Ist das schon Krieg?

Cyberwar und Cybercrime: drei Neuerscheinungen

Christian Stöcker | **Entgleisende Züge, kollabierende Stromnetze, explodierende Raffinerien: So malen Experten das Schreckgespenst eines digitalen Krieges an die Wand. Doch wer sich auf dem Buchmarkt umschaut, kommt zu einem etwas vorsichtigeren Urteil. Bei den Gefahren, die im Internet lauern, geht es noch eher um Kriminalität und Spionage als um Kriegführung.**

Der Krieg hat längst begonnen, glaubt man Richard Clarke. Der gefährlichste aller Computerwürmer ist immer noch da draußen, glaubt man Mark Bowden. Und die Cybergangster dieser Welt sind den Strafverfolgern fast immer einen Schritt voraus, glaubt man Misha Glenny. Alle drei haben in jüngerer Zeit Bücher zum Komplex Cyberwar und Cyberkriminalität vorgelegt, alle drei sind gleichermaßen fasziniert wie besorgt ob der rasant wachsenden Möglichkeiten, die digitale Welt für aggressive oder kriminelle Zwecke zu nutzen. Alle drei müssen letztlich vor der Komplexität ihres Gegenstands kapitulieren – und doch erlauben die drei Bücher in der Zusammenschau einen interessanten, wenn auch zwangsläufig lückenhaften Blick in die digitale Halb-, Unter- und Schattenwelt.

Clarke ist der offenkundige Überzeugungstäter unter den dreien. Sein Buch „World Wide War“, geschrieben gemeinsam mit dem Politikwissenschaftler Robert Knake, ist ein langer Kassandraruf. Clarke war Berater mehrerer US-Präsidenten und vor seinem freiwilligen Rückzug aus dem Weißen Haus im März 2003 der Sonderberater von Präsident George W. Bush für Cybersicherheit. Jahrzehnte im Kreise von Sicherheitspolitikern und Militärs haben Clarkes Weltsicht geprägt: Das Internet ist für ihn primär ein potenzielles Schlachtfeld. Und für die Überlegenheit auf diesem Schlachtfeld, davon ist er überzeugt, wird in den USA noch zu wenig getan: Diejenigen, die die Macht hätten, den Wandel zu gestalten, tun das nicht, weil sie das Netz und seine Auswirkungen nicht verstehen: „Unbemerkt haben die Streitkräfte zahlreicher Länder auf einem neuen Schlachtfeld Aufstellung genommen. Weil man sie nicht sieht, haben die Parlamente und die Bevölkerung die Truppenbewegungen nicht bemerkt. Bisher wissen nur wenige, wozu Cyberkrieger in der Lage sind.“

Clarke hat nicht nur ein Sachbuch zum Thema vorgelegt, sondern zuvor schon einen Roman namens „Breakpoint“ verfasst, in dem er die Szenarien, die er in „World Wide War“ in theoretischer Form skizziert, schon einmal als Thrillerplot durchgespielt hat: gekappte Internetleitungen, gehackte Steuerungssysteme für lebenswichtige Infrastrukturen, kollabierende Computerbörsen – und ein Berater für nationale Sicherheit, der von all dem völlig überrascht wird. „Ich weiß nicht, wie es Ihnen geht, aber ich verstehe nicht, wie dieses ganze Zeug funktioniert.“

Mangel an Beispielen

„Breakpoint“ ist ein leicht missionarisch wirkender Thriller von der Stange, und „World Wide War“ liest sich für Europäer streckenweise mühsam, denn der Insider Clarke klärt den Leser im Detail darüber auf, welche Abteilungen des US-Militärs, welche Geheimdienste und Polizeibehörden derzeit wie um die Vorherrschaft beim Boomthema Cyberwar konkurrieren. Eines wird dabei deutlich: Es geht bei der Vorbereitung auf die möglichen digitalen Kriege des 21. Jahrhunderts nicht zuletzt um Geld.

Gleichzeitig hat Clarke mit einem Problem zu kämpfen, das seine Warnungen weniger dringlich erscheinen lässt: Es mangelt ihm an Beispielen für die beschworene Bedrohung. Fälle, in denen Nationalstaaten nachweisbar über das Netz angegriffen wurden, sind extrem rar – und die USA haben bislang nicht zu den Opfern ernsthafter Attacken gezählt, wenn man von zahlreichen und durchaus beunruhigenden Fällen von Cyberspionage absieht. Nicht nur Clarke, sondern auch die Journalisten Bowden („Worm“) und Glenny („Cybercrime“) führen jeweils das gleiche Beispiel für Cyberwar-Szenarien an: Als es in Estland im Frühjahr 2007 einen Konflikt um die Verlegung eines sowjetischen Kriegerdenkmals gab, wurden die Websites diverser Behörden und Unternehmen über Wochen mit massiven Distributed-Denial-of-Service-Attacken (DDoS) angegriffen. Dabei werden ans Internet angeschlossene Server so lange mit ständigen Anfragen großer Mengen anderer Rechner überlastet, bis sie schließlich den Dienst versagen.

