Cyberwar: Die neue Front

Von **Seymour M. Hersh**

Am 1. April 2001 stieß ein amerikanisches Aufklärungsflugzeug des Typs EP-3E Aries II bei einem Abhöreinsatz über dem Südchinesischen Meer mit einem chinesischen Abfangjäger zusammen und löste so die erste internationale Krise in der Amtszeit George W. Bushs aus. Das chinesische Jagdflugzeug zerschellte, und sein Pilot kam um, während es dem Piloten der US-Maschine, Marine-Leutnant Shane Osborn, gelang, auf einem Stützpunkt chinesischer F-8-Kampfflugzeuge auf Hainan, einer 15 Meilen vom Festland entfernten Insel, notzulanden.

In der amerikanischen Maschine befanden sich 24 Offiziere und Mannschaften, die zum Naval Security Group Command, einer Einsatzgruppe der National Security Agency (Nationale Sicherheitsbehörde, NSA) gehörten. Sie wurden nach elf Tagen repatriiert, wohingegen ihr Flugzeug zurückblieb. Das Pentagon erklärte der Presse, die Besatzung habe ihre Dienstvorschrift befolgt, derzufolge sie die Ausrüstung des Flugzeugs und seine Software mit Hilfe einer Feuerwehraxt und sogar mit heißem Kaffee unbrauchbar machen musste. Dabei ging es unter anderem um ein von der NSA entwickeltes und kontrolliertes Betriebssystem und die zum Abhören verschlüsselter chinesischer Radar-, Sprach- und Elektronik-Nachrichtenverbindungen erforderlichen Treiber. Erst zwei Jahre später gab die Marine zu, dass die Sache nicht so gut gelaufen war. „Eine Gefährdung dadurch, dass der Volksrepublik China unzerstörtes Geheimmaterial in die Hände gefallen ist [...], ist sehr wahrscheinlich und keinesfalls auszuschließen", heißt es in einem Bericht, den die US-Marine im September 2003 herausgab.

Doch der Schaden war sogar noch verheerender, als der Bericht von 2003 nahelegt. Sein ganzes Ausmaß ist bis zum heutigen Tage nicht enthüllt. Von Eric McVadon, einem Vizeadmiral a. D., der einst vor der russischen Küste Patrouille flog und dann in Peking als Militärattaché diente, erfuhr ich, dass die Funksprüche der US-Maschine auf die Zerstörung wesentlicher Teile der elektronischen Ausrüstung schließen ließen. Die Besatzung der EP-3E habe es geschafft, die Festplatte komplett zu löschen – „auszuradieren" –, nicht jedoch die Hardware zu vernichten, weshalb wiederherstellbare Daten zurückblieben: „Niemand hat zum Hammer gegriffen." Schlimmer noch, die Elektronik war erst kürzlich auf den neuesten Stand gebracht worden. „Mancher mag

* Dieser Beitrag des „Blätter"-Demokratiepreisträgers 2007 erschien erstmalig im „New Yorker" vom 1. November 2010. Wir präsentieren die deutsche Erstveröffentlichung in leicht gekürzter Fassung. – D. Red.

gedacht haben, der Schaden werde schon nicht so schlimm ausfallen, aber ich habe an einigen Sitzungen zum Thema der entstandenen nachrichtendienstlichen Kosten teilgenommen", sagte McVadon, „und es sah böse aus." Die Experten der Navy trauten China nicht zu, das von der NSA stammende Betriebssystem des Flugzeugs wieder in Gang bringen zu können, das einem ehemaligen hohen Geheimdienstler zufolge auf zwischen 30 und 50 Millionen Zeilen Computercode zu veranschlagen ist. Wenn sie damit fertig würden, erhielten die Chinesen eine regelrechte Gebrauchsanweisung zur Entschlüsselung geheimer Aufklärungs- und Operationsdaten der US-Marine.

Den US-Verantwortlichen ging erst Ende 2008 das ganze Ausmaß der erlittenen Bloßstellung auf. Wie zwei Mitarbeiter des Nationalen Sicherheitsrats der Bush-Administration sowie deren früherer Aufklärungschef mir eröffneten, begannen die Chinesen einige Wochen nach der Wahl Barack Obamas bestimmte, bekanntermaßen von der NSA überwachte Nachrichtenverbindungen mit einer Flut von *intercepts* – das heißt von den Chinesen abgefangenen amerikanischen Nachrichten – regelrecht zu überschwemmen. Die *intercepts* betrafen unter anderem Einzelheiten geplanter amerikanischer Flottenbewegungen. Offensichtlich ging es den Chinesen darum, den Vereinigten Staaten im Cyber-Poker ihr Blatt zu zeigen.

Doch warum sollten die Chinesen offenbaren, dass sie Zugang zu amerikanischen Nachrichtenkanälen hatten? Einer der *National-Security*-Beamten der Bush-Zeit erzählte mir, manche der damals für Vizepräsident Dick Cheney tätigen Berater hätten geglaubt – oder glauben wollen –, die chinesische Aktion sei als eine Art Begrüßung für Präsident Obama gedacht. Vielleicht ist den Chinesen aber auch, angesichts der Schwierigkeit, in der Cyberwelt mit chirurgischer Präzision zu operieren, lediglich ein Fehler unterlaufen.

