Reporter FORUM

www.reporter-forum.de

Angriff aus dem Cyberspace

Computerhacker fallen über westliche Konzerne her. Oft führen ihre Spuren nach China. Auch die USA rüsten für den digitalen Wirtschaftskrieg. Eine Reise ins Krisengebiet

Von Götz Hamann und Thomas Fischermann, Zeit, 18.02.2010

Die Sache mit den Nacktfotos war primitiv, aber erfolgreich. Die Studentin Yin Hong von der Maritime University in Shanghai hatte sich von ihrem Freund ohne Kleider ablichten lassen, angeblich, und später kursierten 30 solcher Bilder im Internet. Sie verbreiteten sich massenhaft. So weit, so normal.

Allerdings hatten Hacker viele dieser Fotos mit kunstvoll programmierten Datenanhängen präpariert. Sie hatten Programme in ihnen versteckt, die in aller Stille die Computer der Spanner unterwanderten, sobald eins der Bilder geöffnet wurde. Eine Hintertür ging dann für die Hacker auf. Sie konnten Dateien lesen oder löschen. Sie konnten Passwörter entwenden oder gar per Webkamera sehen, wer gerade vor dem Rechner saß.

Solche Tricks gibt es so lange, wie es Computer gibt. Genauso alt ist das Katz-und-Maus-Spiel zwischen anarchischen Computerfreaks und nervösen Sicherheitsexperten, zwischen Flaumbartträgern in Jugendzimmern und Schnauzbärten in Konzernen und Behörden. Die Öffentlichkeit hat sich selten dafür interessiert. Jetzt sollte sie es aber. Denn aus der Spielerei ist Ernst geworden. Ein elektronisch geführter Wirtschaftskrieg, der über die Macht im Informationszeitalter entscheidet. Es geht um die Verteilung von Datenressourcen, die wichtiger sind als Öl. Und es geht um die Verlässlichkeit einer Infrastruktur aus Computern und Datenleitungen, auf der die Staaten des Westens ihren Wohlstand bauen. »Das ist ein Angriff auf das Herz, auf die Quelle unseres Wohlstands«, erregt sich Simon Rosenberg, der Leiter eines Thinktanks namens New Democratic Network. James Mulvenon, ein US-Experte für Militärtechnik und Cyberspionage, sagt: »Wir haben eine neue Eskalationsstufe erreicht.«

Als Vorbote dieses neuen Wirtschaftskrieges gilt eine mehrjährige Angriffswelle, der amerikanische Sicherheitsexperten den Codenamen Titan Rain gaben. Unbekannte Hacker nahmen Anfang des Jahrzehnts systematisch Rüstungs- und Industrieziele in den USA aufs Korn, darunter den Flugzeugbauer Lockheed Martin und Elektrizitätswerke. Sie hätten Baupläne und Geschäftsinformationen im großen Stil entwendet, heißt es in Sicherheitskreisen.

Seither sind die Abstände zwischen den Großangriffen kleiner geworden. Es traf Computersysteme in Nordamerika, Europa, Asien. Anfang des Jahres 2009 stahlen Hacker Baupläne des neuen US-Kampfflugzeugs Lightning II. Im April infiltrierten Unbekannte das Stromnetz der USA und hinterließen Programme, die den Betrieb massiv hätten stören können. Im Sommer wurden 100 kalifornische Hightechunternehmen übers Internet bestohlen.

Und dann kam der Tag, an dem Google zugab: Auch wir sind gehackt worden! Nicht einmal der Konzern, der sich für die größte Versammlung von Computergenies auf dem Planeten hält, hatte sich schützen können. Auch nicht die anderen zwei Dutzend Konzerne, die es bei der gleichen Attacke erwischte: Die Washington Post nennt das Onlineportal Yahoo!, die Softwarehersteller Symantec und Adobe sowie den Rüstungskonzern Northrop Grumman. Auch Banken sollen betroffen sein.

Die Attacke »war gut organisiert«, sagt Google-Vorstand David Drummond knapp.

Doch amerikanische Ermittler erzählen inzwischen mehr, und es ist eine Blamage für den Weltkonzern. »Nach unseren Untersuchungen waren es etwa fünf Leute, nicht viel mehr, die Google und die anderen Firmen angegriffen haben«, sagt Eli Jellenc, Leiter der iDefense Research Laboratories nahe der US-Hauptstadt Washington. Seine Einheit gehört zu einem weltweit führenden Anbieter von Sicherheitssoftware. Der Angriff traf auch einige seiner Kunden. Deshalb hat Jellenc alles darangesetzt, mehr über die Hacker zu erfahren. Es ist ihm gelungen.

