht von *US News* existiert in Belgrad ein Netz von mehr als tausend StudentInnen und SchülerInnen in sechs Computerzentren, die die kriegsbedingten Ferien nutzen, um im Internet gegen die NATO aktiv zu werden. Der größte Teil ihrer Tätigkeit besteht aus dem Füttern von Newsgroups[62] und der Pflege ihrer umfangreichen Webseite, aber der Mail-Müll könnte ebenso wie die Viren von hier gekommen sein.[63] Nach Informationen von Infoworld.com wurden mindestens fünf neue Computerviren mit diesen Emails auf die NATO-Rechner übertragen.[64]

Bei einer anderen Art der Angriffe auf die öffentlichen Server der NATO wurde die Internet-Funktion "Ping" genutzt, mit der an einen Rechner ein kleines Datenpaket gesendet wird, das dieser an den Absender zurückschickt.[65] Ende März wurde die NATO - wie bereits verschiedene andere Institutionen vor ihr - Opfer massenhafter Ping-Anfragen, was dazu führte, daß die Rechner überlastet waren und die Datenleitungen verstopften.[66] Diese Angriffe kamen nach Aussagen des Pentagon ebenfalls aus Serbien, aber nicht unbedingt von Rechnern der serbischen Regierung.[67] Genau wie die massenhafte elektronische Post nutzt diese Art der Angriffe reguläre Funktionen aus, die bei entsprechend häufigen Aufrufen den Rechner zu stark beschäftigen. Bekannt sind solche Angriffe als "Denial of Service Attacks".

Über diese recht simple Art der Störungen hinaus gehen die Angriffe auf diverse Webseiten. Hacker aus Serbien sind in Webserver aus NATO-Staaten eingedrungen und haben die dort abrufbaren Internet-Seiten verändert. Die serbische Hackergruppe *CHC* etwa ersetzte Anfang April die Webseiten zweier US-

59 Der CCC ist die Vereinigung der deutschsprachigen Computerfreaks und Hacker. http://www.ccc.de.

60 SZ, 10.4.99

61 http://www.infowar.com/mil_c4i/99/mil_c4i_042399a_j.shtml

62 elektronische Diskussionsforen

63 U.S. News & World Report, 10.5.1999, http://www.usnews.com/usnews/issue/990510/10info.htm

64 Elizabeth de Bony: NATO reinforces against Net attack from Serbs, InfoWorld Electric, 2.4.1999, http://archive.infoworld.com/cgi-bin/displayStory.pl?99042.einato.htm

65 Ping ist für diagnostische Zwecke gedacht, um festzustellen, ob die Verbindung noch besteht und der Rechner arbeitet. Aus der Laufzeit der Pakete lassen sich auch Rückschlüsse auf die Leitungsqualität ziehen.

66 CNN, 31.3.1999, http://www.cnn.com/WORLD/europe/9903/31/nato.hack/

67 http://www.infowar.com/mil_c4i/99/mil_c4i_042399a_j.shtml

Regierungseinrichtungen sowie der britischen Stadt Croydon durch eine Anti-NATO-Seite, in der diese als “National American Terrorist Organisation” bezeichnet wurde.[68]

Alle diese Angriffe richteten sich gegen die öffentliche Darstellung der NATO oder von NATO-Staaten im World Wide Web. Die Kriegführungsfähigkeit der Militärallianz war dabei nicht gefährdet, denn die internen Kommunikatons- und Kommandonetze verlaufen über ganz andere Kanäle. Die Kommunikation zur Leitung der Kriegseinsätze ist nicht direkt über das Internet oder andere öffentliche Netze zugänglich, und die Sicherheitsvorkehrungen sind hier weitaus größer als bei einem Webserver oder Mailboxrechner. Zudem laufen auf den Militärcomputern teilweise Programme und Betriebssysteme, die auf dem freien Markt nicht erhältlich sind und bei denen es daher schwierig ist, sicherheitsrelevante Informationen zu bekommen.

Einen Schritt weiter als die Web-Hacker sind daher Versuche, in die Militärcomputer selber einzudringen. Auch dies wurde im Kosovokrieg versucht. Einen ernsthafteren Schaden hat nach Berichten der Belgrader Zeitung “Blic” ein Mitglied der serbischen Hackergruppe “Schwarze Hand” angerichtet. Er soll Ende März in einen Computer der Navy eingedrungen sein und alle Daten gelöscht haben. Obwohl das US-Verteidigungsminsiterium diesen Vorfall nie bestätigte, war der Rechner zeitweilig im Internet nicht erreichbar. Die gleiche Hackergruppe, die angeblich in der Tradition einer gleichnamigen serbischen Terrororganisation vom Anfang des Jahrhunderts steht, hatte bereits im Oktober 1998 die Webseite des gemäßigten Albanerführers Ibrahim Rugova gehackt.[69]

Internationale Hacker-Brigaden

Als Reaktion auf die Bombardierung der chinesischen Botschaft in Belgrad durch die USA haben auch chinesische Hacker mehrfach Webseiten amerikanischer Institutionen angegriffen. Mindestens zweimal wurde das Internet-Angebot der amerikanischen Botschaft in Peking durch den Text “Nieder mit den Barbaren!” ersetzt, ähnliches widerfuhr den Seiten des Energieministeriums, auf denen plötzlich zum Protest gegen die “amerikanischen Nazi-Methoden” aufgerufen wurde.[70] Dort stand auch zu lesen “Wir sind chinesische Hacker, die sich nicht um Politik kümmern, aber wir dulden es nicht, wenn wir sehen müssen, daß chinesische Journalisten getötet worden sind.”[71] Auf der Webseite des US-Innenministeriums tauchten Anfang Mai Bilder von den drei Zivilisten auf, die beim Angriff auf die chinesische Botschaft getötet worden waren.[72] Auch gegen die Internet-Darstellung des Weißen Hauses wurden Angriffe unternommen, und die Seite war drei Tage lang nicht online. Obwohl der Sprecher des Weißen Hauses dies mit “Denial of Service”-Angriffen begründete,

68 Betroffen waren in den USA das Los Alamos National Laboratory und das Ohio Department of Development, http://freespeech.org/resistance

69 Royal United Services Institute, Newsbrief, Mai 1999, S. 39.

70 Spiegel Online, 10.5.1999, http://www.spiegel.de/netzwelt/politik/0,1518,21796,00.html

71 Florian Rötzer: Chinesen protestieren auch im Internet, telepolis, 10.05.99, http://www.heise.de/tp/deutsch/inhalt/te/2834/1.html

72 Spiegel Online, 10.5.1999, http://www.spiegel.de/netzwelt/politik/0,1518,21796,00.html

wurde die Nachricht von einem erfolgreichen Einbruch auf der Seite in verschiedenen Hackerforen annonciert.[73]

Auch die russische Ablehnung der NATO-Angriffe wurde nicht nur vom Kreml auf dem diplomatischen Parkett vertreten. Eine russische Hacker-Gruppe mit dem Namen *From Russia With Love*[74] hat eine NATO-Webseite mit dem Vermerk "Haut ab aus dem Kosovo" versehen. Eine Koalition von vier russischen Hackergruppen mit dem Namen *Russian Hackers Union* soll eine Webseite der amerikanischen Marine gelöscht haben.[75] Die Seite einer amerikanischen Windsurfer-Zeitschrift wurde von dem russischen Hacker *SP* durch einen Aufruf ersetzt, den Krieg gegen Jugoslawien zu beenden. Ein Link verwies auf eine jugoslawische Seite, die zu einer Webkampagne gegen die NATO-Angriffe aufruft.[76] Nach Angaben des *Hacker News Network* wurden während des Krieges mindestens 14 militärische oder andere staatliche Webseiten gehackt.[77]

Von der anderen Seite der virtuellen Front gab es verschiedene Angriffe gegen jugoslawische Computer, die ebenfalls nicht staatlich kontrolliert wurden. Hacker aus den USA haben laut Informationen des *Boston Globe* versucht, die Webseite der jugoslawischen Regierung zu knacken, die als extrem sicher gilt. In der *Kosovo Hackers Group* haben sich albanische und europäische Hacker zusammengeschlossen, um gegen die serbische Regierung Cyberguerrilla zu spielen. Ihnen soll es gelungen sein, fünf verschiedene Webseiten zu löschen und auf deren Adresse die schwarz-rote Flagge "Freiheit für Kosovo" zu plazieren. Die serbische Regierung gab zwischenzeitlich auf der Webseite ihrer virtuellen Presseabteilung zu, daß sie technische Probleme hatte. Die Ursachen dafür können aber auch ganz banal zerbombte Telefonleitungen oder Kraftwerke gewesen sein.[78] Die hollandische Hackergruppe *Dutchthreat* hackte sich in eine private serbische Webseite, auf der die NATO als "eine Bande Nazis" bezeichnet worden war. Sie ersetzten die Anti-NATO-Seite mit einer eigenen "Helft Kosovo"-Seite.[79]

In Mitleidenschaft gezogen wurden auch Webseiten in unbeteiligten Staaten. So wurde u.a. die Internet-Präsenz einer ägyptischen Regierungseinrichtung von der russischen Hackergruppe *KpZ* durch ein Bild der MTV-Comicfiguren Beavis & Butthead ersetzt, die zum "Stop der NATO-Morde" aufrufen.[80] Eine private Seite in Brasilien enthielt plötzlich einen Aufruf gegen Milosevic.[81]

73 Sehr übersichtlich ist z.B. das *Digital R3sist4nc3 Archive of Hacked Websites*, http://freespeech.org/resistance.

74 Eine Anspielung auf den James Bond-Film "Liebesgrüße aus Mokau"

75 SZ, 10.4.1999; http://freespeech.org/resistance/nmimc1/med_navy_mil.htm.

76 Die Protestseite ist http://www.alert.org.yu/stopnato.html, vgl. http://freespeech.org/ resistance/ windsurfer/ www_americanwindsurfer_com.html.

77 http://www.hackernews.com/archive/crackarch.html

78 SZ, 10.4.1999

79 Ellen Messmer: Kosovo cyber-war intensifies, in: Network World Fusion, 12.5.1999, http://www.nwfusion.com/news/1999/0512kosovo.html

80 http://freespeech.org/resistance/kpz/nato.html. Das gleiche Bild wurde von KpZ einen Tag später auf einer NASA-Seite hinterlassen.

81 http://freespeech.org/resistance/genetic/berlin_genetic_com_br.html

Politisierte Computerfreaks als Cyberkrieger?

Während Hacker früher ihr Haupinteresse im Aufdecken von Sicherheitslücken sahen, ist dies heute eher Mittel zum Zweck geworden - und die Zwecke der Hacker werden immer politischer. Die Politisierung des Hackens führt inzwischen, analog zur außerparlamentarischen Tradition, auch zu Bündnisbildunden und Koalitionen, wie die *Russian Hackers Union* oder die *Kosovo Hackers Group* zeigen. Diese neue Verbindung von Computerfreaks und und politischem Aktivismus wird mittlerweile als "Hacktivismus" bezeichnet und auf eigenen Webseiten und Mailinglisten diskutiert.[82] Die New Yorker Gruppe *Electronic Disturbance Theater* (EDT) hat bereits das Programm *FloodNet* für gemeinsame Webseiten-Besetzungen von Internetsurfern aus aller Welt entwickelt. Diese virtuelle Form des Sit-in erzielt einen "Denial of Service", indem alle an einer Aktion Beteiligten gleichzeitig eine Webseite besuchen, die von *FloodNet* dann automatisch immer wieder aufgerufen wird.[83] Im September 1998 kam es bereits zu einem virtuellen Schlagabtausch zwischen dem EDT, das ein Cyber-Sit-In auf der Pentagon-Webseite angekündigt hatte, und der Defense Information Systems Agency (DISA), die für die Sicherheit der US-Militärcomputer verantwortlich ist und zurückschlug.[84]

Im Dezember 1998 hatte die Hackergruppe *Legions of the Underground* China und dem Irak den virtuellen Krieg erklärt und dies mit den Menschenrechtsverletzungen begründet. Das selbsterklärte Ziel war es, die Computersysteme in beiden Ländern vollständig zu zerstören.[85] Solche Aktionen sind in der Hackerszene sehr umstritten: Zum einen spiegelt sich in der Parteinahme für oder gegen einen bestimmten Staat die politische Heterogenität der Computerfreaks wider, zum anderen widersprechen virtuelle Kriegserklärungen der klassischen gewaltfreien Hacker-Ethik. Die sieben wichtigsten Hacker-Vereinigungen der Welt, darunter auch der deutsche *Chaos Computer Club* und die Gruppe *Cult of the Dead Cow* verurteilten die Ankündigung der *Legions of the Underground* in einer gemeinsamen Erklärung in aller Schärfe.[86] Bislang ist der dringend nötige Diskussionsprozeß in der Hackerszene noch nicht sehr weit fortgeschritten, z.B. ist völlig unklar, ob Taktiken wie das im Umfeld des *Electronic Disturbance Theater* entwickelte *Bottom Up Information Warfare* oder der "elektronische zivile Ungehorsam" als Guerillakampf oder gewaltfreier Widerstand bewertet werden sollen bzw ob diese Begrifflichkeiten aus der physischen Welt im Cyberspace überhaupt angemessen sind. Was auffällt ist aber, daß die Hacker seltener als früher versuchen, in die Computersysteme einzubrechen, die für militärische Operationen notwendig sind. Mit dem Hacken von Webseiten

82 http://hacktivism.tao.ca

83 Vgl. Stefan Wray: The Electronic Disturbance Theater and Electronic Civil Disobedience, 17.6.1998, http://www.nyu.edu/projects/wray/EDTECD.html; EDT-Homepage: http://www.thing.net/~rdom/ecd/ ecd.html

84 Winn Schwartau: Cyber-civil disobedience. Inside the Electronic Disturbance Theater's battle with the Pentagon, Network World, 11.1.1999, http://www.nwfusion.com/news/0111vigcyber.html

85 Vgl. Elvi Claßen: Infopeace im Cyberspace?, in: ZivilCourage, Nr. 1/99, S. 14.

86 LoU strike out with international coalition of Hackers: A joint statement by 2600, the Chaos Computer Club, the Cult of the Dead Cow, !Hispahack, L0pht Heavy Industries, Phrack and Pulhas, 7.1.1999, http://www.ccc.de/CRD/CRD19990107.html

beeinflussen sie aber nur die mediale Repräsentation des Krieges, nicht seinen Verlauf. Offenbar glauben auch die Hacker, daß der computergestürzte Webdiskurs über den Krieg immer wichtiger wird und die Bedeutung der realen Kriegführung abnimmt.

