Humanistische Union

Cyberspace, der neue Wilde Westen

Cybercrime, Cyberterrorism, Cyberwar – Panikmache oder unterschätzte Gefahren? Aus: vorgänge Nr. 209 (Heft 1/2015), S. 4-17

(Red.) Längst hat der Cyberspace seinen Charme als faszinierende neue Kommunikationswelt hinter sich gelassen. Die Risiken, die mit der kompletten Vernetzung fast aller Lebensbereiche einher gehen, sind erheblich. Überwachung, Kriegsführung und anderer Missbrauch sind nur einige Schattenseiten der Netzwelt, die Bürger- und Menschenrechtsgruppen deutlicher fokussieren sollten, so Stefan Hügel und Dietrich Meyer-Ebrecht.

Cyberspace ist das Synonym für den globalen Datenraum. ‚Cyber' ist die englische Kurzform für Kybernetik, die von Norbert Wiener begründete Wissenschaft von der Steuerung und Regelung von Maschinen, lebenden Organismen und sozialen Organisationen. Wenn dieser Bezug bei der Schöpfung des Begriffs noch nicht Pate gestanden haben mag, beschreibt er heute treffend das synergetische Zusammenwachsen unserer Gesellschaft mit der Informationstechnik. Das Substrat des Cyberspace war zunächst ein feinmaschiges weltumspannendes Netzwerk aus Kabelnetzen, terrestrischen Funknetzen, Kommunikationssatelliten, über das Kommunikationsdienste und verteilte Datenverarbeitung abgewickelt werden. Mittlerweile ist der Cyberspace jedoch weit hinausgewachsen über seine Rolle als Medium für den Informationsaustausch, denn Datenbanken von unermesslicher Speicherkapazität und Computerressourcen mit gigantischer Leistung sind zu unverzichtbaren Elementen des Cyberspace geworden. Und gierig greift unsere Zivilgesellschaft nach den vielfältigen, sich ständig erweiternden Optionen des Cyberspace. Kaum ein Lebensbereich bleibt ausgenommen und unangetastet. Sie begibt sich dabei aber auch in eine immer engere Abhängigkeit – und geht, im Verlass auf ein immer währendes und ungestörtes Funktionieren des Cyberspace und seiner Ressourcen, fundamentale Risiken ein.

Risiken

Ein prominentes Beispiel für die riskante Abhängigkeit von vernetzten IT-Systemen ist die Versorgung mit elektrischer Energie. Sie ist unverzichtbar für fast alle Lebensbereiche. Die Optimierung von Erzeugung, Transport und Verteilung wiederum bedarf einer komplexen vernetzten Steuerung, die mit den ‚smart meters' über das Internet schon bis in die Haushalte hineinreicht. Bereits 2010 hat sich das Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB) in einer Studie das Szenario eines großräumigen Ausfalls der Stromversorgung vorgenommen, um die Gefährdung und Verletzbarkeit unserer Zivilgesellschaft deutlich zu machen: Ein Ausfall von wenigen Stunden Dauer zieht mindestens immense volkswirtschaftliche Kosten nach sich. Dauert ein großräumiger Ausfall Tage, geraten Menschenleben in akute Gefahr. Unruhen und Plünderungen sind bereits nach wenigen Wochen zu erwarten. Bei weiter anhaltendem Ausfall ist mit irreparablen Schäden wie nach konventionellen kriegerischen Angriffen zu rechnen.(1)

Die Energieversorgung ist ein Extremfall, denn von ihr hängen ausnahmslos alle lebenswichtigen Infrastruktureinrichtungen wie Trinkwasserversorgung, Mobilfunknetze oder Verkehrsleitsysteme für Straße, Schiene oder Luftraum ab. Deren Ausfälle werden weniger dramatisch, aber dennoch folgenreich sein. Allein ein länger anhaltender Verkehrskollaps kann das gesellschaftliche Leben empfindlich lahmlegen und nachhaltige Folgen haben, denn unsere Gesellschaft hat sich existentiell abhängig gemacht von einer auf Effizienz getrimmten just-in-time-Produktion und -Logistik, die von komplex vernetzten Rechenprozessen

optimiert und gesteuert werden. Verharmlost werden dürfen selbst Eingriffe in Systeme von Behörden, Institutionen, Dienstleistungsunternehmen oder Medienanstalten nicht. Auch wenn sie keine direkten physischen Auswirkungen haben müssen, kann mittels Desinformation oder Störung von Verwaltungsprozessen eine Destabilisierung der Gesellschaft provoziert werden. Cybersicherheit wird zu einem brisanten Thema.

Ursachen

Die Ursachen für Systemausfall oder Fehlfunktion fallen in zwei Kategorien: Technikversagen oder Missbrauch. Der Gefahr eines Technikversagens kann technisch vorgebeugt werden, durch hohe Zuverlässigkeitsanforderungen und funktionale Redundanzen. Ungleich problematischer ist die Gefahr des Missbrauchs. Hinter einem Missbrauch stehen Menschen, die in Systeme einbrechen, um diese vorsätzlich zu manipulieren, zu stören oder zu zerstören.