»Wir haben Teile des Programmcodes, mit dem die Firmen angegriffen wurden, in chinesischen Hackerkreisen wiederentdeckt«, erzählt Jellenc. Durch einen Informationsaustausch innerhalb der Sicherheitsszene sei zudem herausgekommen, dass diese Hacker »in den sechs Monaten zuvor vergleichbare, wenn auch kleinere Angriffe unternommen haben«. Hacker haben eben Gewohnheiten. Sie schleichen sich auf Wegen an, die ihnen schon vertraut sind.

So war es auch im Google-Fall. Ein Indiz ist der Computer, von dem aus die Angriffe gesteuert wurden. Er steht in Taiwan, und es gebe, so Jellenc, eine Verbindung mit früheren Attacken, die von Hackern verübt wurden, die entweder direkte Agenten des chinesischen Staates waren oder deren freischaffende Zuarbeiter. Die Angreifer hatten es auf Geschäftsgeheimnisse abgesehen. Wie viel sie mitgehen ließen, verrät keines der Opfer. Stattdessen klagte Google laut, bei der Attacke seien E-Mail-Konten politischer Aktivisten abgefischt worden.

Genauer lässt sich rekonstruieren, wie die Angreifer eindrangen, und hier zeigt sich nach Aussage der Ermittler ihre große Könnerschaft. Nicht nur ein oder zwei, sondern rund ein Dutzend Softwarewerkzeuge seien zum Einsatz gekommen. Mit ihnen bahnten sich die Hacker einen Weg durch mehrere bisher unbekannte Sicherheitslücken in populären Programmen. Das begann ähnlich wie bei den Nacktfotos. Nur verschickten die Hacker – statt Fotos einer unbekleideten Frau – freundliche E-Mails, die vielerorts Vertrauen erweckten. Dies zeuge, so iDefense-Leiter Jellenc, »von hoher sozialer Intelligenz«.

In einer Variante brachten die Angreifer ihre Opfer dazu, eine unverfänglich anmutende, aber verseuchte Datei zu öffnen. An ihr hing ein Schadprogramm, Trojan.Hydraq genannt, mit dem man den Computer dann fernsteuern und anzapfen konnte. In einer zweiten Variante stellte die E-Mail eine Verbindung zu einer präparierten Internetseite her. Sobald die Verbindung stand, soll wieder Trojan.Hydraq durch eine Sicherheitslücke im Internetprogramm Explorer auf die Computer geschleust worden sein. So schildern es Ermittler.

Eine Handvoll Hacker hat also ausgereicht, um die Sicherheitssysteme von Google zu knacken. Ein fast unglaublicher Vorgang, der die Frage aufwirft, welches auf einem

Computer gespeicherte Geschäftsgeheimnis in der westlichen Hemisphäre noch sicher ist.

Genau dies ist der Grund, warum die Regierung der Vereinigten Staaten ihr Schweigen gebrochen und die Hackerangriffe zu einem politischen Streitfall ersten Ranges mit China erhoben hat. Denn Hackerangriffe gehen zwar von vielen Ländern aus, von Russland, Brasilien, Taiwan, Israel und sogar von Deutschland – doch Sicherheitsexperten sind davon überzeugt, dass die ganz große Mehrzahl in China ihren Ursprung hat.

Erst meldete sich der stellvertretende Außenminister Kurt Campbell. »Präsident Obama schätzt die Sicherheit im Cyberspace als vordringliches nationales Interesse ein«, erklärte er. Dann sandte die Regierung in Washington eine formelle Protestnote nach China, und Hillary Clinton hielt eine so alarmierende Rede über Internetsicherheit, wie sie noch kein US-Außenminister vor ihr gehalten hatte: »Unsere Fähigkeit, digitale Bankgeschäfte und Onlinehandel zu betreiben, geistiges Eigentum im Wert von Abermilliarden Dollar zu schützen, das alles steht auf dem Spiel, wenn wir uns nicht auf die Sicherheit unserer Informationsnetze verlassen können.«

Verlassen können? Noch während Clinton sprach, waren die Sicherheitsexperten in Aufruhr über eine erneute Großattacke. »Es ist ein wiederkehrendes Muster«, sagt Amit Yoran. Der Mann war bis vor vier Jahren George W. Bushs Gesandter für die digitale Sicherheit des Landes. Heute berät er mit seiner Firma NetWitness jene Unternehmen, die Angst vor Hackern haben, und er sagt: »Wir untersuchen gerade eine riesige Hackerattacke. Der Fall ist noch nicht öffentlich bekannt. Infiltriert wurden rund 100000 Computer in mehr als 1000 Firmen.«

Auch in Deutschland und Europa?