Die Angriffe auf estnische Server wurden mit Hilfe so genannter Botnetze ausgeführt, also mit Netzwerken virenverseuchter Computer, die von einem Cyberkriminellen ferngesteuert werden können. Ein großes Botnetz kann aus Zehntausenden, aber auch, wie im Fall des Wurms „Conficker“, dessen Geschichte Bowden in „Worm“ nachzeichnet, aus Millionen von gekaperten Rechnern bestehen. Deren Besitzer wissen in der Regel nicht einmal, dass ihr Gerät heimlich zum Teil einer Angriffswaffe gemacht wurde.

Die Regierung Estlands ließ 2007 keinen Zweifel daran, dass sie Russland hinter den Attacken vermutete. Bis heute ist jedoch unklar, ob die Angriffe tatsächlich von Moskau aus gesteuert wurden, eine spontane Aktion russischer Cyberkrimineller waren oder eine Kooperation von Geheimdienst und zum Hurrapatriotismus überredeten Netzgangstern. In jedem Fall sind Angriffe auf Websites, wie sie Estland erdulden musste, eher simple und krude Werkzeuge der Cyberaggression. DDoS-Attacken sind

Richard A. Clarke, Robert K. Knake: *World Wide War. Angriffe aus dem Internet. Hamburg: Hoffmann und Campe 2011, 352 Seiten, 22,00 €*

manchmal purer Vandalismus, manchmal werden sie von Verbrechern eingesetzt – etwa um Unternehmen, deren Geschäft vom Internet abhängig ist, zu erpressen. Doch die Gefahren, die Clarke und andere „Cyber-Securokraten“, wie der „Cybercrime“-Autor Misha Glenny sie nennt, beschwören, gehen über ein paar unerreichbare Websites weit hinaus: Clarke warnt vor entgleisenden Zügen, kollabierenden Stromnetzen, explodierenden Raffinerien. Ist so etwas möglich?

Erster Akt digitaler Kriegführung

Mark Bowden: *Worm. Der erste digitale Weltkrieg.* Berlin: Berlin Verlag 2012, 288 Seiten, 19,90 €

Der einzige heute tatsächlich nachvollziehbare Akt digitaler Kriegführung, der in diese Kategorie fällt, ging mutmaßlich von den USA, Israel oder beiden gemeinsam aus: Der Stuxnet-Virus, der in den Anlagen des iranischen Atomprogramms womöglich an die tausend Uranzentrifugen zerstörte, war eine Präzisionswaffe, die nach übereinstimmender Expertenmeinung nicht von einer Einzelperson oder einem Trupp normaler Cyberkrimineller geschaffen worden sein kann. Die Stuxnet-Entwickler, denen es gelang, die iranischen Atomanlagen zu treffen, obwohl die dortigen Rechner nicht einmal ans Internet angeschlossen sind, gingen klug vor und verfügten über große Ressourcen.

Eine Vielzahl von Fachleuten muss an dem Virus gearbeitet haben, gleich mehrere bis dahin unbekannte Sicherheitslücken in Software-Systemen, die auf dem Schwarzmarkt Hunderttausende, wenn nicht Millionen von Euro wert sind, wurden dafür ausgenutzt. In die Aufbereitungsanlage Natans gelangte Stuxnet schließlich wohl über einen verseuchten Speicherstick. Erstmals wurden hier offenbar industrielle Steuerungsanlagen mit einem Software-Angriff so manipuliert, dass großer Schaden entstand. Stuxnet wird wohl als erster echter Akt digitaler Kriegführung in die Geschichte eingehen. Doch dieser Angriff betraf nicht die USA, sondern einen ihrer erklärten Feinde. Was Mahner wie Richard Clarke in Erklärungsnöte bringt: Wenn solche digitalen Präzisionswaffen vom eigenen Lager eingesetzt werden, kann es dann um die Cyberabwehrfähigkeit des Westens wirklich so schlecht stehen?

