Das Wettrüsten im Internet

Wie aus dem „Cyberwar" ein realer Krieg zu werden droht

Von **Daniel Leisegang**

Der Datenverkehr im Internet überwindet scheinbar mühelos alle Grenzen. In Sekundenbruchteilen rasen Informationen von einem ans andere Ende der Welt. Die zunehmende Vernetzung führt jedoch auch Risiken mit sich. Lange Zeit warnten Experten vor allem vor Computerviren oder Betrugsversuchen im Netz. Nun weisen sie auf eine neue, weitaus größere Gefahr hin: Sogenannte Kritische Infrastrukturen gerieten zunehmend ins Visier von professionellen Hackern. Ein Cyberangriff könnte die Energieversorgung, das Finanzwesen oder gar militärische Einrichtungen eines Landes treffen – mit dramatischen Folgen für die Bevölkerung.

Richard Clarke, ehemaliger Bundeskoordinator für nationale Sicherheit unter den US-Präsidenten Bill Clinton und George W. Bush, beschreibt in seinem jüngst auf Deutsch erschienenen Buch „World Wide War" die Folgen eines „Digital Pearl Harbour", eines überraschenden Cyberangriffs auf die USA: Nachdem es Hackern gelungen ist, die Server amerikanischer Energieunternehmen unter ihre Kontrolle zu bringen, lösen sie einen landesweiten Stromausfall aus. Raffinerien gehen daraufhin in Flammen auf und Giftgaswolken treiben auf Ballungsräume zu. Die Verkehrs- und Kommunikationssysteme erleiden einen Totalausfall, infolge dessen kollabiert das Finanzsystem. Schließlich werden die Lebensmittel knapp, Polizei und Notdienste verlieren die Kontrolle über das wachsende Chaos, Tausende Menschen sterben.

Im Cyberwar muss aus Sicht von Sicherheitsexperten somit kein einziger Schuss fallen, um eine Supermacht wie die USA in die Knie zu zwingen. Doch ist dieses Szenario realistisch? Was ist tatsächlich dran am sogenannten Cyberwar?

Für den Sicherheitswissenschaftler Sandro Gaycken ist Cyberwar vor allem eine „Sammelbezeichnung für eine Batterie unterschiedlicher Maßnahmen, die Netzwerke und digitale Kultur für militärische Zwecke nutzen wollen, zentral aber Rechner als dezidiertes Angriffsziel verstehen."[1] Hacker nutzen dabei Instrumente wie ferngesteuerte Netzwerke aus Privatrechnern („Bot-Netze"), manipulierte Links oder E-Mailanhänge („Spearpishing") und Sicherheitslücken, mit deren Hilfe sie Schadsoftware in fremde Computersys-

1 Sandro Gaycken, Cyberwar – Das Internet als Kriegsschauplatz, München 2010, S. 45.

teme einschleusen. Ihr Ziel ist es, die Kontrolle über Rechner oder Netzwerke zu erlangen oder diese gar zu zerstören.

Besonders zwei Großangriffe haben aus Sicht der Experten in den vergangenen Jahren das Bedrohungspotential von Cyberwaffen aufgezeigt: zum einen die digitalen Attacken auf Estland im Jahr 2007, zum anderen der Computerwurm Stuxnet, der im Juni 2010 entdeckt wurde.

Nach der Verlegung eines russischen Kriegerdenkmals aus der Hauptstadt Tallin im April 2007 gerieten Server der estnischen Regierung, von Banken, Zeitungen und anderen Unternehmen ins Visier sogenannter DDoS-Attacken, die zu Überlastungen von Infrastruktursystemen führten.[2] Die estnische Regierung sprach damals von Cyberterrorismus und behauptete, die Angriffe seien von Rechnern des Kreml ausgegangen.