Bankraub für den Frieden? Umstrittener Cyberkrieg der CIA

Ende Mai gelangten die Information über die Cyberangriffe der CIA auf die internationalen Bankkonten des jugoslawischen Präsidenten Slobodan Milosevic an die Öffentlichkeit. Milosevic soll nach Erkenntnissen der Geheimdienste Millionenbeträge bei Banken unter anderem in Rußland, Griechenland und Zypern deponiert haben. US-Präsident Bill Clinton hat laut Newsweek den Hackern der CIA die Genehmingung erteilt, in die Computer dieser Banken einzubrechen, um das Geld auf den privaten Auslandskonten des jugoslawischen Präsidenten “zu verplempern”, so ein US-Beamter. Im Gegensatz zu den bisher genannten Aktionen, die sich direkt gegen eine der Kriegsparteien richteten oder lediglich einen Webserver manipulierten, sind in diesem Fall die Bankencomputer von unbeteiligten Staaten unter Beschuß der USA geraten. Der NATO-Partner Griechenland wäre damit unter virtuelles “friendly fire” geraten. Das Weiße Haus weigerte sich, die Meldung zu kommentieren, und nicht einmal die NATO-Verbündeten waren in die Pläne eingeweiht. Das Vorhaben war laut Newsweek Teil eines umfassenderen Planes, der auf einem Vorschlag des nationalen Sicherheitsberaters Sandy Berger beruhte. Da die US-Regierung ebenso wie der Kongreß und die Öffentlichkeit vor einem Bodenkrieg zurückschreckte, Milosevic aber mit Luftangriffen offenbar nicht beizukommen war, griff der amerikanische Sicherheitsapparat auf ein Mittel zurück, das bereits Tradition hat: Verdeckte Operationen. Neben eher traditionellen Methoden[87] waren auch die Hackerangriffe der CIA in die Banken vorgesehen.[88]

Der Realitätsgehalt dieser Geschichte ist umstritten: Laut Aussagen des Chaos Computer Club ist es technisch möglich, über das internationale Bankensystem Swift Überweisungen zu fälschen. Geheimdienste wie wie amerikanische *National Security Agency (NSA)* seien dazu in der Lage.[89] Einige US-Geheimdienstmitarbeiter, die von den Plänen wußten, äußerten sich dagegen skeptisch über die Möglichkeit der geplanten Cyberangriffe. Um in gut gesicherte Bankencomputer einzudringen, müßten CIA-Agenten zunächst selber jede dieser Banken besuchen, ein eigenes Konto einrichten und danach sorgfältig darüber Buch führen, wie die Institution arbeitet. Erst wenn Schwachstellen in der Datensicherheit gefunden seien, könne die NSA ihre Rechenzentren einsetzen, um die hochentwickelte Verschlüsselung und die vorgeschalteten Schutzwechner (“Firewalls”) zu überwinden.[90]

87 Die CIA sollte danach albanische Rebellen für Sabotageaktionen ausbilden, mit denen die serbische Bevölkerung gegen ihren Präsidenten aufgebracht werden sollte. Zu den Ausbildungszielen gehörten u.a. Häusersprengungen, der Diebstahl von Lebensmittelvorräten oder die Verunreinigung von Benzinlagern.

88 Gregory L. Vistica: “Cyberwar and Sabotage” in: Newsweek, 31.5.1999, S. 22

89 zdf-news, 2.6.1999

90 Gregory L. Vistica: “Cyberwar and Sabotage” in: Newsweek, 31.5.1999, S. 22

Hintergund und politische Folgen

CCC-Sprecher Rieger warnte davor, diese Art der virtuellen Nebenschauplätze für eine ungefährliche Erweiterung des Schlachtfeldes zu halten. Die USA, Deutschland und andere westliche Staaten seien aufgrund ihrer fortgeschrittenen Digitalisierung und Vernetzung weitaus verwundbarer gegenüber solchen Attacken als die Transformationsländer in Osteuropa. “Die Eskalationsmechanismen sind kaum beherrschbar”, so Rieger.[91] Mitglieder der Geheimdienstausschüsse von Kongreß und Repräsentantenhaus in den USA, die von Sicherheitsberater Berger Mitte Mai in einer geheimen Sitzung über die virtuellen Banküberfälle der CIA gegen Milosevic informiert worden waren, äußerten sich ebenfalls besorgt. Eine solche Aktion gegen ausländische Banken würde nicht nur gegen mehrere internationale Verträge verstoßen und NATO-Mitglieder wie Griechenland gegen die USA aufbringen, es könne auch die führende Rolle der USA im weltweiten Bankgeschäft untergraben. Außerdem sei dieser Bruch der Souveränität sogar von verbündeten Staaten ein gefährlicher Präzedenzfall und lade zur Nachahmung, also zu Angriffen auf US-Banken, geradezu ein.[92]

Monate nach dem Kosovokrieg kam dann ein laues Dementi aus dem Pentagon: Man habe den elektronischen Bankraub und andere weitergehende Cyberkriegs-Optionen erwogen, aber nach einer Prüfung durch die Rechtsabteilung des Ministeriums davon Abstand genommen.[93] Lediglich eine elektronische Täuschung des serbischen Luftabwehrsystems sowie Störungen des Telefonnetzes sind demnach durchgeführt worden.[94] Die völkerrechtlichen Implikationen solcher virtuellen Kriegführung sind nämlich bislang völlig unklar, und die US-Streitkräfte wollten sich nicht der Gefahr aussetzten, hinterher als Kriegsverbrecher angegriffen werden zu können. Die USA würden einen serbischen Hacker, der ähnliches an einer New Yorker Bank versucht, im übrigen als “Cyberterroristen” bezeichnen.

Eine mögliche Eskalation von Cyberangriffen und -gegenangriffen kann sich unter Umständen zu einer ernsten Bedrohung der USA entwickeln, die immerhin die am weitesten vernetzte Gesellschaft der Welt sind. Ein von Hackern veranstalteter elektronischer Börsencrash ist seit einigen Jahren der Alptraum der amerikanischen Sicherheitspolitiker, der von den Behörden kräftig genährt wird.[95] Allein in der US-Exekutive beschäftigen sich mehr als 15 Ministerien und Behörden konzeptionell und operativ mit Fragen der “Computerkriegführung” oder Computersicherheit, neben dem Verteidigungsminsterium, der CIA und dem FBI unter anderem auch die Ministerien für Energie, Justiz, Wirtschaft, Finanzen oder Transport sowie

91 zdf-news, 2.6.1999

92 Gregory L. Vistica: “Cyberwar and Sabotage” in: Newsweek, 31.5.1999, S. 22

93 Bradley Graham: Military Grappling With Guidelines For Cyber Warfare. Questions Prevented Use on Yugoslavia, Washington Post, 8.11.1999.

94 Immerhin gelang es der US Air Force nach eigener Darstellung, den Serben durch einen Hack in die Luftverteidigungssysteme falsche Ziele auf die Bildschirme zu spielen. Lisa Hoffman: Special Report. U.S. opened cyber-war during Kosovo-Fight, Washington Times, 25.10.1999.

95 Das beliebte Schlagwort dafür ist “elektronisches Pearl Harbour”, das an den Überfall der japanischen Luftwaffe auf die US-Navy im Zweiten Weltkrieg erinnert, vgl. http://www.soci.niu.edu/~crypt/other/harbor.htm

verschiedene Abteilungen des Weißen Hauses.[96] Zur Abwehr der neuen Verwundbarkeiten der Informationsgesellschaft wurde erst im vergangenen Jahr mit der Präsidenten-Direktive 63 das *National Infrastructure Protection Center (NIPC)*[97] eingerichtet, das zur Bundespolizei FBI gehört, aber auch dem Pentagon unterstellt werden kann.[98] Die Zuständigkeiten sind bisher nur ansatzweise geklärt. Abgeordnete des US-Kongresses warnten bereits davor, daß die Hacker der verschiedenen staatlichen Stellen sich bei ihren Aktivitäten gegenseitig im Weg stehen könnten.[99] Während an der elektronischen Verteidigung gegen Hackerangriffe bereits überall in den USA gearbeitet wird, gibt es für die Entwicklung offensiver Computerkriegsfähigkeiten, also Hackerprogramme, ferngesteuerte Computerviren und ähnliches, bisher keine Grundsatzentscheidung des Präsidenten.[100]

Im Hintergrund arbeiten bereits seit den achtziger Jahren verschiedene staatliche Stellen in den USA an der Erforschung dieser Methoden. Mitarbeiter von CIA und NSA verzeichneten nach eigenen Angaben “beachtliche Erfolge dabei (...), geheime militärische Computersysteme in der Sowjetunion und anderen Ländern zu penetrieren”[101]. Auch die Streitkräfte beteiligen sich seit Ende der achziger Jahre an der Erforschung und Entwicklung von Computerviren, die auch als “nicht-tödliche Waffen” bezeichnet werden. Die staatlichen “Informationskrieger” beziehen dabei einen großen Teil der offensiv verwendbaren Software aus Hackerkreisen.[102]

Seit 1994 existiert bereits eine *School for Information Warfare and Strategy* an der *National Defense University* in Washington D.C., in der Offiziere der Streitkräfte für Informations- und Cyberkriege ausgebildet werden. Bereits 1995 war “Information Warfare” das Leitbild für alle Forschungs- und Entwicklungspläne der US-Streitkräfte[103], und 1996 wurde es in das zentrale Planungspapier der Vereinigten Stabschefs (die *“Joint Vision 2010”*) aufgenommen.[104] Die US Army hat ihre Doktrin

96 Vgl. z.B. Executive Order 13010 von Präsident Bill Clinton, 15.7.1996, wo die an der *Presidential Commission on Critical Infrastructure Protection* (PCCIP) beteiligten Einrichtungen aufgezählt werden, http://www.pccip.gov/eo13010.html.

97 http://www.fbi.gov/nipc/index.htm

98 Vgl. National Security Council: White Paper. The Clinton Administration´s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, Mai 1998, http://www.whitehouse.gov/WH/EOP/NSC/html/NSCDoc3.html

99 Bradley Graham: In Cyberwar, A Quandry Over Rules And Strategy, in: International Herald Tribune, 9.7.1998

100 David A. Fulghum: Cyberwar Plans Trigger Intelligence Controversy, in: Aviation Week&Space Technology, 19.1.1998, S. 55.

101 Jay Peterzell: Spying and Sabotage by Computer, in: Time, 20.3.1989, zit. nach Ute Bernhardt / Ingo Ruhmann: Der Krieg der elektronischen Waffen - Elektronische Kriegsführung, in: dies. (Hg.): Ein sauberer Tod. Informatik und Krieg, Marburg 1991, S. 123.

102 Douglas Waller: Onward Cyber Soldiers, in: Time Magazine, 21.8.1995

103Vgl. Ralf Klischewski/Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie, Studie für das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bonn 1995, S. vi.

