Informationsstelle Militarisierung e.V.

Informationsstelle Militarisierung (IMI) e.V., Hechingerstr. 203, 72072 Tübingen

Hechingerstr. 203
72072 Tübingen
Tel 07071/ 49154
Fax 07071/ 49159
imi@imi-online.de
www.imi-online.de

13.05.2001

US-Streitkräftereform und Infowar

Bush's Neudefinition des Krieges

von Dirk Eckert *

Die militärische Dominanz ergänzen durch die Unverwundbarkeit des eigenen Territoriums, deshalb mehr Mittel für das Militär. Das gehörte zur Wahlkampfrhetorik des George W. Bush. Ein halbes Jahr später ist selbst manch verbündeter Politiker erschrocken darüber, wie Bush als Präsident ohne Rücksicht auf internationale Verträge, ohne Rücksicht auf die Sicherheitsinteressen anderer Länder - auch der NATO-Verbündeten - eine Politik der Hochrüstung forciert. Im Anknüpfen an Reagans Pläne der Weltraummilitarisierung, den Plänen für eine National Missile Defense, NMD, wird das besonders deutlich. Doch während NMD in die Schlagzeilen kommt, bleibt ein anderer Bereich unterbelichtet: Die Streitkräftereform, die die amerikanischen Truppen für den Informationskrieg fit machen soll. Georg W. Bush kann auch hier, wie bei NMD, auf Planungen der Clinton-Administration zurückgreifen.

Bei seinem Besuch auf dem Marinefliegerhorst Norfolk im Februar kündigte George W. Bush eine "umfassende Überprüfung des amerikanischen Militärs, unserer Strategie, der Struktur unserer Streitkräfte und ihrer Haushaltsansprüche" an.[1] Besondere Bedeutung maß der US-amerikanische Präsident dabei den technologischen Veränderungen zu: "Wir sind Zeugen einer Revolution in der Kriegstechnologie, in der Mächte zunehmend nicht mehr über ihre Größe, sondern ihre Mobilität und Schnelligkeit definiert werden. Immer häufiger entstehen Vorteile durch Informationen wie die dreidimensionalen Bilder eines simulierten Kampfes, die ich gerade gesehen habe. " Und weiter: "Sicherheit gewinnt man durch List und Stärke, die über den langgestreckten Bogen präzisionsgesteuerter Waffen projiziert wird. Die beste Art und Weise, den Frieden zu wahren, ist, den Krieg zu unseren Bedingungen neu zu definieren."[2]

Damit spielte Bush auf das an, was als Informationskrieg seit einigen Jahren durch die Planungspapiere des amerikanischen Militärs wie durch die Presse spukt.[3] Inzwischen hat das Pentagon einige Strategiepapiere und Handbücher herausgebracht, in denen die neue Form der amerikanischen Kriegführung skizziert wird. Zusätzlich wurden diverse Forschungseinrichtungen gegründet und einzelne Truppenteile wurden zu "Cyber Warriors" umgerüstet, die auf dem digitalen Schlachtfeld[4] der Zukunft siegreich sein sollen.

Die Zauberworte des Krieges der Zukunft lauten Informationskriegführung und Informationsoperationen. "Wenn wir eine Situation herbeiführen können, in der der Feind sich widersprechende Befehle erteilt, bis seine Truppen völlig verwirrt sind, und wir dann nur noch auf das Schlachtfeld gehen müssen und aufräumen, dann ist das eine effektive Informationsoperation", so Michael L. Warsocki vom U.S. Army Land Information Warfare Center.[5]

Joseph S. Nye und William A. Owens schreiben in der amerikanischen Zeitschrift Foreign Affairs über die Bedeutung dieser Strategie[6]: Eine der Fähigkeiten der Vereinigten Staaten, die sie vor manch anderen Staaten auszeichnet, ist die Fähigkeit, Informationen zu sammeln, zu verarbeiten, auf ihrer Grundlage zu handeln und sie weiter zu verbreiten. Dieser Informationsvorteil könne helfen, gegen traditionelle militärische Bedrohungen eine Abschreckung zu relativ niedrigen Kosten aufzubauen und die Führung in Allianzen oder ad-hoc-Koalitionen zu sichern. Nye/Owens weiter: "So wie früher die nukleare Dominanz der Schlüssel zur Führung in Koalitionen war, so wird Informationsdominanz der Schlüssel im Informationszeitalter sein."[7]

