# Kapitel 6
# Cyber-Terrorismus – Reale Bedrohung oder Mythos?

*Stefan Schumacher*

## 1. Begriffserklärung: Cyber und Terror, Krieg sowie Kriminalität

Ähnlich wie der Begriff „Cyber-Krieg“ findet sich auch „Cyber-Terrorismus“ seit einigen Jahren in der Medienlandschaft und der politischen Diskussion. Allerdings stellt sich dabei die Frage, auf welche technischen Möglichkeiten dieser Begriff rekurriert und ob er folglich überhaupt gerechtfertigt ist – oder ob es sich dabei, ähnlich wie beim Cyber-Krieg, um einen Begriff handelt, der von Experten zumeist als übertrieben und ungerechtfertigt angesehen wird. Daher wird im Rahmen des vorliegenden Artikels untersucht, ob sich das Konzept von Terror und Terrorismus auf das Internet übertragen lässt und damit eine Form von Cyber-Terrorismus möglich ist.

Definitorisch greift der Autor auf die Erklärung aus Meier[1] zurück, und nutzt sie als Arbeitsgrundlage für den Aufsatz:

„Im Allgemeinen lässt sich unter Terrorismus die systematisch vorbereitete Planung und Durchführung illegaler Gewaltakte durch temporär oder dauerhaft zusammengesetzte Gruppen, die in der Regel konspirativ und subversiv, national oder international mit der Zielsetzung kooperieren, eigene oder im Auftrag zu erfüllende politische Ziele zu erreichen. […] Sicherheitspolitisch ist der Gebrauch des Begriffs „Terrorismus“ ohne weitere inhaltliche Präzisierung zur Charakterisierung einer strategischen Herausforderung oder Bedrohung wenig hilfreich, da nichts über die Qualität der Bedrohung und seine Zielrichtung gesagt wird.
Das wesentliche Ziel des politischen Terrors ist die Abschaffung bestehender Herrschaftsverhältnisse, die Beseitigung bestehender Herrschaftseliten und die Etablierung radikaler Alternativen unter Zuhilfenahme von Gewalt, Schrecken und Terror. Zugleich soll aber auch in Teilen der Bevölkerung Sympathie und Unterstützungsbereitschaft erzielt werden. In der Regel haben terroristische Gruppen keine Basis, um offen gegen ein Herrschaftssystem zu rebellieren. Dies hemmt einerseits ihre Wirkung, führt jedoch zugleich zu einem stärkeren Bemühen um Unterstützung und Kooperation im internationalen Bereich. [...]“

1 Meier, Ernst-Christoph/Hannemann, Andreas/Meyer zum Felde, Rainer: Wörterbuch zur Sicherheitspolitik: Deutschland in einem veränderten internationalen Umfeld, Hamburg 2012, S. 488.

Der Wortteil *Cyber* ist inspiriert vom griechischen Wort Kybernetik, welches abgeleitet von *Steuermann* für Regelungs- oder Steuerungstechnik steht. Es lässt sich im Englischen zurückführen auf den US-amerikanischen Autor *William Gibson*, welcher in den 1980er-Jahren in seinen Genre-prägenden Romanen (Johnny Mnemonic, Neuromancer etc.) unter anderem die Begriffe Cyberspace und Matrix schuf. Damit beschrieb er eine damals utopische Form des Internets, in der soziale Handlungen stattfinden. Einige Protagonisten der Romane lebten quasi durchgehend in der virtuellen Realität des Cyberspace und verachteten teilweise sogar ihre fleischliche Existenz. Der Cyberspace selbst besteht aus der technischen und der sozialen Dimension. Die technische Dimension umfasst dabei Hardware und Software, Protokolle und Dienste, welche hier 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.[2]