104Vgl. John M. Shalikashvili: Joint Vision 2010, Joint Chiefs of Staff, Washington D.C. 1996, http://www.dtic.mil/ doctrine/jv2010/jv2010.pdf, S. 16

für Informationskriege bereits 1996 mit dem neuen Field Manual 100-6, "*Information Operations"*, formuliert.[105] Die Befehlshaber der Regionalkommandos wurden mittlerweile aufgefordert, ihre Einsatzpläne daraufhin zu überprüfen, inwieweit diese Techniken konventionelle Waffen ersetzen können. Alle diese Vorhaben zur offensiven Informationskriegführung unterliegen höchster Geheimhaltung und wurden bisher im Kongreß nicht öffentlich diskutiert.[106] Angehörigen der Streitkräfte war es bis letztes Jahr verboten, den Begriff "offensive computer operations" in öffentlichen Debatten zu verwenden.[107] Im Oktober 1998 wurde erstmals ein offizielles Dokument zur US-amerikanischen Informationskriegs-Strategie veröffentlicht, die Joint Doctrine for Information Operations (Joint Publication 3-13)[108].

Informationskrieg ist mehr als Cyberkrieg

Den Krieg um das Kosovo hat die NATO vor allem mit der Zerstörung der jugoslawischen Kommandostrukturen durch rohe Gewalt gewonnen, indem sie gezielt die Kommando- und Kommunikationseinrichtungen der jugoslawischen Streitkräfte bombardiert hat.[109] Diese Spielart des Informationskrieges, die in den USA *Command and Control War (C2-War)* genannt wird, macht die gegnerischen Truppen führungslos und schneidet sie von Aufklärungs- und anderen Daten ab.[110] Blind und auf sich selbst gestellt ziehen sie sich in der Regel zurück oder ergeben sich ohne größeren Widerstand, so zumindest die Erfahrung aus dem Golfkrieg 1991. Die von den Einheiten für psychologische Kriegführung (*PsyOps*) massenhaft verteilten Handzettel "Sie sind ein NATO-Ziel" haben ihr übriges dazugetan. Die paar Millionen Dollar dagegen, um die der jugoslawische Präsident durch die CIA-Hacker unter Umständen erleichtert worden ist, sind dagegen psychologisch wichtig, aber nicht kriegsentscheidend. Zu einem Informationskrieg gehört im amerikanischen Verständnis nämlich weit mehr als nur das Eindringen in gegnerische Computernetze.

Laut dem offiziellen Wörterbuch des Pentagon umfaßt Informationskrieg "Aktionen, die unternommen werden, um die Informationsüberlegenheit zu erlangen, indem die Informationen, informationsbasierten Prozesse, Informationssysteme und computerbasierten Netze beeinträchtigt werden, während die eigenen Informationen, informationsbasierten Prozesse, Informationssysteme und computerbasierten Netze

105 U.S. Army Training and Doctrine Command: Field Manual 100-6, Information Operations, August 1996, http://www.fas.org/irp/doddir/army/fm100-6

106 Bei einer Anhörung des Senates zur defensiven Seite der Informationskriegführung im Juni 1998 antwortete der CIA-Direktor George Tenent auf die Frage, ob offensive Fähigkeiten entwickelt würden, nur mit einem Satz: "We're not asleep at the switch in this regard", zit. nach Bradley Graham: In Cyberwar, A Quandry Over Rules And Strategy, in: International Herald Tribune, 9.7.1998.

107 Vgl. David A. Fulghum: Cyberwar Plans Trigger Intelligence Controversy, in: Aviation Week&Space Technology, 19.1.1998, S. 53.

108 http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

109 vgl. z.B. tagesschau-dossier, 25.5.1999, http://www.tagesschau.de/ts/archiv/1999/Mar/23/ kosovo/ M/chronologie/R/05-25-angriffe.html; NATO Press Conference, Given by Mr Jamie Shea and Major General Walter Jertz, 6.5.1999, http://www.nato.int/kosovo/press/p990506c.htm

110 Kerry A. Blount/Lauren D. Kohn: C^2-Warfare in FM 100-6, in: Military Review, Nr. 4, Juli-August 1995, S. 66-69

ausgenutzt und verteidigt werden"[111]. Demnach wird die *gesamte* "Informationsumgebung" nun zentral für die militärischen Planungen. Es gilt also, nicht nur die Computernetze des Gegners lahmzulegen, sondern auch seine Sensoren zu täuschen, die Bevölkerung zu beeinflussen und an der Heimatfront für die richtigen Kriegsbilder zu sorgen. Das Ziel ist die Kontrolle der globalen Informationssphäre und aller ihrer Teilbereiche im Umfeld eines Krieges. Die Ausweitung des Krieges auf den Cyberspace ist nur ein Bereich von den vielen Informationsarenen, die durch Informationsoperationen auf neue Art ins Interesse der Militärs rücken. Neben diesen neuen, von den Medien begierig aufgenommenen virtuellen Aufgaben werden auch so alte Techniken wie die Bombardierung gegnerischer Kommandostrukturen oder die psychologische Kriegführung unter dem Oberbegriff "Informationsoperationen" zusammengefaßt. Besonders die mediale Repräsentation des Krieges im Fernsehen wird als zentral angesehen.[112] Der damalige Vorsitzende der Vereinigten Stabschefs, General Colin Powell, brachte dies zur Zeit des Golfkrieges 1991 bereits auf den Punkt: "Wenn alle Truppen in Bewegung sind und die Kommandeure an alles gedacht haben, richte deine Aufmerksamkeit auf das Fernsehen, denn du kannst die Schlacht gewinnen oder den Krieg verlieren, wenn du mit der Story nicht richtig umgehst"[113]. In der Pentagon-nahen Denkfabrik RAND Corporation in Santa Monica wird inzwischen über die Aufstellung von "Special Media Forces" nachgedacht.[114]

In diesem erweiterten Verständnis des Informationskrieges reicht auch eine entsprechend glaubwürdig durchgesickerte Meldung über Computerattacken, wenn dadurch der Gegner unter Druck gesetzt werden kann. Die Banken-Geschichte der CIA könnte daher auch eine gezielte Falschmeldung gewesen sein. Nach der Doktrin der Informationsoperationen ist es aber vor allem für die NATO eminent wichtig, sich öffentlich als unangreifbar darzustellen. Insofern haben die Hacker-Angriffe zwar keinen militärischen, aber einen massiven Image-Schaden bei der NATO hinterlassen. NATO-Sprecher Jamie Shea mußte Ende Mai zugeben, daß die aufwendig gemachte NATO-Webseite zeitweise nur sporadisch erreichbar war - eine peinliche Situation für ein Militärbündnis, das gerade dabei ist, die Überlegenheit seiner High-Tech-Streitkräfte vorzuführen.[115]

111 DoD Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/jel/doddict/data/i/02944.html, Übersetzung R.B.

112 U.S. Army Training and Doctrine Command: Field Manual 100-6, Information Operations, August 1996, http://www.fas.org/irp/doddir/army/fm100-6

113 Zit. nach: McKenzie Wark: Virtual Geography. Living with Global Media Events, Bloomington, Indianapolis 1994, S. 41, Übersetzung R.B.

114 John Arquilla / David Ronfeldt: The Emergence of Noopolitik. Towards an American Information Strategy, Santa Monica 1999, S. 50f.

115 Press Conference of the NATO Spokesman, Jamie Shea and Air Commodore David Wilby, 31.5.19991.

Elvi Claßen

Konstruktion von Medienrealität im Kosovo-Krieg[116]

"Die westlichen Führer sind intensiv damit beschäftigt, die Geschichte umzuschreiben, um das Desaster der Bombardierung des Balkans zu rechtfertigen. Der Wandel in der Informationspolitik, in der Rhetorik und in den Begründungen, seit die Bombardierungen am 24. März begannen, lähmt buchstäblich die Sinne. So sehr sie sich auch davor fürchteten, haben sie ein wirklich dunkles Kapitel der Geschichte aufgeschlagen und sehen sich jetzt in der Gefahr, dass ihnen die Kontrolle über die Entwicklungen entgleitet. Eine Möglichkeit, das Versagen als Erfolg darzustellen, ist die Konstruktion einer mächtigen Medienrealität und die Dekonstruktion der realen Realität. Das ist die Essenz des Medienkrieges, und das ist, was gerade geschieht."
(Jan Oberg/TFF)[117]

Nach den Erfahrungen mit der internationalen Medienkommunikation im und über den NATO-Krieg gegen Jugoslawien muss die Bedeutung des Theorems "Das erste Opfer eines jeden Krieges ist die Wahrheit"[118] neu überdacht werden. Noch nie zuvor war die militärisch-politische Informations-Intervention im Krieg so vielschichtig und umfassend, so aggressiv und effektiv wie während der letzten Monate. Aber auch in diesem Kampf um die 'Lufthoheit' über die Herzen und Hirne der massenmedial vernetzten Weltgesellschaft' wurde die Wahrheit nicht erschlagen und unauffindbar verscharrt. Sie wurde bloß verleugnet, unterdrückt, deformiert, verstümmelt und bis zur Lächerlichkeit verkleidet auf den Umschlagplätzen des globalen Nachrichtenmarktes herumgetragen. Trotzdem war und ist sie immer noch da, doch nur die wenigsten wollten oder konnten sie sehen. Während im März/April die Propagandamaschine im Kriegsgebiet und an der "Heimatfront" auf Hochtouren lief, etablierte sich im World Wide Web, in Newsgroups und über E-Mail-Verteiler ein weltweites friedenspolitisches Informationsnetz. Dies macht die Differenz zwischen den 'offiziellen' Interpretationen der Kriegsursachen, Kriegsfolgen und Kriegsziele sowie dem, was in Wahrheit geschah oder geschehen sein könnte, so offensichtlich und öffentlich zugänglich, wie noch niemals in einem Krieg zuvor. Grund genug für einen Rückblick auf die letzten Monate im Hinblick auf die Differenz zwischen Kriegspropaganda und Wahrheit. Die Hauptakteure im Kampf um die Definitionsmacht der Interpretation von dem, was, warum und wie in diesem Krieg geschah, waren die Regierungen und Militärs, die Medien und die Friedensbewegung.

116 Dieser Artikel erschien zuerst in antimilitarismus information (ami) 7/99, S. 124-137. Er wurde leicht überarbeitet nachveröffentlicht online in telepolis (www.heise.de/tp/deutsch/special/info/6508/1.html). Die vorliegende Fassung entspricht der Telepolis-Fassung von Oktober 1999.

117 "Covering up NATO's Balkan Bombing Blunder", Pressemitteilung des Friedensforschungsinstituts Transnational Foundation for Peace and Future Research (TFF) in Lund/Schweden vom 14.4.99; Jan Oberg ist Direktor des TFF.

118 "The first casualty when war comes is the truth." Der vielzitierte Ausspruch aus dem Jahre 1917 stammt von Senator Hiram Johnson, 'Progressive Partei'; er war von 1910-1916 Gouverneur und ab 1917 Senator für den US-Bundesstaat Kalifornien.

Politik und Militär - die Konsensmaschine

Für Politiker und Militärs gilt der Waffengang im Kosovo als gelungener Testfall für künftige “Information Operations”, einem elementaren Bestandteil der “Information Warfare”-Strategie. Deren Ziel ist “Informationsüberlegenheit” (information superiority) im weitesten Sinne: “Die Dominanz über das Informationsspektrum ist so entscheidend für einen Konflikt, wie in früherer Zeit die Besetzung eines Landes oder die Kontrolle über den Luftraum.”[119] Vor dem Hintergrund der aktuellen politischen Konstellationen und Kriegsführungskonzepte bediente man sich dafür teils traditioneller Handlungsmuster, teils qualitativ neuer Techniken und Möglichkeiten.

Feindbildaufbau zur Legitimierung des Krieges

Als die Vorsitzende des internationalen Kriegsverbrechertribunals in Den Haag, Gabrielle Kirk McDonald, am 5. November letzten Jahres Jugoslawien zum “Schurkenstaat” erklärte[120], übernahm sie eine Diktion aus der US-Presidential Decision Directive/PD zur US-Atomkriegsstrategie von 1997. Die PD No. 60 sieht den Einsatz taktischer nuklearer Waffen gegen “Schurkenstaaten” (rogue states) vor, wobei unter Schurkenstaaten Staaten zu verstehen sind, “die schlechte politische Beziehungen mit Washington haben”[121]. In diesem Fall ist der Schurke Slobodan Milosevic. Allerdings musste eines der klassischen Instrument der Kriegspropaganda - die Dämonisierung des Feindes und die Rechtfertigung seiner Vernichtung aus moralischen Gründen - diesmal nicht nur die US-amerikanische Öffentlichkeit überzeugen, sondern insbesondere auch die der Bundesrepublik Deutschland. Von dieser hatte der ehemalige Verteidigungsminister Volker Rühe noch 1992 gesagt, dass sie aufgrund ihrer “Instinkte zehn Jahre (brauche), bis sie psychologisch für Kampfeinsätze gewappnet” sei[122]. Nicht zuletzt die willfährige Übernahme der Milosevic-Hitler-Analogie durch die neue Bundesregierung hat dafür gesorgt, dass es dann doch etwas schneller ging mit dem ersten Kriegseinsatz nach Ende des 2. Weltkrieges. So nutzte Verteidigungsminister Rudolf Scharping Anfang des Jahres den erstmaligen Besuch einer Abordnung der Bundeswehr in Auschwitz, um diesen Einsatz moralisch zu begründen: “Darum ist die Bundeswehr in Bosnien” und darum wird sie “wohl auch in den Kosovo gehen”.