Der Computerwurm Stuxnet dagegen wurde offenbar ganz gezielt zum Angriff auf bestimmte Steuerungsanlagen der Firma Siemens programmiert, die weltweit in Industrieanlagen verbaut sind. Experten mutmaßen, dass der Wurm es vor allem auf die Leittechnik der iranischen Uran-Anreicherungsanlage in Natanz oder des Kernkraftwerks Buschehr abgesehen hatte – und damit gezielt das iranische Atomprogramm aufhalten sollte. Tatsächlich räumte Irans Präsident Ahmadinedschad Ende 2010 ein, dass Stuxnet technische Probleme zur Folge hatte. Etwa ein Zehntel der rund 9000 iranischen Zentrifugen mussten zwischen November 2009 und Januar 2011 ausgetauscht werden.[3] Auch bei Stuxnet gibt es keine gesicherten Erkenntnisse über die Auftraggeber oder die Autoren des Wurms.[4]

In den vergangenen Monaten sorgten darüber hinaus eine wachsende Zahl von Hackerangriffen für Schlagzeilen. So brach eine Hackergruppe, die sich selbst „LulzSec“ nennt (ihr Motto: „Laughing at your security“ – Lachen über Eure Sicherheit), wiederholt in Datenbanken des japanischen Medienkonzerns Sony ein, um nach eigenen Angaben auf Datenschutzprobleme des Unternehmens aufmerksam zu machen. Die Mitglieder einer anderen Gruppierung namens Anonymous legten den Online-Bezahldienst Paypal und das Kreditkartenunternehmen MasterCard („Operation Payback“) lahm, nachdem diese – ohne rechtliche Grundlage – die Spendenkonten der Whistleblower-Plattform Wikileaks eingefroren hatten.

Die Mär vom Cyberwar

Zahlreiche Medien wollten in den jüngsten Angriffen Anzeichen eines aufziehenden Cyberwars erkennen. Dabei übersahen sie, dass bei weitem nicht jeder Hackerangriff mit einem kriegerischen Akt gleichzusetzen ist.

So kam infolge der Blockade estländischer Webseiten kein Mensch ernsthaft zu Schaden. Ebenfalls gab es keine Versuche, in Rechner einzudringen

2 Bei einer DDoS-Attacke (Distributed Denial of Service) werden gezielt viele Anfragen an einen ausgewählten Webserver geschickt, sodass dieser unter der Last zusammenbricht.
3 Vgl. „Streitkräfte und Strategien“, NDR info, 18.6.2011.
4 Vgl. www.golem.de, 28.9.2010.

oder Gelder zu erpressen. Daher sieht der Computerwissenschaftler James Hendler in den Blockaden allenfalls einen großangelegten „Cyberkrawall".[5] Dennoch denkt die estnische Regierung sogar über eine Cyber-Wehrpflicht nach, wonach im Falle eines Internetangriffs sämtliche IT-Experten zur virtuellen Landesverteidigung einberufen werden können. Die Nato sieht ebenfalls Handlungsbedarf: Nach den Angriffen wurde im Jahr 2007 das Tallinner „Exzellenzzentrum für Cyberverteidigung" gegründet, wo Experten aus unterschiedlichen Mitgliedstaaten Cyberangriffe erforschen.

Die Forschungsergebnisse sind auch in den Entwurf der neuen Nato-Cyberstrategie eingeflossen, der im November 2010 auf der Strategiekonferenz des Militärbündnisses diskutiert wurde. Generalsekretär Anders Fogh Rasmussen schlug damals vor, dass ein Cyberangriff auf ein Mitgliedsland den Bündnisfall auslösen kann. Wohlgemerkt: In der Geschichte des Bündnisses wurde der kollektive Verteidigungsfall erst einmal ausgerufen – nach den Anschlägen auf die Vereinigten Staaten am 11. September 2001.

Auch im Falle von Stuxnet ist ungeklärt, welche Motive die Autoren des Wurms tatsächlich verfolgten. Zwar kann man davon ausgehen, dass das Schadprogramm mit militärischer Hilfe entwickelt wurde. Folgen, die denen eines kriegerischen Aktes nahe gekommen wären, blieben jedoch auch hier aus.