Jedenfalls gab das EP-3E-Debakel einer seit Langem geführten Debatte innerhalb des Militärs und in der Obama-Administration neue Nahrung. Viele Militärführer betrachten das chinesische Eindringen in ihren Nachrichtenverkehr als Warnzeichen im Hinblick auf bestehende und künftige Sicherheitslücken – auf die Möglichkeit etwa, dass China oder irgendein anderes Land seine wachsende Cyber-Kompetenz dazu einsetzen könnte, Amerikas zivile Infrastruktur und seinen Militärkomplex anzugreifen. Demgegenüber plädieren andere für eine zivile Reaktion auf diese Bedrohung, insbesondere für einen verstärkten Rückgriff auf Verschlüsselungstechniken. Sie fürchten, wenn man sich zu stark auf das Militär verlasse, werde dies schädliche Folgen für Datenschutz und Bürgerrechte nach sich ziehen.

Nach jahrelanger Vorbereitung nahm im Mai 2010 das *U.S. Cyber Command* offiziell seine Tätigkeit auf. Es führt jetzt die Oberaufsicht über die Aktivitäten verschiedener Sicherheits- und Angriffs-Einheiten im digitalen Bereich, die zuvor über die vier Waffengattungen verstreut waren. Chef des Cyber Command ist General Keith Alexander von der US-Army, ein Geheimdienstler, der erklärtermaßen den E-Mail-Verkehr, soziale Netzwerke und das Internet stärker kontrollieren möchte, um Amerika besser schützen und den Kampf im Cyberspace – in seinen Augen ein neuer Kriegsschauplatz – bestehen zu können. In den kommenden Monaten wird Präsident Obama – der

öffentlich beschworen hat, seine Regierung werde Offenheit und Datenschutz im Internet gleichermaßen schützen – auf diesem Gebiet schwerwiegende Entscheidungen treffen müssen. Es geht um die Zukunft eines sich immer weiter ausdehnenden Labyrinths neuer Kommunikationstechniken: Werden Amerikas Netzwerke der Obhut von Zivilisten oder dem Militär anvertraut? Wird *cyber security* als eine Art Krieg behandelt werden?

Ein militärisch-kybernetischer Komplex

Es geht um eine Menge Geld. Cyber Security ist eine wichtige Wachstumsbranche, und die Warnungen Clarkes[1], McConnells[2] und anderer haben dazu beigetragen, das sich mittlerweile eine Art militärisch-kybernetischer Komplex herausbildet. Die Bundesregierung in Washington gibt derzeit jährlich sechs bis sieben Mrd. US-Dollar für nichtgeheime Aktivitäten im Bereich der digitalen Sicherheit aus und schätzungsweise noch einmal den gleichen Betrag für geheim gehaltene.

Die amerikanischen Geheimdienstler und Sicherheitsexperten stimmen größtenteils überein in der Annahme, das chinesische Militär – aber auch schon ein einzelner unabhängiger Hacker – könnte im Innern der USA theoretisch ein beträchtliches Chaos schaffen. Sachverständige aus Militär, Technik und Geheimdienstpraxis haben mir jedoch gesagt, derartige Befürchtungen seien übertrieben und basierten auf einer grundsätzlichen Verwechslung von Cyber-Spionage und Cyberwar. Bei der ersteren handelt es sich um die Kunst, sich insgeheim in den Nachrichtenverkehr per E-Mail oder andere Formen der Textübermittlung bzw. elektronischer Kommunikation einzuschalten, um Informationen aus Gründen der nationalen Sicherheit oder für geschäftliche Zwecke abzuschöpfen. Beim Cyber-*Krieg* hingegen geht es darum, in ausländische Netzwerke einzudringen, um diese zu stören oder lahmzulegen und funktionsunfähig zu machen. (Einige meiner Gesprächspartner argumentierten, China habe vermittels des EP-3E-Zwischenfalls demonstriert, dass es sich auf Cyber-*Spionage* versteht, den Vorgang jedoch nicht zum öffentlichen Anlass genommen, einen Cyber-*Krieg* zu führen.) Die Verwischung des Unterschieds zwischen Cyberwar und Cyber-Spionage nützt der Rüstungswirtschaft – und entmutigt Datenschutz-Verfechter.

In den meistverbreiteten Horrorszenarien vom Cyberwar geht es um Amerikas Stromnetz. Auch die energischsten Datenschützer würden ja die Notwendigkeit, die Sicherheit der Energieversorgung zu verbessern, kaum bestreiten, doch bisher gibt es überhaupt keinen einzigen Fall, in dem ein Stromausfall nachweislich auf Cyber-Angriffe zurückzuführen wäre. Und die karikaturartige Vorstellung, ein Hacker könne per Knopfdruck im ganzen Lande die Lichter ausgehen lassen, ist ganz einfach irrig. Die Vereinigten

1 Richard Clarke ist ein früherer Berater von US-Präsident Bush zum Thema Cyber-Sicherheit und (Mit-) Autor des Buches „Cyber War: The Next Threat to National Security and What to Do About It", New York 2010. – D. Übs.