Scharpings Hasstiraden (“Mordmaschinerie von Milosevic”, “bestialische” Verbrechen, “Völkermord”, “Schlachthaus”, “ethnische Säuberung”, “Selektierung”, “KZ”, “Blick in die Fratze der deutschen Vergangenheit”) und die gleichzeitige Diskreditierung derjenigen, die den Bonner Kriegskurs kritisierten - z. B. Joseph Fischer: “Weisswäscher eines neuen Faschismus” - sollten die Koordinaten für den

119 General Ronald R. Fogleman: Cornerstones of Information Warfare, zit. nach: Information Operations, Air Force Doctrine Document 2–5, August 1998, S. 1.

120 AP-Meldung vom 5.11.98.

121 Gary Seymour vom Nationalen Sicherheitsrat der USA; vgl. BASIC Press Release: US Nuclear Strategy and the Third World (1.3.98). Ausführlicher zum Konzept der “rogue states”: ami 2/99, S.22ff.

122 Berliner Zeitung, 22.6.92.

Zit. nach: “Die überaus nützliche Dämonisierung der Serben”, taz, 10.5.99.

Zit. nach: Dieter Keiner: “Die neue Auschwitz-Lüge in der Kriegspropaganda der Bundesregierung”, Rede auf der Anti-Kriegsdemonstration auf dem Prinzipalmarkt in Münster/Westfalen am 17.4.99. In

gesellschaftlichen Diskurs über die Unausweichlichkeit des Krieges liefern. Die Presse reagierte prompt darauf: Die Berliner B.Z. nannte Milosevic und seine Frau Mirjana Markovic den “Schlächter und seine Hexe”; im Spiegel hieß es die “Milosevic-Killer”. Die Bild-Zeitung titelte am 31.3. “Sie treiben sie ins KZ” und schrieb dazu: “Auch Verteidigungsminister Rudolf Scharping bestätigte: ‘Es gibt ‘ernste Hinweise’ auf Konzentrationslager der Serben. [...] Es gibt Anzeichen für eine systematische Ausrottung, die an das erinnert, was zu Beginn des Zweiten Weltkrieges in deutschem Namen angerichtet worden ist, zum Beispiel in Polen.’” Der öffentliche Eindruck von der Allgemeingültigkeit dieses Leitthemas wurde dadurch verstärkt, dass es in einer Art Feedbackschleife in den offiziellen Stellungnahmen der NATO und der am Krieg beteiligten westlichen Staaten immer wieder reproduziert wurde. So wiederholte z.B. der NATO-Sprecher Jamie Shea mehrfach seine Warnung, es drohe die "größte humanitäre Katastrophe in Europa seit Ende des Zweiten Weltkrieges"[123], der britische Premier Blair sprach - wie Scharping auch - von “Genozid”, sein Außenminister Robin Cook von einer “Endlösung”, die Milosevic für den Kosovo plane[124].

In der Frankfurter Rundschau vom 22.4.99 bewertete Eric Chauvistré den Vergleich von Milosevic mit Hitler und Stalin, den Außenminister Fischer in einem Interview mit dem US-Nachrichtenmagazin Newsweek benutzt hatte, als geprägt vom überkommenen Freund-Feind-Denken des Kalten Krieges. Die Dämonisierung des militärischen Gegners habe in der jetzigen Situation dazu geführt, “dass die NATO, wenn sie schon mit enormen militärischen Mitteln nicht in der Lage ist, das Elend im Kosovo zu verhindern, zumindest eine massive Bestrafung vornehmen möchte: Die jugoslawische Regierung, so der Tenor in Brüssel, Bonn, London und Washington, soll einen ‘hohen Preis’ für ihr Handeln zahlen. Es geht längst nicht mehr darum, [...] eine humanitäre Katastrophe in Kosovo zu verhindern’, wie Bundeskanzler Schröder noch in der ersten Bombennacht [...] ankündigte. Die Frage, ob Luftangriffe auf Jugoslawien Sinn machen und erfolgreich sind, wird in dieser Logik nicht mehr gestellt.”

Auch von seiten der Auschwitz-Überlebenden Esther Bejarano und Kurt Goldstein wurde die Analogiebildung zwischen Hitler und Milosevic scharf kritisiert. In einem Offenen Brief an Fischer und Scharping verurteilten sie deren Vorgehen scharf: “Wir Überlebenden von Auschwitz und anderen Massenvernichtungslagern verurteilen den Missbrauch, den Sie und andere Politiker mit den Toten von Auschwitz, mit dem von Hitlerfaschisten im Namen der deutschen Herrenmenschen vorbereiteten und begangenen Völkermord an Juden, Sinti und Roma und Slawen betreiben. Was Sie tun, ist eine aus Argumentationsnot für Ihre verhängnisvolle Politik geborene Verharmlosung des in der bisherigen Menschheitsgeschichte einmaligen Verbrechens. Weltfrieden und internationale Sicherheit werden jetzt gefährdet, indem

der Bosnien-Diskussion der Grünen (1995) hatte die sicherheitspolitische Sprecherin der Partei, Angelika Beer, diese Argumentation noch kritisiert: “Jetzt die Pazifisten als Schuldige darzustellen, nur weil sie vier Jahre nicht gehört worden sind, und sie jetzt zu fragen, was wollt ihr denn noch machen - das ist Kriegspropaganda.” Vgl.: taz-Interview, 2.8.95.

123 NATO press briefing am 28.3.99.

124 Reporters Sans Frontières (RSF), Pressemitteilung vom 15.6.99, vgl.: www.rsf.fr/ uk/ rapport/ nato/ nato.html.

gegen ein Gründungsmitglied der UNO Krieg geführt wird, Krieg von deutschem Boden aus. [...] Sich als Begründung für einen solchen Krieg auf Auschwitz zu berufen, ist infam."

Krieg - welcher Krieg?

Neben der Milosevic-Hitler-Analogie war die Begriffsbildung ein zweites wichtiges Element der Kriegspropaganda. Euphemismen wie "humanitäre Intervention", "NATO-Kampagne", "Luftschläge", "collateral damage", "soft targets" oder "impact errors" wurden massiv in Umlauf gebracht. Nach dem Willen einzelner Politiker gehören auch bestimmte Begriffe und Themen auf eine "schwarze Liste", weil sie im Widerspruch zur offiziellen Kriegsrethorik standen und stehen. Zu Beginn der Luftangriffe der NATO am 24. März erklärte Generalsekretär Javier Solana: "Lassen Sie mich klarstellen: Die NATO führt keinen Krieg gegen Jugoslawien." Fischer untersagte Journalisten das Wort "Kriegsflüchtlinge" und forderte als einheitliche Sprachregelung "Vertriebene" bzw. "Deportationen"[125]. In einem Spiegel-Interview erklärte er: "Wir führen keinen Krieg, wir leisten Widerstand, verteidigen Menschenrechte, Freiheit und Demokratie."[126] Auf Berichte, die als Widerspruch zu dieser Definition eingestuft wurden, reagierte man sofort: Als in der ersten Bombennacht in der Tagesthemen-Sendung darüber berichtet wurde, dass ein deutscher Tornado noch nicht zurückgekommen war, fluchte Rudolf Scharping. Auf der Pressekonferenz am folgenden Tag appellierte der Verteidigungsminister an die Verantwortlichkeit der Medien. Kaum waren die Mikrofone aus, berichtet ein Redakteur, habe Scharping explizit die 'Tagesthemen' kritisiert.[127] In Großbritannien griff Tony Blair höchstpersönlich ein, als es darum ging, den BBC-Chefkorrespondenten aus Belgrad abzuziehen; Blair hielt ihn für zu 'serbenfreundlich'.[128]

Die Schlacht der Nebelwerfer

Am 29. März gab die NATO in Brüssel bekannt, dass der Chefberater Ibrahim Rugovas, Fehmi Agani, und fünf weitere bekannte kosovo-albanische Intellektuelle[129] von serbischen Soldaten ermordet worden seien. Der britische General David Wilby - in der Brüsseler Zentrale während der 'Daily Operations Updates' zuständig für den militärischen Lagebericht - hatte die Bluttat gemeldet und sich auf "sehr zuverlässige Quellen im Kosovo" berufen. In der Woche darauf entpuppte sich die weltweit verbreitete Nachricht als Ente: alle sechs waren am Leben. Die "zuverlässige Quelle", so berichten die 'Reporters sans Frontières' (RFS)[130], sei das von Kosovo-Albanern im Exil geleitete Kosovo Information Centre in London. Fehmi Agani wurde drei Wochen später von der serbischen Armee ermordet. Das, so RFS, sei für die NATO dann aber kein Thema mehr gewesen; auch sei die ursprüngliche

125 Neue Rheinzeitung, 8.4.99.

126 Der Spiegel 16/99, S. 34ff.

127 taz, 8.5.99.

128 Ulrich Ladurner: Wahrheit ist das erste Opfer. In: Facts Nr. 18/99.

129 Darunter auch Baton Haxhiu, Herausgeber der albanisch-sprachigen Tageszeitung Koha Ditore.

130 Reporters sans Frontières (siehe Fußnote 10).

Falschmeldung nie zurückgenommen worden: “Wenn in der ersten Woche der Bombenangriffe auf diese Art ein Gerücht zur offiziellen Meldung gemacht wird, sieht das eher nach einer vorsätzlichen Entscheidung als nach einem Fehler aus: ein kleiner positiver Impuls in einer Zeit, in der die öffentliche Meinung über den Erfolg der NATO-Luftschläge eher skeptisch war.”[131]

Falschinformationen, verkürzte Informationen, Informationsbeschränkung und Informationssperren - die Mittel der militärisch-politischen Propaganda sind vielfältig, wenn es darum geht, die eigene Interpretation des Kriegsgeschehens zu “vermarkten”. Am 15. April allerdings stieß die NATO dabei erstmals an ihre Grenzen, als bekannt wurde, dass am Vortag bei Djakovica ein Flüchtlingstreck angegriffen worden war. **“**Das sieht nach einer gestellten Szene aus” zitierte die Nachrichtenagentur AP aus “NATO-Kreisen.”[132] Kenneth Bacon - der Sprecher des US-Verteidigungsministeriums - kommentierte, es gebe keine Hinweise auf zivile Opfer, die Zivilisten seien vielmehr als Vergeltung für die NATO-Angriffe von serbischen Flugzeugen angegriffen worden. Fast 24 Stunden später erst räumte die NATO ein, man habe “versehentlich” ein ziviles Fahrzeug in einem Konvoi getroffen, die Umstände, die zu diesem Unfall geführt hätten, lägen aber in der Verantwortlichkeit von Milosevic. Am 19. April hieß es dann aus Brüssel, dass zwei “Konvois” von NATO-Kampfflugzeugen bombardiert worden seien. Die Bilanz dieses Angriffs auf einen Flüchtlingstreck wurde später von unabhängigen Quellen veröffentlicht: 75 Tote, 100 Verletzte, meist Frauen, Kinder und Alte.[133]

Nicht nur die Medien kritisierten die Informationspolitik der NATO über dieses Bombardement; offenbar alarmierten die unkoordinierten Stellungnahmen aus Brüssel, Bonn, London und Washington auch die Informationsspezialisten in den eigenen Reihen: Am 17. April verabredete die “Media Strategy Group”[134] die Einrichtung eines ‘Media Operations Centre’ (MOC) in Brüssel. Die Leitung des MOC übernahm der Blair-Berater Alastair Campbell, der “als Genie des sogenannten ‘Spinning’ der Kunst, Nachrichten die gewünschte Interpretationsrichtung zu geben” gilt.[135] Campbell, “dem es im letzten Wahlkampf sogar gelungen war, das konservative Revolverblatt The Sun ins Blair-Lager zu ziehen”[136] trommelte 20 PR-Spezialisten aus Regierungen europäischer Länder und den USA - u.a. aus dem Nationalen Sicherheitsrat und dem Pentagon - zusammen und richtete im NATO-Hauptquartier einen “war-room” ein. Dort gebe es seit einer Woche, so meldete die Brüsseler NBC-Korrespondentin Linda Vester am 1. Mai, eine “veritable PR MASH unit of spin doctors”, deren Aufgabe es sei, “die Statements der NATO und der alliierten Verteidigungsministerien so zu koordinieren, dass sie ‘mit einer Zunge

131 Ebd.

132 FR, 16.4.99.

133 CounterPunch, Institute for the Advancement of Journalistic Clarity (Hg.): www.counterpunch.org/dead.html; 4.6.99.

134 Mit dabei die Elysée-Sprecherin Catherine Colonna, der Bonner Regierungssprecher Uwe-Karsten Heye, Joe Lockhart vom Weißen Haus und der Blair-Berater Alastair Campbell.