Gemäß der oben genannten Definition von Terrorismus wäre Cyber-Terrorismus damit Terrorismus, der ganz oder zumindest zu großen Teilen, im Cyberspace, also insb. dem Internet, stattfindet. Um das Phänomen weiter einzugrenzen, betrachtet der Autor nur Vorkommnisse als Cyber-Terrorismus, die ohne das Internet nicht stattfinden könnten. Dies betrifft insbesondere Phänomene wie Online-Propaganda von terroristischen Gruppen beispielsweise über Webseiten, Online-Magazine oder Diskussionsforen.
Damit stellt sich nun die Frage, ob durch die

- systematisch vorbereitete Planung und Durchführung illegaler Gewaltakte im Internet bzw. Cyberspace
- durch temporär oder dauerhaft zusammengesetzte Gruppen, die in der Regel konspirativ und subversiv, national oder international mit der
- Zielsetzung kooperieren, eigene oder im Auftrag zu erfüllende politische Ziele zu erreichen,

---

2 Vgl. Baehr, Dirk D: „Salafistische Propaganda im Internet: Von der reinen Mission bis zum globalen Jihad – Die wesentlichen ideentheoretischen Unterschiede unter den salafistischen Strömungen in Deutschland“, Magdeburger Journal zur Sicherheitsforschung, Band 2(2012); vgl. Holze, Jens: Eine Geschichte der Hackerkultur: Subkultur im Digitalen Zeitalter, Magdeburger Journal zur Sicherheitsforschung, Band 1(2012), S. 263–274; vgl. Krüger, Kristin: IT-Sicherheit in der öffentlichen Wahrnehmung, Magedeburger Journal zur Sicherheitsforschung, Band 1(2012), S. 245–262; vgl. Schumacher, Stefan: „Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil I“, Informationsdienst IT-Grundschutz, 7; vgl. Schumacher, Stefan: „Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil II“, Informationsdienst IT-Grundschutz, 8, 8–9; vgl. Schumacher, Stefan: „Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil III“, Informationsdienst IT-Grundschutz, 10/11, 21–22; sowie weitere Vorarbeiten des Autors, siehe Literaturverzeichnis.

tatsächlich folgende Zwecke erreicht werden können:

- Abschaffung bestehender Herrschaftsverhältnisse
- Beseitigung bestehender Herrschaftseliten
- Etablierung radikaler Alternativen unter Zuhilfenahme von Gewalt, Schrecken und Terror(ismus).
- Zugleich soll aber auch in Teilen der Bevölkerung Sympathie und Unterstützungsbereitschaft erzielt werden.

Aus politikwissenschaftlicher, politischer und auch rechtlicher Sicht ist es notwendig, Cyber-Terrorismus vom Phänomen Cyber-Krieg und Cyber-Kriminalität abzugrenzen. Aus technischer Sicht ist dies meist irrelevant, da es in der technischen bzw. informatischen Diskussion von IT-Sicherheit in der Regel irrelevant ist ob ein Angreifer aus kriegerischen, kriminellen oder terroristischen Motiven heraus handelt. Werden *Buffer Overflows*[3] oder *Cross Site Request Forgeries*[4] ausgenutzt, sind die Motive des Angreifers meist irrelevant und spielen nur in der Strafverfolgung eine Rolle. Für die Politikwissenschaft ist es hingegen äußerst relevant, ob ein Angreifer Industriespionage für eine fremde Macht betrieben hat oder ein gelangweilter Schüler in den Ferien ein paar Webseiten *cracken* wollte. Der vorliegende Aufsatz versteht sich als interdisziplinär, nimmt aber vorwiegend die technische Sichtweise ein.

Analog zu diesem Aufsatz über Cyber-Terrorismus hat der Autor bereits in Vorwerken[5] die Frage nach dem Cyber-Krieg ausgiebig diskutiert, daher werden die Ergebnisse hier nur kursorisch wiedergeben.

Die bekannteste Definition von Krieg nahm Clausewitz (1832) vor: „Der Krieg ist also ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen.“[6] 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 und diesem übergeordnet werden.

3 Wenn zu große Datenmengen in einen dafür zu kleinen Speicherbereich (Buffer) geschrieben und somit Daten überschrieben werden. Siehe: http://www.pcmag.com.