2 Bruce McConnell ist Cyber-Sicherheitsberater der Heimatschutzministerin Janet Napolitano und Leiter der Abteilung *Cyber + Strategy* des Ministeriums. – D. Übs.

Staaten haben gar kein landesweites Stromnetz. Es gibt hier über 100 Energiefirmen in öffentlicher oder privater Hand, die ihre eigenen Netze betreiben, und zwar mit jeweils verschiedenen Rechnersystemen und Sicherheitsvorkehrungen. Diese Firmen haben eine Vielzahl regionaler Netze geschaffen, so dass ein Stromversorger im Fall eines digitalen Angriffs auf die Kapazitäten eines benachbarten Versorgungssystems zurückgreifen könnte. Diese Dezentralisierung, die Sicherheitsexperten wie Clarke und viele Militärs beunruhigt, kann also auch Netze schützen.

Im Juli 2010 wurde berichtet, ein „Stuxnet" genannter Computerwurm habe Tausende von Rechnern in aller Welt infiziert. Die Opfer, die zumeist keinen Schaden erlitten, konnten den Angriffen letztlich erfolgreich begegnen, obwohl es manchmal Stunden oder sogar Tage dauerte, sie überhaupt zu entdecken. Einige der Rechner befanden sich im iranischen Kernkraftwerk Buschir, was Spekulationen auslöste, der Virus könnte von Israel oder den Vereinigten Staaten entwickelt worden sein. Von einem Pentagon-Berater für informationelle Kriegführung erfuhr ich, es könne sich um den Versuch eines „semantischen Angriffs" gehandelt haben, bei dem der Virus oder Wurm so konzipiert ist, dass er das Opfer zu der Annahme verleitet, seine Computersysteme arbeiteten ordnungsgemäß, obwohl dies – möglicherweise schon seit einiger Zeit – nicht mehr der Fall ist. (Die Firma Microsoft, deren Windows-Betriebssysteme von dem „Stuxnet"-Wurm hauptsächlich betroffen waren, hat zwischenzeitlich eine langwierige Sicherheitsüberprüfung durchgeführt und Korrekturen vorgenommen).

Falls Stuxnet speziell auf Buschir zielte, so hat es eine der Schwächen von Cyber-Angriffen offenbart: Sie lassen sich nur schwer exakt zielen und ebenso schwer eingrenzen. Indien und China erlitten größere Schäden als der Iran, und der Virus könnte sich leicht auch in eine andere Richtung ausgebreitet und Israel selbst getroffen haben. Hier zeigt sich erneut, dass gerade die Offenheit des Internet der Abschreckung vor dem Einsatz von Cyber-Waffen dient.

Der Kampf der Bürokratien

Der Kampf der Bürokratien um digitale Sicherheit – und um die mit diesem Sicherheitsthema locker zu machenden Haushaltsmittel –, der zwischen den militärischen und zivilen Agenturen tobt, erschwert seriöse Einschätzungen der Gefährdungsproblematik. General Alexander, der Chef des Cyber Command, fungiert zugleich als Direktor der NSA – eine Doppelfunktion, die manche beunruhigt, besonders unter den Verfechtern von Datenschutz und Bürgerfreiheiten. (Formell liegt die NSA im Geschäftsbereich des Verteidigungsministeriums.) Zu Alexanders vorrangigen Zielen gehörte es sicherzustellen, dass das Militär in Sachen Cyber-Sicherheit und bei der künftigen Gestaltung der Computer-Netzwerke die Führungsrolle erhält.

Nominell ist das Heimatschutzministerium, das *Department of Homeland Security* (DHS), für die Sicherheit der zivilen und privaten Infrastruktur Amerikas verantwortlich, aber die Militärführung glaubt, das DHS verfüge nicht

über die zum Schutz der Strom- und anderer Netzwerke erforderlichen Mittel. (Die Heimatschutzbehörde selbst beabsichtigt, im Lauf der kommenden drei Jahre für Cyber-Sicherheit tausend zusätzliche Mitarbeiter einzustellen.) Dieser Streit gelangte im März 2009 an die Öffentlichkeit, als Rodney Beckstrom, der Leiter des National Cybersecurity Center des DHS, plötzlich zurücktrat. In einem Brief an Heimatschutzministerin Janet Napolitano wies er diese warnend darauf hin, dass die NSA de facto die Cyber-Aktivitäten ihrer Behörde kontrolliere: „Bei aller Anerkennung der entscheidenden Bedeutung der NSA für unsere nachrichtendienstlichen Aktivitäten [...] sind unsere demokratischen Abläufe erheblichen Gefahren ausgesetzt, wenn auf der obersten staatlichen Ebene die gesamte Sicherung und Überwachung der Netze in den Händen einer einzigen Organisation liegt." Beckstrom ergänzte, er habe für eine zivile Kontrolle der Cyber-Sicherheit plädiert, „die mit der NSA abgestimmt ist, aber nicht von dieser kontrolliert wird".

