Humanistische Union

Bedrohung durch Cyberangriffe in der Praxis (vollständig)

aus: vorgänge Nr. 209 (Heft 1/2015), S. 40-48

(Red.) Der NSA-Skandal hat neben der Tatsache der flächendeckenden Überwachung auch die rasante Entwicklung im Bereich von Cyber-Angriffswaffen in den Blickpunkt gerückt. Etliche Staaten, hier vor allem Geheimdienste und Militärs, wenden sehr weitreichende und gezielte Mittel gegen vermutete Gegner_innen an, die immer wieder mit dem Hinweis auf terroristische Aktivitäten gerechtfertigt werden. Dabei hat sich die Ressourcenverteilung deutlich verschoben: mittlerweile übersteigen die Mittel für eigene Angriffsoperationen weitaus die Summen an Geldern, die zur digitalen Gefahrenabwehr bzw. Strafverfolgung eingesetzt werden.

“What is the difference between attacking a country’s weapon-making machinery through a laptop computer or through bunker-buster [bombs]?” (Sanger, 2013: 245)

Schon bevor der Name Edward Snowden weltweite Aufmerksamkeit erlangte, wurde in den Medien bereits über einen der wesentlichen Auslöser seines Entschlusses berichtet, sich an die Öffentlichkeit zu wenden. Snowden erklärte später in einem Interview, dass ihn nicht allein die Überwachung amerikanischer Staatsbürger _innen zur Veröffentlichung der Dokumente bewegt habe, sondern dass vor allem auch die Entwicklung neuer Cyber-Angriffswaffen sein Handeln deutlich beschleunigt habe (Bamford, 2014). Die Überwachung durch die National Security Agency, NSA, hat seither die öffentliche Debatte bestimmt. Cyber Warfare als das weit größere Risiko für die Zivilgesellschaft und die internationale Sicherheit blieb dagegen im Hintergrund. Die von Snowden ermöglichten Einblicke zeigen nun recht detailliert den Umfang dieser von unterschiedlichen Akteuren weltweit betriebenen Aktivitäten auf.

Überwachung für den Cyber War

Die Vorbereitung und Umsetzung der als „Cyber Warfare“ bezeichneten Form der Computermanipulation durch Militärs und Geheimdienste ist der Öffentlichkeit zwar schon länger und ganz unabhängig der von Snowden zugänglich gemachten Dokumente bekannt, die potentiellen Folgen sind ihr jedoch nicht bewusst. Eine Gesellschaft, deren Infrastrukturen abhängig sind vom zuverlässigen Funktionieren von Computern und Kommunikationsnetzen, muss mittlerweile jedoch - wenn auch widerwillig – zur Kenntnis nehmen, in welchem Ausmaß ihre Steuerungstechnik manipulierbar und zum Spielball von Militärs und Geheimdiensten geworden ist.

Die Opfer sind nämlich keineswegs nur gegnerische Militärs. So verübte der eng mit der NSA kooperierende britische Geheimdienst GCHQ einen ausgefeilten Cyberangriff auf die Systemadministrato_innen der belgischen Telekommunikationsgesellschaft BELGACOM. Das Ziel war, zuerst deren Rechner zu infizieren und zu kapern, um dann Schadsoftware in die Systeme der BELGACOM einzuschleusen, um im dritten Schritt dann deren Kund_innen – u.a. die EU-Kommission – ausspionieren zu können (Gallagher, 2014).

Genutzt wurden für diese Operationen automatisierte Cyberwaffen mit dem Namen „Turbulence“ und „QFire“, die dazu entwickelt wurden, den Datenverkehr eines Zieles zu manipulieren und Schadcode innerhalb von Millisekunden in dessen Datenstrom einzuschleusen, bevor die vom Opfer im Internet

gesuchte Webseite antworten kann. Die Voraussetzung für „QFire“ und andere Werkzeuge des „Quantum“-Werkzeugkastens wiederum ist es, dass bei irgendeinem der Internet-Provider oder Telekommunikationsunternehmen möglichst nahe dem anvisierten Ziel ein Computer gekapert wurde und dort mehrere virtuelle Maschinen ohne Wissen des Netzbetreibers installiert und ferngesteuert betrieben werden. Dienste wie die NSA verfügen über gestufte und aufeinander abgestimmte Manipulations- und Angriffssysteme, die Angriffsmöglichkeiten für jede Art von IT-Systemen umfassen – von solchen in Nordkorea bis zu solchen hier bei uns.

