erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Lesen –
Neues für den Bücherwurm

Stefan Hügel

Sandro Gaycken – „Cyberwar"

Das Internet als Kriegsschauplatz

Angriffe auf informationstechnische Infrastrukturen gewinnen an Bedeutung. Die übergreifende Vernetzung durch das Internet macht IT-Infrastrukturen verletzlicher; gleichzeitig stützen sich immer mehr Dienste darauf ab – dadurch steigt unsere Abhängigkeit und damit der Schaden, wenn solche Infrastrukturen geschädigt oder zerstört werden.

Durch Medienberichte wurde uns in der Vergangenheit wiederholt vor Augen geführt, welche Angriffsmöglichkeiten sich selbst für Hacker mit geringem Mitteleinsatz bieten, in Systeme einzudringen. Umso größer sind die potenziellen Schäden, wenn große Organisationen mit entsprechenden Ressourcen – etwa im Rahmen von Militäroperationen – Rechnersysteme angreifen.

Sandro Gaycken, Technik- und Sicherheitsforscher an der FU Berlin, stellt in seiner Untersuchung dar, welche möglichen Bedrohungen sich durch Computerangriffe ergeben. Dabei sieht er vor allem die umfassende Vernetzung als Quelle von Risiken und erwartet, dass diese Vernetzung zum Schutz von Bedrohungen reduziert werden muss und werden wird – nur die „Entnetzung" wird uns aus seiner Sicht dauerhaft schützen.

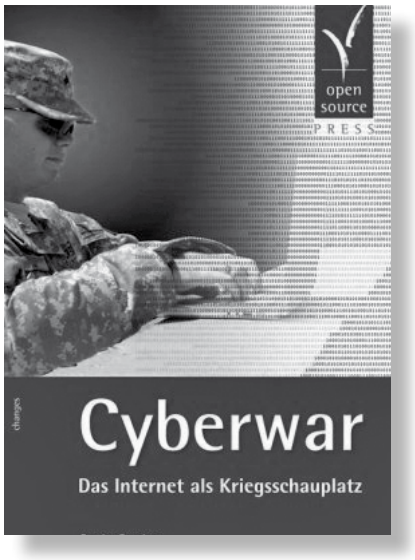
Im ersten Kapitel – Evolution – beschreibt der Autor die Entwicklung der elektronischen Kriegführung – als Cyberwarfare – aus deren strategischen und technischen Erfordernissen. Er stellt fest, dass alle Kriege nach den beiden Weltkriegen vom Prinzip her ebenfalls Weltkriege waren: Es waren immer mehrere Staaten an diesen Kriegen beteiligt; gleichzeitig werden Kriege hochtechnisiert und mit Massenvernichtungswaffen geführt – dem gegenüber stehen Guerilla-Taktiken mit Tarnung und hoher Mobilität bei technisch unterlegenen Gegnern. Für die Bekämpfung solcher mobilen Gegner und zur Steuerung und Kommunikation wird Informationstechnik – C4ISR: Command, Control, Computer, Communication, Intelligence, Surveillance, Reconnaissance – eingesetzt: Wir sind beim Cyberwar.

Das zweite Kapitel – Hacking – gibt einen Überblick über Hacker, die von ihnen genutzten Sicherheitslücken und ihre Techniken. Unterschieden wird zwischen *guten* White-Hat-Hackern, die ohne Schaden anrichten zu wollen, das Eindringen in fremde Rechner als intellektuelle und technische Herausforderung sehen und durch Hinweise auf Sicherheitslücken dazu beitragen, diese zu schließen und die Sicherheit letztendlich zu erhöhen. Sie folgen in der Regel einer eigenen Hacker-Ethik. Black-Hat-Hacker dagegen dringen in Rechnersysteme ein, um dort Schaden anzurichten – das System selbst zu manipulieren oder sich Vorteile zu verschaffen. Prinzipien des Hacking, Sicherheitslücken in Rechnersystemen und Reverse Engineering als Technik zum Entdecken von Zero-Day-Exploits werden beschrieben. In einem Anhang werden Strukturen und Prozesse des Hacking noch detaillierter behandelt, dabei geht der Autor auf Footprinting, Exploitation, Malware und Social Engineering ein.

