Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher und Jan W. Meine
Meine Verlag – Wissenschafts-, Sach- und Fachbuchverlag, Magdeburg

Dieser Artikel erscheint in der Serie »Informationstechnik und Sicherheitspolitik. Wird der dritte Weltkrieg im Internet ausgetragen?« Herausgegeben von Jörg Sambleben und Stefan Schumacher

Vom Cyber-Kriege
Gibt es einen Krieg im Internet?

Stefan »Kaishakunin« Schumacher

Dieser Beitrag untersucht die Frage, ob ein Krieg im Cyberspace möglich ist. Dazu stütze ich mich auf die Kriegs-Definition die Clausewitz aufgestellt hat und wende diese auf die aktuelle Cyberwar-Diskussion an. Ich stelle die aktuellen technischen Möglichkeiten für Cyberattacken in einem kurzen Überblick vor und zeige, wie sich durch die ausbreitende Technik Angriffsvektoren für Cyberattacken öffnen. Außerdem zeige ich, welchen Einfluss die gegenwärtige Entwicklung auf militärische Strategien hat.

Zitationsvorschlag: Schumacher, S. » (2012). Vom Cyber-Kriege: Gibt es einen Krieg im Internet? *Magdeburger Journal zur Sicherheitsforschung*, 2, 285–307. Zugriff am 20. November 2012, unter http://www.sicherheitsforschung-magdeburg.de/journal_sicherheitsforschung.html

Einführung – Warum diese Diskussion?

Inzwischen wird selbst in der Tagespresse IT-Sicherheit thematisiert – dabei fällt der vor allem in den letzten Jahren gebräuchliche Begriff *Cyberwar* oder *Cyberkrieg* immer häufiger. Auffällig ist dabei die Schnelligkeit, mit der der Themenkomplex die Fachpresse verlassen und Einzug in die allgemeinen Medien gehalten hat. Vor 15 Jahren waren Sicherheitsprobleme in der Informationstechnologie meist nur eine Randnotiz wert oder wurden als Kuriosum vermeldet. Der Staatstrojaner schaffte es inzwischen schon auf die Titelseite der Frankfurter Allgemeinen Sonntagszeitung[1], auch »Chinesen« im Bundestag[2] sowie die Angriffe gegen Estland[3] und Georgien[4] in militärischen Konflikten sind ein Thema.

In der Hacker- und IT-Szene sowie im Militär ist die IT-Sicherheit naturgemäß schon wesentlich länger ein Thema. Neben Workshops und Vorträgen auf Konferenzen[5] wird das Gebiet auch in wissenschaftlichen Publikation diskutiert, so dass sich vereinzelt bereits die Politikwissenschaft damit befasst.

An der gesamten Diskussion fällt allerdings die äußerst durchwachsene Qualität der Beiträge auf. Artikel in der Presse und selbst solche im politikwissenschaftlichen Diskurs sind häufig von mangelndem Technikverständnis geprägt und leben des öfteren davon fehlerhafte Artikel zu zitieren und damit die einmal gemachten Fehler weiter zu vererben. Man kann gerne über Technik philosophieren, sollte dann aber auch die Technik verstanden haben.

Jegliche Diskussion um IT-Sicherheit und den Cyber-Krieg als ein Spezialfall davon ist zuallererst eine technische Debatte – denn es handelt sich zuerst um technische Probleme die diskutiert werden müssen. Das heißt ein technisches Problem muss zuerst mit einer technischen Analyse bearbeitet werden um die gesellschaftlichen Auswirkungen der Technik zu untersuchen. Es ist also eine Technikfolgeabschätzung durchzuführen.

Daher möchte ich im Rahmen dieses Artikels die Frage diskutieren, was ein Cyber-Krieg ist bzw. ob es einen Cyber-Krieg überhaupt geben kann. Dazu ist zu klären was ein Krieg ist und ob dieser Krieg im Cyberspace geführt werden kann.

Begriffsklärung: Cyber und Krieg

Der Begriff *Cyberwar* bzw. Cyber-Krieg setzt sich aus den beiden Komponenten *Cyber* und *Krieg* zusammen. Die Komponente Cyber leitet sich aus dem anglisierten griechischen Begriff Kybernetes für Steuermann ab. Es steht in der Zusammensetzung für Cyberspace, einem in den 1980ern geprägten Begriff des Schriftstellers William Gibson, der damit eine utopische Form des Internets beschrieb. Der Cyberspace unterteilt sich in eine technische und eine soziale Dimension. Die technische Dimension umfasst dabei Hardware und

1 http://www.faz.net/dynamic/download/fas/FAS_09_10_2011_S41_S47_Staatstrojaner.pdf, Zugriff am 13.12.2011

2 http://www.spiegel.de/politik/ausland/computer-spionage-fdp-will-chinesische-hacker-angriffe-in-den-bundestag-bringen-a-502253.html, Zugriff am 27.08.2007

3 http://www.sueddeutsche.de/digital/kriegsfuehrung-im-cyberspace-unsichtbare-angriffe-mit-realen-folgen-1.1003586, Zugriff am 27.09.2011

4 http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0, Zugriff am 19.08.2008

5 z.B. meine Vorträge »Electronic Warfare« 2008 in Brüssel sowie »Cyberwar on the Horizon«, »On Cyber-Peace«, »Bringing the Cyber-Peace« von der DeepSec 2010 und 2011 sowie DeepIntel 2012

Software, Protokolle und Dienste, welche hier im Buch diskutiert werden. In den Romanen und inzwischen auch in den Lebenswirklichkeiten vieler Menschen ist der Cyberspace aber auch eine soziale Dimension, die durch Kommunikationsplattformen wie Usenet, Mailinglisten, IRC oder Facebook und Second Life bereitgestellt wird. Phänomene dieser Dimensionen sind zum Beispiel Cybermobbing, Ankündigung von Amokläufen (Leaking) oder psychologische Operationen und Propaganda (vgl. S. Schumacher 2009a,b,c, 2010b, 2011a). In diesem Aufsatz werde ich mich dem Thema entsprechend auf die technische Dimension beschränken.

Der zweite Teil des Begriffs, Krieg, kann unterschiedlich definiert werden.

Die bekannteste Definition von Krieg nahm von Clausewitz (1832) vor: »Der Krieg ist also ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen.« Dazu gelte es, begrenzte Ziele zu erreichen oder einen Gegner derart zu entwaffnen, dass er politisch hilflos und militärisch wehrlos sei.

Clausewitz schreibt weiterhin, dass Krieg die Fortsetzung der Politik mit anderen Mitteln sei, dass die Politik also den Primat über den Krieg habe. Dies erfordere eine Strategie *über* dem Kriege - also Ziele, die der Krieg zu erreichen habe. Dabei handele es sich nicht um militärische Ziele (Lufthoheit, Zerstörung von Einrichtungen etc.) sondern um politische. Diese Ziele müssen daher vor Beginn eines Krieges durch die Politik bestimmt werden und diesem übergeordnet werden.

Wikipedia (2012)[6] schreibt hingegen:

> Krieg ist ein *organisierter* und unter Einsatz erheblicher Mittel mit *Waffen* und *Gewalt* ausgetragener Konflikt, an dem mehrere planmäßig vorgehende Kollektive beteiligt sind. Ziel der beteiligten Kollektive ist es, den Konflikt durch gewaltsame Kämpfe und Erreichen einer *Überlegenheit* zu lösen. Die dazu stattfindenden Gewalthandlungen greifen gezielt die körperliche Unversehrtheit gegnerischer Individuen an und führen so zu *Tod* und *Verletzung*. Krieg schadet so auch der Infrastruktur und den Lebensgrundlagen der Kollektive.

Für die folgende Analyse des Phänomens *Cyber-Krieg* werde ich die Definition von Clausewitz nutzen und dabei besonderen Augenmerk darauf legen, ob der Gegner zur Erfüllung unseres Willens per Internet gezwungen werden kann.

Exkurs: Politik und Recht

Neben der technischen Betrachtung ist auch eine kurze Exkursion in die Bereiche Politik und Recht notwendig, denn nach Clausewitz hat nicht nur die Politik den Primat über den Krieg, sondern der Kriegszustand wird über das Recht definiert. Derzeit gibt es noch keinen internationalen Vertrag, der in irgendeiner Art und Weise explizit »Cyber-Aggressivität« regelt. Möchte man daher diskutieren ob es einen Cyber-Krieg gibt, muss man hierzu das Humanitäre Völkerrecht, umgangssprachlich Kriegsvölkerrecht genannt, heranziehen. Das dort enthaltene jus ad bellum regelt das Recht, in einen Kriegszustand einzutreten bzw. bewaffnete Konflikte zu lösen sowie das jus in bello, welches das Recht im Kriege regelt. Da es keine expliziten Regelungen zur Cyber-Aggressivität gibt, müssen die Juristen im Humanitären Völkerrecht auf Analogien zurückgreifen, beispielsweise auf Konzep-

6 Hervorhebungen durch mich.

te wie Schutzzeichen (Rotes Kreuz), Waffenstillstandsabkommen oder den Status von Non-Kombatanten.