Dabei handelt es sich bei Information Warfare weder um eine "abstrakte Neuerfindung", noch um eine "neue Bezeich-

Kreissparkasse Tübingen
BLZ 641 500 20
Konto 166 28 32

nung bekannter militärischer Operationsformen".[8] Vielmehr ist Information Warfare die schrittweise Weiterentwicklung und Neuordnung militärischer Operationsformen, die auf der Adaption neuer technischer Mittel beruht, wie Bernhardt/Ruhmann schreiben.[9] "Auf strategischer Ebene spielt Information Warfare bei den Überlegungen eine Rolle, dass sich die geopolitischen Interessen der USA nicht mehr allein mit ihrem atomaren Drohpotential durchsetzen lassen und herkömmliche Rüstungsprogramme und Allianzen nicht länger die gewünschten Ergebnisse garantieren."[10]

Planung und Durchführung

Mit der "Joint Vision 2010" legten die Vereinten Stabschefs der US-amerikanischen Streitkräfte 1996 das zentrale Planungspapier für die Kriegführung im 21. Jahrhundert vor. Mit bekannten Bedrohungsszenarien, in denen Cyberterroristen die amerikanische Infrastruktur lahm legen oder die Kurse an der Wallstreet manipulieren, hat diese "Joint Vision 2010", die inzwischen als "Joint Vision 2020" neu aufgelegt wurde, wenig zu tun. Vielmehr geht es in dieser Vision darum, darzustellen wie das amerikanische Militär in der Zukunft kämpfen wird. Die Vorlage wurde in mehreren Doktrinen und Handbüchern konkretisiert, damit verfügt das amerikanische Militär inzwischen über einen umfangreichen Schriftsatz zu Themen wie Psychologischer Kriegführung, Elektronischer Kriegführung oder Informationsoperationen.

Die neue Art der Kriegführung wird in der "Joint Vision 2010" aus der Beschaffenheit des strategischen Umfeldes abgeleitet. Von der Friedensmission bis zum Kampfeinsatz, - allein, mit Bündnispartnern oder in ad-hoc-Koalitionen - in allen Einsätzen sollen die US-Truppen siegreich sein. Konsequent wird in der Planung getrennt zwischen offensiver Informationskriegführung und ihrer defensiven Variante. Letztere wird nicht etwa als Verteidigung vor eventuell auftretenden Bedrohungen bestimmt, sondern in Abhängigkeit von offensiver Informationskriegführung definiert: Sie ist notwendig, um sich bei offensiven Informationsoperationen vor Gegenangriffen zu schützen.

Spätestens mit dem Golfkrieg 1991 wurden die Veränderungen in der Art der Kriegführung augenfällig. "Irak hat den Krieg verloren, bevor er überhaupt begann. Es war ein Krieg von Aufklärung, "Electronic Warfare", "Command and Control" und Spionageabwehr. Irakische Truppen wurden geblendet und taub gemacht ... Moderner Krieg kann durch Informatika gewonnen werden", hieß es 1998 in der "Joint Doctrine for Information Warfare", eine der Doktrinen, mit der die "Joint Vision 2010" auf operativer Ebene umgesetzt wird.[11]

Der Kosovokrieg schließlich hat es der NATO ermöglicht, das ganze Arsenal von Informationsoperations-Waffen einzusetzen. Das ist jedenfalls die Ansicht von William Church, Direktor des Centre for Infrastructural Warfare Studies. Besondere Bedeutung hat für Church, dass im Kosovo Waffen auf die Informationsinfrastruktur gerichtet wurden, "um den Entscheidungsprozess von Regierung und Zivilbevölkerung zu beeinflussen."[12]

Als Beispiele nennt er den Einsatz von Graphitbomben gegen Elektrizitätswerke, um die jugoslawische Regierung unter Druck zu setzen, sowie das Hacken von geheimen Systemen der Luftabwehr, um deren Leistungsfähigkeit zu mindern.[13] Beide Seiten hätten zudem eine umfangreiche psychologische Kampagne geführt. So habe etwa die NATO Flugblätter verteilt und die jugoslawische Bevölkerung vor einer angeblichen Offensive am Boden gewarnt. Hinzu käme das Hacken von Webseiten mit minderer strategischer Bedeutung. Alles in allem habe der NATO-Krieg gegen Jugoslawien gezeigt, dass Informationsoperationen effektiv seien und daher ausgedehnt werden könnten. Church's Prognose: "Nicht-NATO-Staaten werden defensive und offensive Fähigkeit aufbauen, und die NATO wird die Entwicklung vorantreiben, um auf diesem Gebiet führend zu bleiben."