General Alexander selbst hat bisher wenig dazu beigetragen, Kritiker des zunehmenden Gewichts der NSA zu beruhigen. Im öffentlichen Teil der Anhörung zu seiner Ernennung vor dem Streitkräfteausschuss des Senats im April 2010 beklagte er ein „Missverhältnis zwischen unseren technischen Möglichkeiten, Operationen durchzuführen, und den geltenden Gesetzen und politischen Vorgaben." Im weiteren Verlauf griff Alexander ein besonders umstrittenes Thema auf: Wann sollen herkömmliche Militärkräfte eingesetzt werden, um einem Angriff auf Netze zu begegnen oder sogar zuvorzukommen? Eines der Probleme, vor denen das Cyber Command in einem solchen Fall stünde – erklärte der General den Senatoren –, wäre es, auf keiner anderen Grundlage als grob umrissenen Einschätzungen der Absichten eines Hackers Gegenmaßnahmen zu konzipieren.

In der Herbstausgabe 2010 der „Foreign Affairs" veröffentlichte William J. Lynn III, stellvertretender US-Verteidigungsminister, einen Artikel, in dem er von der Nutzung der „Verteidigungskapazitäten" der NSA „über den Bereich der [regierungsamtlichen] Internet-Domäne ‚.gov' hinaus" sprach und versicherte: „In konzeptioneller Hinsicht hat das Pentagon offiziell anerkannt, dass der Cyberspace einen neuen Kriegsschauplatz darstellt." Diese Definition wirft Fragen auf, wo die Kampfzone beginnt und wo sie aufhört. Schließt sie zivile Computer in amerikanischen Wohnungen ein, wenn das Militär im „Cyberspace" operiert?

Lynn bezog sich auch auf einen bis dato geheimen Zwischenfall im Jahre 2008, der einige NSA-Kommandeure angesichts des Eindringens in vermeintlich sichere Netzwerke ihrer Stützpunkte zu dem Schluss veranlasste, der Einbruch sei durch Schadsoftware auf einem USB-Stick verursacht worden; Lynn sagte, dieser sei durch „einen ausländischen Nachrichtendienst" infiziert worden. (Presseberichten zufolge kann das entsprechende Programm ebenso gut von Hackern erzeugt worden sein wie seitens einer Regierung.) Lynn sprach von einem „Weckruf" und von einem „Wendepunkt der US-Strategie in Sachen *cyber defense*". Er verglich die gegenwärtige Situation mit jenem Tag im Jahre 1939, als Präsident Franklin D. Roosevelt einen Brief Albert Einsteins erhielt – mit dem Hinweis auf die Möglichkeit atomarer Kriegführung!

Einen wesentlichen Aspekt der Reaktion der NSA-Kommandeure erwähnte Lynn allerdings nicht: Sie hatten befohlen, alle Anschlüsse der in ihren Stützpunkten befindlichen Rechner mit Flüssigzement zu versiegeln. Eine solche Anordnung wäre einem zivilen Umfeld sicherlich kaum zu vermitteln. (Und ein Pentagon-Berater mutmaßte, viele militärische Computer-Verantwortliche hätten den Befehl wohl schlichtweg ignoriert.)

Ein hochrangiger Mitarbeiter des Heimatschutzministeriums charakterisierte das Gerede vom Cyberwar – wie viele meiner Gesprächspartner – als den Versuch interessierter Bürokratien, „Alarm zu schlagen", um dem Verteidigungsministerium auf diese Weise wachsenden Einfluss auf den Schutz privater Infrastrukturen zu verschaffen. „Vom Cyberwar", sagte er, „hört man allenthalben reden. Dies geschieht" – und er erwähnte als Beleg Äußerungen von Clarke und anderen –, „um eine politische Mobilisierung auszulösen. Wir greifen stets auf Kriegsanalogien zurück, um die Menschen zu mobilisieren."

Obamas Cyber-Zar

Theoretisch wäre der Streit darüber, ob Cyber-Sicherheit in die Zuständigkeit des Pentagon oder aber ziviler Agenturen fallen soll, von Präsident Obamas *Cyber-Security*-Koordinator Howard Schmidt, dem Cyber-Zaren, zu moderieren. Aber Schmidt hat bisher wenig dafür getan, seinen Anspruch durchzusetzen. Er hat keinen eigenen Haushaltstitel und wäre im Krisenfall auf die Gnade derer angewiesen, die wie General Alexander über mehr Mittel verfügen. Er war als Cyber-Zar nicht die erste Wahl der Regierung – wie man hört, lehnten mehrere Kandidaten den Posten ab. Einer E-Mail, in der er das Fehlen einer Gesamtstrategie und die „digitale Plünderung" geistigen Eigentums beklagte, fügte der Pentagon-Berater für informationelle Kriegführung eine abschätzige Bemerkung an, wie ich sie auch von anderen hörte: „Paradoxerweise spielt all das sich direkt unter der Nase unseres ersten Cyber-Präsidenten ab. [...] Vielleicht hätte er einen Cyber-Zaren aussuchen sollen, der mehr hat als nur einen Mailorder-Abschluss." (Schmidts Bachelor- und Master-Titel stammen von der University of Phoenix.)