Ein Systemeinbruch kann von außen erfolgen. Passwörter können mit brute-force-Methoden geknackt werden, speziell wenn sie nicht zu kompliziert aufgebaut sind. Effizienter ist es, nach Angriffspunkten in den Sicherungsmechanismen zu suchen, an denen man diese mit maßgeschneiderten Softwarewerkzeugen, so genannten *Exploits*, aushebeln kann. Mit einem hohen Maß an Kreativität und Fachkenntnis gepaart mit krimineller Energie spüren Angreifer_innen bisher unerkannte Angriffspunkte (‚Schwachstellen') der Software auf, die erst durch den Exploit zur ‚Sicherheitslücke' werden – solange, bis der Exploit bekannt wird und die Software durch einen Work-around an dieser Schwachstelle ertüchtigt werden kann. Wie oft geargwöhnt wird, handelt es sich bei solchen Schwachstellen gar nicht einmal immer um Nachlässigkeiten in der Programmierung, auch wenn Software niemals völlig fehlerfrei sein wird. Vielmehr sehen sich Softwareentwickler_innen hier in der Rolle von Schachspieler_ innen, die die Gegenzüge des Gegners über möglichst viele Spielzüge vorausdenken müssen. Nur hat dieses ‚Spiel' kein definitives Ende und keine festgelegten Regeln. Die hohe Komplexität der Systeme macht die Optionen der Angreifer unüberschaubar. Dies gilt auch für das Aufspüren eines anderen Einbruchsweges, den so genannten backdoors. Hierbei handelt es sich um versteckte Zutrittswege, die von Entwickler_innen in Betriebssysteme oder sogar in Firmware, aus eigener Neugier oder sogar im Auftrag staatlicher Stellen, heimlich eingebaut werden.

Eine weitere Kategorie von Einbruchswerkzeugen umgeht die Sicherungsmechanismen von innen heraus. Dazu gehören Computerviren, Würmer und Trojaner. Das Prinzip ist, über den regulären Datenverkehr unerkannt Schadsoftware einzuschleusen, beispielsweise eingebettet im Anhang einer E-Mail oder geladen bei Aufruf einer speziell manipulierten Webseite, eingefangen von präparierten USB-Sticks oder SD-Karten. Mitunter werden auch Systemkomponenten wie Router, Firewalls oder Festplatten vor ihrer Auslieferung an die Kund_innen abgefangen und mit Schadsoftware präpariert. Die eingeschleuste Schadsoftware kann dazu dienen, einen verdeckten Kommunikationskanal zu Angreifern herzustellen, über den das infizierte System manipuliert werden kann, vom heimlichen Auslesen von Daten bis zur vollständigen Übernahme der Kontrolle. Sie kann auch die zur Ausführung der beabsichtigten Schadfunktion notwendigen Programme eingebettet als so genannte Payload mit sich führen. Oder beides kombinieren. Ein Beispiel für eine besonders raffinierte Schadsoftware dieser Kategorie ist der Computerwurm Stuxnet, der sich über mobile Feldprogrammiergeräte in die von jedweden Netzen isolierten Prozesssteuerungen iranischer Urananreicherungsanlagen einschleusen konnte, um diese in Betriebszustände zu fahren, die sie einer zerstörerischen mechanischen Belastung aussetzen sollten.

Zur Erlangung vertraulicher Zugangsdaten spielt auch *social engineering* eine gewichtige Rolle. Einher geht dies meist mit der Ausschnüffelung des Privatlebens der Zielperson zur Erschleichung ihres Vertrauens oder zur Erpressung. Nicht zu unterschätzen sind die sogenannten Innentäter: Mitarbeiter_innen, die aus Enttäuschung über eine verpasste Beförderung, Verärgerung über den Vorgesetzten oder aus eigenen finanziellen Interessen ihre Zugangsprivilegien nutzen, um in den Systemen ihres eigenen Arbeitgebers

Schäden zu verursachen.

Schutz

Technisch können wir Systeme gegen gewollte Angriffe und Eingriffe nur bedingt schützen. Zwei systemimmanente Phänomene spielen hier eine Rolle. Der Cyberspace ist ein Abstraktum, zumindest für Nutzer_innen ohne tiefe technische Kenntnisse. Was außerhalb des Smartphones oder hinter der Datensteckdose des Arbeitsplatzcomputers mit unseren Daten abläuft, bleibt uns verschlossen. Undurchsichtig bleibt, wo unsere Daten gespeichert, wo sie verarbeitet werden und was über die von uns gewollten Prozesse hinaus mit ihnen passiert (die *Cloud* heißt wohl nicht zufällig „Cloud“ – unsere Vorstellungen bleiben wolkig wie der Begriff). Das gilt ebenso für Menschen in entscheidenden Positionen in Politik und Wirtschaft, wenn sie nicht gerade über eine profunde IT-Fachbildung verfügen. Und selbst IT-Fachleute sind nur noch bedingt in der Lage, die Komplexität des Cyberspace zu durchschauen. Wenn die Vorstellungskraft für die Gefahren fehlt, wenn die Gefahren ebenso abstrakt bleiben wie das Medium, fallen tragfähige Entscheidungen über Sicherheitskonzepte, über konkrete Maßnahmen und Nachdruck für ihre Durchsetzung schwer. Kontraproduktiv kommt hinzu, dass sich das Verständnisdefizit auch auf die öffentliche Diskussion auswirkt. Sie schwankt zwischen den Extremen Panikmache und Unterschätzung oder gar Ausblenden der Gefahren.