Lässt sich Informationskriegführung mit dem Völkerrecht vereinbaren? Um diese Frage zu klären, ließ das Pentagon eine Studie erstellen, die im April 1999, während des Krieges gegen Jugoslawien, unter dem Titel "An Assessment of International Legal Issues In Information Operations" erschien und bereits ein halbes Jahr später eine Neuauflage erfuhr.[14] 1998 hatten die Vereinigten Staaten einen Vorstoß Russlands bei den Vereinten Nationen abgeblockt, ein Abkommen zum Verbot von Entwicklung, Produktion und Gebrauch besonders gefährlicher Informationswaffen auszuarbeiten. Doch schon die Definition dieser Waffen erschien den USA unmöglich. Gleichzeitig gaben sie damals vor es gebe Dringenderes, etwa der Schutz von Informationssystemen vor Kriminellen und Terroristen.[15]

Die Studie kommt zu dem Ergebnis, dass die bisherigen Prinzipien des Kriegsrechtes auch auf "Information Operations" anwendbar sind. Schwieriger sei es mit "Information Operations" bzw. Computer-Netzwerk-Attacken in Friedenszeiten. "Es ist alles andere als klar,

inwieweit die Weltgemeinschaft Computer-Netzwerk-Attacken als "bewaffnete Angriffe" oder "Einsatz von Gewalt" betrachten, und wie die Doktrinen der Selbstverteidigung und Gegenmaßnahmen auf Computer-Netzwerk-Attacken angewandt werden."[16] Die Studie erwartet, dass durch Computer-Netzwerk-Attacken angegriffene Staaten sich verteidigen dürfen. Unter Umständen dürften auch traditionelle militärische Mittel als Selbstverteidigung gegen Computer-Netzwerk-Attacken als gerechtfertigt erachtet werden.[17] Schließlich macht die Studie drauf aufmerksam, dass die Handlungen von Staaten die Entwicklungen eines neuen Rechts beeinflussen. Insofern müssten sich die Regierenden in Washington auch der diesbezüglichen Implikationen ihrer eigenen Handlungen bewusst sein.

Bush im Cyberspace

Drei Tendenzen der Politik der Bush-Regierung lassen sich bereits jetzt ausmachen: Erstens wird die Streitkräftereform vorangetrieben, um die amerikanischen Truppen der Vision der Stabschefs näher zu bringen. Zweitens rückt im Zuge des geplanten Aufbaus des Raketenabwehrsystems der Weltraum ins Zentrum strategischer Planung. Hier schließt sich der Kreis zur Informationskriegführung: Die USA sind nicht zuletzt führend auf diesem Gebiet wegen ihrer Satelliten, die ständig neue Überwachungsdaten liefern - und das weltweit. Drittens wird der Schutz der Infrastruktur in Zusammenarbeit mit der Industrie organisiert und ist nicht etwa alleinige Domäne des Militärs.

Bush skizziert die Richtung wie folgt: "Am Boden werden unsere Panzertruppen leichter und unsere leichte Infanterie tödlicher sein. Alle werden einfacher zu stationieren und zu unterhalten sein. In der Luft werden wir punktgenau angreifen, sowohl mit Flugzeugen als auch unbemannten Systemen. Auf dem Meer werden wir Informationen und Waffen neuartig miteinander verbinden und so unsere Fähigkeit, Macht über Land zu projizieren, maximieren. Im Weltall werden wir das für den reibungslosen Ablauf unseres Handels und die Verteidigung unserer Interessen wesentliche Satellitennetzwerk schützen."[18]