Howard Schmidt mag den Ausdruck „Cyberwar" nicht. „Entscheidend ist, dass *Cyberwar* niemandem nützt", sagte er mir. „Auf diese Tatsache müssen wir uns konzentrieren. Wenn man mir erzählt, irgendjemand oder irgendeine Regierung schicke sich an, das US-Militär durch informationelle Kriegführung unterzukriegen, halte ich dagegen, dass es in der Kriegsgeschichte seit eh und je die Zielvorstellung gibt, die Kommunikation der Kämpfer zu kontrollieren oder zu stören – sei es durch das Umlegen von Telefonmasten oder durch das Abfangen von Morsesignalen. Jetzt haben wir es mit Leuten zu tun, die meinen, Warnungen vor einem ‚Cyberwar' eröffneten unwahrscheinliche Karriereaussichten. Auf einmal sind sie Experten, und man schenkt ihnen große Aufmerksamkeit. ‚Krieg' ist ein großes Wort, und die Medien sind mitverantwortlich dafür, dass die Sache so hochgespielt wird. Manche Leute haben Wirtschaftsspionage im Internet fälschlich als Cyberwar ausgegeben."

Schmidt ist Vietnamkriegsteilnehmer, hat einige Jahre in einem SWAT-Team, einer polizeilichen Spezialeinheit, in Arizona gearbeitet und sich dann beim FBI und der Ermittlungsabteilung der US-Luftwaffe auf Computerkriminalität spezialisiert. 1997 ging er zu Microsoft und wurde dort Sicherheitschef. Nach den Angriffen von *9/11* verließ er die Firma, um der Bush-Administration als Sonderberater für Cyber-Sicherheit zu dienen. Als Obama ihn engagierte, war er gerade Chef der Sicherheitsabteilung von eBay. Auf meine Frage nach dem anhaltenden militärisch-zivilen Streit antwortete Schmidt: „Der Mittelweg besteht darin, keiner einzelnen Gruppe zu viel Macht zu übertragen und sicherzustellen, dass wir unser Wissen miteinander teilen."

„Gewiss", fuhr Schmidt fort, „wir müssen unsere Infrastruktur und unsere Lebensweise schützen. Wir sind in der Tat in mancher Hinsicht verletzlich, und wir sprechen tatsächlich über *Worst-case*-Szenarios" mit dem Pentagon und dem Heimatschutzministerium. „Wenn ein Krieg droht, schaut man nicht einfach zu und wartet ab, bis er da ist." Doch gleichzeitig „müssen wir unsere Seewege offenhalten, weiter Handel treiben und uns frei im Internet bewegen können."

Verschlüsselung als zeitgemäßes Schutzmittel

Wie soll man die Stromversorgung sichern? Es ist für einen versierten Hacker immer noch viel zu leicht, in US-Netzwerke einzudringen. Im Jahr 2008 wurden die Rechner beider Wahlkampfteams, für Obama wie für McCain, Opfer von Hackerangriffen. Man verdächtigte chinesische Hacker. Immer wieder öffnen die Leute E-Mails mit infizierten Anhängen und ermöglichen es so Hackern, ihre Rechner zu „versklaven". Solche Geräte, sogenannte Zombies, können miteinander zu einem „botnet" verbunden werden, das ein großes Netz zu überschwemmen und völlig lahmzulegen vermag. Hacker können auch in einen der großen Server, etwa *Gmail*, eindringen. Schätzungen über die Kosten der Cyber-Kriminalität gehen weit auseinander, aber eine von Präsident Obama in einer Rede vom Mai 2009 zitierte Untersuchung veranschlagte die Kosten auf insgesamt über acht Mrd. US-Dollar in zwei Jahren, 2007/2008. Und im Blick auf geschäftliche Cyber-Spionage fügte Obama hinzu: „Man schätzt, dass Cyber-Kriminelle allein im vergangenen Jahr im weltweiten Geschäftsleben geistiges Eigentum im Wert von bis zu einer Billion Dollar gestohlen haben."

Eine mögliche Lösung besteht in obligatorischer Verschlüsselung: In diesem Fall würde der Staat sowohl Unternehmen wie Privatleute dazu verpflichten, die fortgeschrittensten Schutzinstrumente zu installieren. In dieser oder jener Form erfreut sich diese Option breiter Unterstützung in der IT-Gemeinde und unter Verfechtern der Privatsphäre. Im Gegensatz dazu wehren militärische und nachrichtendienstliche Abhörspezialisten sich bereits seit 1976 gegen eine landesweite Verschlüsselung. (Seinerzeit war gerade der Diffie-Hellman-Schlüsselaustausch – ein von Whitfield Diffie mitentwickeltes Verschlüsselungsinstrument – erfunden worden.) Die Gründe liegen auf der Hand: Ihre

Fähigkeit, Signale abzuhören oder zu stören, würde darunter leiden. In dieser Hinsicht begegnen sich die Interessen der NSA mit jenen der Hacker.