135 Die Welt, 19.4.99: www.welt.de/cgi-bin/out.pl?url=/archiv/1999/04/19/0419au03.htm.

136 SZ, 8.5.99.

sprechen'"[137] Campbells Leute redigierten fortan die Texte der NATO-Pressekonferenzen und faxten "jeden Morgen an die Hauptstädte eine 'Morning Message', die gelegentlich mit der Ansage beginnt: 'Heute morgen sollte klar sein...'"[138] "Die britischen Zeitungen warnen entsetzt: Wo die Nachrichten fatal seien, könne auch kein 'Spin Doctor' helfen. Da der Westen auf dem Balkan auch die Überlegenheit seiner Werte verteidige, dürfe er sich auf keinen Fall auf die Ebene der serbischen Propaganda begeben und mit gleicher Münze also mit 'Spinning', der subtilsten Form der Lüge zurückzahlen."[139]

Der Informationskrieg gegen Jugoslawien

Die zweite Flanke des Informationskrieges der NATO war die psychologische Kriegsführung gegen den Feind und der Kampf gegen seine Kommunikations-Infrastruktur: "In der dritten Kriegswoche hat ein offener Medienkrieg zwischen der Welt und den serbischem Medien begonnen. Er begann mit der Drohung eines NATO-Offiziers, dass auf Grund der Propagandalügen das Gebäude des staatlichen Fernsehens bombardiert würde, falls es nicht der Ausstrahlung von Programmen ausländischer Stationen – oder gar der NATO selbst – zustimme."[140] Noch am 12. April hatte NATO-Sprecher Shea auf eine Anfrage des Generalsekretärs der Int. Journalistenvereinigung, Aidan White, geantwortet: "Die alliierten Streitkräfte [werden] Radio- und Fernsehanlagen nur dann bombardieren, wenn sie sich innerhalb militärischer Anlagen befinden ... Die NATO hat nicht die Absicht, Sendeanlagen grundsätzlich zu bombardieren."[141] In den Morgenstunden des 23. April zerstörte die NATO das Gebäude des serbischen Rundfunks in Belgrad; 15 Menschen starben und 17 wurden verletzt. Allein in den ersten vier Wochen zerschossen alliierte Bomber 23 Rundfunktransmitter im Kriegsgebiet.

Zugleich begann die NATO, ein eigenes "Informationsprogramm" auszustrahlen. Spomenka Lazic, Korrespondentin des Alternative Information Network, berichtete aus Belgrad: "In den jeden Tag kürzer werdenden Pausen zwischen den Bombardierungen kreist ein spezielles Flugzeug im Luftraum, eine Lockheed Hercules C-130. Von dort aus strahlt ein NATO-Fernsehsender Propagandaprogramme in serbischer Sprache und mit in kyrillischer Schrift verfassten Botschaften aus, die an die Bürgerinnen und Bürger Serbiens gerichtet sind. [...] Ein namenloser und unsichtbarer Sprecher wünscht zunächst einen guten Tag: 'Hier ist die vereinigte Stimme der NATO - Ihr Informationskanal, der für sie Kommentare, Nachrichten und den musikalischen Hit des Tages vorbereitet hat.' [...] Das Thema der Sendung ist die Bösartigkeit des Kommunismus. [...] 'Neokommunisten werden erkennen, dass die NATO-Kampagne zu diesem Zeitpunkt

137 At NATO, a crash course in spin (1.5.99): www.msnbc.com/news/.

138 Der Spiegel, 20/99, S. 78 ff.

139 Siehe Fußnote 22.

140 Spomenka Lazic, Alternative Information Network (AIM): Bombardements und Medienkrieg (10.4.99): http://zoom.mediaweb.at/zoom/zoom_299/lazic.html.

141 Pressemitteilung des Int. Freedom of Expression eXchange (IFEX) Clearing House (13.4.99): www.ifex.org/.

die einzige Chance für die demokratisch gesonnene Bevölkerung ist, sich von dem einzigen noch verbliebenen Diktator in Europa zu befreien.'"[142]

Für William Church, Managing Director des Centre for Infrastructural Warfare Studies, haben die "Information Operations" (IO) in Jugoslawien für zukünftige Kriege Maßstäbe gesetzt: "Die Kosovo-Aktion erlaubte der NATO den Einsatz des vollen Arsenals von IO-Waffen. Sie benutzte Graphitbomben gegen die Infrastruktur, [...] offizielle Stellen der Air Force berichten von ausgedehnten Hacker-Eingriffen in das jugoslawische Luftabwehrsystem. [...] Beide Seiten betrieben eine umfassende psychologische Kampagne, deren Aktionsspektrum reichte vom Abwurf von Propagandaflugblättern aus Flugzeugen, auf denen vor einem erfundenen Angriff durch Bodentruppen gewarnt wurde, bis hin zu Hacker-Angriffen auf Internetseiten."[143]

Die Medien - das Öl im Getriebe der Konsensmaschine

Offenbar können sich die politisch und militärisch Verantwortlichen der bereits während des Golfkrieges 1991 selbst von professioneller Seite harsch - aber weitgehend folgenlos - kritisierten Loyalität der etablierten Medien auch weiterhin sicher sein. Die Journalistinnen und Journalisten übernahmen in der Mehrzahl die 'offiziellen' Interpretationen des Kriegsverlaufs und verbreiteten sie weiter. Die Folgen beschreibt Norman Solomons Anekdote über den US-Fernsehsender Fox: "Etwa eine Stunde bevor die ersten Raketen in Jugoslawien einschlugen, hörten die Zuschauer einen nachvollziehbaren Lapsus des Fox-Nachrichtenmoderators: 'Schalten wir jetzt um zu unserem Pentagon-Sprecher - Verzeihung - unserem Pentagon-Korrespondenten'."[144]

Die Verunsicherung der Presse war groß, aber dennoch reichte sie nicht aus, um den Warnungen, die auch aus den eigenen Reihen kamen, Rechnung zu tragen: "Lassen Sie sich nicht für Interessen der am Konflikt Beteiligten einspannen oder missbrauchen. Weder für die NATO noch für Jugoslawien. Berichten Sie über diesen Krieg authentisch und unabhängig. Halten Sie die handwerklich und ethisch gebotene Distanz zu allen Informationsquellen. Die Verantwortlichen in Funk- und Fernsehsendern fordern wir auf, Krieg nicht als "Quotenbringer" zu behandeln. Profit aus dem Krieg zu ziehen ist verwerflich, weil es die Opfer entwürdigt und missbraucht."[145] Doch statt dessen fügte man sich: entweder kriecherisch wie Eberhard "soft missile" Seidel von der taz: "Aber anstatt anzuerkennen, wie genau die NATO bislang die Ziele traf, die sie auch treffen wollte, wie stark, verglichen mit dem Irak-Krieg, die Bemühungen sind, die Zivilisten zu schonen, breitet sich nun

142 Spomenka Lazic, War with Information (21.5.99): www.aimpress.org/dyn/ trae/ archive/ data/ 199905/90521-001-trae-pod.htm; weitere Infos zur "EC-130E/RR" z.B. unter http://www.janes.com/ company/ press/ 210499jdw_briefs.html und http://www.janes.com/ defence/ features/ kosovo/ alliance.html.

143 William Church, Kosovo and the Future of Information Operations: www.infowar.com/info_ops/treatystudyio.shtml; Beispiele für Propaganda-Flugblätter der NATO ("Psychological Operations leaflets dropped on Kosovo") sind auf der Seite http://www.geocities.com/Pentagon/1012/kosovo2.html zu finden.

144 Norman Solomon, Building A Media Agenda For War (26.3.99): www.fair.org/media-beat/ 990326.html.

145 Zit. nach: Erklärung der IG Medien zum Kosovo-Krieg von März 99.

Entsetzen aus. Doch 1.000 zivile Opfer nach fünf Wochen Krieg, so die Angaben des Bruders Milosevic, sind eher ein Beleg für behutsame Bombardements."[146] oder aber mit ehrlichem Unbehagen, das sogar Karl Feldmeyer, den Bonner Korrespondenten der FAZ, erfasst hatte: In einer Diskussion im Frankfurter Presse-Club Ende Mai kritisierte er, dass die JournalistInnen zu Beginn des Kosovo-Krieges den Sprachgebrauch offizieller Verlautbarungen der "gottesdienstmäßigen" Pressekonferenzen unkritisch übernommen hätten. Er selbst habe "große Probleme" damit gehabt, "meine gute alte NATO des Angriffskrieges zu zeihen. Natürlich ist das ein Angriff, aber das ging mir schon unter die Haut".[147] Dass die KorrespondentInnen bei den Pressekonferenzen oder -briefings der NATO eher 'Gewehr bei Fuß' standen, beschreibt auch Jan Oberg von der TFF: "Ein Sprecher eröffnet die Show, sucht die Fragen aus und beantwortet sie mit vorgefertigten Formulierungen, die *nie* überraschend aber immer eloquent sind; dann heißt es 'die nächste Frage, bitte'. Seit dem 24. März haben die wichtigsten Repräsentanten der freien Presse *niemals* den Inhalt des Rambouillet-Diktats hinterfragt, *niemals* die Moral der NATO-Politik angezweifelt, deren destabilisierenden Auswirkungen hervorgehoben oder die Diskrepanz zwischen den erklärten Zielen und den Konsequenzen der NATO-Strategie. Man hat ihnen Fotos und Videos bombardierter Ziele vorgeführt und gesagt, 'das ist ein Panzer' oder 'das ist ein Munitionslager', und *niemand* von ihnen hat gefragt: 'Ich kann das nicht erkennen - wie können wir da sicher sein?'."

Aber anstatt sich nach authentischen und unabhängigen Quellen umzusehen, machten selbst die angesehensten US-amerikanischen Medienvertreter - wie in anderen Kriegen zuvor - den 'Bock zum Gärtner'. "Lawrence Friedman vom King's College/London kritisierte die Informationspolitik der NATO am 15. April in einem BBC-Interview: 'Die NATO behandelt Journalisten wie Pilze: Sie hält sie im Dunkeln und füttert sie mit nichts als Mist.' Am gleichen Tag schickten Chefredakteure und Herausgeber der New York Times, Los Angeles Times, NBC News, des Wall Street Journals, von CNN und Associated Press einen Brief an den US-Kriegsminister Cohen und forderten bessere und mehr Informationen über den Krieg."

Die Friedensbewegung - der Sand im Getriebe der Konsensmaschine

In der Konsequenz führte die Fixierung der JournalistInnen auf "offizielle" Quellen auch dazu, dass die Analysen, Forderungen und Aktionen der außerparlamentarischen Opposition gegen den Krieg in den etablierten Medien nicht vorkam. Dass diese an der Friedensbewegung traditionell wenig interessiert sind, ist ein alter Hut. Jahrelang hat man sich mehrheitlich, wenn überhaupt, "von außen" ein Bild von "der Friedensbewegung" gemacht, das mit der Realität kaum etwas zu tun hatte. Ob es nun an der "Schere im Kopf" lag, an der immer gerne mit 'berufsbedingter Skepsis' begründeten Distanz zu den Diskurs- und Organisationsstrukturen der Bewegung (Abgrenzung gegenüber dem als 'einseitig' wahrgenommenen- weil konsequenten - Antimilitarismus und Pazifismus) oder

146 taz-Kommentar, 30.4.99.

147 FR, 2.6.99.

Jan Oberg: The Information Warfare about Kosovo", Pressemitteilung des TFF, 15.4.99 (Hervorh. durch den Autor).

