Das Ende der Nettigkeiten

Cyberkrieg und Sicherheit im Internet

Misha Glenny | **Dass die Menschen mit der technologischen Entwicklung im Cyberspace nicht Schritt halten können, ist eine Binsenweisheit. In den vergangenen Jahren aber hat es auf einem Sektor rasante Fortschritte gegeben, den wir kaum ignorieren dürfen und gegenüber dem unsere diplomatischen Mechanismen zu versagen scheinen – dem Cyberkrieg.**

Es waren vor allem drei Aspekte des World Wide Web, die den Beobachtern im ersten Jahrzehnt des neuen Jahrtausends die Sorgenfalten auf die Stirn trieben: Cyberkriminalität, Spionage und der Diebstahl geistigen Eigentums, letzteres ein kurioser Hybrid, der Aspekte von Cyberkriminalität und Spionage miteinander verbindet.

Nicht, dass sich das amerikanische Verteidigungsministerium zuvor keine Gedanken darüber gemacht hätte, was es militärisch bedeutet, wenn wir immer stärker von vernetzten Computersystemen abhängig werden. Schon 1997 gab es ein internes Manöver (Codename „Eligible Receiver"), in dessen Verlauf offenkundig wurde, wie schlecht die Vereinigten Staaten darauf vorbereitet waren, Cyberattacken zu bekämpfen. 1998 fand man durch einen Zufall heraus, dass ein Hacker zwei Jahre lang die Computersysteme des Pentagons, der NASA und anderer Forschungseinrichtungen gewissermaßen „angezapft" hatte. Das Verteidigungsministerium verfolgte die Spur zu einem Großrechner in der ehemaligen Sowjetunion zurück; wer aber genau hinter den Attacken steckte, blieb unbekannt; Russland leugnete jede Beteiligung.

Die Alarmglocken schrillen

Erst 2007 begannen sich die Dinge grundlegend zu ändern. Estland erlitt eine Reihe beispielloser Angriffe auf seine Internet-Infrastruktur – viele sagen heute rückblickend, dass es sich dabei um den ersten Akt von Cyberkrieg überhaupt handelte. Die Täter wurden allgemein auf russischer Seite vermutet. Der Vorfall ließ bei der NATO, im US-Kongress und im Pentagon die Alarmglocken schrillen.

Den Attacken auf Estland folgte einige Monate später ein weiterer Vorfall. Im November 2008 wurde ruchbar, dass ein „ausländischer Geheimdienst" (so ein hochrangiger Pentagon-Mitarbeiter) im Irak mithilfe eines infizierten USB-Sticks Schad-

software auf einem Laptop des US-Verteidigungsministeriums installiert hatte. Binnen kurzer Zeit breitete sich die Schadsoftware in den Netzwerken des US-Militärs aus. Der damalige Verteidigungsminister Robert Gates kündigte die Einrichtung eines amerikanischen Cyberkommandos an. Zu den vier Dimensionen der Landesverteidigung Land, See, Luft und Weltraum habe sich, so Gates, mit dem Cyberspace eine fünfte gesellt – im Übrigen ist es die erste von Menschen geschaffene militärische Dimension.

Damit unterstrich die US-Regierung, dass es das Internet als aktuellen oder künftigen Schauplatz für Kriege sieht. Tatsächlich hatten die Vereinigten Staaten und Israel zu dem Zeitpunkt bereits eine Reihe von Viren in Umlauf gebracht, die sich in erster Linie gegen das Atomprogramm des Iran richteten; mindestens eines von ihnen war eindeutig darauf ausgerichtet, die physische Infrastruktur zu beeinträchtigen. Hätte der Iran eine der amerikanischen Nuklearanlagen mit einem Virus infiziert – wir können wohl getrost davon ausgehen, dass Washington dies als einen kriegerischen Akt bezeichnet hätte. In diesem Sinne waren das US-Cyberkommando und die Familie der Viren-Cluster um Stuxnet der Startschuss zum Rüstungswettlauf im Cyberspace.

Horrorszenarien

Zum Thema Cyberkrieg existieren zwei diametral entgegengesetzte Auffassungen. Auf der einen Seite herrscht der Glaube vor, dass wir bereits von einem potenziellen Großangriff bedroht sind, der unsere vernetzten Computersysteme weitgehend lahm legen könnte. Anhänger dieser These meinen, dass unsere sozialen und wirtschaftlichen Infrastrukturen bereits so stark von Computernetzwerken abhängig sind, dass eine Serie von Angriffen mit Schadsoftware eine Katastrophe auslösen könnte. Die bekannteste Beschreibung dieses Szenarios stammt aus dem Buch „Cyber War“ des ehemaligen Präsidentenberaters Richard A. Clarke:

„Du schaust auf deine Armbanduhr. Es ist 8.15 Uhr. In der vergangenen Viertelstunde sind 157 große urbane Zentren Amerikas ins Chaos gestürzt – durch einen landesweiten Stromausfall zur Stoßzeit. Giftgaswolken schweben in Richtung Wilmington und Houston. In Raffinerien verbrennen die Ölreserven mehrerer Städte. Untergrundbahnen sind in New York, Oakland, Washington und Los Angeles verunglückt, Güterzüge vor großen Verkehrsknotenpunkten und Rangierbahnhöfen der vier wichtigsten Schienenstrecken entgleist. Flugzeuge fallen nach Zusammenstößen buchstäblich vom Himmel. Pipelines, die Gas in den Nordosten des Landes transportieren, sind explodiert, Millionen müssen frieren. Auch das Finanzsystem ist eingefroren, Terabytes an Informationen in Datenzentren sind ausgelöscht ...“ Und so weiter in diesem Horrorszenario.