Gegenwärtig werden Cyberattacken im Völkerrecht nicht als kriegerischer Akt betrachtet. Damit kann durch eine Cyberattacke rein rechtlich gesehen kein Kriegszustand ausgelöst werden. Allerdings versucht das US-amerikanische Verteidigungsministerium Cyberaggressionan als »Act of War« zu sehen und gegebenenfalls mit konventionellen Waffen zurückzuschlagen[7] (vgl. *Department of Defense Strategy for Operating in Cyberspace* 2011). Auch die deutsche Regierung plant »Bomben gegen Cyber-Krieger«. Spiegel Online[8] schreibt dazu:

> Die Bundesregierung behält sich grundsätzlich das Recht vor, auf schwere Cyber-Attacken mit Waffengewalt zu reagieren. ›Je nach Eigenart kann ein Cyber-Angriff im Einzelfall als bewaffneter Angriff auf einen Staat zu werten sein‹ zitiert die Nachrichtenagentur Reuters aus einem vertraulichen Bericht der Bundesregierung, der zwischen Innenministerium, Auswärtigem Amt, Bundeskanzleramt und Verteidigungsministerium abgestimmt ist.
>
> Staaten seien bei bestimmten Cyber-Angriffen berechtigt, ›ihr naturgegebenes Recht auf individuelle oder kollektive Selbstverteidigung auszuüben‹, heißt es in dem Bericht laut Reuters. Dies gelte insbesondere dann, wenn die Souveränität des angegriffenen Staates bedroht sei oder die Wirkung der Cyber-Attacke sich mit der Wirkung herkömmlicher Waffen vergleichen lasse. Das Verteidigungsministerium bestätigte auf Anfrage, dass ein entsprechender Bericht existiert. Er sei am 21. September den Mitgliedern des zuständigen Ausschusses beim Bundestag zugegangen. Zum Inhalt äußerte sich das Ministerium unter Verweis auf die Geheimhaltungsstufe ›VS - nur für den Dienstgebrauch‹ nicht.

Allerdings sind diese Aussagen mit Vorsicht zu genießen, es handelt sich dabei wohl vorerst nur um eine Art *Show of Force* um potenzielle *staatliche* Angreifer abzuschrecken. Außerdem gibt es noch weitere, vor allem technische, Probleme, wie ich noch darlegen werde.

Ein wichtiges Kennzeichen kriegerischer Akte ist die staatliche Urheberschaft – ein Krieg kann nur zwischen Staaten (Kriegs*völker*recht) geführt werden. Soll daher eine Cyber-Attacke als Casus Belli angeführt werden muss deren Urheberschaft zweifelsfrei auf eine staatliche Organisation (Militär, Geheimdienst etc.) und einen staatlichen Auftrag zurückgeführt werden. Eine unabhängig handelnde Privatperson kann auch durch eine erfolgreiche Cyber-Attacke keinen Krieg rechtfertigen.

Ich werde noch zeigen dass es nahezu unmöglich sein kann, die Urheberschaft einer Attacke zweifelsfrei festzustellen. Damit ist es auch äußerst problematisch, eine Cyber-Attacke als Kriegsgrund heranzuziehen.

Ein weiterer Punkt der ebenfalls diskutiert wird ist die Herstellung und die Verbreitung von sog. Cyberwaffen, analog zur Nonproliferation von Atom-

7 http://online.wsj.com/article/SB10001424052702304563104576355\623135782718.html, Zugriff am 20.07.2011

8 http://www.spiegel.de/netzwelt/netzpolitik/cyberkrieg-bomben-gegen-cyberkrieger-a-861002.html v. 12.10.2012

waffen. Auch hierzu sind internationale Verträge notwendig, dazu können der Atomwaffensperrvertrag oder der Antarktisvertrag als Vorbild dienen.

Aber auch in der Diskussion um Cyberwaffen gilt: es ist zuerst ein technisches Problem. Cyberwaffen sind nichts anderes als Computerprogramme, Computerprogramme sind nichts anderes als Quellcode[9] und damit schlichtweg »Wissen« bzw. Fähigkeiten, Fertigkeiten und Kenntnisse des Entwicklers. Sie können beispielsweise als gezeichneter Programmablaufplan, mathematische Formel (insbesondere im Bereich Kryptographie) oder einfach als Datei weitergegeben werden. Es ist aber ein praktisches Ding der Unmöglichkeit, die Weitergabe von Programmen zu reglementieren oder gar technisch zu unterbinden. Eine Datei kann über verschiedenste elektronische Wege transportiert werden und dabei durch Verschlüsselung unleserlich und durch Steganographie unsichtbar gemacht werden[10]. Also selbst wenn man alle Internet-Knoten überwacht, wäre es nicht möglich eine bestimmte Datei aufzuspüren und deren Transport gezielt zu unterbinden. Außerdem besteht auch die Möglichkeit Programme auf Datenträgern wie einer 11x15x0,7mm großen Micro-SD-Karte oder ausgedruckt auf Papier oder versteckt in einem Buch zu schmuggeln. Damit erweist sich die Forderung nach einem Sperrvertrag als rein theoretisches Konstrukt.

Darüberhinaus kommt hier auch wie schon bei der Verschärfung des §202c StGB (Hackerparagraph) die Frage auf, was denn eine Cyberwaffe überhaupt ist. Zählen alle Programme dazu, die in irgendeiner Art und Weise zum Angriff auf IT-Systeme verwendet werden können? Also auch `telnet(1)` und `dd(1)`, Metasploit[11] oder alle PAM-Module die schwache Passwörter testen können? Jedes dieser Programme wird von Systemadministratoren und Sicherheitsexperten eingesetzt, um die Sicherheit von IT-Systemen zu testen bzw. zu erhöhen.

Derzeit ist die Entwicklung von Cyber-Kriminalität wesentlich weiter vorangeschritten und gefährlicher als die Entwicklung in der elektronischen Kriegsführung. Auch hier sind internationale juristische Definitionen und Verträge sowie entsprechende Agenturen die handeln notwendig. Die Bekämpfung von Cyber-Kriminalität ist nur durch die internationale Kooperation von Staaten möglich. Solange Täter und Opfer in verschiedenen Staaten sitzen und diese nicht bei der Bekämpfung von Cyber-Kriminalität kooperieren ist ein erfolgreiches Vorgehen dagegen von vornherein zum Scheitern verurteilt.

Ein interessantes Phänomen an der Schnittstelle zwischen Cyber-Crime und Cyber-War ist die Kooperation von Cyber-Kriminellen und staatlichen Organen. Cyber-Kriminelle verfügen in der Regel über eine hohe Kompetenz im Umgang mit IT-Sicherheit und sind Erfahren im Ausnutzen von Sicherheitslücken und im Angriff auf IT-Systeme. Hinzu kommt gerade in Staaten der ehemaligen Sowjetunion eine personelle Überschneidung zwischen Kriminellen und ehemaligen Milizionären und KGB-Offizieren. Einige der Banden werden durch ehemalige Geheimdienstler geführt, die naturgemäß über entsprechende Kontakte in den Untergrund sowie zu den staatlichen Organen verfügen. Es ist daher unter Umständen möglich, dass derartige Gruppen durch

9 Beispiele und nähere Erläuterungen zum Thema Quellcode finden Sie in meinem Kapitel zur Schadsoftware.

10 Siehe die Kapitel zu Verdeckten Kanälen von Steffen Wendzel und Jörg Keller sowie Anonymität von Jens Kubieziel.

11 Siehe das Kapitel zu Metasploit von Michael Kohl.

einfache Bezahlung oder aus patriotischen Gründen zu einer Art »Söldner« in Cyber-Konflikten werden können.

Kann ein Krieg im Internet ausgetragen werden?

Um die Frage zu beantworten, ob ein Krieg in Internet ausgetragen werden kann, werde ich die Clausewitzsche Kriegsdefinition nutzen und untersuchen, ob man die dort definierte Form von Konflikt unter den technischen Bedingungen des Internets möglich ist.

Ziel eines Krieges ist es nach Clausewitz, einen Gegner derart zu entwaffnen, dass er politisch hilflos und militärisch wehrlos ist. Um diese Entwaffnung im Internet durchzuführen, muss eine Gefährdungsanalyse der potenziellen Opfersysteme durchgeführt werden. Derartige Gefährdungsanalysen kann man zum einen als Organisation selbst durchführen, beispielsweise in dem man die ISO 27001[12] anwendet. Vereinfacht stellt man dazu eine Übersicht möglicher Angriffsziele auf und berechnet mögliche Schadensfälle und deren Eintrittswahrscheinlichkeit. Anschließend gewichtet man die Abhängigkeit bzw. Wichtigkeit des Angriffsziel und priorisiert entsprechende Schutzmaßnahmen. Die zentrale Frage ist daher: »Wie hoch ist die Wahrscheinlichkeit, dass ein Asset ausfällt und was passiert wenn es ausfällt?«.

Eine weitere beliebte Möglichkeit ist ein sogenannter Penetration Test (kurz Pen-Test). Diese Tests werden in der Regel von externen Sicherheitsberatern durchgeführt. Die Sicherheitsberater nutzen dabei in der Regel alle Werkzeuge und Methoden die echten Angreifern auch zur Verfügung stehen und versuchen damit, die Systeme einer Organisation anzugreifen und zu übernehmen. Gelingt es ihnen in ein System einzudringen, wird der Angriffsweg dokumentiert und die Dokumentation dem Auftraggeber zur Verfügung gestellt. Dieser kann mit den Informationen Sicherheitslücken identifizieren und Gegenmaßnahmen einleiten.

Dieses Vorgehen ist die einzige praktizierbare Möglichkeit um die Sicherheit eines Systems zu überprüfen. Zwar besteht in der Theorie noch die Variante die Sicherheit oder Fehlerfreiheit eines technischen Systems mathematisch zu berechnen, also zu verifizieren, dies ist aber praktisch unmöglich. Zum einen bestehen Systeme nicht nur aus technischen Anlagen, die theoretisch noch berechenbar wären, sondern auch aus Menschen bzw. Interaktionen von und mit Menschen. Diese sind dann aber nicht mehr sicher berechenbar (vgl. S. Schumacher 2011b, 2012). Außerdem ist die Komplexität eines technischen Systems nicht mehr berechenbar, da der Rechenaufwand zu hoch ist. Man kann theoretische jeden Quellcode, den ein Programmierer schreibt um ein Programm zu entwickeln in ein mathematisches Gleichungssystem umwandeln und dieses lösen, um seine Fehlerfreiheit zu zeigen. Ein derartiges Gleichungssystem ist in der Praxis aber aufgrund der schieren Größe der Gleichungen und der Anzahl der unbekannten Variablen nicht mehr in vertretbarem Zeitaufwand lösbar. Allein das Gleichungssystem um die Fehlerfreiheit eines Betriebssystems zu berechnen ist größer als das Gleichungssystem, das der Wetterdienst lösen muss um das Wetter für die nächsten Monate zu berechnen.