Aber nicht nur Systemadministrator_innen sind wegen ihrer Zugangsmöglichkeiten bevorzugte Angriffsziele. Jede und jeder mit einem nicht ausreichend abgesicherten Computer kann sich als Teil von Angriffsoperationen der NSA oder anderer Dienste wiederfinden. Die Dienste kapern die Computer nichtsahnender Nutzer_innen für ferngesteuerte Botnetz-Operationen und starten von diesen Rechnern aus Denial-of-Service-Attacken (1) oder legen dort einfach nur ausspionierte Daten ab, um selbst einen Tatverdacht von sich weisen zu können (Poulsen, 2014; Storm, 2015).

Integrierte Cyber-Angriffswaffen

Computermanipulationen werden in aller Regel mit jugendlichen oder kriminellen Hacker_innen in Verbindung gebracht. Diese beiden zivilen Akteursgruppen kommen über die Amateurliga nicht hinaus, vergleicht man ihre Ressourcen mit denen von Geheimdiensten und Militärs. Durch Anhörungen des U.S.-Kongresses wurde 2007 bekannt, dass die NSA in den Jahren 2005 bis 2007 annähernd zwei Milliarden US-Dollar für die Entwicklung des später für die BELGACOM-Angriffe genutzte Systeme „Turbulence“ sowie für das System „Turmoil“ aufwandte. Der Kongress bemängelte den hohen Aufwand bei damals noch wenig vorzeigbaren Ergebnissen. Beide Systeme dienen heute der massiven Datensammlung, Manipulation und Kontrolle von Internet-Knotenpunkten und Computersabotage durch selektive Modifikation von Datenpakten (Gorman, 2007).(2) Doch diese vor fast 10 Jahren entwickelten und weiterhin eingesetzten Systeme „Turmoil“ und „Turbulence“ sind nur ein sehr kleiner Teil des Werkzeugkastens der NSA.

Moderner und in der Leistung viel breiter ist das in den Medien oft zitierte NSA-System „XKeyScore“ (Greenwald, 2013; Lischka, Stöcker, 2013), das auch Bundesnachrichtendienst und Bundesamt für Verfassungsschutz einsetzen (Spiegel Online, 2013). XKeyScore wurde medial bekannt als ein Werkzeug der NSA, für die umfassende Erhebung, Analyse und Strukturierung von Inhalten und Metadaten aller Art von Kommunikationsvorgängen von E-Mails, über Chats bis zu Videokonferenzen.

Während hierzulande über die Erkenntnisse aus der automatisierten Metadatenanalyse von Kommunikationsnetzen und der Gewinnung von Informationen aus Google-Suchanfragen berichtet wurde, wies ein Bericht für das EU-Parlament zu XKeyScore schon wenige Wochen nach Beginn der Enthüllungen im September 2013 auch auf dessen Funktionalität als automatisiertes Angriffswerkzeug hin (European Parliament, 2013: 14). „XKeyScore“ erlaubt es, Daten- und Kommunikationsverkehr in Echtzeit zu durchsuchen.(3) So lassen sich etwa alle verschlüsselten Kommunikationsverbindungen in einer Region oder die Suche bei Google mit „verdächtigen“ Schlüsselworten herausfiltern. IT-Sicherheitsfachleuten erschloss sich, dass „XKeyScore“ zusätzlich sicherheitsspezifische Daten zu den Zielsystemen erhebt und dazu beispielsweise gezielt die Systeminternas der Absturzberichte von Softwarepaketen auswertet. Aus Referenzdatenbanken werden bekannte Schwachstellen der Zielsysteme abgerufen. Je nach Auftrag versucht „XKeyScore“, die Zielsysteme daraufhin automatisiert mit Schadsoftware zu infizieren (Lischka, Stöcker, 2013). „XKeyScore“ ist somit – neben einer ganzen Reihe anderer bekannt gewordener Systeme - nicht nur ein Spionage- sondern auch ein Angriffssystem für den „Alltagsgebrauch“ von Cyber-Spionage und Sabotage.