Scott Schaeffer-Duffy, Truth and War (16.5.99): www.nonviolence.org/amhvigil/CathRad.html.

schlicht an der Borniertheit (Desinteresse mangels politischer Sachkenntnis) einzelner Medienschaffender, spielt dabei im Ergebnis keine Rolle. Denn jetzt, in Kriegszeiten, schnappt die selbst erzeugte Wirklichkeitsfalle zu. Die JournalistInnen sehen sich in der von ihnen geschaffenen Nachrichtenlage um und wundern sich: “Wohin ist der deutsche Pazifismus entschwunden? [...] Die NATO führt Krieg, doch der Pazifismus ist still. Man sieht ihn nicht in der Tagesschau. Der Pazifismus läuft nicht mit Plakaten durch die Fußgängerzonen. Er sitzt nicht mehr protestierend vor den Eingangstoren der Kasernen. Er findet sein Publikum nicht mehr. [...] Der Pazifismus ist keine politische Kraft mehr in Deutschland; er ist auf der politischen Bühne nicht einmal mehr als Statist präsent.”[0]

Die Orientierung in der Medienrealität hat eben auch ihre Tücken. Was einem Großteil der Bevölkerung dadurch tatsächlich vorenthalten wurde, ist, dass sich in den letzten Monaten in der Bundesrepublik vielen kleineren und größeren Orten “alte” Friedensbündnisse reaktivierten und neue Initiativen gründeten. Sie organisierten Kundgebungen, gewaltfreie Blockaden, lokale, regionale sowie bundesweite Demonstrationen und Info-Veranstaltungen. ExpertInnen aus der Friedensbewegung, FriedensforscherInnen und ReferentInnen aus dem Kriegsgebiet begründeten in vollen Sälen, in Bürgerradios oder auf Marktplätzen ihre Kritik am Bombenkrieg. Hier und auch in vielen anderen Orten rund um den Globus setzte die Friedensbewegung der über die Massenmedien verbreiteten Deutung des Kriegsgeschehens eine andere Perspektive entgegen. Es wurden historische, politische und strategisch-militärische Kontexte des Kosovo-Konfliktes aufgezeigt. Die RednerInnen benannten die Hintergründe für den Waffengang der NATO und seine unüberschaubaren Risiken. Sie kritisierten den Mangel an politischen Perspektiven und übermittelten authentische Schilderungen aus dem Kriegsgebiet. Ihr Ziel war es, die Kriegsgegnerschaft zu stärken und politische Mehrheiten zu gewinnen für eine Ende der Bombardierungen und eine nicht-militärische Lösung des Konflikts. Dafür nutzten die PazifistInnen und AntimilitaristInnen mit dem Internet - erstmalig in einer Kriegssituation - ein Medium, das sie mit Informationen versorgte, wie sie bisher noch nie so schnell und so leicht reproduzierbar zur Verfügung standen. Für die notwendige Bandbreite, Authentizität und Aktualität sorgten die von Friedensforschungsinstituten, kritischen JournalistInnen, Friedens-, Menschenrechts- und Umweltgruppen aus aller Welt und auch von FriedensaktivistInnen aus dem Kriegsgebiet ins Netz gestellten Dokumente, Berichte und Kommentare. Darüber hinaus standen auch die “offiziellen” Quellen zum direkten Zugriff bereit: Es war ohne großen Aufwand möglich, sich über die Verlautbarungen z.B. des Pentagon, der Hardthöhe oder der russischen Duma zu informieren und darauf zu reagieren. Es gab also erstmals eine alternative Nachrichtenlage, die, was die Zuverlässigkeit betrifft, den massenmedialen Nachrichten mit Sicherheit überlegen und im Hinblick auf die Geschwindigkeit der Nachrichtendistribution zumindest gleichgestellt war. Nur, dort, wo die ‘Schlacht der Lügen’ geschlagen wurde - in den Massenmedien - wurde die Perspektive der KriegsgegnerInnen ausgeblendet. Was übrigens auch für die US-amerikanischen Massenmedien gilt: Die renommierte, 1986 gegründete Organisation ‘Fairness and Accouracy in Reporting’ - (FAIR)[0] ermittelte, dass in den beiden einflussreichen Nachrichtenmagazinen “ABC Nightline” und “NewsHour with

0 So Heribert Prantl, in: SZ, 26.3.99.

Jim Lehrer" (PBS) während der ersten beiden Kriegswochen als Nachrichtenquellen zu 45 Prozent entweder Vertreter der US-Regierung bzw. des US-Militärs oder NATO-Offizielle angegeben wurden; nur acht von hundert verwendeten Quellen wurden von FAIR als 'NATO-kritisch' eingestuft.[0]

In einer FAIR-Pressemeldung zur Washingtoner Demo im Rahmen einer landesweiten Antikriegskampagne Anfang Juni, an der sich 500 Friedensorganisationen in über 40 US-Städten beteiligten, heißt es: "Am 5. Juni [Samstag] protestierten tausende KriegsgegnerInnen gegen die Bombardierung Jugoslawiens und marschierten von der Gedenkstätte der Vietnamveteranen zum Pentagon. Am 7. Juni ergab eine Analyse, dass die Protestaktion in keiner der Hauptnachrichtenmedien (York Times und die Washington Post eingeschlossen, ebenso die Networks ABC, NBC, CBS und die PBS NewsHour) Erwähnung fand; CNN berichtete in einigen Kurzmeldungen."[0] Am 6. April fragt der Londoner Medienwissenschaftler Philip Harmond angesichts einer Pressemeldung der BBC, nach der die "serbischen Medien nach der Pfeife des Patriotismus tanzen": "Nach welcher Pfeife tanzt die BBC, dass sie jede Behauptung der NATO ohne nach Belegen zu fragen, wiedergibt? Zugleich haben die Fernsehnachrichten kaum über die Proteste in aller Welt, nicht nur in Makedonien, Russland, Italien und Griechenland, sondern auch in Tel Aviv, Lissabon, San Francisco, Chicago, Los Angeles, Toronto und Sydney, berichtet. Sollen wir glauben, dass diese DemonstrantInnen alles Serben oder Marionetten der 'streng kontrollierten' jugoslawischen Medien sind?"[0]

Journalistische Wahrnehmungsraster eignen sich offenbar nur schlecht dazu, die im Vergleich mit der offensiven und griffigen militärischen bzw. politischen Öffentlichkeitsarbeit viel komplexeren Erklärungs- und Bewertungsansätze, Quellenlagen und Handlungsstrukturen der PazifistInnen und AntimilitaristInnen zu beobachten, aufzubereiten und adäquat zu präsentieren: "[Es] fehlen der Friedensbewegung einende Sätze oder Images - statt politischer Zeichen oder Handlungen (von wenigen Protestveranstaltungen einmal abgesehen) bekommt man höchstens Ströbele oder, seltener, Gysi als Kronzeugen pazifistischen Denkens gezeigt."[0] Wer druckt oder sendet schon das Statement eines Mitglieds der Friedensbewegung, wenn er ein Mitglied des Bundestages vors Mikro kriegen kann? Was konnten wir in der Bundesrepublik in unseren "Hauptnachrichtenmedien" über die Aktivitäten der weltweiten Friedensbewegung lesen, hören oder sehen, oder über die Proteste in den europäischen Ländern, wie z.B. die Blockadeaktionen gegen NATO-Konvois im Hafen von Thessaloniki; wo immer wieder NATO-Transporte kurzzeitig 'verschwanden', weil irgend jemand dauernd die Wegweiser zum Hafen verstellte? Wer weiß von der Aktion europäischer Friedensinitiativen in Straßburg am

0 FAIR untersucht einseitige Berichterstattung und Zensurmaßnahmen in den US-Medien und macht diese publik. Vgl.: www.fair.org.

0 Norman Solomon: When will the media call it war? (17.5.99): www.fair.org/articles/media-war.html.

0 Media Ignores Major Anti-War March. FAIR Pressemitteilung vom 7.6.99: www.fair.org/activism/march.html.

0 Philip Hammond, 'A War of Words and Pictures', in: The Independent, 6.4.99; Hammond ist Dozent für Media Studies an der South Bank University, London.

0 Jörg Sundermeier: Warten auf Bilder, in: FREITAG,16.4.99.

Ostersonntag oder den Kundgebungen mit 100.000 TeilnehmerInnen am 2. April in Saloniki oder am 3. April (80.000 TeilnehmerInnen), am 10. April (100.000) und 25. April (200.000) in Rom? Von den gewaltfreien Daueraktionen der Friedensbewegung am NATO-Stützpunkt in Aviano?

Was ist zu tun?

Dringend notwendig ist eine intensive Beschäftigung mit den strategischen Konzepten des Informationskrieges. Zum ersten, weil diese Konzepte die Kriegsführung in den aktuellen und (angesichts der bekannten militärischen Planungen und Vertragslagen) erwartbaren Konflikten bestimmen, und sie deshalb als Gegenstand antimilitaristischer Kritik stärker öffentlich gemacht werden müssen. Zum zweiten sollten - insbesondere im Rahmen der friedenspolitischen Konfliktprävention - die Strukturen, Techniken und Intentionen des 'Kriegsmarketings' der Militärs und Politiker als elementares Instrument der Kriegsvorbereitung systematisch analysiert und offengelegt werden. Und zum dritten wird in diesem Kontext von den Vordenkern zukünftiger Kriegsführungsstrategien im Kampf um die "Informationsüberlegenheit" gerade eine neue "Kampflinie" gezogen, die unsere Aufmerksamkeit erfordert: Offenbar werden Nichtregierungsorganisationen (NGOs, z.B. die Friedensbewegung) - zu recht, s.o. - als kommunikationstechnisch und inhaltlich immer "mächtiger", d.h. bedrohlicher wahrgenommen: RAND, die regierungsnahe US-amerikanische Denkfabrik, warnt in ihrer Analyse der mexikanischen Zapatista-Bewegung vor einem zukünftigen "Krieg im Netz", ermöglicht durch den freien Zugriff auf elektronische Medien, Fax, E-Mail und World Wide Web: "Es könnte sich eine dynamische Symbiose zwischen NGOs und den Medien entwickeln [...], in der die Medienpräsenz die jeweiligen Machtverhältnisse ausgleicht und die Regierung ihren Vorteil verliert, zu kontrollieren, wer was über einen Konflikt weiß. Dies führt dann entsprechend zu einer Einschränkung staatlicher Handlungsmöglichkeiten."[0]

Was die Medien betrifft, so kann sich angesichts der vielfältig vorhandenen Informationmöglichkeiten niemand mehr von der individuellen Verantwortung für einen unabhängigen, investigativen und kritischen Journalismus freisprechen. Friedrich Krotz - Medienforscher am Hans-Bredow-Institut in Hamburg - kritisiert, dass die Kosovo-Berichterstattung heute nur noch "nach dem Modell des Krieges von 1870/71 ab[laufe]" und fordert eine stärkere Vernetzung: "Wenn es moderne Informationstechnologie gibt, darf man sich nicht nur auf einzelne Reporter verlassen, sondern muss einen Apparat aufbauen, der es ermöglicht, die Verhüllungsstrategien der Kriegsparteien aufzudecken." Sinnvoll im Sinne einer ausgewogeneren Kriegsberichterstattung wäre es sicher, unter Einbeziehung der Friedensbewegung und -forschung die Berührungsängste bzw. Kommunikationsblockaden zwischen den Medien und den Nichtregierungs-organisationen abzubauen.

Abgesehen von dieser Verbesserung der Kooperation mit den etablierten Medien muss die Friedensbewegung perspektivisch einen eigenen Weg finden, wie sie die Wirksamkeit ihres alternativen Nachrichtenangebots den neu gegebenen

0 RAND (Hg.): The Zapatista "Social Netwar" in Mexico (1998): http://www.rand.org/ publications/ MR/MR994/MR994.pdf/.

Möglichkeiten der Informationsbeschaffung anpasst. *Jede* Bürgerin und *jeder* Bürger hat das Recht auf Gegeninformationen, die es ihr oder ihm ermöglichen, sich - besonders in Krisen oder im Krieg - ein differenziertes Bild von der Situation zu machen. Wenn die etablierten Medien hier, wie in den letzten Monaten geschehen, die Kritik am und den Widerstand gegen den Krieg “tot”-schweigen, obwohl schätzungsweise die Hälfte der BundesbürgerInnen ihn für falsch hält und seine Beendigung fordert,[0] dann muss die Friedensbewegung diese Vernachlässigung ausgleichen. Wünschenswert wäre ein eigenes, unabhängiges und internationales Informationsnetz, dass sowohl dem Austausch untereinander dient, als auch alternative Informationsprogramme (textuell und audiovisuell) anbietet. Dies sollte nicht nur, aber auch als “Agentur” für JournalistInnen in den Massenmedien dienen. Die NGO-Struktur weltweit ist heute schon eine Art KorrespondentInnen-Netz, welches Augenzeugenberichte und Hintergrundinformationen aus aller Welt im Internet bereitstellt. Dieses Material aufzubereiten und zu verbreiten, bedeutet ebenso, die eigene Medienarbeit - auch im elektronischen Bereich (z.B. Bürgerradios oder -fernsehen und World Wide Web) - auszuweiten. Wenn wir den Widerstand gegen die “Informationsüberlegenheit” der Herrschenden verstärken wollen, müssen wir uns auch dafür engagieren, dass mehr Menschen - nicht nur ein privilegierter Kreis von Friedensbewegten, KundgebungsbesucherInnen und Internet-UserInnen - an den alternativen Informationsangeboten partizipieren können.