Daher ist es in der Regel nur praktikabel ein technisches System durch Belastungsstests im Labor zu validieren, wie dies beispielsweise die Automobilhersteller mit Crashtests tun, oder ein System im Feld beispielsweise durch einen Pen-Test anzugreifen und so Schwach-

12 Siehe hierzu das Kapitel »Eine DIN für IT-Sicherheit?« von Dr. Hubert Feyrer

stellen aufzuspüren.

Um einen Pen-Test durchzuführen einigt man sich mit dem Auftraggeber auf ein Ziel. Im Rahmen dieses Artikels ist es die Frage ob man beispielsweise gegen Deutschland einen Krieg im Internet führen kann. Dann versucht man alle notwendigen Assets zu identifizieren, die dazu genutzt werden können ein solches Ziel zu erreichen. Diese Assets untersucht man dann auf sogenannte Angriffsvektoren. Ein Angriffsvektor ist ein »Einfallstor« für einen Angreifer um Rechte auf einem System zu erlangen. In den mittelalterlichen Städten waren beispielsweise Schwachstellen in der Stadtmauer, die Stadttore oder die Wasserversorgung Angriffsvektoren. In modernen IT-Systemen sind es in der Regel Authentifikationsmechanismen[13] (Passwörter, PINs, ID-Karten und ähnliches) oder Sicherheitslücken in Anwendungsprogrammen. Diese Sicherheitslücken, sogenannte Vulnerabilities, also Verwundbarkeiten, können ausgenutzt werden um beispielsweise Administratorenrechte in einem System zu erlangen. Programme die eine solche Vulnerability ausnutzen nennt man »Exploit«, was von ausnutzen, ausbeuten abgeleitet ist.

Die Schwierigkeit des Pen-Tests besteht in der Praxis vor allem darin, die geeigneten Assets zu identifizieren und diese auf Sicherheitslücken hin zu untersuchen.

In diesem Artikel kann man sich mit der gegebenen Fragestellung einige mögliche Angriffsvektoren überlegen, welche man dann später weiter auf ihre Sicherheit hin untersucht:

- Stromversorgung
- Versorgung mit Erdöl, Erdgas, Heizöl, Treibstoffen, Kraftstoffen, Schmierstoffen etc.
- nationale Kommunikationsnetze (Telefon-Netze, GSM, Funknetze, BOS-Funk)
- Vernetzung der Banken, Geldautomaten, EC-Kartensysteme, Kreditkarten etc.
- Smart-Meter in Haushalten
- Steuerungssysteme in intelligenten Häusern (Smart Homes)
- vernetzte Computersysteme (das ominöse »Internet«)
- Industriesteuerungsanlagen (SCADA)
- Satelliten
- Geo-Positionssysteme (GPS, Glonass, Galileo)

Nachdem man eine solche Liste erstellt hat, kann man die identifizierten Assets gewichten und priorisieren. Beispielsweise ist eine Ausfall der öffentlichen Handy-Netze verkraftbar, wenn eine Ausweichmöglichkeit für Sicherheitsbehörden existiert, wie Satelliten-Telefone oder Richtfunkstrecken. Ebenso kann man die Verfügbarkeit bzw. Zuteilung von Heizöl und Diesel unterschiedlich gewichten.

Nach der Priorisierung untersucht man die Assets systematisch auf Schwachstellen, welche dann wiederum selbst gewichtet und priorisiert werden und idealerweise geschlossen werden. Leider werden in der Praxis nicht alle bekannten Sicherheitslücken in akzeptabler Zeit geschlossen, einige aus verschiedenen Gründen auch nie. Ein Problem bei dieser Analyse ist, dass Unternehmen und andere Organisationen kaum oder gar keine Daten zu Sicherheitsvorfällen oder Analysen veröffentlichen. Daher ist es kaum bis gar nicht möglich den gegenwärtigen Sicherheitszustand einzelner Systeme einzuschätzen und verlässlich zu bestimmen. Hier sind gegebenenfalls rechtliche Maßnahmen sowie empirische Untersuchungen notwendig.

13 Siehe das Kapitel zur Authentifikation von Frank Hofmann.

Mögliche Angriffsvektoren

Die Definition des Krieges von Clausewitz geht davon aus, dass ein Beteiligter den Krieg nutzt, um den Gegner zur Erfüllung des eigenen Willens zu zwingen. Dazu müsse der Gegner derart entwaffnet werden, dass er politisch hilflos und militärisch wehrlos sei. Um diese Frage in der Praxis zu klären, ist eine oben beschriebene Gefährdungsanalyse notwendig. Gefährdungen von IT-Systemen gehen von sogenannten Angriffsvektoren, einer Art »Einfallstor« aus. Daher werde ich hier in einem Gedankenexperiment man diese Analyse für einige relevante Angriffsvektoren beispielhaft durchexerzieren.

Besonders interessant sind hierbei die sogenannten Smartmeter: also intelligente Stromzähler. Diese intelligenten Stromzähler sind keine einfachen Geräte mehr die nur den Strom messen, sondern netzwerkfähige Computer, die auch den Stromverbrauch messen können. Smartmeter können beispielsweise dazu eingesetzt werden, um den Stromverbrauch eines Haushalts zu protokollieren und auszuwerten. Diese Möglichkeit kann sinnvoll im Rahmen der Energiewende eingesetzt werden, da das Smartmeter hier über die Protokollierung des Verbrauchs Feedback für die Benutzer geben kann, beispielsweise um den Stromverbrauch und damit die Kosten zu senken.

Die gewünschten Smartmeter verfügen darüberhinaus auch über Netzwerkfunktionen, so können die Verbrauche an die Energieversorger oder Stadtwerke quasi in Echtzeit gemeldet werden. Es ist daher nicht mehr notwendig einen Mitarbeiter zum Ablesen des Stromverbrauchs in die Haushalte zu schicken. Außerdem wünschen viele Stromversorger eine Abschalt-Funktionalität, das heisst sie möchten von der zentralen Leitwarte aus bestimmte Smartmeter abschalten und damit die angeschlossenen Haushalte vom Stromnetz abkoppeln.

Genau diese Funktionalität kann zu schweren Sicherheitsproblemen führen. Wird ein Smartmeter ausgerollt, das Sicherheitslücken hat, kann diese von einem Angreifer ausgenutzt werden. Gelingt es über die Sicherheitslücke den Smartmeter abzuschalten bzw. die Stromversorgung abzuschalten, können unter Umständen Stromnetze oder Kraftwerke überlastet werden und damit die Stromversorgung in bestimmten Gebieten zusammenbrechen. Stellt man sich nun vor es ist der 24. Dezember 18 Uhr, es schneit bei -17°C und die Stromversorgung bricht zusammen. Wenn dann noch die Erdgaslieferungen ausbleiben, kann man sich einige der potenziellen Auswirkungen ausmalen.

Ein weiteres interessantes Phänomen ist Stuxnet. Stuxnet wird im Kapitel zu Malware von mir näher und vor allem auf technischer Ebene beschrieben. In diesem Aufsatz spielt jedoch die strategische Ebene eine größere Rolle, daher werde ich hier Stuxnet auch nur aus strategischer Sicht besprechen.

Es wird vermutet[14], dass Stuxnet von israelischen und/oder amerikanischen Diensten entwickelt wurde, um das iranische Atomprogramm zu stören. Die Analysen der Schadsoftware gehen davon aus, dass die Urananreicherungsanlagen in Natanz oder das Kernkraftwerk in Buschehr gestört werden sollten.

Aus militär-strategischer Sicht wäre eine Bombardierung der Anlagen zu riskant. Zum einen könnte es der irani-

14 http://www.heise.de/thema/Stuxnet v. 19.04.2012; http://www.zeit.de/2010/34/T-Stuxnet-Trojaner v. 19.04.2012; http://www.spiegel.de/netzwelt/gadgets/spektakulaere-virus-analyse-stuxnet-sollte-irans-uran-anreicherung-stoeren-a-729329.html v. 19.04.2012; http://www.faz.net/aktuell/feuilleton/debatten/digitales-denken/trojaner-stuxnet-der-digitale-erstschlag-ist-erfolgt-1578889.html v. 19.04.2012

schen Luftwaffe bzw. Flugabwehr gelingen angreifende Flugzeuge auszuschalten und unter Umständen sogar überlebende feindliche Piloten gefangen zu nehmen und anschließend öffentlich vorzuführen. Eine Cyber-Attacke wie Stuxnet bietet hier den Vorteil der geringeren Sichtbarkeit und der besseren Abstreitbarkeit. Man kann zwar abschätzen wer als Urheber und was als Ziel der Attacke in Frage kommt, dies jedoch schwer zweifelsfrei beweisen. Geht man davon aus, dass das politische Ziel über dem Kriege die Ausschaltung des iranischen Atomprogramms ist, stellt sich auch Stuxnet nur als taktische Ebene, als einzelne Schlacht, dar und nicht als eigenständiger Cyber-Krieg.