Der zweite Punkt ist ein Antagonismus: Wenn ich mich in meinem Haus nicht einmauern will, wenn ich mich auch in der Außenwelt bewegen möchte, wenn ich auch mir genehme Besucher_innen einlassen möchte, muss ich Türen vorsehen, die ich zwar kontrolliere, doch sobald eine Tür im Haus ist, wird es Mittel geben, sie missbräuchlich zu öffnen. Der Aufwand steigt, je perfektionierter die Sicherungsmaßnahmen werden, und damit wachsen auch die Einschränkungen, die ich mir selber auferlegen muss. Der chilenische Systembiologe und Philosoph Humberto Maturana hat diesen Antagonismus zu einem grundlegenden Merkmal lebender Systeme erklärt: Die biologische Zelle braucht eine Hülle, die sie gegenüber ihrer Umgebung schützt. Die Hülle muss jedoch von innen nach außen und von außen nach innen durchlässig sein können – kontrolliert. Denn die Zelle hat einen Stoffwechsel, und sie muss sich über Signale (hier Botenstoffe) mit ihrer Umgebung arrangieren. Wie im biologischen Mikrokosmos gelte dies, so Maturana, ebenso für soziologische, ökonomische, politische Systeme – ‚lebende Systeme’ im Sinne Maturanas. Wir können dieses Paradigma auf den Cyberspace übertragen. Er ist ein System aus Systemen, die jedes für sich erst durch den Informationsaustausch untereinander ihre funktionale Mächtigkeit gewinnen. Synergie führt zu einer Gesamtfunktionalität, die über die Summe der Einzelfunktionalitäten hinausgeht. Sie führt jedoch auch zu einem qualitativen Sprung in der Komplexität. In seinen unüberschaubaren Wechselwirkungen mit der Lebendwelt wird der Cyberspace gleichsam zu einem maturana'schen Lebendsystem. Zwischen seinen Teilsystemen müssen wir den Informationsaustausch zulassen, und damit gehen wir unvermeidbar das Risiko ein, dass die notwendigen Öffnungen missbraucht werden können.

Natürlich sind diese Türen gegen unerwünschte Eindringlinge mittlerweile verriegelt. Sorgfältig kontrolliert werden die eingehenden und ausgehenden Datenströme. Dass sich dennoch immer wieder neue Möglichkeiten zur Umgehung der Kontrollen ergeben, hat auch mit der Entwicklungsgeschichte des Internet zu tun. Es gab eine Zeit, als Computernetze noch ein Experimentierfeld waren und in der Gemeinde der an der Entwicklung Beteiligten ein professionelles Vertrauen herrschte, wie in einer abgelegenen Dorfgemeinschaft, in der man das Fahrrad nichtangeschlossen an der Hauswand stehen lassen darf, die Haustür unverschlossen bleiben darf. In dieser Zeit wurden die grundlegenden Mechanismen für den Datenaustausch zwischen vernetzten Computern konzipiert, ohne Vorstellung über wachsende Anforderungen an ihre Schutzbedürftigkeit, wenn das Netz einmal wachsen und die abgeschlossene Domäne der Wissenschaft verlassen würde. In seiner Komplexität kann das Internet als ein kontinuierliches Experiment betrachtet werden, das sich evolutionär auf der Basis seiner Urkonzepte entwickelt hat und ständig weiterentwickelt. Alle nachträglich konzipierten Sicherungsmechanismen müssen auf diese frühen Konzepte aufgesetzt werden. Sie werden dadurch komplizierter als notwendig und bieten in der Folge mehr

Ansatzpunkte, um sie missbräuchlich zu umgehen.

Ein radikaler Vorschlag ist die Entnetzung, also die physische Trennung vom öffentlichen Netz, gerade bei kritischen Systemen.(2) In der Tat stellt sich die Frage, ob solche Systeme, wie beispielsweise (Kern-) Kraftwerke mit dem weltweiten Internet vernetzt und damit für Angreifer technisch weltweit zugänglich sein müssen. Mindestens für besonders kritische (Teil-) Systeme kann dies ein Ansatz sein. Doch in vielen Fällen ist es heute schlicht nicht mehr realistisch, diese Trennung vorzunehmen, wenn die zugrundeliegenden Dienste immer stärker miteinander vernetzt sein müssen. Und gegen physisch eingeschleuste Datenträger, wie beim erwähnten Stuxnet, sind auch solche Maßnahmen machtlos.

Letztlich ist vollständige Sicherheit – wie überall – nicht zu erreichen. Das Ziel der IT-Sicherheit ist, zu minimalen eigenen Kosten die Kosten für Angreifer zu maximieren – bis ein Angriff nicht mehr wirtschaftlich ist. Doch müssen wir angesichts eines Gegners wie der NSA, die über praktisch unbegrenzte Ressourcen verfügt, diese Zielsetzung nicht überdenken?

Akteure

Wer sind die Angreifer? Und was sind ihre Ziele? *Cybercrime* ist die erste Kategorie – Kriminelle, die in Computernetze eindringen, um Daten zu stehlen, illegale Geldtransfers zu veranlassen oder Systeme mit Schadsoftware in erpresserischer Absicht zu infiltrieren. Bedrohlicher ist eine zweite Kategorie: terroristische Angriffe auf Systeme im Internet, *Cyberterrorism*. Einen kleinen Vorgeschmack haben wir mit der Lahmlegung des Computernetzwerks des französischen Fernsehsenders TV5 erlebt. Lediglich die zeitweilige Störung einer Fernsehsendung? Aber: Wer heute einen TV-Sender hackt, könne morgen die Stromversorgung lahmlegen, so Falk Garbsch, Sprecher des Chaos Computer Club.(3) Die Barriere ist zwar höher, aber nicht unüberwindbar. Dass Terrorist_innen nicht über die für aufwändigere Cyberangriffe notwendigen technischen Ressourcen verfügen würden, kann kaum als Argument taugen, um die potentielle Bedrohung herunterzuspielen. Unauffällig ist die Beschaffung der Ausrüstung, ebenso die Vorbereitung, wenn die digitalen Spuren gut verwischt werden. Ein florierender Schwarzmarkt stellt – für entsprechendes Geld – geeignete Werkzeuge zur Verfügung, auch spezielle Exploits. Die Akteure können ortsungebunden agieren. Eine Rückverfolgung bis zur Quelle eines Angriffs – die so genannte Attributierung (4) – ist äußerst schwierig.