In komplizierten Fällen, wenn ein automatischer Angriff nicht möglich oder das Zielsystem gar nicht mit

dem Internet verbunden ist, ist das 1998 gegründete »Office for Tailored Access Operations« (TAO) der NSA gefordert (Aid, 2009; Kingsbury, 2009). Dessen Aufgaben sind „neben der Aufklärung auch Attacken in Computernetzen als integrierter Teil militärischer Operationen“, so eine frühere Leiterin (Appelbaum et. al, 2014). Neben Schadsoftware – wie etwa Stuxnet - hat das TAO Techniken zur Infektion von Zielrechnern entwickelt mit Erfolgsquoten von bis zu 80 Prozent und verschafft sich durch Besuche vor Ort auch einen „physischen Zugang“ (Appelbaum et. al, 2014). Das TAO führte – einem Snowden-Dokument zufolge mit Daten aus der Zeit vor Mitte 2012 - zu dieser Zeit pro Woche über 2.800 „Computer Network Operations“ durch (4); seinen Aufgaben gemäß also gezielte Cyberangriffe auf komplexe Ziele. Die Hacker des TAO dürften also für gezielte Angriffe auf 150.000 Computersysteme pro Jahr verantwortlich sein, die für die Folgejahre angepeilte operative Zielmarke für Angriffe sind mehrere Millionen infizierte IT-Systeme (Gellman, Nakashima, 2013).

Cyber Warfare – ein Aktionsfeld mit vielen Akteuren

Mehrere Vorfälle zeigen, dass ähnlich spezifische Schadsoftware auch von anderen Ländern eingesetzt wird. Im Jahr 2007 wurden die digitalen Infrastrukturen Estlands durch Cyberattacken gestört, was letztlich dort die Einrichtung eines Cyber-Sicherheitszentrums der NATO zur Folge hatte (Tikk, 2008). 2008 begann der bewaffnete Konflikt zwischen Georgien und Russland mit gezielten Cyber-Manipulationen in Georgien durch Angreifer, die im Voraus über russische Militäraktionen informiert waren (Cyber Consequences Unit, 2009). Die im Frühjahr 2015 in ihren Aktionen analysierte „Great Cannon“ ist ein Angriffswerkzeug, das Datenverkehre in die VR China gezielt kapert, die Inhalte der übertragenen Daten verändert und zusätzlich die von außerhalb Chinas in die Volksrepublik hinein kommunizierenden IT-Systeme so manipuliert, dass diese in eine massive verteilte Denial-of-Service-Attacke (DDoS-Angriff) eingebunden werden (Marczak et. al., 2015). Die Eigenschaften dieses Systems und dessen Manipulationen werden als ähnlich dem Quantum-System der NSA bewertet und lassen auf staatliche Akteure als Urheber schließen.

Schließlich wurde 2010 mit Stuxnet ein Computerwurm zur Manipulation eines Anlagensteuerungssystem der Firma Siemens identifiziert. Die Analyse von „Stuxnet“ zeigte Aufwände weit außerhalb der Möglichkeiten gewöhnlicher Krimineller. Zwei Jahre nach der Entdeckung erklärten Vertreter_innen der US-Regierung, „Stuxnet“ sei zusammen mit Israel entwickelt worden, um die Urananreicherung in iranischen Anlagen zu sabotieren (Sanger, 2012: A1). Weitere Analysen haben seither gezeigt, dass „Stuxnet“ nur ein Teil einer ganzen Familie von Schadsoftware mit derselben Code-Basis ist, die vor allem in Nahen Osten Schäden in einer Höhe verursacht hat wie herkömmliche Cyber-Kriminelle (Kaspersky Lab, 2012). Auch der beim Angriff auf die BELGACOM sowie in Deutschland und Brasilien eingesetzte Trojaner REGIN stammt nach forensischen Analysen der Codebasis aus den Programmierwerkstätten der NSA (Rosenbach et. al., 2015).