Und die zahlreichen Hackerangriffe der vergangenen Monate? Die Angriffe der sogenannten Hacktivisten lassen die Grenzen zwischen politischem Aktivismus, Vandalismus und kriminellen Absichten mehr und mehr verschwimmen. Den sogenannten *White Hats* („Weiße Hüte"), welche die Mehrheit der Hacker ausmachen, geht es in erster Linie um das Aufdecken von Sicherheitslücken; sie operieren zum Teil auch im Dienst von Behörden oder Unternehmen. *Black Hats* bzw. *Cracker* verfolgen dagegen vor allem eigennützige Interessen – neben cyberkriminellen Absichten und finanziellen Interessen geht es ihnen nicht selten schlicht um die Lust an der Zerstörung von IT-Systemen. Die Angriffe der jüngsten Zeit gehen jedoch auf das Konto sogenannter *Grey Hats*. Dabei handelt es sich um Hacker, die sich in einer rechtlich-moralischen Grauzone bewegen: Sie verstoßen gegen bestehende Regeln und Gesetze – allerdings nicht zum eigenen Vorteil. Ihr Ziel besteht stattdessen darin, mit teilweise durchaus illegalen Mitteln auf Mängel etwa beim Datenschutz oder auf gravierende politische Missstände hinzuweisen.

Die Kulisse eines drohenden Cyberwars fällt damit in sich zusammen. Mehr noch: Die Diskussion um „Cyberwar" – oder gar „Cyberterrorismus" – ebnet die Unterschiede zwischen den grundverschiedenen Attacken und den Motiven der Angreifer ein. Stattdessen ist es notwendig, zwischen Internet-Kriminalität, Industriespionage, militärischer Spionage (und Sabotage) sowie politischem – und bisweilen kriminellem – „Hacktivism" genau zu unterscheiden, um nicht fahrlässig mit dem Begriff Cyberwar zu operieren. [6]

5 Vgl. www.heise.de, 12.6.2007.

6 Mit Internet-Kriminalität sind Straftaten gemeint, die mithilfe eines Computers und des Internet durchgeführt werden. Dazu gehören beispielsweise der Betrug bei eBay oder das Ausspähen privater Daten. Industrie- bzw. Militärspionage bedeutet die illegale Beschaffung von Informationen konkurrierender Wirtschaftsunternehmen bzw. anderer Staaten. Hacktivism wiederum bezeichnet eine meist politisch motivierte Form des Online-Vandalismus bzw. das gezielte Blockieren ausgewählter Webseiten.

Aufrüstung im Cyberspace

Auch Wissenschaftler der University of Oxford und der London School of Economics kritisieren, der Begriff Cyberwar werde durch seine inflationäre Nutzung in den Medien geradezu „over-hyped". In einer im Auftrag der OECD durchgeführten Studie kamen sie Anfang dieses Jahres zu dem Schluss, dass uns in naher Zukunft kein digitaler Großangriff droht. Auch ein reiner Cyberkrieg zwischen Staaten sei derzeit äußerst unwahrscheinlich.[7] Selbst im Fall eines großangelegten Cyberangriffs sind kritische Infrastrukturen der USA ausreichend geschützt: Tatsächlich befinden sich selbst verletzliche Steuerungssysteme auf unterschiedlichen Hardware-Plattformen, die zum Teil sogar in eigenen Programmiersprachen geschrieben sind. Komplexe Cyberangriffe sind daher zwar technisch durchaus möglich, aufgrund ihrer begrenzten Wirkung sind negative Auswirkungen allerdings auch nur in einem sehr begrenztem Umfang zu befürchten.

Dennoch hat die Regierung der Vereinigten Staaten jüngst ihre Aktivitäten im Bereich der Cyberabwehr massiv ausgeweitet. Sie plant zudem, virtuelle Angriffe fortan mit aller Härte zu erwidern – wenn nötig auch mit militärischer Gewalt. Erst im Juli veröffentlichte das US-Verteidigungsministerium ein Strategiepapier mit dem Titel „Department of Defense Strategy for Operating in Cyberspace". Demnach soll das Pentagon das Internet künftig als eigenen Einsatzbereich („operational domain") behandeln. Ein erster Entwurf sah zudem vor, dass die USA einen virtuellen „Erstschlag" auch mit Waffengewalt erwidern können.[8] Auch wenn die Obama-Administration ihr Vorhaben, schwere Hackerangriffe als Kriegshandlung einzustufen, vorerst auf Eis gelegt hat – die Pläne digitaler Kriegsführung sind damit längst nicht vom Tisch. Denn das Verteidigungsministerium hat weiterhin die Absicht, gemeinsam mit verbündeten Staaten eine „kollektive Selbstverteidigung" im Cyberspace aufzubauen.[9] Daneben soll aber auch das offensive Potential der Cyberwaffen genutzt werden. Denn die neuartigen Wunderwaffen versprechen vielfältige Angriffsmethoden: Nahezu alle technischen Ziele, vor allem mit Informationstechnologien gesteuerte Infrastrukturen und Datenbanken, sind heute vernetzt und stellen damit aus Sicht der USA militärisch interessante Zielobjekte dar.