„Züge entgleisen, Pipelines explodieren, Flugzeuge fallen vom Himmel, Tetrabytes an Informationen sind gelöscht“

Die andere Denkschule geht davon aus, dass die Gefahr des Cyberkriegs systematisch übertrieben wird und dass die Albtraumvisionen von Richard Clarke und anderen nur in deren Gedankenwelten existieren. Politisch motivierte „Hacktivisten“ wie die

Gruppe „Anonymous“ argumentieren, dass das Säen von Angst und Zweifel dazu beitragen solle, die Gewinne der wachsenden Cybersicherheitsindustrie zu mehren und zugleich die hohen Investitionen des Militärs in Hochtechnologiewaffen zu rechtfertigen.

Thomas Rid, der War Studies am King’s College London lehrt, sieht das anders. Sein Hauptargument lautet, dass es sich bei den meisten der Vorkommnisse, die reflexhaft als Cyberkriegsakte dargestellt werden, um alltägliche Akte von Spionage handele. Rid verweist auf die Abwesenheit von Gewalt im militärischen Bereich des World Wide Web und legt damit nahe, dass dies konventioneller Kriegsführung vorzuziehen sei. Nun hat Rid sicherlich recht damit, dass wir deutlicher erklären müssen, was wir meinen, wenn wir von der Militarisierung des Internets sprechen. Die Debatte um den Cyberkrieg ist von den Diskussionen über die Computersysteme, die unsere soziale, wirtschaftliche und politische Welt revolutioniert haben, wohl diejenige, die am ungenauesten definiert ist.

Das Säen von Angst und Zweifel solle dazu beitragen, die Gewinne der Cybersicherheitsindustrie zu mehren

Was ist Cyberkrieg?

Sicherheitsstrategien für das Internet berühren sehr schnell auch andere cyberrelevante Fragen wie Rede- und Meinungsfreiheit, die so genannte Netzneutralität (die Forderung, dass die Übertragung von Daten im Internet frei von kommerziellen Interessen oder Sponsoren sein solle), Fragen des geistigen Eigentums, das Zurückhalten von Daten oder die Möglichkeit, im Netz anonym zu bleiben. Die Schwierigkeit, genau die Schnittmengen dieser Fragen zu definieren, gehört zu den vielen Problemen, mit denen die meisten Debatten über Cyberkrieg behaftet sind. Aber die wohl überragende Schwierigkeit ist die Frage der Definition. Was ist Cyberkrieg? Gibt es ihn? Und wie gefährlich ist er?

Das US-Cyberkommando, das eingerichtet wurde, um diese neue Sphäre zu kontrollieren, hat zwei zentrale Missionen. Die erste ist verhältnismäßig einfach: Das Kommando soll sicherstellen, dass es zu keinem unerlaubten Zugriff auf die amerikanischen Militärnetze kommt. Die zweite ist problematischer: Das US-Cyberkommando ist verpflichtet, „umfassende Cyberkriegsoperationen vorzubereiten, und, wenn ihm ein entsprechender Befehl erteilt wird, auszuführen, um die Handlungsfreiheit der Vereinigten Staaten und ihrer Verbündeten im Cyberspace zu gewährleisten und diese unseren Gegnern zu versagen.“ Diese unschärfste aller Militärdoktrinen behindert den Versuch einer Definition von Cyberkrieg eher, als dass sie dabei hilft. Und sie nährt den Verdacht, dass die USA dabei sind, bei den offensiven Cyberfähigkeiten einseitig aufzurüsten.

Die besonders engen Beziehungen zwischen Militär und Geheimdiensten im Cyberspace spiegelten sich auch in der Wahl des Chefs des US-Cyberkommandos wider. Keith Alexander, ein Vier-Sterne-General, war bereits Chef der National Security Agency (NSA), die eine maßgebliche Rolle im Rahmen der US-Cybersicherheitstrategie spielt.

Hinzu kommt, dass amerikanische Nachrichtendienste wie die NSA Zugriff auf Datenquellen haben, die auch Länder wie Russland oder China

Bild nur in Printausgabe verfügbar

liebend gern nutzen würden – die Konten von Unternehmen wie Google, Facebook und Twitter, allesamt in den USA registriert und im Besitz riesiger Speicher mit persönlichen Daten. Da es keinen legalen Weg gab, beschlossen die Chinesen 2010 und 2011, Google und neun andere große Unternehmen zu hacken, darunter auch Adobe, von dem der „PDF-Reader" stammt (PDF-Dokumente gehören zu den am weitesten verbreiteten „Trägermedien" für Spionage- oder kriminelle Attacken).