Das Eindringen in die IT-Systeme von Sony und das Entwenden von Daten dort sowie die zeitweilige Übernahme der IT des französischen TV-Senders TV 5 Monde im Frühjahr 2015 unterstreichen, dass die Nutzung von Manipulations- und Sabotagewerkzeugen mittlerweile zum Alltag bei der Austragung von Konflikten nahezu jeder Art gehört. Diese Cyber-Kriegsführung, die Manipulation von Computern und Rechnernetzen, richtet sich zunächst gegen den Computereinsatz für militärische Zwecke auf militärischen Infrastrukturen. Durch die Vernetzung des offenen Internets mit militärischen Netzwerken bedeutet „Informationskriegsführung“ aber auch die potenzielle Bekämpfung aller, die im Internet Daten und Informationen sammeln und verarbeiten.

Kollateralschäden

Es sind nicht nur gezielte Angriffe auf IT-Systeme ziviler Nutzer_innen, die die NSA und vergleichbare Dienste weltweit zu einer Gefahr machen. Noch größer ist die Gefahr durch ihre unermüdliche Arbeit zum Abbau der IT-Sicherheit.

Die Berichterstattung über den so genannten „Heartbleed-Bug“ machte auch Internet-fernen Zeitgenosse_innen die Bedeutung von Verschlüsselungsverfahren im Internet deutlich. Heartbleed bezeichnete einen am 31.12.2011 eingepflegten Programmierfehler in der Software der Secure Socket Layer (SSL)-Software, der es ermöglichte, den für so gut wie jede gesicherte Bestellung und Finanztransaktion im Internet genutzten Verschlüsselungsmechanismus auszuhebeln und Bankdaten und andere sensitive Informationen mitzulesen und zu verfälschen. Fast alle Anbieter von Internetzugängen rieten ihren Nutzer_innen dringend dazu, ihre Konten zu prüfen und neue Passwörter anzulegen. Die Öffentlichkeit lernte dabei als wichtiges Prinzip des Internets, dass die gesamte Sicherheitsinfrastruktur bei e-Commerce, Telebanking und anderen sensitiven Abläufen von einer Open Source-Software abhängt, für deren Erstellung ein_e einzige_r Programmierer_in fest angestellt ist und für die keine Alternativen verfügbar sind. Für Cyber-Angreifer_innen ist dieses Nadelöhr ein wichtiges Ziel. NSA-Dokumente über einen Anfang August 2007 gehaltenen Vortrag enthalten bereits Hinweise auf die Nutzung von Schwachstellen in der SSL-Verschlüsselung durch die NSA.(5)

Auch die Verschlüsselung von „Virtuellen Privaten Netzwerken“ (VPN) ist von höchstem Interesse für die NSA. VPN werden von Unternehmen und Behörden, aber auch Privaten genutzt, um die Internetkommunikation zwischen verschiedenen Organisationsteilen rund um den Globus zu verschlüsseln und gegen Mitlesen und Manipulationen zu sichern. VPN-Netze werden nicht nur durch die Nutzung von Schwachstellen in den Produkten ausgehebelt, sondern durch den gezielten Einbau von Hintertüren, die einige Hersteller auf Veranlassung der NSA in ihre Produkte integrieren.(6) Mehrere der publizierten NSA-Dokumente enthalten Anleitungen, mit welchen Werkzeugen VPN-Datenverkehr automatisiert entschlüsselt und ausgewertet werden kann.