»Ja.«

Wurde etwas gestohlen?

»Geistiges Eigentum, Finanzinformationen und persönliche Daten der Mitarbeiter.«

Was genau?

»Das darf ich nicht sagen. Und im Detail können wir es auch noch nicht überblicken.«

Wer war es?

»Die Spuren führen in mehrere Staaten – aber auch wieder nach China.«

Der Meisterhacker hat ein Schlupfloch aufgetan. Es ist Montagabend in Toronto, draußen ist es dunkel geworden, und Nart Villeneuve wird gleich seine kleine Tochter ins Bett bringen. Aber mit seinen Gedanken ist er bei drei interessanten Computern, die er im Internet entdeckt hat. Es sind sogenannte Kommandoserver, die es Hackern ermöglichen, weitere Computer im Internet zu kontrollieren. Rechner in Firmen oder Wohnzimmern, die sie vorher mit Viren und ähnlichem digitalem Ungeziefer verseucht haben.

Hacker, die so etwas tun, führen selten Gutes im Schilde. Es gibt Kommandoserver, die Hunderte, Tausende und sogar Zehntausende Rechner steuern können. Ein Mausklick, ein paar Eingaben, und diese Computer werden zu einer Armee in den Händen der Hacker: Sie verschicken Werbe-E-Mails, sie bombardieren

Computersysteme, bis diese wegen Überlastung abgeschaltet werden müssen, und sie können der Spionage dienen. Villeneuve will herausfinden, für welche Aufgaben die frisch entdeckten Kommandoserver vorgesehen sind. »Wenn man so etwas gefunden hat, muss man dranbleiben. Man weiß ja nie, wie lange dieses Schlupfloch noch offen ist«, sagt er.

Nart Villeneuve. 35 Jahre alt. Ein großer, kräftiger Typ, der bequeme Gebrauchskleidung in Khaki trägt und einen abwaschbaren Anorak darüber. Ungeduldig stapft er vom linken auf den rechten auf den linken Fuß, die kräftigen Finger vor dem Bauch verschränkt, während der Drucker einige Seiten mit technischen Detailangaben produziert. Er wirkt ungeduldig. Es geht ihm zu langsam, hier draußen in der richtigen Welt.

Wenn Villeneuve erst in den Cyberspace eintaucht, wenn er einen seiner Codenamen wie MC annimmt und durch ferne Datennetze streift – dann zeigt sich die wahre Qualität eines Meisterhackers. Er hat die Geduld eines Jägers. Er kann unendlich lange verharren und lauern. Aus kleinsten Datenspuren liest er ab, wie die Guten ihre Sicherheitsprogramme konfigurieren und wohin die Bösen ihre Schadprogramme schicken. Er notiert Internetadressen, E-Mails, die eitlen Künstlernamen anderer Hacker. Er schaut nach, ob sie schon einmal früher benutzt worden sind und ob man Orte, Namen, gar Telefonnummern mit ihnen verbinden kann.

»Früher oder später machen Leute einen Fehler«, sagt er. »Dann kann ich ganz genau sehen, was sie treiben.«

Villeneuve will auf der Seite der Guten stehen. Er will ergründen, wer hinter den Attacken auf Bürgerrechtler, Firmen oder Staaten steckt. Mal arbeitet er für die Universität Toronto als Internetforscher. Mal ist er Cheftechniker einer kleinen Firma, die Zensursperren im Internet knackt. Dann wieder wirkt er als Vordenker an aufsehenerregenden Studien der »OpenNet Initiative« mit, die staatliche Internetzensoren in 71 Ländern überwacht.