Nicht zu vergessen sind an dieser Stelle *Hacker* oder *Script-Kiddies*, die versuchen, in fremde Systeme einzudringen, um ihrerseits Schwachstellen zu finden, um die Betreiber darauf hinzuweisen oder um einfach nur auszuprobieren, was möglich ist. Sie verfolgen in der Regel zunächst keine finanziellen Interessen, und sie haben auch nicht das Ziel, Systeme zu stören oder gar zu zerstören. Doch auch ihre Angriffe setzen Rechnersysteme einem Risiko aus – und der Verlockung, die dabei gewonnenen Erkenntnisse und ertüftelten Exploits zu Geld zu machen, können am Ende vielleicht doch nicht alle widerstehen.

Cyberspace heute, eine Kolonie der Militärs

Zwei weitere Kategorien, *Cyberspionage* und C*yberwarfare*, gehören eng zusammen wie auch deren Akteure, staatliche Sicherheitsdienste, Geheimdienste und Militärs. Das Wirken dieser Akteure ist uns lange weitgehend verborgen geblieben, bis uns Edward Snowden 2013 mit seinen Enthüllungen der NSA-Aktivitäten das massive Ausmaß der Ausspähung und den zielstrebigen Aufbau eines Angriffspotentials vor Augen geführt hat. Eine führende Rolle spielen hier die Militärs.

Wie die Schöpfung des Computer und die Entwicklung vieler für die Informationstechnik wichtiger Methoden und Technologien geht auch die Entwicklung des Internets auf Initiativen und Ambitionen der Militärs zurück, hier der US-Streitkräfte. Bereits 1969 realisierte die ARPA (heute DARPA, *Defense Advanced Research Projects Agency* des US-Verteidigungsministeriums) eine erste Datenfernverbindung zwischen Rechnerknoten in den USA. Hinter dem Projekt stand das strategische Ziel, die militärischen Rechenzentren angesichts ihrer zunehmenden Bedeutung geografisch zu verteilen und Redundanzen zu schaffen, um die Verletzlichkeit der USA durch physische Angriffe auf die Anlagen zu mindern – es war die Zeit des Kalten Krieges mit ihrer Angst vor Atomschlägen.

Die traditionell enge Verknüpfung zwischen Rüstungsforschung und ziviler Forschung in den USA sorgte dafür, dass sich sehr schnell die Wissenschaftsszene für die Idee einer Vernetzung ihrer Rechenzentren interessierte, die sich bald nicht nur auf die USA beschränkte. 1978 wurde das *Internet Protocol* (TCP/IP) spezifiziert und 1984 das Domain Name System (DNS) eingeführt, das Netzwerk aus dezentralisierten Leitstellen für die Datenflüsse. Beides waren Voraussetzungen für eine allgemeine Öffnung des Internets. Die anfängliche Vernetzung der Rechenzentren von Universitäten und Forschungseinrichtungen wuchs zu dem heutigen weltweiten Datennetz, das mittlerweile vorwiegend kommerziellen Interessen dient. Jedoch die Militärs haben nie ihr Interesse daran verloren, und insbesondere haben die USA bis heute versucht, die Hoheit über den Cyberspace zu behalten – wenn auch nicht administrativ, so doch technologisch und kommerziell.

Mit der *Joint Vision* 2010 legte der US-Generalstab der US-Regierung 1996 ein Positionspapier für die zukünftige Entwicklung der US-Streitkräfte vor, vier Jahre später aktualisiert in der *Joint Vision 2020*. Als Kernbotschaft wird eine gründliche Restrukturierung der Streitkräfte mit dem Ziel einer umfassenden Nutzung moderner Kommunikations- und Informationstechnologie in Waffen, in Waffensystemen und in den zu ihrem Einsatz notwendigen Infrastrukturen gefordert.(5) Die darauf basierende aktuelle Kriegsführungsdoktrin umfasst auch den Cyberspace als Operationsraum.

Die Szenarien beschreiben den Einsatz von Cyberoperationen in drei Phasen. Phase 0, ‚Konditionierung' genannt, dient dem Erkennen der Absichten des Gegners. Ziele sind unter anderem das Ausspionieren der politischen Haltung, der militärischen Pläne und der rüstungsindustriellen Entwicklungen. Geheime Zugänge zu dessen Netzwerken werden angelegt, um sie unbemerkt ausbeuten zu können. Für die Aufgabe, Schwachstellen auch in besonders geschützten Computersystemen zu finden, steht der NSA unter besonderer Geheimhaltung die Spezialeinheit *Tailored Access Operations* (TAO) zur Verfügung.
Dass unsere Systeme von der NSA und anderen Geheimdiensten ausspioniert werden, ist seit Jahren die Regel. Es ist auch offenkundig, dass das Anlegen geheimer Zugänge bereits eine Vorbereitung auf die nachfolgenden Phasen militärischer Cyberoperationen ist: In Phase 1, ‚Abschreckung', sollen dem Gegner mit harmloseren, aber spürbaren Eingriffen in seine Systeme ‚die digitalen Muskeln gezeigt' werden. In Phase 2, ‚Dominieren', werden schließlich Operationen zur Schwächung des Gegners eingeleitet, wie Sabotageakte oder die Übernahme der Kontrolle über kritische Systeme. Spätestens in dieser Phase werden Cyber-Operationen zu kriegerischen Aktionen.

Es stellt sich allerdings die Frage, wie denn die vorbereitenden Operationen zum Anlegen der geheimen Zugänge für die späteren kompromittierenden oder schadenstiftenden Operationen zu bewerten sind. Eingegriffen wird in Einrichtungen eines souveränen Staates, mit dem sich der Angreifer nicht in einem erklärten Krieg befindet.