Das Brechen von Verschlüsselungsverfahren gehört zu den wichtigsten Fähigkeiten der NSA, ihrer Partnerdienste ebenso wie aller anderen Kommunikationsnachrichtendienste. Die NSA hat für die Steuerung des FLAME-Trojaners das auf Verschlüsselungssystemen beruhende System der Softwarezertifikate von Microsofts Software-Updates ausgehebelt (Microsoft Security Research & Defense, 2012). Die NSA rühmt sich, führend in der Entschlüsselung der gängigen Verfahren zu sein und war vor zwei Jahren dabei, die Entschlüsselung in Echtzeit anwenden zu können.(7)

Die Entschlüsselung zu brechen, ist aber nicht nur wichtig für die Spionage. Auch hier liefert der BELGACOM-Angriff Belege für die Nutzung von Fähigkeiten zur Entschlüsselung in Echtzeit, um Schadcode in entschlüsselte Kommunikationsdaten einzufügen und weiterzuleiten. IT-Sicherheitsverantwortliche, die erwarten, dass ihre verschlüsselte Kommunikation nicht als Ursache infrage kommt, wenn Schadsoftware ins Unternehmen gelangt, müssen ihre gesamte Sicherheitsphilosophie und alle Verfahren auf den Prüfstand stellen, was den Aufwand vervielfacht und obendrein voraussetzt, die geheim gehaltenen Zugänge der Geheimdienste zu erraten.

Der Heartbleed-Bug zeigte der Allgemeinheit der Internetnutzer die Verwundbarkeit grundlegender Sicherheitsverfahren wie SSL. Doch schon Jahre vor der Programmierung dieser Lücke erklärte die NSA, in der Lage zu sein, dieses Verfahren auszuhebeln. Firmeninterna, die über das Internet per VPN gesichert übermittelt werden, sind ebenfalls seit Jahren mitlesbar und kompromittiert. Welche weiteren Sicherheitsmechanismen die NSA und andere Dienste ausgehebelt und kompromittiert haben, wird von IT-Sicherheitsexperten diskutiert (Weber, 2015). Entscheidend ist dabei, dass es keine Aufarbeitung der

Sicherheitssysteme gibt, die nach heutigem Wissen als wirkungslos, zweifelhaft sicher oder wahrscheinlich sicher eingestuft werden müssen. Dementsprechend gibt es immer noch keine zuverlässigen Aussagen, welche Anwendungen im Internet noch sicher sind, oder ob die NSA und andere Dienste solche Datenkommunikation mitlesen und manipulieren können.

Die Erkenntnis aus der Analyse der NSA-Dokumente kann daher heute nur lauten, dass die Überwachung des Internets für die NSA genauso wie für deren gegnerische Dienste nur der Ausgangspunkt für die Manipulation von IT-Systemen ist. Spätestens seit Stuxnet hat Cyber Warfare die Schwelle zur Verursachung physischer Schäden überschritten.

Von der NSA wissen wir darüber hinaus, dass sie und ihre Partnerdienste ihrem eigenen Verständnis nach einen uneingeschränkten und unterschiedslosen Cyberkrieg gegen vermutete Gegner_innen, ebenso wie gegen die eigenen Verbündeten führen. Für diese Manipulationen und Angriffe auf IT-Infrastrukturen wurden spezielle Werkzeuge entwickelt und grundlegende IT-Sicherheitsmechanismen wie Software-Zertifikate, Verschlüsselungs- und Authentisierungsmechanismen kompromittiert. Technische Alternativen existieren nicht. Ohne diese durch die NSA, ihre Verbündeten und Gegner_innen ausgehebelten Mechanismen für Sicherheit und Zuverlässigkeit der IT werden der zivilen Informationsgesellschaft massive Risiken aufgebürdet.