"Dominanz ... von Stammeskriegen bis zum Informationskrieg, von Raketen bis zu Biowaffen", ist das Ziel von Andrew Marshall, Chef im Planungsstab des Pentagon.[19] Marshall hat seine Arbeit bereits unter Clinton begonnen. Jetzt beginnt sie Früchte zu tragen: Eine "neue Strategie der Beherrschung eines jeden Konflikts mit begrenzten, aber flexibel einsetzbaren Mitteln fortgeschrittener Technologie", wird das Resultat sein, so die Ansicht von Lothar Rühl, ehemaliger Staatsekretär im bundesdeutschen Verteidigungsministerium.[20]

Die Informationsdominanz erlaubt dem Militär Einsätze, die Lothar Rühl wie folgt beschreibt: "Kleinere Kampfgruppen mit leichterer Ausrüstung, aber optimierten Präzisionswaffen, hoher Zielwirkung und einer Elektronikunterstützung, die den Waffeneinsatz nicht nur punktzielgenau, sondern auch zeitnah zur Zielaufklärung und seine Schadenswirkung schnell überprüfbar macht, sollen den amerikanischen Streitkräften die lang gesuchte, aber nie erreichte weltweite Beweglichkeit und Einsatzflexibilität mit einem breiten Fächer situationsgerechter operativ-taktischer Optionen geben."

Als Donald H. Rumsfeld am 28. Dezember 2000 der Öffentlichkeit als zukünftiger Verteidigungsminister vorgestellt wurde, nannte er die Informationskriegführung eine der Bedrohungen der Zukunft.[21] Auf der Münchner Wehrkundetagung, die sich jetzt Sicherheitskonferenz nennt, erklärte er als neuer US-Verteidigungsminister Anfang des Jahres: "Heute sind wir gegenüber der Bedrohung eines massiven Atomkriegs sicherer als zu jedem anderen Zeitpunkt seit dem Anbruch des Atomzeitalters - aber wir sind heute verwundbarer durch die Kofferbombe, den Cyberterroristen, die rohe und zufällige Gewalt eines verbrecherischen Regimes oder eines mit Raketen und Massenvernichtungswaffen ausgerüsteten Schurkenstaats. Diese sogenannte Welt nach dem Kalten Krieg ist eine integriertere Welt. Folglich sind Waffen und Technologien, die einst nur in wenigen Ländern vorhanden waren, jetzt überall zugänglich."[22]

Konkrete Bedrohungen kann aber bisher niemand nachweisen, deshalb müssen alte und neue Feindbilder herhalten, von Fidel Castro bis Osama bin Laden. So erklärte Tom Wilson, Chef der "Defense Intelligence Agency", bei einer öffentlichen Anhörung im Februar 2001 vor dem "Senate Intelligence Committee", dass die Gefahr bestünde, dass Kuba Informationskriegführung oder eine Computer-Netzwerk-Attacke gegen die USA durchführe. Konkretes konnte er auch auf Nachfrage nicht vorlegen, versicherte dem fragenden Senator aber: "Kuba ist... keine starke konventionelle militärische Bedrohung. Aber seine Fähigkeit zu trickreichen asymmetrischen Taktiken gegen unsere militärische Übermacht könnte bedeutsam sein. Sie haben einen starken Geheimdienstapparat, einen guten Sicherheitsdienst und das Potenzial, unser Militär durch asymmetrische Taktiken zu stören."[23]

Aufsehen sorgte dieses Jahr eine Ankündigung von James Adams, Berater des Geheimdienstes NSA, gegenüber dem Handelsblatt, nachdem die USA den Aufbau eines Abwehrsystems planen, um ihre Computernetzwerke, seien sie staatlich oder privat, vor Angriffen zu schützen. "Das Projekt ist in seiner sicherheitsrelevanten und finanziellen Dimension mit dem NMD zu vergleichen", so Adams unter Anspielung auf die geplante Raketenabwehr, National Missile Defense (NMD).[24] Und Adams weiter: "Wenn ein Staat unsere Wasserversorgung mit einer Cyber-Attacke unterbricht, müssen wir im Stande sein, seine Stromversorgung oder sein Bankensystem lahm zulegen."