Dass alle technologisch hochentwickelten Staaten ein Arsenal von Werkzeugen für militärische Operationen im Cyberspace aufbauen, kann als sicher angenommen werden – auch Deutschland, wie aus einem geheimen Strategiepapier des Bundesverteidigungsministeriums hervorgeht.(6) Dass die Aufrüstung im Cyberspace unter strenger Geheimhaltung geschieht, ist selbstverständlich. Nur durch Zufälle werden heute bereits durchgeführte Übergriffe wie beispielsweise durch die bereits genannte Schadsoftware Stuxnet bekannt. Die besondere Heimtücke an der Einbeziehung des Cyberspace in die militärischen Szenarien ist, dass die militärischen Operationen in den zivilen Datenströmen unerkannt mitschwimmen, auch deren Vorbereitung

und Erprobung. Kollateralschäden dürfen nicht ausgeschlossen werden.

Geheimhaltung erschwert die öffentliche Diskussion und behindert die politische Handlungsfähigkeit. Die physische Nichtfassbarkeit militärischer Cyberoperationen hebt alle Grenzen auf: geografische Grenzen, politische Grenzen, die Grenze zwischen Krieg und Nicht-Krieg, die Grenze zwischen Militär und Zivilgesellschaft. Cyberangriffe von Militärs und Geheimdiensten sind nach internationalem Recht Kriegshandlungen.

Wie aber sollen angesichts der Entgrenzung zum Beispiel die Genfer Konvention Anwendung finden? Kriegerische Cyberoperationen beschwören erhebliche Eskalationsgefahren herauf, denn sie können konventionelle militärische Reaktionen provozieren. Die aber können aufgrund des Attributierungsproblems – der Verursacher ist erst durch langwierige Untersuchungen und dann oft nicht einmal sicher zu identifizieren, siehe oben – den Falschen treffen. Wer Cyberwar vorbereitet und führt, gefährdet die internationale Sicherheit in einem bisher meist weit unterschätzten Maß.

Cybersicherheit und Bürgerrechte

Wie lässt sich die Sicherheit wiederherstellen? Derzeit erleben wir, wie Sicherheitspolitiker_innen und Sicherheitsbehörden darauf abzielen, den Bedrohungen mit umfangreichen Überwachungsmaßnahmen zu begegnen. Die Ausspähung der Internet-Kommunikation durch Geheimdienste wie die US-amerikanische National Security Agency (NSA) und den Bundesnachrichtendienst (BND) sind aus deren Sicht Maßnahmen, die Sicherheit im Internet wiederherzustellen. Im Bereich der inneren Sicherheit fallen polizeiliche Maßnahmen wie die Vorratsdatenspeicherung – abgelehnt vom Europäischen Gerichtshof und den Verfassungsgerichten mehrerer Mitgliedsstaaten, dennoch immer noch auf der politischen Agenda – in diese Kategorie. Was aus Sicht der Sicherheitspolitiker_innen und -behörden der Sicherheit dient, bedroht auf der anderen Seite unsere Grundrechte.

Gleichzeitig können selbst Überwachungsmaßnahmen, die gegen andere Staaten gerichtet sind, bereits als Cyberangriffe gewertet werden, wenn sie erfordern, in fremde Rechnersysteme einzudringen und dabei bestehende Schwachstellen dieser Systeme auszunutzen oder neue zu schaffen. Dies ist, folgt man dem *Tallinn-Manual*,(7) in dem NATO-Expert_innen den Versuch unternommen haben, völkerrechtliche Regelungen in den Cyberspace zu übersetzen, ein kriegerischer Akt, der nach ihrer Ansicht sogar mit konventionellen militärischen Gegenschlägen beantwortet werden kann.

Dem Staat kommt dabei eine verfassungsrechtliche Schutzpflicht zu, wie die Verfassungsrechtler Hans-Jürgen Papier, Wolfgang Hoffmann-Riem und Matthias Bäcker gegenüber dem NSA-Untersuchungsausschuss des Deutschen Bundestages festgestellt haben.(8) Der Staat muss seine Bürger_innen vor Cyberangriffen, wie sie die NSA unternimmt, schützen. Folgt man den Berichten in den Medien, ist er angesichts der exorbitanten Überwachungskapazität der NSA dazu nicht nur nicht in der Lage. Vielmehr hat er offenbar, aus Gründen der Staatsraison, überhaupt kein Interesse daran.

Hier zeigt sich die Ambivalenz der Cybersicherheit. Wie können wir einerseits ein angemessenes Sicherheitsniveau gegenüber Angreifern herstellen, ohne dass dies die Grundrechte beeinträchtigt? Wie können wir uns andererseits vor der Ausspähung durch unsere eigenen Verbündeten (und unseren eigenen Staat) schützen?

Vertrauen

Unsere Gesellschaft basiert auf Vertrauen, diese Bedeutung hat Niklas Luhmann in seiner soziologischen Theorie (in der er übrigens an Maturana anknüpft) bereits lange vor dem Siegeszug des Internet herausgearbeitet.(9) Nach Luhmann ist Vertrauen notwendig, um die soziale Komplexität unseres Umfeldes zu reduzieren. Nur so können wir die große Zahl an Entscheidungen treffen, die uns die Realität täglich abverlangt – ohne Vertrauen würde diese Zahl ins unermessliche wachsen, bis wir nicht mehr in der Lage wären, damit umzugehen. Wie sich zeigt, war im Internet dieses Vertrauen noch nie berechtigt.(10) Jetzt ist es zerstört – diese Gewissheit haben wir spätestens seit den Enthüllungen von Edward Snowden.