John Arquilla, der seit 1993 an der Postgraduate School der US-Marine im kalifornischen Monterey unterrichtet, schreibt in seinem Buch „Worst Enemies": „Es wäre für uns alle weitaus besser, wenn praktisch der gesamte – zivile, kommerzielle, amtliche und militärische – Nachrichtenaustausch stark verschlüsselt wäre." Stattdessen aber hätten viele Sicherheitsverantwortliche sich die Auffassung zu eigen gemacht, dass der „Cyberspace mit Hilfe virtueller Festungsanlagen verteidigt werden kann – im Wesentlichen mit den allgemein bekannten ‚Firewalls'. [...] Es dominiert eine Art Maginot-Linien-Mentalität." Die amerikanischen Geheimdienste und Strafverfolgungsbehörden, ergänzte Arquilla, hätten sich durchgängig gegen eine Verschlüsselung gewehrt, weil sie fürchteten, ein ernst zu nehmender, breit angelegter Versuch der Datensicherung würde ihre Fähigkeit einschränken, potentielle Straftäter oder internationale Terroristen aufzuspüren und zu verfolgen. Doch dies hat versierte Übeltäter nicht daran gehindert, Hacker zu engagieren oder Dateien zu verschlüsseln. Nur die Öffentlichkeit bleibt dabei ungeschützt, schreibt Arquilla. „Drogenbarone erfreuen sich heutzutage ebenso wie viele Angehörige von Terrornetzwerken immer noch gesicherter Internet-Kommunikation, die meisten Amerikaner dagegen nicht."

Schmidt, der Cyber-Zar, sagte mir, er befürworte eine obligatorische Verschlüsselung im Hinblick auf das amerikanische Stromnetz und die elektrische Infrastruktur, allerdings nicht darüber hinaus. Doch Präsident Obama habe Anfang 2009 die Unterstützung eines solchen Vorhabens abgelehnt, zum Teil wegen der Kosten, die Unternehmen daraus erwachsen würden, sagte Schmidt. Zusätzlich zu den Einrichtungskosten bringen hochentwickelte Verschlüsselungssysteme weitere Belastungen mit sich: Abhängigkeit von Sicherheits-Cards und ständig wechselnden Passwörtern sowie steigende Anforderungen an die Beschäftigten und eine Abgabe von Kontrollbefugnissen der Leiter an ihre Sicherheitsteams.

General Alexander dringt unterdes weiterhin auf die Ausdehnung seiner Machtbefugnisse, sogar auf eine gesonderte Internet-Domäne – noch eine Maginot-Linie, möglicherweise. Im vergangenen September verkündete er eines Morgens vor Journalisten, das Cyber Command benötige eine „Sicherheitszone", wie er sich ausdrückte – einen abgetrennten Bereich im Internet, um Militär und Schlüsselbranchen gegen Cyber-Angriffe abzuschirmen. Diese Sicherheitszone müsse strikter staatlicher Kontrolle unterliegen. Zugleich versicherte er den Journalisten laut „New York Times", dass „wir die bürgerlichen Freiheitsrechte, die Privatsphäre schützen und dennoch unsere Aufgabe erfüllen können."

Der Staat als Spion

Im Sommer 2010 berichtete das „Wall Street Journal", die NSA habe die Finanzierung eines geheimen Überwachungsprogramms namens *Perfect*

Citizen aufgenommen, das Eindringversuche in die Rechnernetze privater Energieerzeuger feststellen soll. Das Programm verlangt, in den betreffenden Netzwerken staatlicherseits gestellte Sensoren zu installieren, die auf ungewöhnliche Aktivitäten achten sollen. Das „Journal" bemerkte, einige Unternehmen hätten Datenschutz-Bedenken geäußert und gemeint, statt dieser Sensoren benötigten sie eigentlich eine bessere Anleitung, wie man sich im Falle eines groß angelegten Cyber-Angriffs verhalten solle. Die NSA reagierte öffentlich, was äußerst selten geschieht, und betonte, mit dem Programm sei keine „Überwachungstätigkeit" verbunden: „Wir halten uns streng an Geist wie Buchstaben der US-Gesetze und -Regeln."

Ein ehemaliger NSA-Agent, mit dem ich sprach, kommentierte *Perfect Citizen* so: Dieses Programm „würde die NSA in die Lage versetzen, unser nationales Kommunikationsnetz zu überwachen. Handelte es sich ausschließlich um amtliche [.gov] Adressen, würde ich mir über die Sensoren keine Sorgen machen, aber was ist, wenn Privatfirmen sich in ihrer Kommunikation auf *Gmail* oder *att.net* [von AT&T] verlassen? Dies [Programm *Perfect Citizen*] könnte dazu führen, dass die NSA schließlich in jedem Internet-Service-Provider des Landes steckt."