Auffällig an Stuxnet ist, dass es mehrere Programmierer bzw. Programmierteams gab und diese koordiniert werden mussten. Es handelt sich also nicht um einen einzelnen Täter, sondern um mehrere, die generalstabsmäßig koordiniert wurden. Desweiteren verfügten die Stuxnet-Entwickler über eine Testgestellung des SCADA-Systems samt Frequenzumrichter, die genutzt werden können um Zentrifugen zur Urananreicherung zu steuern. Vereinfacht gesagt ist ein Frequenzumrichter eine Anlage, in die Wechselstrom eingespeist wird. Der Wechselstrom wird intern in Gleichstrom gerichtet und wieder als Wechselstrom zur Verfügung stellt, welcher in Frequenz und Amplitude moduliert werden kann. Der Frequenzumrichter kann beispielsweise vor einen Elektromoter geschaltet werden um diesen mit einer niedrigeren Drehzahl laufen zu lassen. Ein Frequenzumrichter wird auch eingesetzt, um in Zentrifugen die Drehzahl anzupassen und konstante Werte sicherzustellen. In der Praxis werden dazu Frequenzumrichter über Feldbusse (CAN, EtherCAT, Profibus, EtherNET/IP) miteinander und mit Steuerungsrechner gekoppelt, die eine automatische Rückkopplung beziehungsweise computergesteuerte Programmierungen erlaubt. Manipuliert ein Angreifer die SCADA-Steuerungsanlage (Supervisory Control and Data Acquisition) kann er die Ausgangsfrequenz der Frequenzumrichter und damit die Drehfrequenz der Zentrifugen manipulieren. Ist die Abweichung der Frequenz zu gering um mit dem bloßen Auge erkannt zu werden und hat der Angreifer neben der Steuerung auch die Überwachung im SCADA-System manipuliert, haben die Opfer in der Regel keine Chance die Manipulation zu entdecken.

Stuxnet nutzte mehrere sogenannte Zero-Day-Exploits aus, also Exploits, die dem Hersteller der Software und anderen Sicherheitsforschern nicht bekannt ist. Damit hatten die Entwickler und Anwender des Systemes keine Möglichkeit es durch ein Softwareupdate zu schützen. Desweiteren wurde Stuxnet über mehrere Angriffsvektoren ausgerollt, darunter auch über USB-Sticks, was voraussetzt, dass eine Person physisch in das Zielgebiet der zu kontaminierenden Rechner eindringt und den Stick dort verteilt oder einsetzt. Dies ist eine klassische Geheimdienstaufgabe.

Man kann davon ausgehen, dass Stuxnet ein organisierter Akt der »Gewalt« ist, allerdings ist fraglich, ob der Urheber seinen Gegner zur Erfüllung seines Willens zwingen konnte. Es ist weder offiziell bekannt wer der Urheber ist, noch sind seine Forderungen und damit Ziele bekannt. Es ist daher müßig über den Erfolg des Unternehmens Stuxnet zu spekulieren. Fakt ist lediglich, dass Stuxnet enttarnt wurde, was definitiv keinen Erfolg der Schadsoftware darstellt.

Ein weiterer Zwischenfall ist der Absturz bzw. die Entführung des »Beast of Kandahar«, einer Drohne vom Typ Lockheed Martin RQ-170 Sentinel im Iran, siehe Abbildung 1. Bei der Drohne handelt es sich um ein unbemanntes Flug-

objekt (Unmanned Aerial Vehicle UAV) welches zu Überwachungszwecken selbständig über ein definiertes Zielgebiet kreist und Video- oder Photoaufnahmen erstellt. Da das UAV unbemannt ist, benötigt es einen Steuerungsmechanismus. Entweder wird es per Funk von einem Piloten ferngesteuert oder es navigiert selbständig. Die selbständige Navigation kann über ein Trägheitsnavigationssystem und/oder GPS erfolgen. Trägheitsnavigationssysteme existieren bereits seit 1910 und wurden unter anderem im deutschen Aggregat 4 - der V2 - oder auf der USS Nautilus (SSN-571) eingesetzt. Diese Systeme haben aber den bekannten Nachteil einen Positionsfehler bzw. Kreiselfehler aufgrund der Erdkrümmung zu entwickeln. Um diese Messfehler zu minimieren werden in der Praxis neben Trägheitsnavigationssysteme auch GPS-Systeme oder ähnliches eingesetzt, meist auch gekoppelt.

Vorteil des GPS ist die hohe Genauigkeit - Nachteil ist aber die Angreifbarkeit des Signals bzw. des Systems. Ein GPS-Navigationsgerät peilt den eigenen Standort über die Triangulation (Dreieckspeilung) gegenüber 4 Satelliten (je einen für die Länge, Breite und Höhe sowie die Zeit). Dazu empfängt es die Daten der Satelliten und berechnet deren Signallaufzeit um die eigenen Koordinaten zu bestimmen. Diese Signale zwischen Satellit und Navigationssystem können wie jedes andere Funksignal auch gestört oder mit falschen Daten überschrieben werden. Dies ist sogar relativ einfach möglich, da der Leistungspegel nur -155 dBW beträgt[15]. Um dieser Gefahr vorzubeugen, gibt es neben dem offenen zivilen GPS noch ein verschlüsseltes System mit höherer Genauigkeit und Schutz vor Manipulationen. In der Praxis nutzen militärische Systeme nur das militärische GPS. Allerdings besteht oftmals die Möglichkeit auf das zivile Signal zurückzufallen, wenn das militärische gestört ist. Das zivile Signal kann aber mit einem gefälschten Signal überschrieben werden und falsche Daten liefern. So wäre es in der Praxis möglich die Signale zwischen Satellit und Drohne zu stören, so dass die Drone auf die zivile Version zurückfällt. Die zivilen Signale können dann mit falschen Daten überschrieben werden und der Drohne so falsche Positionen vorspiegeln, die sie zur Landung zwingen. Der Iran behauptet die Drohne so erbeutet zu haben. Die USA bestreiten den Einsatz von GPS in der Drohne. China fälscht GPS-Signale auf dem chinesischen Festland um die Positionierung zu erschweren. Man könnte sich auch vorstellen, dass die USA die Drohne gezielt in iranische Hände gespielt hat um den Iranern falsche Technik oder sonstige »rote Heringe« unterzuspielen.

Routing und Resilienz des Netzes

Im Jahre 1962 startete die Advanced Research Project Agency des US Verteidigungsministeriums ein Entwicklungsprojekt, welches ein neues Kommunikationsnetz hervorbringen sollte. Dieses sogenannte Arpanet entwickelte sich im Laufe der Zeit über verschiedene Zwischenschritte zum sogenannten »Internet« weiter.

Bei der Entwicklung des Netzes wurde Wert auf Ausfallsicherheit gelegt, so dass eine hierarchische Vermittlung in Bäumen nicht in Betracht gezogen wurde. Stattdessen wurde das Routing paketvermittelnd implementiert. Das Routing legt dabei fest, wie ein Paket vom Absender zum Empfänger vermittelt wird, also welchen Weg es nehmen soll. Ist das Netzwerk als Baum implementiert, existiert nur genau ein Weg vom Absender zum Empfänger, die Route wird also schon durch das Netz selbst festgelegt.

15 http://www.phrack.org/issues.html?issue=60&id=13#article v. 12.05.2008



Abbildung 1: Lockheed Martin RQ-170 Sentinel im Iran
Quelle: http://cdn4.spiegel.de/images/image-291837-galleryV9-tldk.jpg

Gibt es allerdings mehrere mögliche Routen, muss das Paket oder die Vermittlungsstation eine bestimmte Route nach definierten Kriterien auswählen. Es führen schließlich viele Wege nach Rom, so dass ein Navigationssystem oder Routenplaner verschiedene Strecken nach Länge, Stauwahrscheinlichkeit oder Sehenswürdigkeiten auswählen kann. Analog dazu muss in einem paketvermittelnden Netz der jeweilige Router entscheiden, über welche Route ein Paket weitervermittelt werden soll.

Der Vorteil der Paektvermittlung liegt in der erhöhten Resilienz des Netzwerkes, denn es stellt die Erreichbarkeit verschiedener Knoten auch dann sicher, wenn ein oder mehrere Knoten ausgefallen sind.

Abbildung 2 zeigt ein Netzwerk, das als Baum organisiert ist. Es existiert somit nur genau ein Pfad von einem beliebigen Knoten zu einem anderen. Fällt auf diesem Pfad ein Knoten aus, ist die Verbindung zwischen allen Knoten oberhalb und unterhalb des betroffenen Knoten gestört. Fällt also im Beispiel der Knoten Magdeburg aus, sind alle anderen sachsen-anhaltischen Knoten nicht mehr erreichbar. Um diesen Fall auszuschließen, muss der Baum zu einem gerichteten Graphen mit redundanten Pfaden erweitert werden. Dazu werden einfach weitere Verbindungen zwischen den Knoten eingefügt, so dass im Idealfall jeder beliebige Knoten mit jedem anderen Knoten über eine direkte Kante verbunden ist. In diesem Fall existiert zwischen jedem Knoten mindestens eine direkte Verbindung zu einem anderen Knoten sowie noch mindestens $n-2$ indirekte Verbindungen, welche über andere Knoten als Zwischenschritte führen. Insgesamt hat ein Netzwerk mit n Knoten dann $n\frac{n-1}{2}$ Kanten. Damit ein Knoten im idealen Netz nicht mehr erreichbar ist, müssen alle $n-1$ inziden-

ten Kanten ausfallen oder ausgeschaltet werden. Die Frage ob ein beliebiger Knoten von einem anderen beliebigen Knoten aus noch erreichbar ist, das sogenannte Erreichbarkeitsproblem, ist NL-vollständig berechenbar. Der Prim-Algorithmus um aus einem zusammenhängenden, ungerichteten aber kantengewichteten Graphen mit E Kanten und V Knoten einen Spanning Tree aufzuspannen ist in $\mathcal{O}(|E| + |V| \log |V|)$ berechenbar.

Aufgrund dieser von Anfang gewollten und implementierten Ausfallsicherheit ist es fast unmöglich das Internet (oder Teile davon) auszuschalten. Fällt ein Knotenpunkt aus, können immer noch genügend Routen über andere Knoten gefunden werden. Um einen Knoten komplett aus dem Netz zu entfernen, müssen alle inzidenten Kanten zerstört werden, das selbe gilt auch für ein beliebiges Subnetz (mehrere Knoten). Ebenso ist es problematisch Netzwerkpakete zu ihrem Ursprungsort zurückzuverfolgen, da jedes Paket einen anderen Weg durch das Netzwerk nehmen kann und Absenderadressen auch gefälscht werden können.