Zunächst muss dieses Vertrauen wieder hergestellt werden – hier sind vertrauenswürdige, transparente staatliche Institutionen erforderlich. Das Grundgesetz spielt dabei eine wesentliche Rolle – nicht zufällig zählt das Bundesverfassungsgericht zu den Instanzen, denen am meisten Vertrauen entgegengebracht wird.(11)i Zu häufig musste es in der Vergangenheit verfassungswidrige Entscheidungen der Exekutive und Legislative korrigieren. Verfassungsgemäße politische Entscheidungen, die auch nicht versuchen, das Grundgesetz bis an die Grenze des Erlaubten auszureizen, wären ein erster Schritt in diese Richtung.

Technische Absicherung

Ein wesentliches Element der Abwehr von Cyberangriffen ist die technische Absicherung von Rechnersystemen dagegen. Diese beginnt mit der Erstellung sicherer Systeme – zu häufig sind die heute betriebenen Systeme nicht hinreichend sicher, dies zeigen allein schon die zahlreichen Medienberichte der vergangenen Monate und Jahre. Hier haben die Enthüllungen von Snowden zu einer Sensibilisierung geführt – zur technischen, aber auch zur organisatorischen Absicherung der Systeme, beispielsweise durch Einführung und Weiterentwicklung von Informationssicherheits-Management-Systemen, die die betriebsinternen Prozesse für IT-Sicherheit festlegen.

Manche empfehlen, zum Selbstschutz zu greifen. Cryptoparties werden organisiert, um Anwender_innen zu befähigen, ihre im Internet kommunizierten Daten zu verschlüsseln. Die für Überwachung besonders anfälligen Metadaten sollen verschleiert werden, beispielsweise durch Nutzung des TOR-Netzwerks. Solche Initiativen sind zu begrüßen und zu unterstützen – dürfen aber in ihrer Wirkung angesichts eines übermächtigen Gegners wie der NSA, der nahezu unbegrenzte Ressourcen zur Verfügung stehen, nicht überschätzt werden.

Quelloffene Programme (so genannte Open-source-Software) und Rechnersysteme können für technische Transparenz sorgen. Doch auch deren Nutzung ist keine Allheilmittel – Schwachstellen können zwar prinzipiell von der Community erkannt werden, dies setzt aber voraus, dass sich kompetente Menschen intensiv damit auseinandersetzen. Auch in quelloffenen Systemen dauert es mitunter lange, bis Sicherheitslücken gefunden werden – als Beispiel sei der Heartbleed-Bug genannt, der den sicheren Aufruf von Web-Seiten über *OpenSSL* gefährdet hat. Immerhin ist man hier nicht, wie bei proprietären, geschlossenen Systemen, auf das Herstellerunternehmen allein angewiesen – zumal es auch bei einigen (prominenten) Unternehmen Hinweise auf eine Zusammenarbeit mit den Geheimdiensten gibt.(12) Letztlich ist staatliches Handeln gefordert – durch einen Staat, der transparent und vertrauenswürdig agiert und auf funktionierenden demokratischen Institutionen basiert.(13) Eine sichere Infrastruktur muss geschaffen werden, die die Bürgerrechte wahrt und gleichzeitig Sicherheit gegen äußere Angriffe bietet.

Folgerungen

Doch was muss nun geschehen? Die Enthüllungen von Snowden haben gezeigt, wie anfällig unsere Gesellschaft heute gegen Cyberangriffe von staatlicher Seite ist. Cyberkriminalität und Cyberkriegführung müssen bekämpft werden – oberstes Gebot ist es, die Menschen- und Bürgerrechte dabei zu bewahren.

Dabei gilt der Satz des IT-Sicherheitsexperten Bruce Schneier: „If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"(14) – ausschließlich technisch können die Probleme nicht gelöst werden; Maßnahmen auf der politischen und rechtlichen Ebene sind notwendig.

Innenpolitische Folgerungen

Innenpolitisch ist zunächst der aktuelle Spähskandal aufzuklären und die Öffentlichkeit umfassend zu informieren. Der Skandal muss eingehend untersucht werden, und die daran Beteiligten müssen zur Verantwortung gezogen werden. Gleichzeitig müssen die öffentlichen Kontrollrechte verbessert werden, nachdem sich die bisherige Kontrolle der Geheimdienste als ineffektiv erwiesen hat. Das parlamentarische Kontrollgremium (PKG) gewährleistet in seiner heutigen Form keine effektive Kontrolle – das hat uns der Geheimdienstskandal deutlich vor Augen geführt.

Auch wenn das von der Bundesregierung ins Gespräch gebrachte *No-Spy*-Abkommen sich offenbar gerade als Wahlkampftäuschung herausstellt: am Abschluss von Abkommen mit den USA führt kein Weg vorbei. Das ineffektive *Safe-Harbor*-Abkommen zum Datenschutz muss durch ein effektives Datenschutzabkommen ersetzt werden. Auch die Zusammenarbeit von Sicherheitsbehörden muss so geregelt werden, dass der Schutz der Persönlichkeitsrechte, Privatheit und der Datenschutz wirksamer als bisher gewährleistet werden. Maßnahmen zur illegitimen Totalu?berwachung der Bevölkerung mu?ssen sofort beendet werden. Dies gilt umso mehr innerhalb der Europäischen Union – es ist unglaublich, dass sich deren Mitglieder gegenseitig ausspionieren.

Auch nachdem die EU-Richtlinie zu Vorratsdatenspeicherung 2006/24/EG vom Europäischen Gerichtshof (EuGH) und – in der einzelstaatlichen Umsetzung – von mehreren nationalen Verfassungsgerichten eine klare Absage erteilt wurde, wurde die Debatte u?ber ihre Einfu?hrung fortgesetzt. Forderungen nach einer neuen, „gerichtsfesten" EU-Richtlinie, oder nach einer „verfassungsgemäßen" Umsetzung der Vorratsdatenspeicherung werden erhoben; mittlerweile ist die Vorratsdatenspeicherung – in Orwell'scher Sprachmanipulation nun als „Höchstspeicherfrist" bezeichnet – in Deutschland verabschiedet, Verfassungsbeschwerden sind angekündigt.