4 CSRF ist eine *Websiten*-übergreifende Anfragenfälschung, siehe: http://www.techopedia.com.

5 Vgl. Schumacher, Stefan: „Timeo Danaos et dona ferentes: Zur Funktionsweise von Schadsoftware“, 2012(b), S. 45–78; vgl. Schumacher, Stefan: „Vom Cyber-Frieden“, 2012(c), S. 1–26, 337–361; Schumacher, Stefan: „Vom Cyber-Kriege“, 2012 (d), S. 1–26; vgl. Schumacher, Stefan: „Vom Cyber-Frieden“, 2013, 354–369.

6 Von Clausewitz, Carl: Vom Kriege, Berlin 1832.

In der Analyse des Phänomens Cyber-Krieg anhand der Definition von Clausewitz kommt der Autor zu dem Schluss, dass der Begriff Cyber-Krieg unangemessen ist, da es gegenwärtig nicht möglich ist, einen Gegner allumfassend zur Erfüllung eines Willens per Internet zu zwingen.

Doch wenngleich der Begriff Cyber-Krieg übertrieben und keine neue Form des Krieges im Internet möglich ist, sind Angriffe auf die IT-Infrastruktur durch staatliche Akteure dennoch durchführbar. Diese geschehen aber im Rahmen der elektronischen Kampfführung als Teil eines Krieges, wie dies bereits seit dem Ersten Weltkrieg der Fall ist. Eine neue Dimension oder gar Form des Krieges *sui generis* ist durch das Internet nicht entstanden.

Ein weiteres Phänomen der IT-Sicherheit ist die Cyber-Kriminalität oder Internet-Kriminalität. Auch hier liegt erst einmal die Definition[7] der klassischen Organisierten Kriminalität zu Grunde:

„Organisierte Kriminalität ist die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,

- unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder
- unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken. Der Begriff umfasst nicht Straftaten des Terrorismus."

Analog zum Cyber-Terrorismus ist organisierte Cyber-Kriminalität damit organisierte Kriminalität, die komplett, oder zumindest in großen Teilen, im Internet stattfindet. Cyber-Kriminalität kann ohne das Internet nicht funktionieren. Damit können beispielsweise Betrügereien via *eBay* o. ä. ausgeschlossen werden, da derartige „Maschen" auch über Kleinanzeigen in Zeitungen funktionieren können und nicht direkt eine neue Form der Kriminalität darstellen. Der Begriff Cyber-Kriminalität ist enger gefasst als die Definitionen der Internet- und Computer-Kriminalität der deutschen Polizeien.

Cyber-Kriminalität ist hier von Interesse, da es bei den Akteuren Überschneidungen zwischen terroristischen und kriminellen Gruppen geben kann. So nutzen beispielsweise auch terroristische Gruppen kriminelle Methoden wie Kreditkarten- oder Scheckbetrug, um an Geld zu gelangen. Außerdem besteht die Möglichkeit, dass kriminelle Gruppen aus (zugleich) politischen oder religiösen Motiven terroristische Taten begehen oder von terroristischen Gruppen quasi als „Subunternehmer" beauftragt werden.

7 Vgl. Richtlinie über die Zusammenarbeit von Staatsanwaltschaft und Polizei bei der Verfolgung der Organisierten Kriminalität Gem. RdErl. d. MJ u. d. MI v. 16.07.2008, 4208-S4.84, P23.23-12334/4 (Nds.MBl. Nr.30/2008 S.825) -VORIS 21021.

