1999/32 webredaktion

https://shop.jungle.world/artikel/1999/32/die-digitale-intervention

Die digitale Intervention

Von **ralf bendrath**

Von Hacker-Attacken auf feindliche Websites bis zu verdeckten Operationen des US-Militärs: Der Kosovo-Krieg war auch ein Testfall für den Cyberwar.

Nach Science-fiction klang die Meldung, die das US-Nachrichtenmagazin Newsweek im Mai dieses Jahres verbreitete: Hacker des US-Geheimdienstes CIA seien dabei, in die Computer ausländischer Banken einzubrechen und Slobodan Milosevics Konten zu löschen. Autorisiert sei dieser Plan von US-Präsident Bill Clinton selber. Sind damit die in Schundromanen und Hollywoodproduktionen 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 Cyber-Krieg entwickelt und futuristische Planungspapiere geschrieben. Der stellvertretende US-Verteidigungsminister John Hamre bezeichnete den Krieg gegen Jugoslawien bereits im April als den ersten Cyber-Krieg, den die USA führen.

Ein Blick hinter die Kulissen, soweit er möglich ist, relativiert dieses Bild in mehrerlei Hinsicht: 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

Kurz vor Ostern meldete die Nato einen jugoslawischen Angriff aus dem Cyberspace. Die "Attacke", die von einem Belgrader Computer ausging, war allerdings bei genauerem Nachlesen lediglich eine Massensendung von Tausenden E-Mails, die das elektronische Postfach des Militärbündnisses für andere Besucher mehrere Tage lang unzugänglich machte. Frank Rieger, Sprecher des Chaos Computer Clubs (CCC), hält es sogar für wahrscheinlicher, daß die Nato sich einen Computervirus wie "Melissa" eingefangen hat. Dieser Virus, der die Adreßverzeichnisse

von E-Mail-Programmen benutzt, um sich selbsttätig zu verbreiten, hatte im März bereits im Pentagon sein Unwesen getrieben.

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 nutzten, um im Internet gegen die Nato aktiv zu werden. Der größte Teil ihrer Tätigkeit besteht aus dem Füttern von Newsgroups und der Pflege der eigenen umfangreichen Webseite, aber der Mail-Müll könnte ebenso wie die Viren von hier gekommen sein. Nach Informationen von Infoworld.com wurden mindestens fünf neue Computerviren mit diesen E-Mails auf die Nato-Rechner übertragen.

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. 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. Diese Angriffe kamen nach Aussagen des Pentagon ebenfalls aus Serbien, aber nicht unbedingt von Rechnern der serbischen Regierung. 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-Regierungseinrichtungen sowie der britischen Stadt Croydon durch eine Anti-Nato-Seite, in der diese als "National American Terrorist Organization" bezeichnet wurde.

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 Kosovo-Krieg versucht. Einen ernsthafteren Schaden hat nach Berichten der Belgrader Zeitung Blic ein Mitglied der serbischen Hackergruppe Schwarze Hand angerichtet. Es soll Ende März in einen Computer der Navy eingedrungen sein und alle Daten gelöscht haben. Obwohl das US-Verteidigungsministerium diesen Vorfall nie bestätigte, war der Rechner zeitweilig im Internet nicht erreichbar. Dieselbe Hackergruppe, die angeblich in der ideologischen Tradition einer gleichnamigen serbischen Terrororganisation vom Anfang des Jahrhunderts steht, hatte bereits im Oktober 1998 die Webseite des gemäßigten Albanerführers Ibrahim Rugova gehackt.

Internationale 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 passierte mit den Seiten des Energieministeriums, auf denen plötzlich zum Protest gegen die "amerikanischen Nazi-Methoden" aufgerufen wurde. Dort stand auch zu lesen: "Wir sind chinesische Hacker, die sich nicht um Politik kümmern, aber wir dulden es nicht, wenn sehen zu müssen, daß chinesische Journalisten getötet worden sind."

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.

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, wurde die Nachricht von einem erfolgreichen Einbruch auf der Seite in verschiedenen Hackerforen annonciert.

Auch die russische Ablehnung der Nato-Angriffe wurde vom Kreml nicht nur auf dem diplomatischen Parkett vertreten. Eine russische Hacker-Gruppe mit dem Namen "From Russia With Love" - der Titel eines Bond-Films - 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. 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. Nach Angaben des Hacker News Network wurden seit Kriegsbeginn bisher mindestens 14 militärische oder andere staatliche Webseiten gehackt.

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 Cyber-Guerilla 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 zerbombte Telefonleitungen oder Kraftwerke gewesen sein. Die holländische 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.

Betroffen waren auch Webseiten unbeteiligter 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 "Stopp der Nato-Morde" aufrufen. Eine private Seite in Brasilien enthielt plötzlich einen Aufruf gegen Milosevic.