Die geschätzten Kosten von 50 Mrd. Dollar, von denen das Handelblatt unter Berufung auf amerikanische Regierungskreise berichtet, sind bisher allerdings offiziell nicht bestätigt. Zudem gibt es in Fachkreisen einige Bedenken gegen die Machbarkeit einer virtuellen Abwehr.[25] Nicht zu vergessen: Im "National Plan for Information Systems Protection" aus dem Jahre 2000 hatte die Clinton-Regierung betont: "Die Bundesregierung kann die kritische Infrastruktur der USA nicht alleine schützen."[26] "Die Regierung schützt sich nur noch selbst", kommentierte Ralf Bendrath treffend.[27] So würde ein virtuelles NMD dem Militär einen Kompetenzzuwachs bringen, da es zur Zeit nur mit dem Schutz der eigenen, militärischen Infrastruktur beschäftigt ist.

Dafür, dass die Bush-Administration weiter auf eine Zusammenarbeit von Staat und Industrie setzt, spricht eine Stellungnahme des Weißen Hauses, nach der - gemeinsam mit der Industrie - eine neue Version des Nationalen Plans für Sicherheit im Cyberspace und zum Schutz kritischer Infrastruktur erarbeitet werden soll.[28] Auch eine Äußerung von Bushs Sicherheitsberaterin Condoleezza Rice weist in diese Richtung.[29] Da nahezu jeder Wirtschaftszweig von funktionierenden Computern abhängig sei, sei der Schutz der kritischen Infrastruktur ein Schlüsselthema für den Nationalen Sicherheitsrat, versicherte sie vor dem Internet Security Policy Forum II in Washington Ende März. Sie setzt weiterhin auf die Zusammenarbeit zwischen Staat und Industrie, die sie als "ohne Beispiel in unserer Geschichte" bezeichnete.

---

* Dirk Eckert ist freier Journalist in Köln und Beirat der Informationsstelle Militarisierung (IMI).

Weitere Informationen zum Thema im Internet:

- Special der Online-Zeitung Telepolis: http://www.telepolis.de/deutsch/special/info/
- Deutsche Mailingsliste Infowar: http://userpage.fu-berlin.de/~bendrath/liste.html
- Information Warfare-Seite der Federation of American Scientists (FAS), mit vielen Links: http://www.fas.org/irp/wwwinfo.html

Fußnoten:

[1] George W. Bush: NATO, Solange wir zusammenstehen, wird die Macht immer auf der Seite von Frieden und Freiheit sein. Rede von Präsident Bush am 13. Februar 2001 im Marinefliegerhorst Norfolk, USINFO-DE.

[2] George W. Bush: NATO, a. a. O.

[3] Vgl. bspw. Ralf Bendrath: Postmoderne Kriegsdiskurse. Die Informationsrevolution und ihre Rezeption im strategischen Denken der USA, in: telepolis, 13.12.1999, http://www.heise.de/tp/deutsch/special/info/6562/1.html

[4] Vgl. Ute Bernhardt/Ingo Ruhmann: Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle, in: Wissenschaft und Frieden, Dossier 24, 1997.

[5] In: Thomas E. Copeland (Hrsg.), The Information Revolution And National Security, August 2000, http://carlisle-www.army.mil/usassi/ssipubs/pubs2000/inforev/inforev.htm

[6] Joseph E. Nye/ William A. Owens: America's Information Edge, in: Foreign Affairs, März/April 1996, S. 20-36.

[7] Nye/Owens: America's Information Edge, a.a.O., hier S. 20.

[8] Vgl. Ute Bernhardt/Ingo Ruhmann: Vom Cyberwar zur digitalen Entspannungspolitik, in: WechselWirkung, Mai/Juni 2001, S. 36-43, hier S. 39.

[9] Vgl. Ute Bernhardt/Ingo Ruhmann: Vom Cyberwar zur digitalen Entspannungspolitik, a.a.O., hier S. 39.

[10] Ute Bernhardt/Ingo Ruhmann: Vom Cyberwar zur digitalen Entspannungspolitik, a.a.O., S. 39.

[11] Lieutenant General S. Bogdanov, Chief of the General Staff Center for Operational and Strategic Studies, Oktober 1991, in: Joint Doctrine for Information Operations, Joint Pub 3-13, 9.10.1998, http://www.dtic.mil/doctrine/jel/c_pubs2.htm, S. II-15.