Distributed Denial of Service

Eine Denial-of-Service-Attacke ist eine Angriffsform, bei der ein Server, der einen bestimmten Dienst anbieten soll durch Überlastung ausser Gefecht gesetzt wird. Dazu wird der Server derart mit Anfragen bombardiert, dass er entweder abstürzt oder aber nicht mehr erreichbar ist, da das Netzwerk bzw. die Hardware des Servers überlastet wird. Dies kann der Angreifer erreichen, in dem er beispielsweise mit seinem eigenen Rechner den angebotenen Dienst (zum Beispiel eine Webseite) immer wieder abruft. Da heutzutage ein einzelner Rechner mit einer Endkunden-Internetanbindung nicht mehr ausreicht um einen ordentlich dimensionierten Server lahmzulegen, wurden sogenannte distributed-Denial-of-Service-Attacken (dDoS) entwickelt. Dazu greifen viele verteilte (distributed) Rechner den Zielserver an und überlasten ihn so gemeinsam.

Die verteilten Rechner werden dabei entweder von ihren Benutzern koordiniert gesteuert - beispielsweise über die bei Anonymous Script Kiddies beliebte Low Orbit Ion Cannon, LOIC[16] - oder in dem ein Angreifer fremde Rechner unter seine Kontrolle bringt.

Dazu nutzt ein Angreifer Schadsoftware aus um Rechner mit Sicherheitslücken unter seine Kontrolle zu bringen. Die Opferrechner, im Jargon Zombie genannt, werden zentral gesteuert und können auf Geheiß ihres Meisters bestimmte Befehle ausführen, beispielsweise einen Zielserver mit Anfragen bombardieren. Die Gesamtheit der Zombies nennt man dann Bot-Netz, abgeleitet von Roboter.

Rechtlich problematisch ist hier die Herrschaft über den Rechner der unter Umständen ein Zombie ist. Selbst wenn es gelingt den Angreifer (also Zombierechner) zu identifizieren, ist noch nicht sichergestellt das der Inhaber des Internet-Anschlusses auch Urheber der Attacke ist. Es ist ebenso möglich, dass der Rechner von einer anderen Person trojanisiert und zum Zombie gemacht wurde, so dass schon rein rechtlich gesehen hier einige Probleme entstehen.

Aus Sicht der IT-Sicherheit sind derartige Attacken besonders problematisch, da deren Ausführung relativ simpel ist, während die Verteidigung beliebig komplex und damit teuer werden kann. Praktisch wurden diese Attacken schon mehrfach umgesetzt, beispielsweise im

16 http://www.scip.ch/?labs.20101219, Zugriff am 22.04.2011

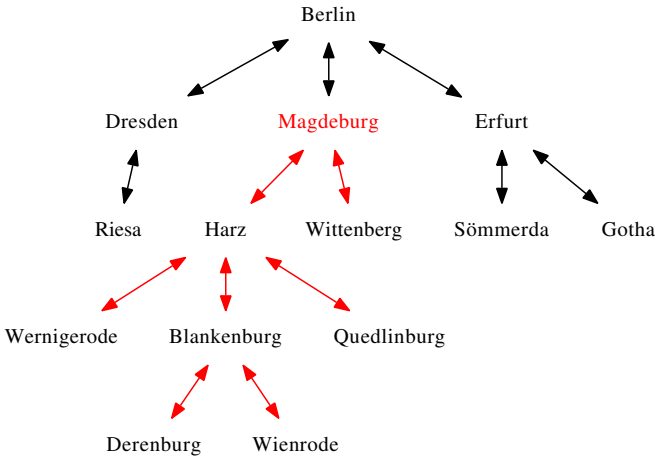


Abbildung 2: Beispiel eines Netzwerkes in Baumstruktur

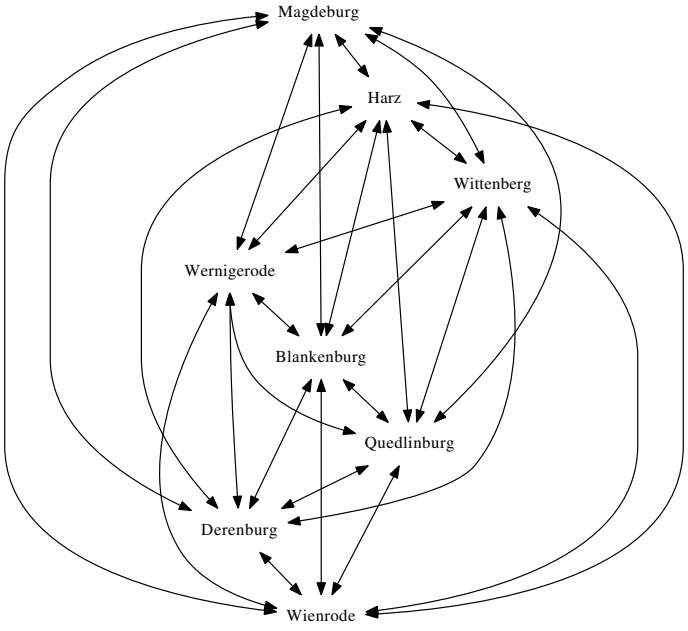


Abbildung 3: Beispiel eines Netzwerkes in Form eines gerichteten Graphen, der kein Baum ist

Jahre 2000, als der 15-jährige kanadische Schüler mit dem Alias *Mafiaboy* mehrere US-Amerikanische Server mit dem deutschen dDoS-Tool *Stacheldraht*[17] lahmlegte und nach Medienberichten Schaden in Höhe von 1,7 Milliarden kanadischen Dollarn anrichtete. Bei Mafiaboy handelt es sich übrigens nicht um einen Hacker, sondern um ein Script Kiddie. Hacker frönen dem kreativen Umgang mit der Technik und verfügen über umfangreiche technische Handlungskompetenz. Script Kiddies hingegen nutzen vorgefertigte Programme (sogenannte Scripte, hier Stacheldraht) ohne überhaupt zu wissen was sie tun. Damit können sie unter Umständen extrem gefährlich werden.

Auch die Angriffe auf Estland[18] im Jahr 2007 und Georgien[19] 2008 waren dDoS-Attacken, die insbesondere im estnischen Fall weitreichende Konsequenzen hatten.

In der Informatik bzw. der IT-Sicherheit werden verschiedene Diagnosekriterien festgelegt, die der Sicherheitsdiagnose von Software, Hardware und ganzen IT-Systemen dienen. Ein derartiges Verfahren ist auch als forensische Analyse notwendig, um zu überprüfen ob ein Angriff von einer bestimmten IP-Adresse stammt.

Die bekanntesten Sicherheitskriterien im deutschsprachigen Raum sind die sogenannten VIVA-Kriterien, also Vertraulichkeit, Verfügbarkeit, Integrität und Authentisierung, welche unter anderem vom Bundesamt für Sicherheit in der Informationstechnik (2006) wie folgt definiert werden:

Vertraulichkeit Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

Integrität Die Daten sind vollständig und unverändert. Der Begriff »Information» wird in der Informationstechnik für »Daten« verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.

Verfügbarkeit Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.

Authentisierung Bei der Anmeldung an einem System wird im Rahmen der Authentisierung die Identität der Person, die sich anmeldet, geprüft und verifiziert. Der Begriff wird auch verwendet, wenn die Identität von IT-Komponenten oder Anwendungen geprüft wird. Ist die Authentisierung erfolgreich, spricht man auch davon, dass die Person oder ein Datum authentisch ist bzw. die Authentizität gewährleistet ist.

Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein anderer Begriff dafür ist »IT-Sicherheit« (Bundesamt für Sicherheit in der Informationstechnik 2006, S. 8).

Sicherheitsüberprüfungen in der Informatik wenden daher meist die oben genannten VIVA-Kriterien an und überprüfen ein System hinsichtlich deren Einhaltung. Dabei wird in der Regel der

17 http://www.sans.org/security-resources/malwarefaq/stacheldraht.php, 19.04.2008

18 http://en.wikipedia.org/w/index.php?title=2007_cyberattacks_on_Estonia&oldid=514966602, 15.10.2012

19 http://en.wikipedia.org/w/index.php?title=Cyberattacks_during_the_2008_South_Ossetia_war&oldid=481694597, 15.10.2012

Anwender aus der Betrachtung ausgeschlossen.

Ich möchte dies am Beispiel des E-Mailsystems erläutern: Alice und Bob möchten vertrauliche Daten per E-Mail austauschen. Wenn sie diese Daten per E-Mail verschicken wollen, müssen sie eine VIVA-Analyse (Diagnose) des E-Mail-Systems durchführen:

Vertraulichkeit E-Mails werden als einfache Textdatei zwischen den Mailservern weitergeleitet. Jeder der Zugriff auf die Mailqueue hat, kann die E-Mails auf einem Server lesen. Ebenso kann der Netzwerkverkehr an zentraler Stelle abgefangen und ausgewertet werden. Eine E-Mail ist also nicht vertraulich.

Integrität Jeder der schreibenden Zugriff auf die Mailqueue eines Mailservers hat, kann dort eine Mail verändern. Eine E-Mail ist also nicht integer.

Verfügbarkeit E-Mails können im Netz abgefangen werden und erreichen den Empfänger daher nicht. Die Verfügbarkeit von E-Mails ist nur eingeschränkt möglich.

Authentizität Zusammem mit der Integrität kann auch die Authentizität manipuliert werden, das heißt ein Angreifer kann nicht nur den Inhalt der Mail, sondern auch Absender und Zeitstempel ändern. Die Authentizität einer E-Mail ist daher nicht gewährleistet.