Die NSA verfügt über eigene Hacker. Viele von ihnen sind in der Nähe von Baltimore in einem geheimen Nebengebäude des Thurgood International Airport untergebracht. Dort sitzen Angreifer-Teams, die in die Kommunikationsnetze befreundeter wie gegnerischer Regierungen einzudringen versuchen, neben Verteidiger-Teams, die Eindringaktionen und -versuche in US-Systeme aufspüren sollen. Der eben zitierte NSA-Agent, der in einer wichtigen Geheimanlage als hochrangiger Observationsspezialist tätig war, erzählte mir, während des Irakkriegs von 1991 habe die NSA unschätzbare Praxiserfahrungen mit digitaler Spionage sammeln können. Im Kosovokrieg 1999 und später im Kampf gegen Al Qaida im Irak habe sie ihre Techniken vervollkommnet. „Was auch immer die Chinesen gegen uns unternehmen könnten, wir können es besser", sagte dieser Praktiker. „Unsere offensiven Cyber-Kapazitäten sind erheblich weiter entwickelt."

Dennoch behauptet Marc Rotenberg, Präsident des *Electronic Privacy Information Center* und führender Datenschützer, die NSA sei ganz einfach nicht kompetent genug, um in Sachen Cyber-Sicherheit eine Führungsrolle zu übernehmen. „Lassen wir das Thema der Vertraulichkeit in der Kommunikation einmal beiseite", sagte Rotenberg, der früher als Senatsmitarbeiter tätig war und oft vor dem Kongress über Verschlüsselungsstrategien und Verbraucherschutz ausgesagt hat. „Die eigentliche Frage ist doch: Wollen wir, dass eine Agentur, die mehr oder weniger erfolgreich Spionage treibt, für die Gewährleistung der Sicherheit unseres Landes verantwortlich sein soll? Wer das will, muss verrückt sein."

Vor fast zwei Jahrzehnten erklärte die Clinton-Administration unter dem Druck der NSA, sie werde den Export von mit Verschlüsselungstechnik ausgerüsteten Rechnern nur unter der Bedingung gestatten, dass die amerikanischen Hersteller sich bereit erklären, in jeden dieser Rechner einen amtlich registrierten Chip, den sogenannten Clipper Chip, einzubauen. Später kam

heraus, dass der Clipper Chip es Strafverfolgungsbehörden ermöglichen würde, sich Zugang zu den Computern zu verschaffen. Der dadurch entfachte Datenschutz-Tumult brachte den Präsidenten in Verlegenheit, woraufhin die mit Verschlüsselungstechnik ausgestatteten Rechner doch ohne den ominösen Chip exportiert werden durften – was auf ein Zusammenstauchen der NSA hinauslief.

Diese Geschichte könnte sich wiederholen. Die Obama-Administration erwägt derzeit, eine neue Rechtslage zu schaffen, die es den Verantwortlichen für Nationale Sicherheit und den Strafverfolgungsbehörden gestatten soll, Online-Verbindungen zu kontrollieren. Nach der so veränderten Rechtslage wären die Hersteller von Geräten wie dem „Smartphone" *BlackBerry* und alle in- wie ausländischen Kommunikationsanbieter wie etwa *Skype*[3], ähnlich wie schon vor zwei Jahrzehnten in der Debatte über den Clipper Chip angepeilt, zur Entwicklung technischer Vorkehrungen verpflichtet, die der Bundesregierung das Abschöpfen und Entschlüsseln des Nachrichtenverkehrs gestatten.

„Der NSA geht es um Sicherheit, gewiss, aber sie möchte auch möglichst viele Daten erbeuten können. In ihren Augen erhält man optimale Sicherheit, so lange man mithört", sagte Rotenberg. „General Alexander hat kein Interesse am Datenschutz. Er drängt nicht etwa darauf, dass verschlüsselt wird. Er möchte mehr über die Leute wissen, die im Internet sind – er will Zugang zu den originären IP-Adressen, mit denen die Computer zu identifizieren sind, die E-Mails verschicken. „Alexander will die Benutzer-IDs. Er möchte wissen, mit wem Sie sprechen."

Rotenberg gesteht dem Staat zu, dass er auch in der Cyber-Welt eine Rolle zu spielen hat. „Wir Datenschutz-Leute wollen wirksame Verschlüsselungsverfahren zur Sicherung der amerikanischen Infrastruktur", sagte er. Er unterstützt auch Howard Schmidts Wunsch, für die wenigen Industriezweige, deren Störung ein Chaos auslösen könnte, die Datenverschlüsselung verbindlich vorzuschreiben.

Ein Feind wird gebraucht

Was ist mit China? Stellt es eine so große Bedrohung dar, dass allein diese es rechtfertigt, das Thema digitale Sicherheit kriegsmäßig anzugehen? Die Vereinigten Staaten haben China lange Zeit als militärstrategische Bedrohung angesehen, und in dem nunmehr 60 Jahre andauernden Streit um Taiwan galt es als potentieller Kriegsgegner. In Krisenplänen aus der Zeit des Kalten Krieges finden sich Empfehlungen, Amerika solle militärisch reagieren und eine Flugzeugträgergruppe entsenden, falls eine chinesische Flotte in die Formosastraße einliefe. Doch die Vorstellung einer Seeschlacht um Taiwan und ihrer Eskalation zu einem Cyber-Angriff auf Amerikas Infrastruktur erscheint ziemlich abwegig. Im Juni 2010 schloss Taiwan ein Handelsabkommen mit China, das – im Endergebnis – auf eine politische Annäherung zielt.