Die neue US-Strategie soll mit Hilfe der im vergangenen Jahr gegründeten Spezialeinheit „Cyber Command" umgesetzt werden. Zu den Aufgaben dieser Cyberkriegereinheit gehört es, in fremde Hochsicherheitssysteme einzubrechen. Es ist davon auszugehen, dass sich die militärischen Vorkehrungen der USA vor allem gegen Russland und China richten. Über die Cyberstrategien dieser beiden Staaten ist dagegen bisher nur wenig bekannt.[10]

7 Vgl. www.ox.ac.uk/media/news_stories/2011/111701.html

8 Ein ranghoher Angehöriger des US-Militärs brachte es auf den Punkt: „Wenn ihr unser Stromnetz abschaltet, werden wir vielleicht eine Rakete in euren Schornstein feuern." In: „The Wall Street Journal", 31.5.2011.

9 Vgl. www.heise.de, 14.7.2011. Die Cyberstrategie der USA kann abgerufen werden unter www.defense.gov/news/d20110714cyber.pdf.

10 China soll über mindestens eine Cyberwar-Einheit namens „The Blue Army" verfügen, vgl. „The Guardian", 3.6.2011.

Allerdings fehlen den USA für Operationen im Netz derzeit noch die erforderlichen qualifizierten Kräfte. Viele Behörden versuchten daher auf der diesjährigen Hacker-Messe „Def-Con", junge Hackertalente für den staatlichen Cyberwar zu gewinnen. Auch der US-Militärnachrichtendienst NSA wirbt inzwischen gezielt Menschen mit „Hacking Skills" an. Der ehemalige CIA-Chef Michael Hayden schlug sogar vor, eine der berüchtigten US-Söldnerfirma „Blackwater" vergleichbare Organisation aufzustellen, die als Dienstleistungsunternehmen dem Privatsektor eine „aktive" und „aggressive" Verteidigung anbietet. Dort sollen dann auch, so Hayden, Dinge möglich sein, „die wir dem privaten Sektor im physischen Raum niemals erlauben würden."[11]

Aber nicht nur die USA bereiten sich auf den digitalen Krieg vor. Über 140 Staaten arbeiten bereits an eigenen Cyberwar-Programmen – Tendenz steigend. Auch hierzulande rüstet man sich: Am 1. April dieses Jahres nahm in Bonn das Nationale Cyber-Abwehr-Zentrum (NCAZ) seinen Dienst auf. Mitglieder des Bundesamtes für Sicherheit in der Informationstechnik, des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe sowie des Bundesamtes für Verfassungsschutzes arbeiten hier für die Auswertung von Angriffen und die Vernetzung zwischen den unterschiedlichen Behörden zusammen. Eine wichtige Rolle in der bundesdeutschen Cyberabwehr spielt auch das Gemeinsame Internetzentrum (GIZ). Unter Führung des Verfassungsschutzes versammelt es 51 Experten aller deutschen Geheimdienste für eine „bestimmte Form der Zusammenarbeit" mit dem Ziel der "Bekämpfung des islamistischen Terrorismus im Internet".[12] Zudem sucht die Bundesregierung, gemäß ihrer Cyber-Sicherheitsstrategie, die enge Kooperation mit verbündeten Staaten, insbesondere mit der EU. Schließlich gibt es in Rheinbach bei Bonn das Bundeswehr-Kommando „Strategische Aufklärung", dem etwa 7000 Männer und Frauen angehören. Eine streng abgeschottete Abteilung mit der Bezeichnung „Abteilung Informations- und Computernetzwerkoperationen" verfolgt hier das Ziel, nicht nur die elektronische Infrastruktur der Bundesrepublik vor Angriffen zu schützen, sondern auch in Netzwerke anderer Staaten einzudringen, diese zu manipulieren oder gar zu zerstören.[13]