Alice und Bob stellen also fest, dass das E-Mailsystem ihren Sicherheitsanforderungen nicht genügt. Sie befassen sich daher mit einem Verschlüsselungssystem für E-Mails und führen nun die Diagnose anhand der VIVA-Kriterien erneut für eine verschlüsselte Mail durch:

Vertraulichkeit Eine verschlüsselte E-Mail kann zwar weiterhin abgefangen, aber nicht mehr gelesen werden, solange das Kryptosystem sicher ist.

Integrität Eine signierte E-Mail kann nicht manipuliert werden, solange das Kryptosystem sicher ist.

Verfügbarkeit Auch verschlüsselte E-Mails können abgefangen und gelöscht werden, die Verfügbarkeit von verschlüsselten E-Mails ist nur eingeschränkt möglich.

Authentizität Zusammen mit der Integrität schützt die Verschlüsselung und Signatur auch die Authentizität, da der Inhalt der E-Mail nicht verändert werden kann, solange das Kryptosystem sicher ist.

Anhand dieser Diagnose können Alice und Bob feststellen, dass ein verschlüsseltes E-Mailsystem ihren Anforderungen genügt und daher als »sicher« zu bezeichnen ist. Sie ignorieren hierbei aber die Sicherheit des KryptosystemsAußerdem ignorieren sie ihre eigenenEntscheidungen bzw. die Entscheidungen der Anwender. So muss jeder Anwender über ein starkes Passwort verfügen und dies geheim halten. Derartige Anforderungen sind sozialer Natur. In der Praxis zeigt sich, dass die Annahme, Benutzer würden ihr Passwort sicher auswählen und geheim halten, nicht zutrifft.

Wie die Beispielanalyse der E-Mail-Sicherheit zeigt, kann man die Integrität und Authentizität einer Datenübertragung elektronisch nicht ohne weiteres sicherstellen. Lediglich der Einsatz von Kryptographie kann durch die Verschlüsselung eines Datums die Vertraulichkeit sichergestellt werden. Die Authentizität und Integrität eines Datums kann durch kryptographische Signaturen (auch digitale Unterschrift genannt) sichergestellt werden – aber nur wenn beide Kommunikationspartner dies auch wollen. Ist ein Kommunikationspartner böswillig, kann der andere Partner dessen korrekte Identität nicht

sicherstellen. Hierfür wäre eine unabhängige Zertifizierungsstelle notwendig, die beide Kommunikationsparter unabhängig voneinander überprüft und deren Identität zertifiziert.

Da eine derartige Zertifizierung nur für spezielle Fälle wie beispielsweise E-Mail umzusetzen ist, nicht jedoch für andere Kommunikationsformen (Telnet, SSH, Nmap etc. pp.), kann ein böswilliger Angreifer seine Identität verschleiern in dem er beispielsweise IP-Pakete fälscht. Möchte der Angreifer nicht erkannt werden, kann er dies relativ einfach erreichen, erst recht wenn er mit staatlicher Unterstützung durch Militär und Geheimdienst agiert. Insofern ist die eingangs dargestellte Schlagzeile von chinesischen Superhackern, die in den Bundestag eingedrungen sind mit entsprechender Vorsicht zu genießen – handelt es sich um Superhacker, lassen sie sich nicht so ohne weiteres Identifizieren. Lassen sich die Angreifer einfach identifizieren[20], sind es keine Superhacker.

Ein weiteres Problem in der Zuordnung der Urheberschaft von Attacken ist die technische Herrschaft über einen Rechner. Selbst wenn die Quelle einer Attacke zweifelsfrei identifiziert werden kann, heißt das nicht dass der Eigentümer des Rechners auch der Angreifer ist. Schließlich ist es für einen Angreifer notwendig, nicht identifiziert werden zu können. Daher werden nicht nur Verschleierungstechniken verwendet, sondern auch sogenannte Proxies benutzt. Das heißt ein Angreifer greift nicht direkt von seinem Rechner aus das Zielsystem an, sondern benutzt Zwischenstationen, um seine Herkunft zu verschleiern. Dazu bieten sich schlecht gesicherte Rechner in Staaten an, deren Polizei mit der Aufklärung von Internetkriminalität überfordert ist und die mit den Staaten, in denen das Zielsystem bzw. der Angreifer sitzt nicht kooperieren. Das heißt der Angreifer übernimmt zuerst Rechner in der Ukraine, Südafrika, Mexiko, China und Serbien, bevor er den Zielrechner in Wien attackiert, siehe Abb. .

Wird der Angriff auf das Zielsystem erkannt, können die lokalen Strafverfolgungsbehörden lediglich den letzten genutzten Proxy in Serbien identifizieren. Sie können aber nicht zweifeslfrei belegen, dass der Eigentümer des serbischen Rechners (beziehungsweise der Inhaber des Internetsanschlusses von dem aus die Attacke zur Angriffszeit begangen wurde) auch wirklich der Angreifer ist und sein Rechner nicht durch einen anderen Hacker oder Trojaner missbraucht wurde. Dazu müssten hier die österreichischen Strafverfolgungsbehörden mit den serbischen kooperieren und den missbrauchten Rechner forensisch untersuchen. Sind die serbischen Behörden dazu nicht bereit, bleibt den österreichischen Behörden keine Möglichkeit, den Angreifer zu identifizieren.

Kooperieren die österreichischen und serbischen Behörden und es gelingt ihnen den Angriff auf das Proxysystem aufzukären, stehen sie wieder vor dem selben Problem: der Angreifer ist über einen chinesischen Rechner in den serbischen eingedrungen. Das heißt die österreichischen und serbischen Behörden müssen nun gemeinsam mit den chinesischen den Einbruch in das chinesische System aufklären. Um dann den Proxy in Mexiko zu enttarnen und das selbe Verfahren von vorne zu beginnen.

Noch problematischer wird die Aufklärung, wenn der Angreifer IP-Pakete spoofed, also fälscht. IP-Pakete sind das grundlegende Atom der Kommunikation im Internet, sie sind die eigentlichen Pakete in denen die Daten (z. B. eine Mail oder Webseite) transportiert werden. Die IP-Pakete tragen in ihrem

20 Siehe hierzu das Kap. zu Anonymität von Jens Kubieziel

sogenannten Kopf oder Header Metadaten mit, wie den Absender, Empfänger, Time-To-Live oder Optionen (vgl. S. Schumacher 2005b). Im Prinzip kann der Absender alle Daten nach belieben manipulieren, zum Beispiel auch die Absender-Adresse[21]. So kann man beispielsweise mit dem Programm Hping3 und der Option `hping3 -1 -flood -a 10.10.10.10 127.0.0.1` die IP-Adresse 127.0.0.1 mit ICMP Echo Requests fluten, deren Absender auf 10.10.10.10 gesetzt wird. Im schlimmsten Fall kann ein Angreifer eine dDoS-Attacke mit einem Zombie-Netz fahren, das seine IP-Adressen systematisch fälscht. Abbildung zeigt wie ein Angreifer von Deutschland aus mehrere Zombies kontrolliert (grün) und mit ihnen ein Ziel in den USA angreift (blau). Dabei werden die IP-Pakete systematisch gefälscht und spiegeln eine Absenderadresse in China vor (rot). Für die amerikanischen Verteidiger sieht es daher so aus als käme der Angreifer aus China. Was unter Umständen fatale Folgen haben kann.

Cyber-Angriffe und militärische Strategie und Taktik

Einen Cyber-War gibt es nicht, da es nicht möglich ist über Cyber-Attacken einen Gegner derart zu entwaffnen, dass er politisch hilflos und militärisch wehrlos ist. Daher ist der Begriff Cyber-War oder Cyber-Krieg falsch und eigentlich nicht zu gebrauchen. Zumindest dann nicht wenn man eine hinreichend realistische Definition von Krieg zu Grunde legt und den Begriff nicht analog zu *Wirtschaftskrieg* oder *Zickenkrieg* verwendet, um auf Streitereien in einem Top-Model-Haus hinzuweisen.

Nach von Clausewitz (1832) ist die »Taktik die Lehre vom Gebrauch der Streitkräfte im Gefecht, die Strategie die Lehre vom Gebrauch der Gefechte zum Zweck des Krieges«. Die Strategie verfolge daher ein Zweck im Kriegsplan, das dem des Krieges entspräche.

Was jedoch möglich ist, ist der Einsatz von IT und Angriffen auf IT, um den konventionellen Kriegsverlauf zu unterstützen. Dies ist in Deutschland unter dem Begriff *Elektronische Kampfführung* (EloKa) bekannt. Ich plädiere daher dafür, diesen Begriff zu nutzen. Er wird auch der Natur dieser Angriffe gerechter, da die EloKa in jedem Truppenteil und jeder Truppengattung zum Einsatz kommt. Cyber-Attacken erfolgen in der Regel auf taktischer, seltener auf strategischer Ebene. Sie begleiten und unterstützen konventionelle Kampfhandlungen und können nur mit diesen verbunden strategische Ziele erreichen. Die EloKa wird im Konzept des Gefechts der verbundenen Waffen bzw. Operation verbundener Kräfte[22] neben Feuer, Bewegung und Sperren als wichtiger Bestandteil geführt. Cyber-Attacken fallen damit als EloKa-Operation unter die Führungsunterstützung.