[12] Vgl. William Church: Kosovo and the Future of Information Operations, http://www.infowar.com/info_ops/treatystudyio.shtml

[13] Church beruft sich dabei auf ranghöhere Air Force-Beamte.
[14] Department of Defense (Office of General Counsel), An Assessment of International Legal Issues In Information Operations, April 1999, http://www.infowar.com/info_ops/info_ops_061599a_j.shtml
[15] Vgl. Department of Defense, An Assessment of International Legal Issues In Information Operations, a.a.O.
[16] Vgl. Department of Defense, An Assessment of International Legal Issues In Information Operations, a.a.O.
[17] Die USA berufen sich nach Art. 51 UN-Charta auf das Recht auf Selbstverteidigung "im Falle eines bewaffneten Angriffs", "bis der Sicherheitsrat die zur Wahrung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen getroffen hat" (UN-Charta Art.51). Als Beispiele aus jüngster Zeit, bei denen die USA das Recht auf Selbstverteidigung in Anspruch nahmen, nennt die Studie: Die Bombardierung von Libyen 1986, die Angriffe auf Irak 1993 (nachdem Attentatspläne auf den früheren Präsidenten Bush bekannt geworden waren), die Angriffe auf eine sudanesische Fabrik und ein Trainingslager in Afghanistan 1998.
[18] George W. Bush: NATO, a.a.O.
[19] So die Charakterisierung von Michael Stürmer in der Welt, 28.3.2001.
[20] Lothar Rühl: Zurück zu interkontinentalen Reichweiten? Das Pentagon öffnet die Perspektiven einer neuen Globalstrategie, in: FAZ, 3.5.2001. Vgl. auch Bernhardt, Ute/Ruhmann, Ingo, Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle, in: Wissenschaft und Frieden, Dossier 24, 1997.
[21] The 43rd President; Comments by Bush and Rumsfeld on Selection for the Secretary of Defense, in: New York Times, 29.12.2000.
[22] Donald H. Rumsfeld: Raketenabwehrsystem soll Bevölkerung und Streitkräfte vor begrenztem Angriff mit ballistischen Raketen schützen, Rede des US-Verteidigungsministers bei der Münchner Konferenz zur Sicherheitspolitik vom 3. Februar 2001, in: USINFO-DE.
[23] Declan McCullagh: Feds Say Fidel Is Hacker Threat, in: Wired News, 9.2.2001, http://www.wired.com/news/politics/0,1283,41700,00.html
[24] Burkhard Ewert/Peter Littger, USA bauen Internet-Schutzschild auf, in: Handelsblatt, 4.3.2001.
[25] Vgl. Ralf Bendrath: Homeland Defense, virtuelle Raketenabwehr - und das schnöde Ende einer Medienhysterie. Die neue US-Regierung auf der Suche nach einer Cyber-Sicherheitspolitik - und die Medien auf der Suche nach einer Story, in: telepolis 28.3.2001, http://www.telepolis.de/deutsch/special/info/7234/1.html. Dort findet sich eine sehr detaillierte Darstellung des derzeitigen Standes der Cyber-Politik der Bush-Administration.
[26] Zit. n. Ralf Bendrath: Elektronisches Pearl Harbor oder Cyberkriminalität? Die Reformulierung der Sicherheitspolitik im Zeitalter globaler Datennetze, in: S+F. Vierteljahresschrift für Sicherheit und Frieden, 2/2000, Manuskript, http://userpage.fu-berlin.de/~bendrath/SuF_2000.rtf
[27] Bendrath: Elektronisches Pearl Harbor oder Cyberkriminalität?, a.a.O.
[28] Vgl. White House Statement on the Review of Critical Infrastructure Protection and Cyber Security, 9.2.2001.
[29] Vgl. Kevin Poulsen: Hack attacks called the new Cold War, in: The Register, 23.3.2001, http://www.theregister.co.uk/content/8/17820.html

---

Datum: 7/2001
Erschienen in: Wissenschaft und Frieden, Nr. 3, 19. Jg, S. 43-46

Original unter:
http://www.dirk-eckert.de/texte.php?id=233