Der cyber-militärische Komplex

Die entscheidende Frage aber lautet: Warum rüsten sich die Staaten für den Cyberwar, wenn ein Cyberkrieg derzeit ausgeschlossen scheint?

Die oben genannte OECD-Studie warnt, dass sich durch die zunehmende Verflechtung von Sicherheitsunternehmen und politischen Institutionen in den USA derzeit ein sogenannter cyber-militärischer Komplex herausbilde. Dieser Begriff lehnt sich an ein Phänomen an, das US-Präsident Dwight D. Eisenhower vor 50 Jahren am Ende seiner Amtszeit als militärisch-industriel-

11 www.futurezone.at, 2.8.2011; vgl. auch Rolf Uesseler, Neue Kriege, neue Söldner. Private Militärfirmen und globale Interventionsstrategien, in: „Blätter", 3/2005, S. 323-333.
12 Wie auch im NCAZ wird im GIZ die Trennung von polizeidienstlicher und nachrichtendienstlicher Tätigkeit aufgeweicht.
13 Vgl. „Spiegel Online", 7.2.2009.

len Komplex beschrieb: Durch den Zweiten Weltkrieg und im Zuge des Kalten Krieges hatte die Rüstungsindustrie seit den 40er Jahren in den Vereinigten Staaten erheblich an Einfluss gewonnen. Die enge Verflechtung von Rüstungsunternehmen, dem Militär und staatlicher Verwaltung beeinflusste seit den 50er Jahren mehr und mehr die Verfahren und Entscheidungen der amerikanischen Politik – und drohte, so Eisenhower, das demokratische System der USA gänzlich zu untergraben.

Gegenwärtig vollzieht sich eine ähnliche Entwicklung wie vor 50 Jahren: Rüstungsunternehmen wie Sicherheitsberater überzeichnen die möglichen Folgen eines Cyberangriffs und instrumentalisieren auf diese Weise die Diskussionen um Hackerangriffe zu ihren eigenen Zwecken.

Diese Lobbyarbeit zahlt sich bereits kräftig aus. Der Journalist Seymour Hersh schätzt, dass allein die US-Regierung im vergangenen Jahr sechs bis sieben Mrd. US-Dollar „für nichtgeheime Aktivitäten im Bereich der digitalen Sicherheit" aufwendete.[14] Im Juli d.J. kündigte der damalige US-Verteidigungsminister Robert Gates an, die Ausgaben für Cybersicherheit – trotz rigider Sparauflagen für andere Bereiche des Militärhaushalts – bis zum Jahr 2014 auf über 12 Mrd. US-Dollar zu erhöhen. Dies entspricht einer Anhebung um fünfzig Prozent im Vergleich zu 2009.[15] Von dieser Erhöhung dürfte, welch Zufall, auch der Autor und Propagandist des Cyberwar Richard Clarke profitieren. Nachdem er in 30 Dienstjahren unter vier US-Präsidenten im Bereich der Sicherheitspolitik seinem Land diente, leitet er heute das Unternehmen Good Harbour Consulting – eines seiner Hauptgeschäftsfelder: Cybersicherheit. Seit 2007 sitzt Clarke zudem im Aufsichtsrat des Unternehmens AirPatrol Corp., das Produkte im Bereich der Sicherheit drahtloser Datenverbindungen anbietet. Und erst im vergangenen Juni wurde er in den Verwaltungsrat zweier weiterer Unternehmen berufen: Veracode und Visible Assets Inc. Auch diese verdienen ihr Geld im Bereich der Cybersicherheit.[16]