Nart Villeneuve hatte maßgeblich seine Finger im Spiel, als Ende 2008 das GhostNet enttarnt wurde. Der Fall machte damals Schlagzeilen in aller Welt: Unbekannte Hacker hatten es geschafft, mindestens 1295 Computer in 103 Ländern zu einem Verbund zusammenzuschalten, der nur einen Zweck haben konnte – Spionage im ganz großen Stil.

Der Dalai Lama, ausgerechnet der Dalai Lama, hatte eine Gruppe von Sicherheitsexperten im Umfeld der Universität Toronto um Hilfe gebeten. Die tibetische Exilregierung sorgte sich. Wurden die Computer ihres Hauptquartiers im indischen Dharamsala und die in London, Brüssel und New York von Hackern unterwandert? Von militärischen Staatssicherheitskräften gar? Ein Kollege Villeneuves fuhr hin und merkte schnell: Auf den Computern waren einige wohlbekannte Schädlinge abgelegt, unter denen das chinesische Spionageprogramm »gh0st Rat« war. Die Geisterratte.

Noch während die Kanadier die Computer näher untersuchten, merkten sie, dass wirklich jemand aus der Ferne am Werk war. Dokumente wurden vor ihren Augen kopiert und an einen unbekannten Ort im Internet verbracht. Und als das Team um Nart Villeneuve die Schadprogramme einem Virustest unterzog, fanden nur 11 von 34

Antivirusprogrammen überhaupt etwas Beanstandenswertes. »Eine Menge von diesem Zeug rauscht an den Schutzprogrammen einfach vorbei«, sagt der Meister.

Es ist eine unbequeme Wahrheit. Ohne Computer und das Internet läuft heute so gut wie nichts mehr – aber sie stecken voller Sicherheitslücken. Das Internet war ursprünglich eine Erfindung amerikanischer Militärs, doch selbst die Militäroffiziere hatten es nie so konzeptioniert, dass es besonders sicher war. Das Internet sollte einfach funktionieren, es sollte auch unter widrigen Bedingungen die Kommunikation und den Datenaustausch aufrechterhalten. Und die kommerziellen Firmen, die später die Weiterentwicklung des Internets übernahmen, fanden Sicherheitsfragen eher störend. Sie wollten Kunden gewinnen. Auch solche, die von Technik keine Ahnung haben. Sie sollten alles einfach bedienen können. Das war die Hauptsache, doch so viel Sorglosigkeit macht es Hackern leicht.

Villeneuve gelang es am Ende, selbst die Kontrolle über jene Computer zu übernehmen, die da offenbar die Tibeter überwachen sollten. »Die hatten das nicht vernünftig gesichert«, sagt er, während ein diebisches Lächeln über sein Gesicht huscht. Zwei Wochen lang war er selbst der Herr über dieses Schattennetz. Er hätte den Marsch der Geisterratten befehligen können. Doch er sah nur zu, zu welchen Missionen sie unterwegs waren.

Und tatsächlich: Der Dalai Lama war offenbar nur eine Nebenfigur. Das GhostNet reichte in mehrere Außenministerien hinein, in Botschaften, Verbände, Banken, Nachrichtenagenturen, Wirtschaftsprüfungsgesellschaften und Handelsfirmen. »Völlig zweifelsfrei konnten wir nie nachweisen, wer hinter diesen Angriffen steckt«, sagt Villeneuve. Er fand heraus, dass die Rechner der Hacker irgendwo auf der chinesischen Insel Hainan standen. Und dass sie offiziell nicht zu einer militärischen oder staatlichen Einrichtung gehörten.

Einzelne Hacker oder ganze Staaten? Mit der Frage ist Villeneuve oft konfrontiert, und er weiß, wie schwer sie zu beantworten ist. Er hat schon kleine Hackergruppen und sogar Einzeltäter – Studenten in Moskau, einsame Computergenies in Birma – überführt, die so geschickt im Internet betrogen oder randalierten, dass alle eine gewaltige Organisation dahinter vermuteten. Und umgekehrt.

Xiao Wang schlägt als Ort für ein Treffen das Village vor, das modernste Ausgehviertel von Peking. Es wurde erst zu den Olympischen Spielen eröffnet. Die Glasfassaden hat ein japanischer Architekt entworfen und so verwinkelt aufstellen lassen, dass ein Labyrinth aus Gassen, Übergängen und Tunneln entstanden ist.