0 Diverse Umfrageergebnisse belegen, dass es in der Bundesrepublik auch während der Bombardierungsphase durchaus keinen Konsens über den Krieg gab: Für das am 21. Mai 1999 veröffentlichte ZDF-Politbarometer ermittelte die Forschungsgruppe Wahlen, dass in Westdeutschland 43 Prozent für und 52 Prozent gegen eine Unterbrechung der Luftangriffe waren; in Ostdeutschland sprachen sich sogar 66 Prozent für eine Feuerpause (29 Prozent dagegen) aus. In einer Online Umfrage des Express/Köln vom 7. Juni antworteten auf die Frage “Ist der NATO-Einsatz im Kosovo richtig?” 37,4 Prozent mit Ja und 60,3 % mit Nein (2,3 Prozent unentschieden). Und selbst in einer von der Bundeswehr in Auftrag gegebenen Emnid-Umfrage im Mai fanden es zwar 62,4 Prozent der Befragten richtig, “dass die NATO im Kosovo-Konflikt mit Luftschlägen militärisch eingegriffen hat” (33,1 Prozent dagegen, 4,4 Prozent unentschieden); aber dass der Konflikt mit dem Militäreinsatz zu lösen ist (“Glauben Sie, dass das militärische Eingreifen der NATO zu einem Einlenken Milosevics führt?”) hielten nur 44,8 Prozent der Befragten für wahrscheinlich (Nein 50,7 Prozent, 4,6 Prozent unentschieden).

Elvi Claßen

Ich sehe was, was Du nicht siehst

Warum findet der Widerstand gegen den Krieg in den Medien nicht statt?[0]

Am 31. März schreibt Jan Ross unter dem Titel “Die Deutschen und der Krieg. Warum eigentlich herrscht so große Ruhe im Land?” in der ZEIT: “Gleichwohl ist die Selbstverständlichkeit atemberaubend, mit der die Bundesrepublik zu Beginn der Angriffe nicht nur ein halbes Jahrhundert gewaltferner Außenpolitik hinter sich gelassen hat, sondern auch einen gesellschaftlichen Pazifismus, den man tief verwurzelt glaubte.” Herrscht wirklich Ruhe im Land? Woher holen sich Jan Ross und seine KollegInnen ihre Informationen? Oder anders gefragt: Was erfährt der Durchschnittsmensch, sofern er via Massenmedien informiert wird, über die Aktivitäten der Friedensbewegung - und wer da eigentlich warum demonstriert, blockiert und appelliert? Letzte Frage: Machen wir etwas falsch oder warum findet in den etablierten Printmedien oder im Fernsehen der Widerstand gegen den Krieg nicht statt? Natürlich herrscht keine Ruhe im Land. Aber der Beantwortung der anderen Fragen müssen sich die genannten Akteure (selbst-)kritisch annehmen.

Es gibt keinen Konsens über den Sinn des Krieges

Politisch-militärische Analysen der Friedensbewegung spielen in der aktuellen Medienberichterstattung über den Krieg kaum eine Rolle. Weder werden z.B. friedenspolitische Argumente zu den Ursachen des Krieges, den Beweggründen des westlichen Militärbündnisses, noch zu grundsätzlicheren politischen Argumente gegen den Krieg und für eine nicht-militärische Konfliktlösung präsentiert. Wer thematisiert in der allgemeinen Öffentlichkeit den “tief verwurzelten gesellschaftlichen Pazifismus”? Wer fragt danach, ob diese Gesellschaft tatsächlich gerade dabei ist, ihn zu “überwinden”? Oder, wenn er noch vorhanden ist - was hier angenommen wird, wer thematisiert sein Vorhandensein und den Konflikt, den der Kosov@-Krieg zwischen Regierungspolitik und “gesellschaftlichem Pazifismus” schafft? Und wer hat es zu verantworten, daß die Hälfte der Bevölkerung mit ihrer eher kritischen Haltung zu diesem Krieg in den Medien nicht repräsentiert ist? Diverse Umfrageergebnisse belegen, daß es durchaus keinen Konsens über den Krieg gibt: Für das am 21. Mai 1999 veröffentlichte ZDF-Politbarometer ermittelte die Forschungsgruppe Wahlen, daß im Westen 43 Prozent für und 52 Prozent gegen eine Unterbrechung der Luftangriffe sind, im Osten sprachen sich sogar 66 Prozent für eine Feuerpause und 29 Prozent dagegen aus. In einer Online Umfrage des Express/Köln vom 7. Juni antworteten auf die Frage “Ist der NATO-Einsatz im Kosovo richtig?” 37,4 Prozent mit Ja und 60,3 % mit Nein (2,3 Prozent unentschieden). Und selbst in einer von der Bundeswehr in Auftrag gegebenen Emnid-Umfrage finden es zwar 62,4 Prozent der Befragten richtig, “daß die NATO im Kosovo-Konflikt mit Luftschlägen militärisch eingegriffen hat” (33,1 Prozent Nein, 4,4 Prozent unentschieden); aber daß der Konflikt mit dem Militäreinsatz zu lösen ist (“Glauben Sie, daß das militärische Eingreifen der NATO zu einem Einlenken Milosevics führt?”) glauben nur 44,8 Prozent der Befragten (Nein 50,7 Prozent, 4,6 Prozent unentschieden).

0 Dieser Artikel erschien zuerst in: Der Krieg biegt die Wahrheit krumm ... Ein Diskurs über die Wirklichkeit in Zeiten militärischer Gewalt, ZivilCourage 3/1999, S. 10-11.

In der Realität der Massenmedien "existiert" die Antikriegsbewegung nicht

Die Nicht-Thematisierung dieser Kontroverse manifestiert sich z.B. in der Tatsache, daß neben Journalisten fast ausschließlich, entweder Politiker und Militärs oder vielleicht noch Politikwissenschaftler die Gelegenheit bekommen, den Krieg vor einem Massenpublikum zu kommentieren oder Fragen von Zeitungs- oder Nachrichtenredakteuren zu beantworten; oder daß in Diskussionsrunden im Fernsehen fast immer genau diese Personengruppen wiederum das debattieren, was sie selbst oder die Zusammenhänge, in denen sie arbeiten, zuvor als "politische Fakten" öffentlich gemacht haben. Und der Themenrahmen ist meist eng gesteckt: die Flüchtlingszahlen in den Lagern werden aktualisiert; die militärischen Aktionen werden bewertet und die politische Befindlichkeit innerhalb und außerhalb des NATO-Bündnisses wird reflektiert. NATO-Briefings, Pressekonferenzen aus Washington oder Bonn usw. werden auf den Nachrichtenkanälen täglich live übertragen. Warum gibt es aber - z.B. - keine Live-Reportage von einer gewaltfreien Blockade der Rhein-Main-Airbase in Frankfurt/M., oder eine Dokumentation über die Arbeit einer Friedensgruppe in Münster, Greifswald, Darmstadt, Ilmenau etc.? Sogar die sonst in ihrer Kosov@-Berichterstattung meist vorbildliche Frankfurter Rundschau versäumt es, in ihrer Internet-Linkliste zum Kosov@-Dossier ("Noch nie zuvor war es für alle Konfliktparteien so einfach, sich weltweit zu artikulieren") www-Adressen aus der hiesigen oder internationalen Friedensbewegung zu veröffentlichen.

Die andere Realität: Es herrscht keine Ruhe, weder hier noch anderswo!

In der Bundesrepublik haben Friedensgruppen aus allen Teilen des Landes allein in der bzw. für die Zeit vom 22. Mai bis 28. Juni ca. 700 Veranstaltungen - lokale/regionale und bundesweite Demos, Info-Veranstaltungen mit ReferentInnen, gewaltfreie Blockaden, Kundgebungen usw. durchgeführt bzw. angekündigt. An über hundert größeren und kleineren Orten in der Bundesrepublik finden regelmäßig, oft täglich, meist mehrmals wöchentlich oder wöchentlich Mahnwachen, Kundgebungen oder sonstige Aktionen statt. Es zirkulieren mehr als 50 Aufrufe, in denen sich Friedensgruppen, -organisationen und -bündnisse klar und eindeutig gegen den NATO-Krieg gegen Jugoslawien aussprechen und ein sofortiges Ende der Bombardierungen fordern. Ein kleiner Ausschnitt aus der Chronologie der Antikriegsbewegung soll hier stellvertretend für alle Aktivitäten einen Eindruck von der Vielfalt und Menge der bisher gelaufenen Aktionen vermitteln:

24.-.31.3.: über 70 Demonstrationen u. Aktionen in der BRD, u.a. in Bonn, Chemnitz, Erfurt, Frankfurt/M., Mainz, Berlin, Bochum, Bremen, Münster, Stuttgart; Demos in Rom, Genua, Turin, Mailand, Verona, Aviano, Athen, Nikosia, Wien, Oslo, Sofia, Moskau, London, Den Haag, Prag, Los Angeles, San Francisco, Sydnes, Melbourne; 2.-5. April, Ostermärsche: die Info-Stelle Ostermarsch in Frankfurt/M. meldet Kundgebungen in 150 Städten, doppelt so viele wie 1998; auch die Zahl der Teilnehmer habe sich verdoppelt, teilweise sogar verdreifacht; 9.4.: DGB-Kundgebung in Erfurt; 10.4.: gewaltfreie Sitzblockade vor der Haupteinfahrt der US-Air-Base Spangdahlem; 17./18.4. Aktionen u.a. in Frankfurt/M., Potsdam, München sowie in Sydney, Ottawa, Toronto, Brüggen, Oslo, Bergen u. in vielen US-Städten; 24.4.: Demos in Heidelberg, München, Rom; 25.4.: Demos in Hamburg, Nürnberg, Erfurt, Dortmund; 29.4: Die Polizei beschlagnahmt bei der Mahnwache der Horber Initiative für den Frieden ein selbstgefertigtes Plakat mit der Aufschrift "Soldaten verweigert

jetzt". 1.5.: 1.Mai-Demonstrationen; die "Erklärung von Gewerkschafterinnen und Gewerkschaftern - NATO-Angriffe sofort beenden!" unterschrieben bis 28.4. insgesamt 3.286 Menschen (bis 15.5.: 10.122); Aktionstag in Griechenland mit Demos in Athen, Thessaloniki, Solinka, Piräus, Patras; 8.5.: Antikriegs-Demonstrationen "Stoppt den Krieg! Helfen statt bomben!" in Berlin sowie in u.a. in Münster, Stuttgart, Bonn, Darmstadt; 9.5. Gewaltfreie Blockade der Rhein-Main-Airbase/NATO-Nachschubbasis; 13.05.: vom 25.4. bis 13.05. sammelte der Bund demokratischer Wissenschaftlerinnen und Wissenschaftler/Marburg von 120 HochschullehrerInnen, 350 WissenschaftlerInnen und AkademikerInnen, 427 Studierenden und 159 wissenschaftliche MitarbeiterInnen Unterschriften gegen den Krieg; Italien: zweiter Generalstreik gegen den Natokrieg; 15./16.5, Int. KDV-Tag: DFG-VK Freiburg startet eine "Kommunale Initiative zum Schutz von Kriegsdienstverweigerern und Deserteuren aus Kriegsgebieten"; weitere Aktionen u.a. in Nürnberg, Wipperfürth, Templin, Warendorf; Demos in Italien mit über 100.000 TeilnehmerInnen; 17./18.5. Veranstaltungen in Berlin, Bonn, Düsseldorf, Köln, Marburg, Wetzlar; 21.5.: Aktion gegen ein Bundeswehr-Gelöbnis in Horb; 27.5.: Freiburg: Darko Kovacev (Frauen in Schwarz/Belgrad) spricht über die Situation der Opposition, der Deserteure und Verweigerer, Witten: Infoveranstaltung zum "Kosov@-Konflikt; 30.5.: Gewaltfreie Blockade der Rhein-Main-Airbase/NATO-Nachschubbasis; Connection e.V. kündigt die Einrichtung einer Anlaufstelle für Deserteure und KDVer aus Jugoslawien in Budapest an; 3.-5.6.: Aktionen u. Veranstaltungen in Stuttgart, Erlangen, Vlotho, Backnang, Münster, Kassel usw. ...