Es gibt keine eigenständige »fünfte Domäne«[23] in der Hacker einen ominösen Cyber-Krieg führen können. Stattdessen werden Cyber-Operationen konventionelle Angriffe vorbereiten und unterstützen und damit in den klassischen Domänen Land, See, Luft und auch Weltraum stattfinden. Ohne den Einsatz von IT in diesen Domänen ist eine Fünfte namens Cyberspace überhaupt nicht möglich. Konventionelle Kriegsführung kann auf den Einsatz von IT verzichten und so erst die Entstehung eines Cyberspace verhindern. Ein Cyberspace al-

21 Eigentlich sollten die Netzwerkprovider und diversen Switches auf dem Weg gefälschte IP-Adressen herausfiltern.

22 vgl. Heeresdienstvorschrift 100/100, 100/200, VS NfD

23 http://www.economist.com/node/16478792 v. 31.12.2010

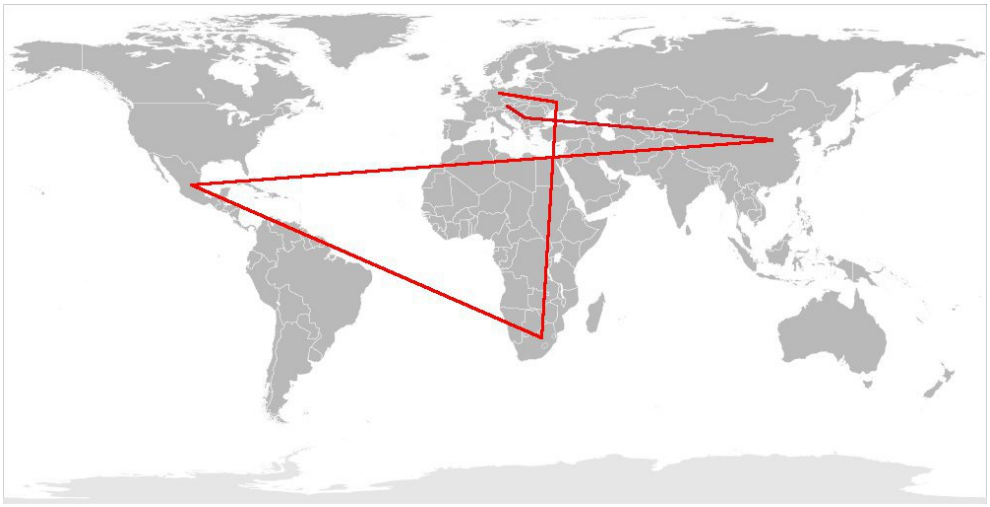


Abbildung 4: Angriff auf ein Zielsystem, verschleiert durch mehrere Proxies in der Ukraine, Südafrika, Mexiko, China und Serbien

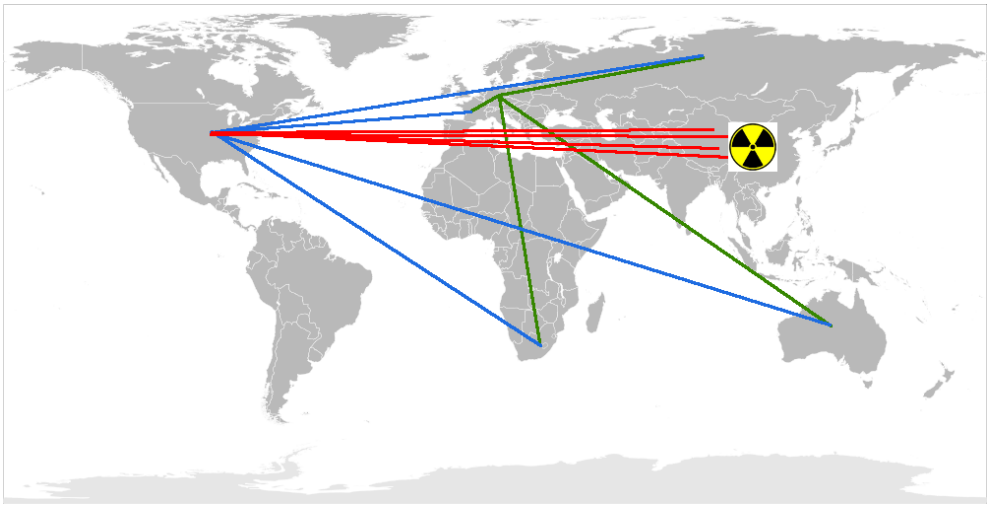


Abbildung 5: Distributed Denial of Service mit gespooften Absendeadressen

lein ist aber für einen Krieg nicht geeignet. Es ist daher nicht wirklich sinnvoll von einer »fünften Domäne Cyberspace« zu sprechen, wenn es sich bei den Cyber-Operationen nur um einen einfachen Sonderfall von Elektronischer Kampfführung handelt - die es so schon im ersten Weltkrieg gegeben hat.

Cyber-Attacken können ein fundamentales militärisches Paradigma ändern. von Clausewitz (Sechstes Buch: Verteidigung 1832) schreibt: »die verteidigende Form des Kriegführens ist an sich stärker als die angreifende«. Er definiert die Verteidigung als »das Abwehren eines Stoßes« und das »Abwarten dieses Stoßes«. Verteidigung im IT-Sicherheitssinne bedeutet daher, die Systeme derart abzusichern und zu konfigurieren, dass ein Angriff ins Leere läuft, der Angreifer also keine Sicherheitslücken im System finden oder ausnutzen kann. Dazu überlasse man nach Clausewitz die Initiative dem Feinde und erwarte sein Erscheinen vor der eigenen Front. Das Erwarten erfolgt aber nicht passiv, sondern in dem man die eigenen Systeme absichert. Der Verteidiger ist hier im Vorteil, da er die Logistik und Geländekenntnisse für sich nutzen kann und auch die Nebel des Krieges für ihn arbeiten.

Diese Absicherung ist aber in IT-Systemen ungleich komplexer als der Angriff. Bereits eine einfache stochastische Überlegung belegt dies: der Angreifer muss nur eine einzige geeignete Sicherheitslücke finden und ausnutzen. Der Verteidiger muss jede Sicherheitslücke identifizieren und stopfen. Stellt man sich nun in einem Gedankenexperiment eine mittelalterliche Stadt vor, die durch eine Stadtmauer gesichert wird, kann man den Arbeitsaufwand der Angreifer und Verteidiger abschätzen. Starten nun je ein Angreifer und Verteidiger damit, jeden einzelnen Stein der Mauer abzuklopfen und zu prüfen ob dieser noch stabil ist, ist der Verteidiger im Nachteil. Denn er muss jeden einzelnen Stein abklopfen und gegebenenfalls austauschen. Gelingt es dem Angreifer vor ihm einen morschen Stein zu finden und einzuschlagen, kann der Angreifer diese Sicherheitslücke ausnutzen.

Dabei gilt auch zu beachten, dass es praktisch unmöglich ist, die Sicherheit von IT-Systemen mathematisch zu verifizieren. Es ist zwar theoretisch möglich, ein Computerprogramm wie ein Betriebssystem in ein mathematisches Gleichungssystem zu überführen und zu berechnen um Fehler zu entdecken. Ein derartiges Gleichungssystem ist allerdings so komplex, dass es praktisch nicht mehr zu berechnen ist. Zum Vergleich ein paar Daten zur Größe des Betriebssystems NetBSD, Version 5.0: es besteht aus 163 000 Quelldateien, 57 228 442 Codezeilen und 1 991 091 842 Zeichen. Zum Vergleich: Goethes Faust I besteht »nur« aus ca. 4 600 Zeilen mit 200 000 Zeichen. Es ist daher praktisch unmöglich, dass eine Person den gesamten Überblick über das NetBSD-System hat. Und in der Praxis läuft auf einem Computer nicht nur das Betriebssystem sondern meist noch wesentlich komplexere Anwendungsprogramme. Allein durch den Einsatz von IT-Systemen wird hier eine Komplexitätsstufe eröffnet, die kaum noch beherrschbar ist.

Bereits erwähnt habe ich die Nebel des Krieges. So schreibt von Clausewitz (Erstes Buch: Über die Natur des Krieges, 1832) dazu: »Der Krieg ist das Gebiet der Ungewißheit; drei Vierteile derjenigen Dinge, worauf das Handeln im Kriege gebaut wird, liegen im Nebel einer mehr oder weniger großen Ungewißheit«. Jene Ungewissheit kann in der Informationstechnologie eine gewichtige Rolle spielen, denn es ist möglich dem Angreifer (oder auch Verteidiger) Tatsachen vorzuspielen. Im Zweiten Weltkrieg gelang es der Abwehr und der Sicherheitspo-

lizei ein Netzwerk der Special Operations Executive und Military Intelligence Division in den Niederlanden umzudrehen und zu nutzen um falsche Nachrichten nach Großbritannien zu übermitteln (vgl. Schafranek und Tuchel 2004).

Derartige Spiele sind auch in der IT möglich und hier sogar noch einfacher durchzuführen. Beispielsweise kann man hier sogenannte Honeypots oder Honeynets einsetzen. Ein Honyepot ist ein Programm, das auf einem Hostrechner läuft und prinzipiell beliebige Gastsysteme emulieren kann. So kann man beispielsweise auf einem NetBSD-Server 20 Windows XP-Systeme emulieren und einen Klassenraum voller Windows-PC vorspiegeln. Der Sinn hinter diesem Programm ist es, einen Angreifer auf die emulierten Systeme zu locken um ihn entweder zu analysieren oder um seine Kräfte auf nutzlosen Systemen zu binden. Während sich der Angreifer um die vermeintlichen XP-PCs kümmert und diese angreift. So kann er zum einen entdeckt werden, zum anderen kann seine Vorgehensweise komplett aufgezeichnet und analysiert werden, um damit beispielsweise neue Angriffssignaturen für Intrusion Detection Systeme oder Penetration-Werkzeuge zu generieren (vgl. S. Schumacher 2005a, 2010a).

So wäre es in der Praxis durchaus möglich, beispielsweise das Netz des deutschen Bundestages in einem Honeynet zu emulieren und somit feindliche Angreifer anzulocken. Desweiteren kann man nicht nur deren Vorgehen analysieren, sondern ihnen auch gefälschte Dokumente unterschieben.