Im dritten Kapitel – Strukturen – geht es um die Rahmenbedingungen für Operationen im Cyberspace insgesamt. Sie werden bestimmt durch die Komplexität informationstechnischer Sys-

teme und die daraus resultierende Verwundbarkeit, die Globalität von Rechnernetzen, die weltweite Interkonnektivität und die sich ergebenden Schwierigkeiten für die globale Regulierung. Vernetzung und Interoperabilität führt dazu, dass Angriffe mulitiplikativ geführt werden können – wie im Fall von Bot-Netzen können sie von einem Knoten aus über viele weitere Knoten geführt werden. Angriffe können aber auch unkontrolliert migrieren: Verwenden weitere Knoten dieselbe Technik wie das Angriffsziel können sie ungeplant ebenfalls Opfer des Angriffs werden.

IT-Sicherheit hat zum Ziel, gegen Angriffe auf Rechnersysteme zu schützen. Es zeigt sich aus Sicht des Autors jedoch, dass IT-Sicherheit in der Regel nur Schutz gegen Low- oder Mid-Level-Hacker bieten. Gegen High-Level-Hacker mit speziellen Fähigkeiten, Sicherheitslücken zu finden und Zero-Days zu entwickeln, helfen auch Verfahren der IT-Sicherheit nichts. Gerade bei militärischen Cyber-Angriffen wird man es aber zumeist mit Angreifern zu tun haben, die diese Fähigkeiten besitzen. An dieser Stelle hilft aus Sicht des Autors nur eins: Abkoppeln vom Netz.



Ein wichtiger Aspekt im Zusammenhang mit Cyberwar ist das Problem der Non-Attribution – dem Umstand, dass die Identität und der Ort eines Angreifers häufig nicht nachverfolgt und Identitätsinformationen zusätzlich verschleiert werden können. Im Bereich der Strafverfolgung wird versucht, dieses Problem durch Vorschriften wie der zur Vorratsdatenspeicherung zu lösen – ein Ansatz, der mit der rechtsstaatlichen Unschuldsvermutung und dem Recht auf Privatheit kollidiert. Fähige Angreifer werden stats Wege finden, ihre Attribution zu verschleiern. Auch die Motivation von Angreifern kann häufig nicht erkannt werden (motivationale Non-Attribution). Die Wirksamkeit von Gegenmaßnahmen ist aber häufig von der Motivation des Angreifers abhängig; damit können in solchen Fällen nicht ohne Weiteres geeignete Gegenmaßnahmen abgeleitet werden.

Im vierten Kapitel werden die Ziele von Angreifern behandelt. Dabei geht es zunächst um die Frage der Verwundbarkeit von Informationsgesellschaften, die Ziel eines Angriffs werden können. Angriffe können dabei Informationen gelten: Ziel ist dann, diese Informationen zu erhalten, um aufzuklären oder zu manipulieren, um den Gegner damit zu täuschen. Weiteres Angriffsziel sind Identitäten: die Überwachung von Identitäten zu Erkennung der tatsächlich dahinterstehenden Person oder die unbefugte Erlangung von Identitäten zur missbräuchlichen Verwendung und Verschleierung der eigenen Identität.

Großen Schaden bei einem Gegner kann ein Angreifer durch Attacken auf Infrastrukturen verursachen. Die Ausschaltung kritischer Infrastrukturen wie Strom, Wasser, Transport oder Gesundheitsversorgung kann für den Angegriffenen katastrophale Folgen haben und umgekehrt den Angreifer in eine strategisch günstige Position bringen. Damit ist der Schutz solcher Infrastrukturen von besonderer Bedeutung. Beispiel für einen Angriff auf Infrastrukturen ist Stuxnet, der zielgerichtet Kontrollsysteme kritischer Infrastrukturen angriff.