Ressourcen im Ungleichgewicht

Wenn heute über NSA und Computerspionage berichtet wird, wird dabei meist vergessen, wie alt diese Form der Informationsbeschaffung ist. Bereits 1986 wurde durch Anhörungen vor dem U.S. Senat bekannt, dass Militärs und Geheimdienste der USA und der Sowjetunion Diebstähle von Datenträgern und Einbrüche in Computerinstallationen vor Ort dazu nutzten, Daten aus gegnerischen Computersystemen zu beschaffen und diese Systeme auch zu sabotieren (U.S. Senate Select Committee on Intelligence, 1986; Peterzell, 1989).

Das Internet hat diese Art der Spionage beträchtlich vereinfacht (Ruhmann, Bernhardt, 2014). Seit Ende der 1990er Jahre wurde die Zahl der Hacker_innen im Staatsdienst kontinuierlich vergrößert. Heute haben über 100 Staaten Warfare-Kapazitäten aufgebaut, die immer zuerst defensiv ausgerichtet sind und über die Zeit auch offensive Aspekte umfassen. Das UN-Institut für Abrüstungsforschung - United Nations Institute for Disarmament Research (UNIDIR) - hatte bereits 2013 in Medienverlautbarungen 41 Staaten ausgemacht, die militärische Cyberaktivitäten verfolgen (The Cyber Index, 2013: 3). Auch die Bundeswehr führte 2002 ganz nach dem Vorbild der NSA alle Einheiten zur elektronischen und psychologischen Kriegsführung im Kommando Strategische Aufklärung (KSA) zusammen. Seit 2006 gehört zum KSA auch eine ursprünglich mit 76 Mitarbeiter_innen begonnenen Hacker_innengruppe für „Computer Netzwerk Operationen“.(8)

Heute verfügt das KSA auf der „Angreiferseite“ im Information Warfare insgesamt über 5.500 Soldat_innen und 500 zivile Mitarbeiter_innen.(9) Vergleicht man dies in Deutschland mit der zivilen Strafverfolgung sowie dem Austausch zwischen Nachrichtendiensten und Strafverfolgern über Computerdelikte, dabei vor allem die Beobachtung des Internet für terroristische Aktivitäten, so lassen sich bundesweit – nach Abzug der Mitarbeiter_innen mit Doppelaufgaben – zwischen 900 und 1.000 Ermittler_innen und IT-Fachleute aufseiten der zivilen Ermittlungsarbeit zählen(10). Auf finanzieller Seite wendet die Bundesregierung 30 Mio. Euro pro Jahr für die zivile IT-Sicherheitsforschung auf, der BND beantragte Ende 2014 300 Mio. Euro für den Ankauf von IT-Sicherheitslücken zur Nutzung für Cyberattacken und die Aufstockung von Personal für offensive Cyberaktionen.

Auch für die USA sind solche Vergleichsdaten ermittelbar. Zur Umsetzung der im Juli 2011 veröffentlichten ersten U.S. Strategie für Operationen im Cyberspace (U.S. Department of Defense, 2011) plante der Kommandeur des U.S. Cyber Commands – seit 2008 in Personalunion Leiter der NSA -, die Zahl seiner für

Cyber-Operationen vorgesehenen Truppen ab 2013 zu verfünffachen - von 900 auf 4.900 Soldat_innen und Zivilist_innen (Nakashima, 2013). Dies wird fortgesetzt mit der im April 2015 vorgestellten neuen Cyber-Strategie des U.S. Department of Defense (DoD), die den zusätzlichen Aufbau einer „Cyber Mission Force“ aus weiteren 6.200 Militärs, Zivilist_innen und kommerziellen Auftragnehmern vorsieht (U.S. Department of Defense, 2015), die die Hacker_innen der ebenfalls dem Cyber Command untergeordneten NSA unterstützen sollen.