Ein weiteres Problem ist die Wirkung von Cyber-Waffen. Egal wie elaboriert eine Schadsoftware sein kann, es ist immer problematisch nur bestimmte Rechner (beispielsweise die einer Armee oder in einem spezifischen Land) zu identifizieren. Die Identifikation ist aber der erste Schritt und die Rechner gezielt anzugreifen. Ähnlich wie sich eine Senfgasgranate nicht dafür interessiert ob sie über deutschen oder französischen Truppen explodiert, interessiert sich ein Schadprogramm per se nicht dafür ob es einen chinesischen, russischen oder deutschen Rechner als Ziel hat. Es ist daher relativ unwahrscheinlich dass ein staatlicher Angreifer gewollt eine Schadsoftware in die freie Wildbahn entlässt, die ungezielt möglichst viele Rechner identifiziert und lahmlegt. Denn damit würde der Angreifer in der Regel auch die eigenen Systeme und Netze lahmlegen, sich also selbst der Computersysteme und des Internets berauben. Dies kann eigentlich nur dann erfolgreich sein, wenn die IT in den Streitkräften des Angreifers keine Rolle spielt oder wenn sie erfolgreich abgeschaltet werden kann, da Alternativen bereitstehen.

Schließlich gibt es auch noch eine zentrale Frage, die jede elektronische Attacke ins Leere laufen lassen kann. Das potenzielle Opfer muss sich nur fragen, wie abhängig es vom angegriffenen System ist. Es kann sich selbst aussuchen, ob es dieses System einsetzen will oder ob Alternativen genutzt werden sollen. Oder ob es im Konfliktfall das System nicht einfach abschaltet und auf eine Alternative ausweicht. Damit wird die Kampfkraft einer »Cyber-Waffe« fast ausschließlich vom angegriffenen System bestimmt. Eine Situation, die für konventionelle Waffen nicht so einfach gilt. Zwar kann die Bevölkerung eine Stadt vor einem Bombenangriff verlassen oder in Bunkern unterziehen, die materiellen Werte wie Häuser, Strassen und Fabriken können aber nicht einfach versetzt oder versteckt werden.

Problematisch ist allerdings zur Zeit, dass sich unsere Gesellschaft immer weiter von IT-Systemen abhängig macht. Der Einsatz von Smartmetern ist nur

ein Punkt. Ein normaler Drehstromzähler kann nicht über das Internet angegriffen werden, damit ist auch Sicherheitsanalyse oder Alternative nicht notwendig. Trotzdem werden die potenziellen Sicherheitsprobleme kaum dezidiert diskutiert.

Wie bereits eingangs erwähnt, möchten die USA und Deutschland in Zukunft auf Cyber-Attacken mit konventionellen Gegenschlägen reagieren. Also Bomben auf Botnetze werfen. Wie ich in diesem Aufsatz versucht habe zu zeigen, ist dies ein äußerst problematischer Vorschlag. Im schlimmsten Falle eskaliert die dDoS-Attacke eines 15-jährigen Script Kiddies zum NATO-Bündnisfall mit konventionellen Gegenschlägen. Hierbei ist besonders auf die zeitliche Entwicklung zu achten. Erstreckte sich die Kuba-Krise noch über 13 kritische Tage, kann eine derartige Cyber-Attacke schon in Minuten zu einer folgenschweren Eskalation führen. Ohne dass es überhaupt möglich wäre, eine Untersuchung zu den Verursachern durchzuführen die gerichtsfest wäre.

Ein weiterer interessanter Angriffsvektor im militärischen Bereich ist die sogenannte netzwerkzentrierte Kriegsführung (Network Centric Warfare) (vgl. Alberts u. a. 1999). Dabei werden Strategien aus dem Management von Unternehmen und der Wirtschaftsinformatik übernommen, beispielsweise sogenanntes Data Warehousing. Die zentrale Idee dahinter das jeder Soldat und jedes Waffensystem mit elektronischen Sensoren versehen wird und die gesammelten Daten in einen zentralen Speicher, das Warehouse, eingeliefert werden. Dort laufen dann verschiedene Computerprogramme, die die Daten nach bestimmten Kriterien ordnen, sortieren und so versuchen neue Kenntnisse zu generieren, beispielsweise über den Zustand der eigenen Truppe oder Absichten des Gegners. Derartige Techniken wurden in den USA unter dem Titel *Future Combat Systems* bzw. werden seit 2010 als *Brigade Combat Team Modernization* erforscht. In der Bundeswehr läuft das Projekt *Infanterist der Zukunft*. Problematisch ist hierbei, dass die Systeme auf den Einsatz von IT setzen. Diese kann unter Umständen manipuliert oder gehackt werden und damit den Einsatz der eigenen Truppe gefährden - eine Gefährdung die bei »klassischen Soldaten« ohne digitalen Assistenten nicht existiert. Außerdem besteht die Gefahr, dass die Systeme bereits mit einer Backdoor oder einem Trojaner aber Herstellerwerk versehen sind. So ist es möglich, in einen Chip ein Verfallsdatum zu implementieren. Wenn dieser Chip dann im Feuerleitsystem der Panzerhaubitze 2000 oder des Leopard 2 eingesetzt wird, könnten die Chips zu einem beliebigen Datum den Dienst einstellen und die Waffensysteme nahezu nutzlos zurücklassen. Deutschland ist derzeit kaum in der Lage die notwendigen Microchips selbst herzustellen, sondern auf ausländische Lieferanten angewiesen.

Negativ fällt ebenso auf, dass es keine koordinierte internationale Strategie zur IT-Sicherheit gibt. Das Internet ist ebenso international wie Cyber-Kriminalität und elektronische Kampfführung im Internet. Daher kann auch nur durch internationale Kooperationen in diesem Bereich Sicherheit hergestellt werden.

Auch wenn wir uns derzeit noch in einer Experimentierphase der IT-Sicherheit bzw. der EloKa befinden, möchte ich im Hinblick auf militärische Konflikte den alten Leitsatz *Pedites pugnas decernent* anbringen. Es sind die Infanteristen, die den Krieg entscheiden. In diesem Sinne: Horrido!

Literaturverzeichnis

Alberts, D., Garstka, J. & Stein, F. (1999). *Network Centric Warfare: Developing*

and Leveraging Information Superiority. Ccrp Publication Series. National Defense University Press.

Bundesamt für Sicherheit in der Informationstechnik (Herausgeber). (2006). Leitfaden IT-Sicherheit IT-Grundschutz kompakt. Zugriff am 16. Oktober 2006, unter http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf

Department of Defense Strategy for Operating in Cyberspace. (ohne datum). Zugriff am 29. Juli 2011, unter www.defense.gov/news/d20110714cyber.pdf

Schafranek, H. & Tuchel, J. (2004). *Krieg im Äther: Widerstand und Spionage im Zweiten Weltkrieg* (Gedenkstätte Deutscher Widerstand & Dokumentationsarchiv des Österreichischen Widerstandes, Herausgeber). Picus.

Schumacher, S. (2005a). Einbruchserkennung in Netzwerke mit Intrusion Detection Systemen und Honeypots. Zugriff am 21. November 2006, unter http://www.kaishakunin.com/publ/einbruchserkennung.pdf

Schumacher, S. (2005b). Spass im Netzwerk mit tcpdump & Co. Zugriff am 3. Oktober 2005, unter http://www.net-tex.de/tcpdump.pdf

Schumacher, S. (2009a). Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil I. *Informationsdienst IT-Grundschutz*, *7*, 11–13. Zugriff am 22. Juli 2009, unter http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_7-2009_11_13.pdf

Schumacher, S. (2009b). Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil II. *Informationsdienst IT-Grundschutz*, *8*, 8–9. Zugriff am 24. August 2009, unter http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_8-2009_8_9.pdf

Schumacher, S. (2009c). Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil III. *Informationsdienst IT-Grundschutz*, *10/11*, 21–22.

Schumacher, S. (2010a). Auf dem Weg zum Intrusion Detection System der nächsten Generation. In Team der Chemnitzer Linux-Tage (Herausgeber), *Chemnitzer Linux-Tage 2010: Tagungsband* (Seiten 19–24). Technische Universität Chemnitz. Chemnitz: Universitätsverlag.

Schumacher, S. (2010b). Psychologische Grundlagen des Social-Engineering. *Die Datenschleuder: Das wissenschaftliche Fachblatt für den Datenreisenden*, *#94*, 52–59. Zugriff am 10. Oktober 2010, unter http://ds.ccc.de/pdfs/ds094.pdf

Schumacher, S. (2011a). Die psychologischen Grundlagen des Social Engineerings. *Magdeburger Journal zur Sicherheitsforschung*, *1*, 1–26. Zugriff am 31. Januar 2011, unter http://www.wissens-werk.de/index.php/mjs

Schumacher, S. (2011b). Sicherheit messen: Eine Operationalisierung als latentes soziales Konstrukt. In S. Adorf, J.-F. Schaffeld & D. Schössler (Herausgeber), *Die sicherheitspolitische Streitkultur in der Bundesrepublik Deutschland: Beiträge zum 1. akademischen Nachwuchsförderpreis Goldene Eule des Bundesverbandes Sicherheitspolitik an Hochschulen (BSH)* (Seiten 1–38). Magdeburg: Meine Verlag.

Schumacher, S. (2012). Zum Verhältnis von psychischen, sozialen und technischen Dimensionen des Einsatzes von IT-Systemen. Bachelor-Arbeit. Otto-von-Guericke-Universität Magdeburg.

Schumacher, S. » (2012). Vom Cyber-Kriege: Gibt es einen Krieg im Internet? *Magdeburger Journal zur Sicherheitsforschung*, *2*, 285–307. Zugriff am 20. November 2012, unter http://www.sicherheitsforschung-magdeburg.de/journal_sicherheitsforschung.html

von Clausewitz, C. (1832). *Vom Kriege*. Ferdinand Dümmler.

Wikipedia. (2012). Krieg — Wikipedia, Die freie Enzyklopädie. [Online; Stand 10. Oktober 2012]. Zugriff am unter http://de.wikipedia.org/w/index.php?title=Krieg&oldid=108549681