Im fünften Kapitel geht es um Strategien. Dabei spielen Erkennen und Täuschen, Angriff, Abschreckung und Verteidigung eine Rolle. Strategien bauen in der Regeln nicht auf die gegebene, sondern auf die mögliche Situation auf; es müssen also mögliche Zukunftsszenarien antizipiert werden.

Wichtigstes Element der Cyberwarfare ist die militärische Form des Hackens. Durch Einbruch und Manipulation gegnerischer Rechnerinfrastrukturen kann aufgrund deren universeller Nutzbarkeit eine große Bandbreite an Schäden angerichtet werden.

Erster Schritt ist der Zugriff auf den Rechner. In einfachen Fällen kann der Zugriff oberflächlich sein – bei DoS-Angriffen; meistens wird das Ziel eines Angreifers die Manipulation oder der Diebstahl von Daten sein, oder er schleust Software ein, die im Rechnersystem oder darüber hinaus Schäden verursacht. Neben der Art des Zugriffs müssen auch Zugriffswege auf die Systeme bedacht werden – zum Beispiel von außen über das Internet oder von innerhalb der angegriffenen Organisation, z. B. durch Einsatz im Kampfgebiet. Genutzt werden auch Backdoors, die den unbefugten Zugriff ermöglichen. Der Angegriffene muss sich dagegen durch geeignete Verteidigungsmaßnahmen schützen oder Maßnahmen zur Abschreckung ergreifen.

Das sechste Kapitel – Realitäten – stellt Beispiele für cyber-militärische Operationen dar – Estland, Georgien, die Operation Orchard, Conficker, Stuxnet – und nennt konkrete Planungen und Konzepte aus den USA und China. Zuletzt werden die Kapazitäten und Strukturen des US-Cybercommand beschrieben, soweit sie öffentlich bekannt sind.

Den Abschluss bildet ein Ausblick, der die Zukunft des Cyberwar behandelt. Er lässt keinen Zweifel, dass der Cyberwar kommen wird und heute Kapazitäten dafür aufgebaut werden. Rechtsfragen bilden den folgenden Abschnitt; dabei stellt die Non-Attribution ein großes Problem für die Regulierung dar. Regulieren kann man im Bereich des Schutzes, beispielsweise durch Vorgabe von Schutzanforderungen an die Betreiber kritischer Infrastrukturen. In diesem Zusammenhang spielen auch Haftungsfragen eine Rolle. Auch Freiheitsrechte sind zu berücksichtigen, zu denen Regulierungsmaßnahmen häufig im Konflikt stehen. Hier ist eine Abwägung notwendig.

Zentrale These des Bandes ist die Notwendigkeit zur Entnetzung insbesondere kritischer Systeme, die häufig als ein Rückschritt

gesehen wird. Doch bereits heute sind erste Ansätze zur Entnetzung – beispielsweise in den USA – zu erkennen.

Der Band gibt einen umfassenden Überblick über die verschiedenen Aspekte der Cyberwarfare. Dabei ist er stets sachlich und detailliert – er beschreibt die Sachverhalte ohne den vor allem in der Politik häufig anzutreffenden Alarmismus. Mit seiner These der Entnetzung greift er gleichzeitig in die öffentliche Debatte zur Sicherheit von Rechnernetzen ein – einer These, die sich augenscheinlich gegen die aktuelle Entwicklung stellt.