Die Zeiten für hohe Profite sind derzeit mehr als günstig: Ein anderes führendes US-Unternehmen auf diesem Markt, Endgame Systems (sic!), bietet Lösungen zum Schutz vor Cyberrisiken an. Die Firma wurde von Chris Rouland gegründet, der zuvor Chefentwickler bei der Internetsparte von IBM war. Ende 2009 erhielt das Unternehmen von US-Regierungsstellen eine gewaltige Finanzspritze. Seitdem läuft das Geschäft – und das Unternehmen ist angesichts der aktuellen US-Rüstungspläne dazu „verdammt, zu wachsen": Derzeit verdoppelt Endgame Systems im Durchschnitt seinen Umsatz – jährlich.[17]

Paradigmenwechsel im Völkerrecht: Der Dreiviertelbeweis

Tatsächlich stellt die Instrumentalisierung des Cyberwar derzeit eine weitaus größere Bedrohung dar als ein echter Cyberangriff. Denn das Bedrohungs-

14 Vgl. Seymour Hersh, Cyberwar: Die neue Front, in „Blätter", 1/2011, S. 47. Hinzu käme, laut Hersh, der gleiche Betrag für geheim gehaltene Aktivitäten.
15 Vgl. „Deutsche Welle", 21.7.2011.
16 Vgl. www.huffingtonpost.com, 14.9.2011.
17 Vgl. „Bloomberg Businessweek", 20.7.2011 sowie „Atlanta Business Chronicle", 17.6.2011.

szenario eines möglichen Cyberwar droht zu einer selbsterfüllenden Prophezeiung zu werden. Die Aufrüstung der Staaten führt zu einem regelrechten Rüstungswettlauf. Ironischerweise könnte gerade dieser den Krieg im Internet erst herbeiführen. Am Ende könnte sich dieser vermeintlich „saubere" Cyberwar dann sogar zu einem höchst realen Krieg entwickeln.

Entscheidend für diese gefährliche Entwicklung sind die besonderen Eigenschaften der Cyberwaffen. Anders als bei herkömmlichen Waffen ist der Ursprung eines Cyberangriffs leicht zu verschleiern. Aus Sicht potentieller Angreifer stellt diese Non-Attribution (Nicht-Zuweisung) den größten strategischen Vorteil digitaler Waffen dar – und zugleich die internationale Rechtsordnung vor schier unlösbare Herausforderungen.

Dies zeigte sich erst kürzlich im estnischen Tallinn: Im Rahmen einer internationalen Nato-Konferenz diskutierten hier vor wenigen Wochen mehr als 400 Juristen, in welchem Verhältnis der Cyberwar zum klassischen Völkerrecht steht. Im Zentrum stand dabei die Frage, ob ein Cyberangriff auch Gegenschläge mit herkömmlichen „kinetischen" Waffen rechtfertigen kann. Wegen der Non-Attribution tendierten die Rechtsexperten dazu, den Grad der Gewissheit über die Identität eines Angreifers herabzustufen. In Zukunft soll bereits ein begründeter Verdacht ausreichen, um auch mit Waffengewalt gegen vermeintliche Angreiferstaaten vorzugehen. Ein Gegenschlag könnte in Zukunft bereits dann erfolgen, wenn zu 75 Prozent feststehe, „wer der Bösewicht ist, beispielsweise mit Blick auf den Schutz der Cybersicherheit, einer Anklage oder auch hinsichtlich der Abschreckungspolitik für eine internationale Cyberattacke."[18] Wie ein solcher Dreiviertelbeweis aussähe, ließen die Juristen allerdings offen.

Die Hürde für den Einsatz militärischer Gewalt wäre damit erheblich gesenkt. Das entscheidende Problem dieser „Beweisführung" bestünde außerdem darin, dass die Identität von Angreifern allein über den politischen Kontext hergeleitet würde. Die zur Beweisführung herangezogenen Hinweise entstammten dann technischen, nachrichtendienstlichen und diplomatischen Quellen – wären aber zugleich kaum mehr als Indizien.