Die NSA hatte für 2013 einen Etatansatz für Cyberangriffe und Entschlüsselung von über 12 Mrd. Dollar zur Verfügung, davon 625 Mio. US-Dollar für die Entwicklung von Schadsoftware zur Verfügung, und 10 Mrd. Dollar für das „gemeinsame kryptologische Programm“ für „bahnbrechende kryptoanalytische Fähigkeiten […], um den Internetverkehr auszuwerten“ (Gellman, Miller, 2013).(11) Im Vergleich dazu erklärte das für die Bekämpfung von schwerwiegenden Computerdelikten in den USA zuständige FBI, durch 152 Neueinstellungen bis Ende 2015 landesweit die Zahl von 750 Agenten für die Aufklärung von Computerdelikten verfügbar haben zu wollen (Mandak, 2014). Der gesamten, dem U.S.-Justizministerium zugeordneten Strafverfolgung von Computerdelikten stand 2014 ein Budget von 722 Mio. Dollar zur Verfügung (Moore, 2014), was auch die Mittel für den Schutz der eigenen IT-Systeme einschließt. Allein dem TAO der NSA steht somit mehr Personal für Hackerangriffe zur Verfügung als der Strafverfolgung durch das FBI und fast ebenso viele Finanzmittel für die Schadsoftware-Entwicklung wie für die gesamte zivile Strafverfolgung von Cyberattacken durch das FBI.

Die Gegenüberstellung der verfügbaren Daten über finanzielle und personelle Ressourcen in den USA und Deutschland macht trotz der lückenhaften Datenlage deutlich, dass der „Angreiferseite“ in der Regel die sechs- bis zehnfachen Ressourcen für Cyberattacken und die Kompromittierung der IT-Sicherheit zur Verfügung stehen im Vergleich zur „Verteidigerseite“ der IT-Sicherheit. Die Daten dokumentieren ein unerwartet klares Ungleichgewicht und eine Prioritätensetzung der Regierungen in den USA, in Deutschland, aber den Indizien nach auch in anderen Staaten zugunsten der Cyber-Angreifer_innen und die im Vergleich geringe Bedeutung, die von staatlicher Seite auf die Stärkung der IT-Sicherheit, die zivile Strafverfolgung und die Analyse von IT-Sicherheitsvorfällen gelegt wird.

Militär und Geheimdienste als Cyber-Angreifer können nahezu jeden Aufwand treiben, weil sie Cyberattacken als günstige Alternative zu konventionellen Militärschlägen sehen. IT-Sicherheitsverantwortliche und die Zivilbevölkerung sollten möglichst schnell mit der Einsicht umgehen lernen, dass IT-Sicherheit so weder für zivile noch militärische Systeme zu leisten ist.

Der Vergleich der Ressourcen für Militärs und Geheimdienste für Cyberangriffe macht deutlich, dass nur ein radikales Umsteuern helfen kann, die umfassende Kompromittierung aller Facetten unserer IT-Infrastruktur zu beenden und durch neue, sichere Systeme zu ersetzen. Investiert werden muss in die Sicherung von IT, nicht in neue Angriffsstrategien und –werkzeuge.

Parlament und Exekutive sind an die Beachtung der Grundrechte gebunden. Bei Cyber Warfare geht es in Deutschland neben dem Fernmeldegeheimnis und dem Grundrecht auf informelle Selbstbestimmung ganz wesentlich um den Schutz des 2007 vom Bundesverfassungsgericht formulierten Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Der eigentliche Skandal an den Enthüllungen um die NSA-Dokumente ist heute die Erkenntnis, dass das Telekommunikationsgeheimnis faktisch abgeschafft ist, der Datenschutz aufgegeben wurde, die Integrität von IT-Systemen fundamental kompromittiert ist – und diesem Rechtsbruch bisher kaum Einhalt geboten wird.