Sandro Gaycken (2011): Cyberwar. Das Internet als Kriegsschauplatz. München: Open Source Press

Britta Schinzel

Hans-Jörg Kreowski (Hg.) – Informatik und Gesellschaft

Verflechtungen und Perspektiven

Der Band fasst beispielhaft wichtige Themen aus dem Bereich von Informatik und Gesellschaft zusammen. Sie sind sowohl von InformatikerInnen als auch in interdisziplinärer Perspektive aus den Bereichen Jura, Technikgeschichte, Medienphilosophie und aus der Praxis geschrieben. Dabei sind einige Beiträge sehr allgemein gehalten, wie z. B. Dirk Siefkes' Plädoyer für die von Wolfgang Coy ins Leben gerufene Theorie der Informatik mittels seines Textes über informatische Muster, oder Marie-Theres Tinnefelds Beitrag zum Schutz der Menschenwürde als archimedischem Punkt einer Zivilgesellschaft. Andere wiederum sind sehr spezifisch herausgegriffen, wie Eric Töpfers Untersuchung zur Videoüberwachung, bei der zwar nationale Unterschiede interessant erscheinen, aber der Trend zur angelsächsischen Mammutüberwachung zu beobachten ist, oder Volker Grasmucks Beitrag zu DRM (digital rights management). Es gibt Technik-Historisches, wie Hans Dieter Helliges Untersuchung zur Entwicklung des Internet als Lernprozess, theoretisch Philosophisches wie Bernd Robbens Überlegungen zum Computer als Medium, und auch wieder sehr konkret Praktisches wie Dagmar Boedickers leider nur zu realistische Fallbeispiele zu gröbsten Verstößen gegen den Datenschutz, Rikke Frank Joergensens Darstellung der UNO-Deklarationen zu Human Rights im Zusammenhang mit der Informationsgesellschaft und Hans-Jörg Kreowskis Plädoyer für das FIfF.

Im Folgenden greife ich einige Texte aus dem Band heraus. Nach einer Einleitung durch den Herausgeber legt Arno Rolf zum Thema Informatik und Gesellschaft eine Anforderung an ein breiteres Orientierungswissen (Mittelstraß 2001) in Ergänzung zum inzwischen kanonisierten informatischen Verfügungs- und Expertenwissen vor, das es erlaubt, die Wechselwirkungen zwischen Informatik und Gesellschaft in den Blick zu nehmen und zu systematisieren. Rolf nutzt ein 3-stufiges Schalenmodell, ausgehend vom „soziotechnischen Kern", der in sozialen Kontexten entstandenen Formalisierung, Algorithmisierung und Maschinisierung der Kopfarbeit qua Dekontextualisierung (Coy 1992, Nake, 1992) und ihrer Rekontextualisierung in alten und neuen Zusammenhängen, über die „Mikrokontexte", in denen die mit IT beschäftigten und von ihr betroffenen Akteure sich in Arenen bewegen und handeln, und so reflexiv und rekursiv auf die von IT modulierten Strukturen einwirken, bis schließlich zu den „Makrokontexten", den Organisationen, Wissenschafts- und Innovationsmilieus mit ihren Werten, Traditionen in globalen Zusammenhängen. Aus diesem Modell entwickelt er einen systemtheoretischen Orientierungsrahmen zum Verständnis der globalen Netzwerke mit dem Ziel, InformatikerInnen Orientierung und Gestaltungskompetenz zu ermöglichen.

In ihrem zweiten Beitrag in diesem Band entwickelt Marie-Theres Tinnefeld aus historischen Rechtskulturen den Datenschutz als rechtskulturelle Leistung, sieht ihn jedoch massiv bedroht, nicht nur durch die offene Gesellschaft und aktive Gesetzesüberschreitungen, sondern auch durch die neuen technischen Möglichkeiten sowohl quantitativer als auch qualitativer Natur. Die Informations- und Bilderflut, verbunden mit den Möglichkeiten der Speicherung, Datenintegration, dem Data Mining und Warehousing sowie den Überwachungsmöglichkeiten mittels RFID und Biometrie im Verein mit Videoüberwachung und neuen Möglichkeiten der Integration und Auswertung aller Arten von Daten, erzeugt eine neue informationelle Gewalt, die der gebotenen öffentlichen Informationsaskese zuwider läuft und Rechtsgüter bedroht. Tinnefeld plädiert daher für eine dialogische Kultur zwischen Bürgern, Staat und Unternehmen, um grundlegende Datenschutzrechte trotz der Wünsche nach mehr Kontrolle im Interesse der Inneren Sicherheit aufrecht zu erhalten (Anmerkung der Rezensentin: Einer Sicherheit, die wie bekannt durch den Überwachungsstaat nicht erfüllt wird, sondern vielmehr der Kontrolle aller Bürger dient).