Aufgrund der Non-Attribution bleibt ebenfalls offen, ob es sich bei einem Cyberangriff überhaupt um einen Kriegsakt handelt – und damit: ob die Armee oder die Strafverfolgungsbehörden zuständig sind. Aus dem gleichen Grund ist die Eindämmung zwischenstaatlicher Cyberattacken unmöglich: Internationale Abkommen könnten zwar das Ziel verfolgen, bestimmte Formen von Cyberattacken auszuschließen. Wie aber soll das Völkerrecht die Einhaltung solcher Abkommen gewährleisten, wenn die Staatengemeinschaft die Identität eines Angreifers nicht zweifelsfrei belegen kann? Mit dem Einsatz von Cyberwaffen wird schließlich auch das Prinzip der militärischen Abschreckung, das im Kalten Krieg noch für einen prekären Waffenstillstand sorgte, obsolet. Mehr noch: Der Cyberwar befördert geradezu asymmetrische Konflikte. Denn offensiver Cyberwar ist – im Gegensatz zur Absicherung der eigenen Rechnernetzwerke – vergleichsweise leicht zu haben. So benötigte

18 „Deutsche Welle", 8.6.2011.

beispielsweise Nordkorea, das nur über eine schwach ausgebaute Netzstruktur verfügt, lediglich kompetentes Personal, um andere Staaten im Cyberspace anzugreifen. Dem entgegen verfügen Staaten wie die USA über eine weit verzweigte Netzwerkstruktur, die sich nur mit großem Aufwand gegen Angriffe von Außen schützen lässt. Allein das amerikanische Militär muss täglich 15 000 Netzwerke und rund sieben Mio. Computer vor Angriffsversuchen aus dem Netz schützen.[19]

Rhetorische Abrüstung und das Konzept der Entnetzung

Der Cyberwar gleicht somit dem Geist, den man heraufbeschwor, nun aber nicht mehr los wird. Welcher Ausweg bietet sich daher noch, um zu verhindern, dass aus einem Cyberwar am Ende ein blutiger Krieg wird?

Derzeit wirken Medien und Politik eifrig mit am Mythos der drohenden Apokalypse, wenn sie statt von IT-Sicherheitsproblemen gleich vom Cyberkrieg sprechen. Die politische Reaktion auf die Aufrüstung im Internet sollte daher zuerst einmal darin bestehen, rhetorische Abrüstung zu betreiben – und auf diese Weise die Hysterieblase der Sicherheitsberater platzen zu lassen. Das bedeutet nicht, die technischen Probleme, allen voran die zahlreichen Lücken der IT-Sicherheit, leichtfertig zu ignorieren. Tatsächlich ist die Cyberwar-Debatte vor allem auch als Eingeständnis zu werten, dass die Politik das Thema Daten- und Cybersicherheit jahrelang vernachlässigt hat.

Hundertprozentige Sicherheit wird es im Internet allerdings niemals geben: Selbst eine bessere Computerbildung der Nutzer oder auch höhere IT-Sicherheitsstandards können nur bedingt vor Hackerangriffen schützen. Die entscheidende technische Antwort zur Verteidigung der eigenen Daten lautet daher: Die Staaten und Unternehmen müssen die Verbindungen kappen und die Kritischen Infrastrukturen von großen externen Netzwerken physikalisch, also real und nicht bloß digital, abkoppeln.[20] Denn die Zunahme von Hackerangriffen verweist auf eine weitere fatale Entwicklung der letzten Jahrzehnte: Die Server vieler Ministerien, Behörden und Unternehmen sind an das Internet angeschlossen, obwohl eine solche Vernetzung nicht notwendig ist. Die Entnetzung wäre somit eine konsequente Maßnahme, die weder die Freiheitsrechte der Bürger einschränkt, noch kriegerische Aufrüstung forciert.

Sowohl rhetorische Abrüstung als auch Entnetzung könnten erste, aber entscheidende Schritte darstellen, um dem cyber-militärischen Komplex den Geldhahn zuzudrehen. Gelingt dies nicht, könnte aus Hackerangriffen und IT-Sicherheitslücken am Ende tatsächlich ein realer Krieg erwachsen.

19 Vgl. „New York Times“, 25.8.2011.
20 Vgl. Gaycken, a.a.O., S. 206 ff.