Der Mann kennt in Peking viele Hacker persönlich, kennt ihre Gesichter und nicht nur ihre Codes. Xiao Wang, das ist sein Tarnname, bestellt einen Thunfisch und trinkt einen Waldbeerensaft. Im Restaurant Element Fresh mischen sie gern chinesische und westliche Rezepte. Xiao Wang sagt, dass »die Hackerszene in Peking ähnlich heterogen ist wie die Musikerszene«. Immerhin, einen Unterschied gebe es. Während Musiker und ihre Fans wenigstens zu Konzerten zusammenkommen, sind die Hacker hauptsächlich übers Web verbunden. Sie hausen in irgendwelchen Plattenbauten, mieten die Wohnungen für ein paar Monate, stellen ihre Computer auf Spanplattentische, nebendran eine Klappliege, und los geht’s. Wenn es sein muss, haben sie ihre Sachen in 30 Minuten gepackt.

Es ist ein Paradox, dass mitten in China – in einem Staat, der Polizisten in Internetcafés aufpassen lässt und das Netz streng kontrolliert – schon Mitte der neunziger Jahre eine Kultur von Hackern entstand. Manche sind politisch motiviert: nationalistisch gesinnte junge Leute, die sich zu Gruppen wie der »Roten Hackerallianz« zusammengefunden haben, um ihren Nationalstolz an ausländischen Webseiten auszuleben. Einzelgänger geben sich Künstlernamen wie »Guter Wille« oder »Einsamer Schwertkämpfer«. Die chinesischen Hacker gehören zu den besten der Welt.

Zunehmend spielen kriminelle Motive eine Rolle – ähnlich wie in jenen russischen Hackerbanden, die Kreditkartendaten über das Internet stehlen oder Computer lahmlegen und die betroffenen Firmen dann erpressen. Scott Henderson, der für ein Geheimdienstinstitut der US-Armee jahrelang die Szene untersucht hat, sagt über die neuen chinesischen Banden: »Die verkaufen Hintertüren in Onlinespiele, sie veräußern Viren, Trojaner und Hackertricks, das alles hat eine sehr geschäftsmäßige Seite entwickelt.« Eine bislang unentdeckte Lücke in einem beliebten Programm oder Computerbauteil könne einem Hacker Zehntausende Dollars einbringen.

Informanten aus der chinesischen Hackerszene berichten aber auch, dass es zuletzt vereinzelte Kooperationen mit dem Staat gegeben habe. Das Militär zahle gut, wenn eine freie Hackerbude in seinem Auftrag ein Problem löse. »Wir kennen einige Mitglieder solcher Hackergruppen, die in den Staatsdienst gewechselt sind«, sagt der Geheimdienstmann Henderson dazu. »Ich denke, das ist einfach ein Teil des Erwachsenwerdens. Ein Karriereschritt.« Der Beginn einer Beamtenkarriere chinesischer Art.

In Hackerkreisen machen sie keinen Hehl daraus, dass die Volksarmee unter ihnen ist. Hohe Offiziere reisten durchs Land und veranstalteten Hackerwettbewerbe, berichten einschlägige Foren im Internet. Auf mindestens zwei Hackerwebseiten hat das Forschungsinstitut der Staatssicherheit Jobanzeigen veröffentlicht. Die Regierung hat Universitätsprogramme gegründet, die in der Kunst des Cyberkampfes unterrichten.

»Die staatlichen chinesischen Hackerangriffe haben einen bestimmten Stil«, sagt Xiao Wang. Da werde »nicht wild herumgestöbert, sondern gezielt ausgeräumt«. Chinesische Armeehacker forschten in größeren Gruppen an neuen Techniken, an Schwachstellen in den Computern, Programmen und Netzbauteilen des Westens. Sie führten komplexe Angriffe aus, die einzelne Hacker gar nicht koordinieren könnten. Großangriffe mit militärischer Präzision. Und doch kommen die Staatsspione gelegentlich später als die freien Hacker. »Manchmal haben sie«, grinst der Informant Xiao Wang, »schon Nachrichten in US-Unternehmen vorgefunden, nach dem Motto: Ätsch, wir waren schon drin.«

Aus all diesen Gründen ist China bemüht, das private Cybertreiben in geordnete Bahnen zu lenken. 2002 erklärte das Regime die Hackerangriffe für illegal, im Februar 2009 wurden strenge neue Gesetze dagegen erlassen, und gerade hat man mit großer Publizität eine bekannte Hackerseite geschlossen und die Verantwortlichen inhaftiert. »Die Gesetze sollen nicht dazu dienen, das Hacken zu verhindern, sondern es zu kontrollieren«, glaubt Xiao Wang. Nun kooperierten Hacker häufiger mit dem Staat. Mitmachen oder Strafe, das sei die Wahl.