Den Widerstand gegen den Krieg gemeinsam öffentlich machen

Also: Woher holen sich Jan Ross und seine KollegInnen ihre Informationen? Neben der selektiven Wahrnehmung, mit der die meisten JournalistInnen sich fast ausschließlich an “offiziellen Quellen” orientieren, könnte ein zweiter Grund für die Nichtberichterstattung über die Antikriegsbewegung sein, daß es keinen Knotenpunkt gibt, an dem die Termine der überwiegend dezentralen Aktivitäten der Friedensbewegung nicht nur gesammelt und veröffentlicht werden (wie es z.B. in dankenswerter Weise das Netzwerk Friedenskooperative/Bonn tut). Vielleicht fehlt eine Art “friedenspolitischer Pressedienst”, der die bundesweit vorhandenen Informationen systematisch sammelt, journalistisch aufbereitet und den Medien in Übersichtsartikeln usw. anbietet: Wo finden/fanden Aktionen statt; welcher Art sind die Veranstaltungen, welche ReferentInnen sprechen zu welchen Themen, wie verliefen die Aktivitäten, gibt es Fotos, Videos, überregional nutzbare Materialien usw. Eine solche “Moderation” der vor Ort sehr gut laufenden Öffentlichkeitsarbeit würde möglicherweise dafür sorgen, daß zum einen die Antikriegsbewegung in den Massenmedien eher wahrgenommen wird; zum anderen könnte sie die Aktiven dabei unterstützen, sich selbst einen besseren Überblick über den Stand der Dinge zu verschaffen, die eigene politische Arbeit einzuordnen und mit Gleichgesinnten in Kontakt zu treten (Austausch von Aktionserfahrungen und -ideen, Info- und Aktionsmaterialien usw.).

So entlarvend die Frage “Warum eigentlich herrscht so große Ruhe im Land?” für die journalistische Praxis ist, so notwendig ist es andererseits auch, in der Friedensbewegung darüber nachzudenken, was getan werden muß, damit der breite und vielfältige Widerstand gegen den Krieg, die “Unruhe im Land”, der allgemeinen Öffentlichkeit nicht mehr vorenthalten werden kann.

Ralf Bendrath

What do you want to know today?

Geheimdienstarbeit in Zeiten privater Datenquellen[0]

Als im Golfkrieg 1991 die ersten westlichen Bomben auf die irakischen Streitkräfte fielen, konnten die Irakis die gegnerischen Stellungen noch tagelang aus dem Weltraum beobachten. Das Regime, das selber über keine Satelliten verfügt, erhielt die Bilder aus einem Land, dessen Truppen zur gleichen Zeit Bomben auf Bagdad abwarfen – aus Frankreich. Sie kamen von dem 1990 gestarteten kommerziellen Fotosatelliten SPOT-2, wurden regulär bezahlt und erlaubten eine Auflösung von immerhin 10 Metern – genug, um kleinere Truppenverbände zu entdecken.[0] Erst nach Hinweisen der USA schalteten die französischen Satellitenbetreiber die Verbindung ab.

SPOT-2 war ursprünglich wie sein Vorgänger SPOT-1 am Himmel plaziert worden, um geologische, landwirtschaftliche, umwelttechnische und andere zivile Untersuchungen zu erleichtern. Er wird jedoch ebenso von Streitkräften, Geheimdiensten und Militärbündnissen genutzt, die nicht auf eigene Aufklärungssatelliten zurückgreifen können. Seit einigen Jahren gehört auch die Westeuropäische Union, der militärische Arm der EU, zu den SPOT-Kunden. Das WEU-Satellitenzentrum im spanischen Torrejon arbeitet mit Material von SPOT-1 und SPOT-2. Zusätzlich werden kommerzielle Spionagebilder der russischen Firmen Sovinformsputnik und Priroda eingekauft, die seit 1992 das von dem ehemaligen Geheimdienstsatelliten KVR-1000 gesammelte Material in einer Auflösung von 2 Metern anbieten.[0]

Dieses neue Angebot an hochaufgelöstem Bildmaterial, das auf dem freien Markt erhältlich ist, steht stellvertretend für die veränderte Situation der Geheimdienste in Zeiten des Internet. Sie sind nicht mehr wie ehedem die einzigen Hüter von Informationen, sondern müssen sich mit privaten Anbietern von Bildern, Daten und aufbereitetem Wissen auseinandersetzen. Die heute vorhandene Menge an frei verfügbaren Informationen stellt die Sonderrolle der staatlichen Informationssammler, ihre personelle Ausstattung und natürlich ihren Haushalt immer stärker in Frage. Sie geraten unter Rechfertigungsdruck, sobald die gleichen Daten billiger, schneller oder effektiver aufbereitet auf dem Markt erhältlich sind.

Seit Sommer 1998 kann zum Beispiel jedermann im World Wide Web Satellitenbilder vom größten Teil der Erdoberfläche per Mausklick abrufen. Die Datenbank Terraserver (www.terraserver.com), die von Microsoft zusammen mit Digital Equipment, Sovinformsputnik, Kodak, Aerial Images und dem US Geological Survey entwickelt wurde, enthält etwa ein Terabyte Bilder, die vor allem von KVR-1000 sowie aus freigegebenen US-Spionageaufnahmen der siebziger Jahre stammen.[0]

0 Dieser Artikel erschien zuerst in FifF-Kommunikation, Nr. 3, September 1999. Er wurde nachgedruckt in antimilitarismus information (ami), 10/1999.

0Vipin Gupta: New Satellite Images for Sale, in: International Security, Nr. 1, Sommer 1995, S. 94-125.

0 Briefing in der WEU, Brüssel, Februar 1998.

0Duncan Campbell: So where do you want to spy today?, in: The Guardian Online, 18.6.1998, http://go2.guardian.co.uk/technology/898099634-spysat.html

Auch nichtvisuelle Informationen über politische Entwicklungen, wirtschaftliche Konkurrenz oder militärische Planungen sind zum großen Teil öffentlich zugänglich. Beim deutschen Bundesnachrichtendienst werden bereits seit Jahren ungefähr 80% der Informationen aus offenen Quellen gewonnen, vor allem durch Auswertung der internationalen Presse. Andere Geheimdienste arbeiten ähnlich. Im Gegensatz zu früher sind heute aber alle großen Zeitungen im Internet vertreten und werden durch spezielle Suchmaschinen wie Paperboy (www.paperboy.de) erschlossen; andere können online durch Datenbankanbieter wie GENIOS bezogen werden.

Der herrschenden neoliberalen Logik folgend drängt sich daher die Frage auf, ob es billiger und effektiver ist, solche Aufgaben aus der Geheimdienstarbeit auszulagern. In der Tat wird bereits vielerorts an Schritten in diese Richtung gearbeitet. Nur einige Beispiele: Das International Center for Security Analysis, die politikberatende Abteilung des King´s College in London, betreibt seit zwei Jahren ein “Open Source Intelligence Programme”, in dessen Rahmen Geheimdienstmitarbeiter für die Arbeit an Internet-Suchmaschinen ausgebildet werden.[0] Die US-Streitkräfte, die derzeit ihre Soldaten digital vernetzen, beziehen unter dem Label “All Source Analysis” auch offene Quellen systematisch in ihre Aufklärungs- und Überwachungssysteme ein.[0] Im sicherheitspolitischen Forschungsinstitut der WEU in Paris wird darüber nachgedacht, ob eine Privatisierung der Datensammlung dazu beitragen kann, die sehr zögerliche westeuropäische Geheimdienstzusammenarbeit zu effektivieren.[0]

Führend in diesem Bereich sind wieder einmal die USA: Bereits seit 1992 arbeitet die Firma Open Source Solutions (www.oss.com) an einer Lobbykampagne zur Privatisierung der Geheimdienstarbeit. Ihr größter Erfolg bisher war eine Konferenz in Washington im Mai 1998, bei der mehr als 500 internationale Spione und Geheimdienstmitarbeiter über die Zukunft ihrer Arbeit in Zeiten des Internet diskutierten. Die Teilnehmer aus 23 Ländern, darunter die USA, Saudi-Arabien, Japan, Großbritannien und Südafrika, waren sich weitgehend einig darüber, daß offene Quellen weit stärker genutzt werden sollten als bisher. Anstelle einer grundsätzlichen Debatte über die politischen Folgen solcher Reformen unterhielt man sich auf der Konferenz bereits über Preise und Abrechnungsmodalitäten in der privatisierten Geheimdienstarbeit.[0]

Dieser Trend, der offensichtlich zunimmt, wirft allerdings viele Fragen auf. Wenn Daten über militärische und andere Entwicklungen von kommerziellen Anbietern eingekauft werden, dann können dies auch potentielle Gegner tun. Dies müssen nicht einmal mehr Staaten wie der Irak sein: Die mittlerweile aufgelöste südafrikanische Söldnerfirma Executive Outcomes (EO) unterhielt enge Verbindungen mit der Grupo El Vikingo International, einem dubiosen Anbieter von Verschlüsselungstechnologien, Kommunikationsanlagen und Satellitenausrüstung. Mit Hilfe dieser Technik waren die Söldner von EO in mehreren Kriegen Afrikas in der

0 http://www.kcl.ac.uk/orgs/icsa/osint.htm

0 John F. Stewart: Intelligence Strategy for the 21st Century, in: Military Review, Nr. 5, Sepember-Oktober 1995, S. 78.

0 Andrew Rathmell: The Privatisation of Intelligence: A Way Forward for European Intelligence Cooperation, Papier für eine Konfernez des WEU Institute for Security Studies, Paris, 13.-14.3.1997

0 International Spies And Analysts Define New Model For Intelligence: Global Intelligence Forum Brings Together Twenty-Three Countries Including Saudi-Arabia, Japan, Israel, PRNewswire, 23.5.1998

Lage, zahlenmäßig weit überlegene Gegner zu besiegen.[0] Der Handel mit militärisch relevanten Informationen wird daher bereits als neues Problem der Rüstungskontrolle diskutiert.[0]

Eine weitere naheliegende Frage ist sicherlich, ob die öffentliche Verfügbarkeit von Aufklärungsdaten auch von sozialen Bewegungen genutzt werden kann. In der Tat wird die Überprüfung von Abrüstungsverträgen oder Umweltschäden mit diesen Mitteln einfacher. John Pike, Weltraumexperte der Federation of American Scientists (www.fas.org), hat dies mehrfach demonstriert. Er weist auf die neuen Möglichkeiten hin, illegale Waffenfabriken, Flüchtlingslager oder Massengräber aufzuspüren und so einen fundierteren Umgang mit der massenmedialen Kriegsberichterstattung zu entwickeln.[0] Das Problem dabei ist jedoch, daß viele Informationen zwar heute theoretisch für jedermann zugänglich sind, aber die begrenzten finanziellen Mittel der meisten Nichtregierungsorganisationen eine systematische Auswertung nicht erlauben. Anstelle der staatlichen Kontrolle der Informationen können wir daher über kurz oder lang eine marktgestützte Asymmetrie von wissenden und unwissenden politischen Akteuren erwarten.

Was passiert darüber hinaus auf grundsätzlicher Ebene mit dem Herrschaftsanspruch des Staates, wenn sein Wissen über die politische und gesellschaftliche Umwelt nicht mehr in seiner Kontrolle ist? Diese Frage kann bisher niemand beantworten. Man kann sie allerdings umgehen. Die US-Geheimdienste setzen neben einem begrenzten Outsourcing vor allem auf eine andere Strategie: Sie bieten ihre Daten verstärkt anderen Staaten an. Damit verhindern sie deren Rückgriff auf private Anbieter und können die angebotenen Informationen bei Bedarf filtern. Der “nukleare Schirm” soll auf diese Weise durch einen “Informationsschirm” ersetzt werden, so konnte man bereits 1996 in einem Schlüsseltext der Präsidentenberater Joseph Nye und William Owens in der Zeitschrift “Foreign Affairs” nachlesen. Diese Strategie der “sanften Macht” (“Soft Power”) soll die amerikanische Hegemonie auch in Zeiten globaler offener Datenquellen sichern.[0] Wenn theoretisch jeder auf alles Wissen Zugriff hat, dann ist es eben nicht mehr wichtig, *was* man wissen kann, sondern *wer* bestimmte Sachen wissen will. Die kommerziellen US-Satellitenbetreiber sind daher verpflichtet, ihre Kunden und die abgerufenen Bilder an die Bundesregierung zu melden.[0] Wer sich beim Urlaub in den USA keinen Ärger mit der Einwanderungsbehörde einhandeln will, sollte daher beim nächsten Blick in den Sternenhimmel das Lächeln nicht vergessen.

0 William Reno: New South African Business in Africa´s weak States, Papier präsentiert auf der 38. Annual Convention der International Studies Association, Toronto, März 1997; Bartholomäus Grill/ Caroline Dumay: Der Söldner-Konzern; in: Die Zeit, 17.1.1997.

0 Klischewski, Ralf/Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie, Studie für das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bonn 1995, S. 51.

0 Duncan Campbell: So where do you want to spy today?, in: The Guardian Online, 18.6.1998, http://go2.guardian.co.uk/technology/898099634-spysat.html (Fußnote 2)

0 Joseph S. Nye, jr./William A. Owens: America´s Information Edge, in: Foreign Affairs, März/April 1996, S. 20-36.

0 Vipin Gupta: New Satellite Images for Sale, in: International Security, Nr. 1, Sommer 1995, S. 94-125 (Fußnote 1)