Volker Grassmuck höchst spannender Beitrag zur Erfindung des DRM (digital rights management) beschreibt ausführlich, wie mittels DRM eine Lösung gefunden wurde, um aus den eigentlich kostenlosen elektronischen Kopien im Internet enorme und unterschiedlich gestufte Gewinne zu ziehen. Doch das ist nicht das einzige Paradox, mit dem die Rechteinhaber kämpfen müssen, das nächste ist die Tatsache, dass etwas, was beliebig verfügbar ist, verknappt werden muss, also Zugang ermöglicht werden muss, anstatt ihn – wie für die Preissteigerung nötig – zu verhindern. Grassmuck zeichnet die Überlegungen und Entscheidungen der Verwertungsgesellschaften und ihrer Akteure akribisch nach, zitiert, welche geschäftspolitischen

Überlegungen und negativen Annahmen über InternetnutzerInnen, nämlich die, dass sie sämtlich unehrlich seien, die Akteure der Verwertungsgesellschaften zur Erfindung der so genannten „trusted systems“ geführt haben. Er zeigt auf, welche negativen Wirkungen die bisher entwickelten Systeme auf Systemsicherheit, Privatheit, Wahlfreiheit und Expropriation haben. Schließlich erwähnt er auch die politischen Probleme beim Versuch einer Durchsetzung globaler Lizenzen und die unterschiedlichen Widerstände, die dagegen in Europa, vor allem aus Frankreich aufgebracht werden. Dazu ist das letzte Wort nicht gesprochen, denn ebenfalls mächtige Gegner sind die Open-Access Bewegungen.

Hans-Dieter Helliges Analyse der Entwicklung des Internet beschreibt dieselbe als Agglomeration viefältigster Erfindungen und Entwicklungen, die weder von Anfang an beabsichtigt noch vorhergesehen wurden. Die (geringen) TCP/IP-Protokollfestlegungen standen in harter Konkurrenz zu den starreren europäischen OSI-Protokollen und haben sich gerade wegen ihrer Unvollständigkeit und Erweiterbarkeit letztlich durchgesetzt. Helliges sehr genaue und differenzierte Darstellung der Entwicklungswege des Internet zeigen deren Kontingenzen und soziotechnischen Bedingtheiten zwischen militärischen Anfängen, Firmeninteressen, studentischen Bedürfnissen und Einzelentwicklern. Die durch die auf Akteure zentrierte Technikgeschichtsschreibung nachträglich in die Welt gesetzten Heldenmythen deuten die Geschichte aus Sicht der „Sieger“, unterschätzen die strukturellen Bedingungen, und blenden Theorie- und Methodenprobleme bei der Verknüpfung der Einzelereignisse und Entwicklungsmomente aus. Stattdessen zeigt Hellige, dass die Leitbildfixierung der „heroischen“ Entwickler durch immer neue Gruppen von Nutzern gemäß ihrer Nutzungsbedürfnisse überwunden wurde.