Westliche Geheimdienste deuten das so: China rüstet für den Cyberkrieg – und die Hacker sind eine Art fünfte Kolonne, die auf militärische und industrielle Ziele

losgelassen wird, wo immer sie angreifbar erscheinen. In China dagegen sieht man sich zu Unrecht verdächtigt. Der Westen »bauscht die Chinabedrohung auf«, sagt der Sprecher des Außenministeriums, Ma Zhaoxu. »Sogenannte Experten«, sagt Zhong Ping vom Pekinger Institut für Internationale Beziehungen, versuchten China doch bloß »zum Reich des Bösen zu stempeln«.

Alle Abgeordneten aus Kongress und Senat haben sich am 27. Januar erhoben, um dem Mann zu applaudieren, der zu ihnen gekommen ist, um Rechenschaft über den Zustand der Nation abzulegen: Barack Obama steht ruhig hinter seinem Rednerpult, nickt und blickt in alle Richtungen. Er sammelt sich. Hinter ihm hängt die rot-weiß gestreifte Fahne mit dem blauen Feld und seinen 50 Sternen. Diese Nation und ihre Fahne hat er zu schützen geschworen. Noch am gleichen Tag kapern Hacker die Internetseiten von 49 Kongressabgeordneten. Sie hinterlassen eine Botschaft: »Fuck Obama!! Red Eye Crew!!!«

Der Präsident faltet die Hände und sagt, die Führer der Vereinigten Staaten kämen seit 220 Jahren in den Kongress, um Bilanz zu ziehen. »Sie taten das in Zeiten des Wachstums und der Ruhe – und sie haben es im Krieg getan, unter Druck, in Zeiten großer Mühen und Kämpfe.« So wie heute. Zwei Jahre tiefster Rezession liegen hinter dem Land. Die Zahl der Arbeitslosen hat sich mehr als verdoppelt. »Ich akzeptiere nicht, dass wir zurückfallen«, sagt Obama unter erneutem Beifall.

Doch sein Versprechen wird ernsthaft infrage gestellt, wenn die Attacken gegen das Internet und auf das geistige Eigentum der US-Wirtschaft nicht beendet werden können. Denn sie richten sich gegen das größte Vermögen, das dieses Land hat.

Das gilt besonders für die Computer- und Internetkonzerne. Sie übertreffen längst alle anderen im S&P 500, dem Index der größten börsennotierten US-Firmen. Viele von ihnen, Apple und Google etwa, sind sogar in der Krise gewachsen. Allein im vierten Quartal 2009 erzielten die Hightechfirmen zusammen einen Gewinn von 33 Milliarden Dollar. Die gesamte Energiebranche kam gerade mal auf gut die Hälfte. Und die Autobranche? Verlor weitere Milliarden. Auf den Weltmärkten ist die amerikanische Überlegenheit nirgendwo so deutlich wie in der Informationstechnik. US-Konzerne führen bei Computerchips (Intel), Computerdesign und -handel (Hewlett-Packard, Dell), Bürosoftware (Microsoft), IT-Dienstleistungen für Konzerne (IBM) und Unterhaltungselektronik (Apple). An amerikanische Internetgiganten reicht kein Rivale heran – an die Suchmaschine Google so wenig wie an das Auktionshaus eBay, an den Onlinehändler Amazon, an das Soziale Netzwerk Facebook.

Als Hillary Clinton vor drei Wochen in ihrer Internet-Rede hervorhob, wie wichtig ihr ein freier Zugang zu Informationen sei, dachte sie an die US-Konzerne, die für ihre internationalen Geschäfte auf ein freies und sicheres Internet angewiesen sind. Aber die Außenministerin hatte zugleich politische Hintergedanken. Internetkonzerne sind ein Mittel der US-Geopolitik geworden.