Stuxnet und die Folgen

Als diese Angriffe bekannt wurden, hielt Hillary Clinton eine Rede, in der sie letztlich Google als Bestandteil der amerikanischen nationalen Sicherheit definierte. Das löste eine Welle diplomatischer Bemühungen aus, sich mit Cyberwar auseinanderzusetzen. Doch während diese noch liefen, kam es zu einem anderen bedeutenden Vorfall – der Entdeckung des Stuxnet-Virus. Die meisten vermuteten, dass entweder die USA oder Israel oder beide gemeinsam hinter der Herstellung dieses Virus steckten, das dafür sorgen sollte, die Zentrifugenmechanismen in der iranischen Urananreicherungsanlage in Natanz sowie in weiteren Einrichtungen zu zerstören. Allerdings gab es keinen eindeutigen Beweis. Das unterstreicht ein zentrales Problem beim Cyberkrieg – die Frage nach der Verantwortlichkeit. Man kann sich nie sicher sein, woher der Angriff kommt.

Im April 2012 ließ das Weiße Haus allerdings gezielt an die *New York Times* durchsickern, dass die Vereinigten Staaten und Israel hinter Stuxnet stünden. Es ist schwer zu sagen, welches Kalkül dahinter steckte: In jedem Fall hat der Vorgang die Lage völlig verändert. Stuxnet gilt allgemein als Startschuss für ein ungeregeltes Wettrüsten im Cyberspace, wenngleich Moskau und Peking argumentieren könnten, dass das bereits in den neunziger Jahren begonnen habe.

Bis zu diesen Zeitpunkt hatten USA und EU die recht glaubhafte Haltung eingenommen, sie würden Schadsoftware und Hacker quer durchs Netz verfolgen – im Gegensatz zu einer Reihe von Staaten, insbesondere Russland und China, die bereit seien, Schadsoftware für Spionage einzusetzen. Aber seit Stuxnet ist Schluss mit den Nettigkeiten. Angesichts des digitalen Durcheinanders im Cyberspace wäre es wünschenswert, eine Form der Regulierung einzuführen oder sich zumindest auf einige grundlegende Prinzipien zu einigen, was Staaten im Cyberspace tun und was sie lassen sollten.

Angesichts des digitalen Durcheinanders wäre es wünschenswert, eine Form der Regulierung zu schaffen

Die drei maßgeblichen Staaten im Cyberspace sind die USA, Russland und China (Israel, Frankreich, Deutschland und Großbritannien bilden die zweite Garde). In den vergangenen Jahren haben sie versucht, in bilateralen Gesprächen Fortschritte zu erzielen. Allerdings hat sich schnell herausgestellt, dass ihre Positionen nicht miteinander vereinbar sind. Der Westen pocht auf die Erfüllung der „Budapester Konvention gegen Datennetzkriminalität“, die postuliert, dass Staaten es Strafverfolgungsbehörden gestatten sollen, auch in Netzwerke einzudringen, die unter ausländischer Jurisdiktion stehen.

Das wiederum ist ein rotes Tuch für Russland und China. Moskau und Peking mögen bereit sein, einem Abkommen über Cyberwaffen zuzustimmen, aber nur zu dem Preis, dass die USA ihnen einräumen, über das Netz unter ihrer eigenen Jurisdiktion die volle Souveränität auszuüben.

Als Reaktion auf das Scheitern der Verhandlungen haben Russland und China die Gespräche nun in die Vereinten Nationen und deren Sonderorganisation Internationale Fernmeldeunion (ITU) verlagert. Für Dezember 2012 ist ein Gipfeltreffen in Dubai geplant, an das sich ein diplomatischer Marathon anschließen könnte.

Im Moment herrscht ein kontrollierter Friede im Cyberspace. Aber wenn sich die Logik der vergangenen Jahre fortsetzt, ist folgende Entwicklung zu erwarten: Erstens wird sich das globale Internet immer weiter in eine Reihe gigantischer Intranets aufsplitten. Der Iran hat bereits angedeutet, dass er vorhat, sich vom Internet abzukoppeln, zum Teil, um sich vor weiteren Cyberangriffen zu schützen, zum Teil aber auch, um „kultureller Kontamination“ vorzubeugen.

Zweitens werden Länder in der ganzen Welt offensive Cyberwaffen entwickeln, in der vermutlich richtigen Annahme, dass potenzielle Feinde das Gleiche tun. Derzeit befinden wir uns in einer sich immer schneller drehenden Rüstungsspirale. Ob das die katastrophalen Folgen hat, die Beobachter wie Richard C. Clarke fürchten, oder ob, wie Thomas Rid argumentiert, die Verlagerung von Spionage in den Cyberspace tatsächlich Spannungen abbauen und die Gefahren eines Krieges unter den großen Mächten reduzieren wird, ist eine offene Frage.

MISHA GLENNY ist Journalist und Autor von „CyberCrime: Kriminalität und Krieg im digitalen Zeitalter“ (DVA 2012).