Stattdessen müssen künftige Überwachungsmaßnahmen die Grundrechte in den Vordergrund stellen und sich am Schutz der Privatsphäre orientieren, nicht am gerade noch verfassungsrechtlich Erlaubten. Internationale Verhandlungen u?ber Datenschutzabkommen, aktuell die Verhandlung der Datenschutz-Grundverordnung in der Europäischen Union, sind einem starken Lobby-Druck ausgesetzt. Die Bundesregierung muss sich für ein starkes Datenschutzrecht in Europa und darüber hinaus einsetzen.

Sowohl das Grundrecht auf informationelle Selbstbestimmung als auch das Telekommunikationsgeheimnis statuieren nicht nur Abwehrrechte gegenüber der deutschen Staatsgewalt, sondern auch Schutzpflichten des Staates gegenüber Eingriffen durch andere. Die nachrichtendienstliche Ausspähung der deutschen Bevölkerung ist unzulässig und strafbar. Der Generalbundesanwalt muss gegen die Verantwortlichen

effektiv ermitteln. Der Schutz der Grundrechte darf nicht hinter die außenpolitischen Belange der Bundesrepublik Deutschland zurücktreten. Rechtsstaatliche Verfahren müssen die Rechte der Betroffenen wahren, beispielsweise bei der Umsetzung des G10-Gesetzes, das die Einschränkung des Brief-, Post- und Fernmeldegeheimnisses regelt.

Aus technischer Sicht wird ein Großteil der Kommunikation im Internet heute immer noch ungesichert abgewickelt – so haben Nachrichtendienste und andere Angreifer leichtes Spiel, die Daten abzugreifen und auszuspähen. Bestehende Sicherheitsmechanismen werden häufig nicht genutzt. Bisherige Ansätze von Behörden zur Bereitstellung solcher Infrastrukturen sind unzureichend. Die Bundesregierung und die zuständigen Behörden müssen die sichere Möglichkeit der Kommunikation im Internet durch eigene Maßnahmen und durch die Gesetzgebung fördern, die die Privatsphäre der Menschen wahrt und sie vor Angriffen von jeder Seite nach dem Stand der Technik schützt.

Vertrauen und Vertraulichkeit ist zwischen Staaten und im innerstaatlichen Regierungshandeln essentiell. Doch gleichzeitig ist größtmögliche Transparenz erforderlich, um das Vertrauen der Öffentlichkeit wiederherzustellen. Illegales, unlauteres oder skandalöses Verhalten verdient keinen Schutz. Whistleblower_innen leisten der Öffentlichkeit einen großen Dienst – nur durch sie kann häufig für eine wirksame Durchsetzung des Rechts gesorgt werden. Sie dürfen nicht kriminalisiert werden.

Außenpolitische Folgerungen

Doch auch außenpolitisch muss gehandelt werden. Leitbild ist die Entmilitarisierung des Internet und dessen ausschließlich friedliche Nutzung.(15) Militär und Geheimdienste müssen international kontrolliert, und diese Kontrolle muss durch völkerrechtliche Abkommen abgesichert werden. Cyberwarfare muss international geächtet, die Integrität des Internets, das Primat seiner friedlichen Nutzung und der Schutz vor militärischem und politischem Missbrauch sichergestellt werden. Daraus ergeben sich grundlegende Forderungen. Sie betreffen:

- Rüstungskontrollbestimmungen für offensive Cyberwaffen und Überwachungstechnologie,
- eine der Genfer Konvention entsprechende internationale Übereinkunft, die vor allem verbietet, dass sich Cyberangriffe gegen Zivilpersonen richten,
- den Verzicht auf Entwicklung und Einsatz offensiver Cyberwaffen,
- die Veröffentlichungspflicht für IT-Schwachstellen, insbesondere für staatliche Behörden und Unternehmen,
- eine gesetzliche Verankerung ausspähsicherer und menschenrechtswahrender Kommunikationsinfrastrukturen.

Das Internet sei, so zitiert Martin Kutscha in diesem Heft die Verfassungsrichterin Susanne Baer, „ein großartiger Raum des Wissens, der Debatte, der Filme, der Musik, der Chats, der Blogs, der Aufsätze, der Lexika, der Chatter und Twitter. So viele Möglichkeiten!“ Staaten, Militärs, Politiker_innen, Gesellschaften und Wirtschaftsunternehmen tragen die Verantwortung dafür, dass dieser großartige Raum zum Nutzen der Menschen bestehen bleibt, und nicht durch technische Bedrohungen, Cyberwarfare und Cybercrime zerstört wird – und dass der Cyberspace nicht wirklich zum „Wilden Westen“ wird. Der oft erhobene Vorwurf einer Panikmache ist angesichts der Faktenlage nicht mehr haltbar.

STEFAN HÜGEL *ist Vorsitzender des Forums InformatikerInnen für Frieden und gesellschaftliche*

Verantwortung (FIfF) und Mitglied der Humanistischen Union in Frankfurt am Main.