Tatsächlich scheinen die Gefahren, die derzeit im Internet Gestalt annehmen, mehrheitlich von der Art zu sein, die der Journalist Mark Bowden in „Worm“ beschreibt – es geht eher um Kriminalität und Spionage als um Kriegführung. Bowden zeichnet die Entwicklung des Conficker-Virus nach, und die Geschichte einer kleinen Gruppe von Fachleuten im Westen, die sich zusammentaten, ihn zu bekämpfen. Conficker hatte augenscheinlich die Aufgabe, ein gewaltiges Botnetz zu erschaffen, das bis heute existiert – aber noch nie wirklich eingesetzt wurde. Bowden äußert die Vermutung, dass der bis heute unbekannte Conficker-Schöpfer Teile seines Botnetzes an zahlende Kunden vermietet, für DDoS-Attacken etwa oder für den Versand von Spam-Mails.

Vor allem aber beschreibt der Journalist den Kampf einer lose zusammengewürfelten Allianz selbsternannter Verteidiger des freien Netzes gegen Conficker. Und gegen die eigene, als ziemlich unfähig porträtierte Sicherheitsbürokratie. Bowden stellt dem Leser eine Vielzahl von Protagonisten dieses Kampfes in Miniatur-

porträts vor, und ausgerechnet darin liegt eine der größten Schwächen seines durchaus lesenswerten Buches. Der Leser verliert schnell den Überblick über all die Freiwilligen, die sich in einer „Kabale“ zusammenschlossen, um Conficker zu besiegen, denen der letzte Erfolg jedoch versagt blieb.

Aus der Schattenwelt des Netzes

Ähnlich ergeht es Misha Glenny, der in „Cybercrime“ gewissermaßen das Gegenbild zur Szene der aufrechten, guten Hacker zeichnet: Auch sein Bericht aus der Schattenwelt des Netzes wird ob der Vielzahl der Protagonisten unübersichtlich. Glenny erzählt die Geschichte der vom FBI unterwanderten Plattform „Darkmarket“, deren Nutzer auf Kredit- und Geldkartenbetrug spezialisiert waren. Trotz aller Kurzbiografien aber wird das Zusammenwirken all der Hacker, „Carder“ und Administratoren dem Leser selten wirklich deutlich, was viel mit der unsicheren Quellenlage zu tun haben dürfte.

Und auch was die handelnden Personen mit ihren Computern tatsächlich tun, bleibt, anders als bei Bowden, im Ungefähren. Das Buch basiert maßgeblich auf Interviews mit den Beteiligten, mit Ermittlern, aber auch mit kriminellen Hackern, Kreditkartenbetrügern und ihren Gastgebern im Netz. Ob jemand aber ein kleiner oder doch ein dicker Fisch war, ist oft nicht zu erkennen. Gemeinsam ist Bowden und Misha eine starke Faszination für das Wesen ihrer – durchwegs männlichen – Protagonisten: Die Cybergangster aus der Ukraine, den USA oder der Türkei, die Glenny porträtiert, gehören ebenso wie Bowdens aufrechte, wenn auch verschrobene Helden aus den USA zu einer neuen Kaste der Wissenden, mit Eigenheiten und großen Egos.

Einig sind sich die Autoren darin, dass das Netz und seine Gefahren längst nicht mehr nur ein Thema für weltfremde Eigenbrödler ist. Glenny skizziert, wenn auch bruchstückhaft, die Professionalisierung der Cybercrime-Szene, die Übernahme der Kontrolle durch Verbrechersyndikate, die Kreditkartenbetrug und gehackte Online-Banking-Konten als Teil ihres kriminellen Portfolios begreifen. Clark und Bowden beschreiben auf unterschiedlichen Ebenen die langsame Professionalisierung der Gegenseite, der Kämpfer gegen Verbrechen, Spionage und Bedrohungen aus dem Netz.

Clarkes Buch ist das trockenste der drei, doch sein Autor kann den greifbarsten Erfolg für sich verbuchen: Eine seiner zentralen Forderungen wurde bereits erfüllt. Ende Mai 2011 erklärte das Pentagon, man werde Cyberattacken auf die USA künftig unter Umständen als kriegerischen Akt werten und womöglich mit konventionellen Waffen beantworten. Das *Wall Street Journal* zitierte einen Sprecher des Verteidigungsministeriums mit den Worten: „Wenn Sie unser Stromnetz abschalten, schießen wir Ihnen vielleicht eine Rakete in den Schornstein.“

Misha Glenny: *Cybercrime. Kriminalität und Krieg im digitalen Zeitalter.* München: DVA 2012, 352 Seiten, 19,99 €

Dr. CHRISTIAN STÖCKER ist Ressortleiter Netzwelt bei Spiegel Online.