Früher bedurfte es mühsamer Geheimoperationen, um politische Bewegungen in fernen Ländern zu unterstützen. Heute reicht oft ein wenig Kommunikationstechnik aus dem Westen. Clinton weiß, dass Google gerade bei chinesischen Dissidenten sehr beliebt ist. Der Kurznachrichtendienst Twitter half während der Unruhen in Iran, Demonstrationen zu organisieren und die staatliche Zensur zu umgehen. Das Soziale

Netzwerk Facebook diente politischen Aktivisten in Ägypten dazu, einen Generalstreik zu organisieren.

Konsequent: Für Ende Februar hat Clinton die Vorstandschefs von führenden IT-Konzernen eingeladen, um über ein gemeinsames Vorgehen zu beraten. Der technische Geheimdienst der USA, die National Security Agency, baut eine ganz neue Organisation für Kriege im Internet auf. Schon heute geben die USA jährlich geschätzte 15 Milliarden Dollar für solche Zwecke aus. »Es ist ganz klar, dass diese neue Cyberagentur der Verteidigung wie auch dem Angriff dient«, sagt James Bamford, ein amerikanischer Geheimdienstexperte. Die Trennlinien zwischen strategischer, militärischer Operation und kommerziellen Interessen verschwimmen.

Und das nicht bloß in Amerika. Die kalifornische Sicherheitsfirma McAfee schätzt, dass derzeit 120 Länder ihre Cyberarmeen aufbauen oder erweitern. Auch Deutschland rüstet auf. Die Bundeswehr schult – streng abgeschottet von der Öffentlichkeit in Rheinbach bei Bonn – 76 Mann in den neuesten Methoden. Sie sollen in fremde Netzwerke eindringen, diese auskundschaften und manipulieren können. Die Gruppe untersteht Brigadegeneral Friedrich Wilhelm Kriesel, der das Kommando Strategische Aufklärung bei der Bundeswehr leitet. Offiziell nimmt das Verteidigungsministerium aber »zu Fragen der Offensivverteidigung« keine Stellung.

Die Eskalation im Cyberspace bedroht die Weltwirtschaft. Schließlich waren die geringen Kosten der Datenkommunikation ein wichtiger Treiber für den vergangenen Boom, und künftig will man sich erst recht darauf verlassen. Längst wird Software für deutsche Firmen in Indien entwickelt. Ingenieurteams planen rund um die Uhr in Singapur, New York und München neue Großanlagen für Siemens.

Konzernsoldaten reisen um die Welt und tauschen Geschäftsgeheimnisse über Laptops mit der Zentrale aus. Menschen tragen Mobiltelefone, kaufen damit ein, erledigen Bankgeschäfte, hinterlassen eine Datenspur über ihre Aufenthaltsorte, Vorlieben und sozialen Beziehungen. Kaum noch ein Wasserwerk, eine Ampelschaltanlage oder ein Stromnetz funktioniert heute ohne Computer, die ans Internet angeschlossen sind. Im Stromnetz der Zukunft soll sogar jeder Zähler ein kleiner vernetzter Computer werden!

Und das soll sicher sein?

Das Vertrauen in die Grundlagen dieser Welt schwindet bereits. In einer Umfrage der amerikanischen Sicherheitsfirma RSA unter 4500 Verbrauchern in 22 Ländern gibt ein Drittel an, schon einmal das Opfer eines Hackers geworden zu sein. Zwei Jahre zuvor waren es nur zehn Prozent. Die Zahl derer, die sich um die Sicherheit des Internets sorgen, ist in den vergangenen zwei Jahren von 10 auf 90 Prozent gestiegen.

In Washington erfährt deshalb Matthew Sklerov mit seinen Thesen viel Aufmerksamkeit. Er arbeitet im Verteidigungsministerium und fordert, Staaten sollten für alle Hackerangriffe verantwortlich gemacht werden, die von ihrem Boden ausgehen. Nach dem Motto: Entweder werden die Schuldigen ausgeliefert, oder man betrachte das Hacken als einen Kriegsakt! Ronald Deibert, ein Cyberwar-Experte an der Universität Toronto, sieht ebenfalls die Staaten in der Pflicht. »Es wäre besser, durch internationale Abkommen und die Zusammenarbeit der Polizeibehörden das Hacken und die Spionage einzudämmen«, sagt er.

Aber was soll man tun, wenn die Hacker selbst im Dienst des Staates stehen? »Das ist hier genauso wie bei den Atomwaffen«, sagt Deibert. »Die richtige Antwort auf eine Rüstungsspirale ist ein Abkommen zur Waffenkontrolle«.