***DIETRICH MEYER-EBRECHT** hatte von 1984 bis zu seiner Emeritierung 2004 einen Lehrstuhl für Bildverarbeitung an der RWTH Aachen inne. Er engagiert sich seit 1987 im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), dessen stellvertretender Vorsitzender er heute ist.*

Begriffe

***Cyberangriff:** Aktionen mit der Absicht, Informationen in einem Computer und/oder einem Computernetz abzugreifen oder zu zerstören, oder den Computer und/oder das Computernetz selbst zu schwächen, zu stören oder zu zerstören, oder durch einen solchen Eingriff Störungen oder Zerstörung darüber hinaus zu bewirken.*

***Cybercrime:** Kriminelle oder illegale, strafbare Aktivitäten, die Dienste des Cyberspace nutzen.*

***Cyberspionage:** Die Nutzung des Cyberspace, Staaten, ihre Repräsentanten, Gesellschaften und Wirtschaftsunternehmen auszuspähen, um sich einen Informationsvorteil zu verschaffen.*

***Cyberspace:** Die Gesamtheit der Informations- und Kommunikationsinfrastrukturen, Hardware wie Software, öffentlich wie privat, offen wie eingeschränkt zugänglich. Sie schließt Einrichtungen oder Werkzeuge ein, die nicht mit einem Netz verbunden sind, jedoch über Datenzwischenträger mit dem Netz kommunizieren können.*

***Cyberterrorism:** Gewaltsame kriminelle Aktivitäten durch Nicht-Regierungs-Akteure, die darauf abzielen, politische Systeme durch die Erzeugung von Angst und Unsicherheit zu destabilisieren und zu verändern.*

***Cyberwaffe:** Jede Software oder Hardware, die durch Ausnutzen von Schwachstellen für die Ausführung eines Cyberangriffs angewendet werden kann. Cyberwaffen nutzen üblicherweise Schwachstellen aus, die geheim gehalten werden, und deren destruktiver Charakter aus der Unmöglichkeit erwächst, Effekte seiner Ausnutzung abzuschwächen. Durch die Veröffentlichung der Schwachstelle können Gegenmaßnahmen eingeleitet werden.*

***Cyberwar:** Ein Krieg, der ausschließlich oder flankierend zu einem konventionellen Krieg im Cyberspace geführt wird, sehr wohl aber Auswirkungen außerhalb des Cyberspace haben kann, von psychologischen Effekten über Destabilisierung der Zivilgesellschaft bis zu physischer Zerstörung.*

***Cyberwarfare, Cyberkriegführung:** Die Nutzung von Computertechnologie um die Aktivitäten eines Staates oder einer Organisation zu stören, speziell der gezielte Angriff auf Kommunikationssysteme und kritische Infrastrukturen durch einen anderen Staat oder eine andere Organisation mittels Cyberangriff.*

Anmerkungen:

(1) Thomas Petermann et al. (2010): Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung. Büro für Technikfolgenabschätzung beim Deutschen Bundestag, Arbeitsbericht Nr. 141, November 2010, http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab141.pdf. Wer es spannender mag, lese dazu Marc Elsbergs Techno-Thriller „Blackout“, der auf der Grundlage der TAB-Studie ein dramatisches Szenario aufbaut.

(2) Z.B. Sandro Gaycken (2011): Cyberwar. Das Internet als Kriegsschauplatz. München: Open Source

Press.

(3) Anne Fromm (2015): Das ist erst der Anfang. TAZ, 09.04.2015, http://www.taz.de/CCC-Sprecher-ueber-den-TV5-Hack/%21157880/.

4) Sylvia Johnigk und Kai Nothdurft (2015): Attributierung von Cyberangriffen – Das Problem und seine Folgen. Wissenschaft & Frieden 2015-3, Dossier 79.

(5) Joint Vision 2010 – America's Military: Preparing for Tomorrow (1999), http://www.dtic.mil/jv2010/jv2010.pdf.

(6) Matthias Gebauer (2015): Geheime Bundeswehr-Strategie: Von der Leyen rüstet an der Cyberfront auf. SPIEGEL online, 10.07.2015, http://www.spiegel.de/politik/deutschland/bundeswehr-ursula- von-der-leyen-ruestet-an-der-cyber-front-auf-a-1042985.html.

(7) Michael N. Schmitt (2013): Tallinn-Manual on the International Law applicable to Cyber Warfare, Cambridge University Press.

(8) Matthias Bäcker (2014): Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes. Stellungnahme zu Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014. Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV 2-3 zur A-Drs. 54, Wolfgang Hoffmann-Riem (2014): Stellungnahme zu Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014. Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV 2/1 neu zur A-Drs. 54 und Hans-Ju?rgen Papier (2014): Gutachterliche Stellungnahme, Beweisbeschluss SV-2 des ersten Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode. Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV 2/2 zur A-Drs. 54

(9) Niklas Luhmann (1968): Vertrauen. 4. Auflage 2000. Stuttgart: Lucius & Lucius

(10) Dazu Josef Foschepoth (2012): Überwachtes Deutschland. Post- und Telefonu?berwachung in der alten Bundesrepublik. Göttingen, Bristol: Vandenhoek & Ruprecht

(11) Z.B. in Die Zeit online (2012): Großes Vertrauen in Karlsruhe, wenig in die Regierung. http://www.zeit.de/politik/deutschland/2012-07/umfrage-institutionen-karlsruhe

(12) Kritisch zur Wirkung von Open Source auch Evgeny Morozov, Big Data für alle. Lettre International Nr. 108, Frühjahr 2015

(13) Im Gegensatz zur rein formalen oder „simulativen" Demokratie, vgl. dazu Colin Crouch (2008): Postdemokratie, Frankfurt am Main: Suhrkamp und Ingolfur Blühdorn (2013): Simulative Demokratie. Neue Politik nach der postdemokratischen Wende. Berlin: Suhrkamp.

(14) Bruce Schneier (2000): Secrets & Lies. Digital Security in a Networked World. Indianapolis: John Wiley & Sons.

(15) Dies fordert die Kampagne Cyberpeace des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), https://cyberpeace.fiff.de.

https://www.humanistische-union.de/publikationen/vorgaenge/209/publikation/cyberspace-der-neue-wilde-westen/
Abgerufen am: 26.04.2024