Schließlich plädiert Eckhard Kanzow in seinem unkonventionellen Text „Zu lebenden und nicht lebenden Systemen – braucht die Infomedizin die Informatik?“ für eine neue, auf eine ganzheitliche Alternativmedizin gerichtete Teildisziplin der Informatik, die Infomedizin. Er entwickelt zunächst die aus den Gender Studies bekannten Deutungen zur Entwicklung der Natur- und Technikwissenschaften, zieht dann die aus Konstruktivismus und Systemtheorie geholten Theorien der Selbstorganisation und Autopoiesis zur Überwindung der Trennung von Geist und Körper heran, um schließlich zu seinem eigentlichen Thema überzuleiten, Leben basierend auf Information. Dabei meint er mit Informationsflüssen nicht nur die durch Transmitter, Botenstoffe und elektrische Signale auf Nervenbahnen transportierte Information, sondern auch solche, die über mit Lichtgeschwindigkeit oszillierende Felder gesendet werden, wie sie in der Physik schon seit langem bekannt sind. In Biologie und Medizin sind solche Theorien noch nicht allgemein anerkannt, sondern werden in der Alternativmedizin, etwa mit der Elektroakupunktur und den Bioresonanzmethoden vorwiegend diagnostisch, aber auch therapeutisch (Homöopathie) angewendet. Sie knüpfen auch an alte asiatische Medizinrichtungen, wie die TCM, an, indem etwa die Messungen der Schwingungen an Meridianen vorgenommen werden können. Viele dieser in den westlichen Alternativansätzen entwickelten Erprobungen bedienen sich softwaregesteuerter Mess- und Behandlungsmethoden. Sie sind weder kanonisiert noch wissenschaftlich ausreichend erhärtet, was zum Teil auch an den Standardisierungsanforderungen der Schulmedizin und Pharmazie für Medikamente und Therapien liegt, welche sich individualisierten Medizinen wie der Homöopathie verschließen, da sie gleiche Ergebnisse über eine größere Population erfordern. Alternative Begründungen, Methoden, Therapien und Standardisierungen erhofft sich Herr Kanzow nun von der Infomedizin.

Gegen Ende des Bandes sind die Stellungnahmen einer Anhörung zu Visionen für die Anforderungen an die Informatik im Jahr 2020 abgedruckt. Wie zutreffend sie sind, wird in gar nicht so ferner Zukunft festzustellen sein. Am Ende steht ein aus den 1970er Jahren stammender Text von Hans-Jörg Kreowski, der Zitate aus Konrad Zuses Buch „Der Computer – mein Lebenswerk“ in ein fiktives Interview montiert. Er zeigt so etwas holzschnittartig, wie Zuses vermeintlich apolitische Haltung beim Versuch, während des Dritten Reiches die Entwicklung der Zuse Z2 zu finanzieren und sie für die Fernsteuerungsberechnungen der V2 zum Einsatz zu bringen, dem NS-Regime zuarbeitete. Der Text schließt sehr gut ergänzt mit selbstkritischen Zitaten von Galileo Galilei aus Berthold Brechts „Leben des Galilei“.

Da das Buch vom Jahre 2008 stammt, d. h. 2006 bis 2007 geschrieben wurde, und sich in der Zwischenzeit Webanwendungen, Data Mining, die Integration der Medien, Cloud Computing, die sozialen Medien und der Internetkommerz sehr dynamisch weiter entwickelt haben und mit alledem Probleme der Sicherheit und des Schutzes von Persönlichkeitsrechten enorm zugenommen haben, wäre heute schon ein neues Buch zu schreiben, was dem FIfF empfohlen werden soll. Doch zeigt der Band exemplarisch, wie wichtig für die und innerhalb der Informatik ein ergänzender kritischer Blick auf ihre Theorien und Ziele, ihre Entwicklungen und Problemlösungen ist, um Sinnloses zu vermeiden und Schäden von der Gesellschaft abzuwenden.

Hans-Jörg Kreowski (Hrsg.): Informatik und Gesellschaft – Verflechtungen und Perspektiven, Reihe Kritische Informatik, LIT-Verlag, Band 4 des FIfF (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung), 2008