UTE BERNHARDT *ist Informatikerin und beschäftigt sich seit Jahren mit "Informatik und Gesellschaft" sowie der folgenreichen Beziehung von Informatik und Militär. Sie war Lehrbeauftragte der Fachhochschule Bonn-Rhein-Sieg und der FernUni Hagen. Zudem ist sie Mitglied des FIfF und war FIfF-Vorstandsmitglied von 1991 bis 1998. Sie arbeitet als wissenschaftliche Mitarbeiterin.*

INGO RUHMANN *ist Informatiker und arbeitet im Bereich Technikfolgenabschätzung, Forschungspolitik, IT-Sicherheit, Information Warfare, „Cyberwar“, Geschichte der Geheimdienste und Datenschutz. Er ist Lehrbeauftragter im Studiengang „Security Management“ der Fachhochschule Brandenburg. Zudem ist er*

Mitglied des FifF, in dessen Vorstand er von 1991 bis 1998 aktiv war.

Anmerkungen:

(1) Denial of Service (DoS) sind gezielte Anfragen an sog. Dienstprogramme, die auf einem Webserver laufen. Werden solche Anfragen als massenhafte DDoS-Attacke von vielen Rechnern aus gleichzeitig durchgeführt, können damit angegriffene Server oder Webdienste außer Betrieb gesetzt und deren Anbieter u.U. beträchtlich geschädigt werden.

(2) Turmoil und Turbulence werden in den NSA-Dokumenten zu XKeyScore zu einem Vergleich heran gezogen, so S. 8 der vom Guardian dokumentiertem XKeySore-Präsentation der NSA, http://www.documentcloud.org/documents/743252-nsa-pdfs-redacted-ed.html .

(3) So die von The Guardian dokumentierte NSA-Präsentation »XKeySore« vom 25.2.2008, http://www.documentcloud.org/documents/743252-nsa-pdfs-redacted-ed.html.

(4) Die Daten beruhen auf dem Dokument http://www.spiegel.de/media/media-35657.pdf , Folie 21.

(5) Dies bezieht sich auf S. 7ff in dem NSA-Dokument http://www.spiegel.de/media/media-35520.pdf.

(6) Die Ursachen bleiben im Detail unklar; eindeutig werden aber sowohl fehlerhaft implementierte als auch gezielt eingebaute Lücken genutzt, da in NSA-Dokumenten neben Systemen aus US-Herstellung wie Cisco auch Produkte aus der VR China wie etwa Huawei genannt werden, vgl. das NSA-Dokument http://www.spiegel.de/media/media-35551.pdf.

(7) Vgl. dazu die Präsentation zum Programm Bullrun, http://www.spiegel.de/media/media-35532.pdf.

(8) Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan van Aken, Andrej Hunko, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE. Elektronische Kampfführung der Bundeswehr, BT-Drs. 18/3963.

(9) Das KSA verfügte zu Beginn über 6.300 Soldaten und 700 zivile Mitarbeiter (http://www.bundeswehr.de/portal/a/bwde/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pPKUVL3ikqL
) Nach Umstrukturierungen 2007 und 2013 belief sich die Personalstärke noch auf insgesamt 6.000. Zu den Aufgaben siehe: http://www.spiegel.de/politik/deutschland/strategische-aufklaerung-bundeswehr-belauscht-die-welt-a-575417.html .

(10) Die Daten sind ermittelt aus: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE. Die Strategie der Bundesregierung zur Bekämpfung der Internetkriminalität – Das Nationale Cyber-Abwehrzentrum. BT-Drs. 17/5694 Frage 4. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Wolfgang Wieland, Volker Beck (Köln), Jerzy Montag, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN. Das Gemeinsame Terrorismusabwehrzentrum – Sachstand 2008. BT-Drs. 16/10007, Frage Nr. 1. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau u. a. und der Fraktion DIE LINKE. Die Strategie der Bundesregierung zur Bekämpfung der Internet-Kriminalität; Gemeinsames Internetzentrum, BT-Drs. 17/5557, Frage Nr. 1.

(11) Im Detail: FY 2013 Congressional Budget Justification, National Intelligence Program Summary; http://s3.documentcloud.org/documents/781537/cbjb-fy13-v1-extract.pdf.

https://www.humanistische-union.de/publikationen/vorgaenge/209/publikation/bedrohung-durch-cyberangriffe-in-der-praxis-vollstaendig/
Abgerufen am: 15.10.2026