Hacktivismus

Während Hacker früher ihr Hauptinteresse im Aufdecken von Sicherheitslücken sahen, ist dies heute eher Mittel zum Zweck geworden - und die Ziele der Hacker werden immer politischer. Die Politisierung des Hackens führt inzwischen, analog zur außerparlamentarischen Tradition, auch zu Bündnissen, wie die Russian Hackers Union oder die Kosovo Hackers Group zeigen.

Diese neue Verbindung von Computerfreaks und politischem Aktivismus wird als "Hacktivismus" bezeichnet. 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.

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.

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

Bankraub für den Frieden

Ende Mai gelangten die Information über die Cyber-Angriffe der CIA auf die internationalen Bankkonten des jugoslawischen Präsidenten Slobodan Milosevic an die Öffentlichkeit. Milosevic soll nach Erkenntnissen der Geheimdienste Millionenbeträge bei Banken u. a. in Rußland, Griechenland und Zypern deponiert haben. US-Präsident Bill Clinton hat laut Newsweek den Hackern der CIA die Genehmigung 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 unbeteiligter Staaten von den USA angegriffen worden. Der Nato-Partner Griechenland geriet damit virtuell unter friendly fire. 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 zurückschreckten, 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 waren auch die Hacker-Angriffe der CIA auf die Banken vorgesehen.

Der Realitätsgehalt dieser Geschichte ist umstritten: Nach Aussage des Chaos Computer Club ist es technisch durchaus möglich, über das internationale Bankensystem Swift Überweisungen zu fälschen. Geheimdienste wie die amerikanische National Security Agency (NSA) seien dazu in der Lage. Einige US-Geheimdienstmitarbeiter, die von den Plänen wußten, äußerten sich dagegen skeptisch über die Möglichkeit der geplanten Cyber-Angriffe.

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 Schutzrechner ("Firewalls") zu überwinden.

Cyber-Krieg-Offensive

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.

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, sie 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, ein. Die USA würden einen serbischen Hacker, der ähnliches an einer New Yorker Bank versucht, im übrigen als "Cyber-Terroristen" bezeichnen. Eine mögliche Eskalation von Cyber-Angriffen und -Gegenangriffen kann sich unter Umständen zu einer ernsten Bedrohung der USA entwickeln.

Ein von Hackern veranstalteter elektronischer Börsencrash ist seit einigen Jahren der Alptraum der amerikanischen Sicherheitspolitiker, der von den Behörden kräftig genährt wird. 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 verschiedene Abteilungen des Weißen Hauses.

Zum Schutz gegen Angriffe auf die Informationsgesellschaft wurde erst im vergangenen Jahr mit der Präsidenten-Direktive 63 das National Infrastructure Protection Center (NIPC) eingerichtet, das zur Bundespolizei FBI gehört, aber auch dem Pentagon unterstellt werden kann. 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.

Während an der elektronischen Verteidigung gegen Hacker-Angriffe 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. Die öffentliche Debatte der Angriffe auf Nato-Computer kam dem Geheimdienst offenbar gerade recht. Mit den virtuellen Bankeinbrüchen der CIA ist jetzt ein Präzedenzfall geschaffen, der auch nach außen hin, also gegenüber Kongreß und Bevölkerung, einen offensiven Cyber-Krieg legitimiert.

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 (Ö), geheime militärische Computersysteme in der Sowjetunion und in anderen Ländern zu penetrieren". Auch die Streitkräfte beteiligen sich seit Ende der achtziger 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.

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, und 1996 wurde es in das zentrale Planungspapier der Vereinigten Stabschefs (die "Joint Vision 2010") aufgenommen.

Die US Army hat ihre Doktrin für Informationskriege bereits 1996 mit dem neuen Field Manual 100-6, "Information Operations", formuliert. 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. Angehörigen der Streitkräfte ist es verboten, den Begriff "offensive computer operations" in öffentlichen Debatten zu verwenden.

Info-Krieg

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. 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. 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 Golf-Krieg 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, 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. Nach dem offiziellen Wörterbuch des Pentagon umfaßt der 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 ausgenutzt und verteidigt werden". 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. Der damalige Vorsitzende der Vereinigten Stabschefs, General Colin Powell, brachte dies 1991, zur Zeit des Golf-Krieges, 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."

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 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 nicht erreichbar war - eine peinliche Situation für ein Militärbündnis, das gerade dabei ist, die Überlegenheit seiner High-Tech-Streitkräfte vorzuführen.

Ralf Bendrath ist Politikwissenschaftler und Redakteur der Zeitschrift ZivilCourage. Er promovierte an der FU Berlin über "Das Militär der Informationsgesellschaft" und betreibt eine Internet-Mailingliste zu diesem Thema, unter userpage.fu-berlin.de. - Der Text erschien zuerst in antimilitarismus information, Heft 7 /1999.