3 So nennt sich eine kostenlose Software, die das Telefonieren per PC ermöglicht. – D. Übs.

Über eines sind sich die Experten in Sachen Cyber-Sicherheit überraschend einig: nämlich dass die unmittelbare Cyber-Bedrohung nicht von herkömmlichen Terrorgruppen wie Al Qaida ausgeht, jedenfalls nicht im Augenblick. „Terroristische Organisationen sind gegenwärtig nicht besonders gut darin, unser Computersystem anzugreifen", sagte mir John Arquilla. „Sie sind daran nicht so interessiert – noch nicht. Die Frage ist: Gibt es tatsächlich Sicherheitslücken im amerikanischen Binnenland? Wenn es sie gibt, werden die Terroristen sie sich eines Tages zunutze machen." Arquilla fügte eine beunruhigende Überlegung hinzu: „Die Terroristen von heute sind auf den Cyberspace angewiesen, und sie müssen sich mit Cyber-Sicherheit auskennen, um *ihre eigenen* Operationen zu schützen." Wenn Terrorgruppen aber die Cyber-Defensive besser beherrschen, könnten sie sich am Ende der Offensive zuwenden.

Was spricht dagegen, die Datenschutz-Gemeinde zu ignorieren und die Cyber-Sicherheit als potentiellen Kriegsschauplatz zu behandeln? In einer Zeit des internationalen Terrorismus und wachsender Spannungen zwischen Amerika und der islamischen Welt mag es vielen weise erscheinen, dem Militär besseren Zugang zur privaten Internetkommunikation zu gestatten. Doch militärische Aktivitäten zeitigen stets unvorhergesehene Konsequenzen – darunter solche, deren Bewältigung dann möglicherweise viele Jahre dauert. Paradoxerweise bietet die eingangs berichtete Geschichte des EP-3E-Flugzeugs, das vor der chinesischen Küste zum Absturz gebracht wurde, ein schlagendes Beispiel.

Der Absturz im Interregnum

Die Geschichte beginnt, wie ein bestens informierter US-Diplomat a. D. mir berichtete, mit dem Streit um die Bestimmung des Wahlsiegers im November 2000 – Vizepräsident Al Gore oder George W. Bush. In jenem Herbst war eine militärische Routineprüfung zu dem Schluss gekommen, bestimmte Aufklärungsflüge vor der Ostküste der früheren Sowjetunion – tägliche Einsätze von Luftwaffen- und Marinefliegern von Stützpunkten auf den Alëuten aus – seien überflüssig geworden. Es wurde empfohlen, die Zahl dieser Einsätze einzuschränken. „Schließlich wurden die Flüge am Vorabend der Wahl tatsächlich reduziert", berichtete der frühere Diplomat. „Aber es gab niemanden, der befugt war, Änderungen vorzunehmen, und jedermann suchte nach einem Job." Tatsache ist, dass kein Militärbefehlshaber jemals von sich aus eine Mission aufgeben würde. „Also schaltete das System automatisch auf das nächste Ziel um, nämlich China, und die dortigen Aufklärungsflüge wurden von einmal alle 14 Tage auf ungefähr einmal pro Tag vermehrt", fuhr der Ex-Diplomat fort. Anfang Dezember dann „reagierten die Chinesen aggressiv auf unsere mittlerweile vermehrten Erkundungsflüge, und wir wiederum führten bei unseren Militärs Klage über die chinesischen Beschwerden. Aber in Washington gab es damals niemanden, der sich politisch befugt sah, zu reagieren oder Erläuterungen abzugeben." Niemand hätte den Chinesen erklärt, dass die Zunahme der amerikanischen Aufklärungstätigkeit keine

andere Ursache hatte als die, dass der politische Alltag in Washington in jenen Wochen dem Trägheitsgesetz unterlag. Es gab im Verteidigungsministerium keine Führungsverantwortung, solange Demokraten wie Republikaner gleichermaßen darauf warteten, dass der Oberste Gerichtshof über das Schicksal der Präsidentschaft entschied.

Das vorhersehbare Ergebnis bestand in einem zunehmend provokativen Verhalten der chinesischen Jägerpiloten, die die US-Aufklärer abhören und beschatten sollten. Es entstand ein Muster der Belästigung: Chinesische Kampfflieger kurvten nur wenige Dutzend Yards entfernt vor der langsam dahinfliegenden EP-3E herum, zündeten dann plötzlich die Nachbrenner, schossen davon und hinterließen eine Schockwelle, die das amerikanische Flugzeug übel durchrüttelte. Am 1. April 2001 passierte es dann: Der chinesische Pilot schätzte den Abstand zwischen der eigenen und der amerikanischen Maschine falsch ein. Welche Folgen dieser Fehler für die amerikanische Debatte über Cyber Security letztlich haben wird, ist überhaupt noch nicht absehbar.