## 2. Akteure und deren Motive sowie Handlungskompetenzen

Neben einer juristischen bzw. politikwissenschaftlichen Nomenklatur von Akteuren wie beispielsweise Soldat, Zivilist, Terrorist, Krimineller etc. gibt es auch in der Hackerszene eine eigene Klassifizierung der Akteure. Dies geschieht hier in der Regel basierend auf der technischen Handlungskompetenz, also den Fertigkeiten im Umgang mit Informationstechnologie und Sicherheitsmaßnahmen. Dies ist notwendig, um das technische Know-how und damit das Angriffs- und Schadenspotenzial einzuschätzen. Außerdem muss in der weiteren Forschung über terroristische Gruppen abgeschätzt werden, wie der Nachwuchs bezüglich IT-Sicherheit bzw. Angriffen auf IT-Systeme ausgebildet ist und wird. So wäre es vorstellbar, dass beispielsweise wohlhabende Unterstützer von terroristischen Gruppen einzelne Mitglieder zum Informatik-Studium „delegieren" und ein Stipendium bereitstellen. Diese studierten Informatiker könnten sodann mit der Sicherung der eigenen Infrastruktur oder auch Angriffen auf lohnende Ziele beauftragt werden.

Die wichtigste Unterscheidung in der Sicherheitsszene ist die zwischen Hackern und *Script Kiddies*. Raymond definiert *Script Kiddies* als:

„[t]he lowest form of cracker; script kiddies do mischief with scripts and rootkits written by others, often without understanding the exploit they are using. Used of people with limited technical expertise using easy-to-operate, pre-configured, and/or automated tools to conduct disruptive activities against networked systems. Since most of these tools are fairly well-known by the security community, the adverse impact of such actions is usually minimal."[8]

*Script Kiddies* zeichnen sich also dadurch aus, dass sie vorgefertigte Programme nutzen um Rechner anzugreifen oder Sicherheitslücken auszunutzen. In der Regel wissen sie dabei nicht, wie diese Programme und die ausgenutzten Sicherheitslücken funktionieren. Sie werden von Hackern und IT-Sicherheitsexperten „verachtet", da sie eben über eine kaum ausgeprägte Handlungskompetenz verfügen, aber durch ihre Angriffe durchaus Schaden anrichten können. Zwar sind die meisten eingesetzten Scripte bekannt und es wurden bereits Gegenmaßnahmen entwickelt und bereitgestellt, allerdings sind viele IT-Systeme nicht auf dem aktuellsten Stand und können daher trotzdem Opfer solcher Angriffe werden.

In den letzten Jahren wurde auch der Gebrauch von verschiedener sicherheitsrelevanter *Software* immer weiter vereinfacht. War es vor 15 Jahren noch äußerst komplex Netzwerke auf Sicherheitslücken hin zu überprüfen, wurden in der Zwischenzeit diverse Softwarepakete entwickelt, die diese Aufgaben

8 Raymond, Eric: The Cathedral and the Bazaar, Sebastopol 1999.

weiter vereinfachen. Dadurch können auch technisch weniger versierte Anwender mithilfe von *Zenmap*, *Nessus*, *Metasploit* oder *Armitage* Sicherheitslücken finden und ausnutzen. Damit steigt das Schadenspotenzial von *Script Kiddies* enorm an. *Hacker* dagegen sind:

„1) A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. RFC1392, the Internet Users' Glossary, usefully amplifies this as: A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. [...]", ein Cracker hingegen ist „One who breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of hacker [...]."[9]

*Hacker* und *Cracker* unterscheiden sich von *Script Kiddies* durch ihr technisches Verständnis und ihre Handlungskompetenz im Gebrauch von Informationstechnologie. Die Unterscheidung von *Hacker* und *Cracker* basiert mehr auf dem „ethischen Hintergrund" der Handlung. Als *Cracker* werden demnach in der Regel Kriminelle bezeichnet, bzw. jene die nicht der Hackerethik folgen. Die Hackerethik wurde erstmals von Levy[10] niedergeschrieben und für den deutschsprachigen Raum vom *Chaos Computer Club*[11] adaptiert und erweitert. Sie lautet:

- Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Misstraue Autoritäten – fördere Dezentralisierung.
- Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftliche Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können dein Leben zum Besseren verändern.
- Mülle nicht in den Daten anderer Leute.
- Öffentliche Daten nützen, private Daten schützen.

Die Hackerethik ist gerade in Deutschland viel diskutiert worden und dient auch der Rechtfertigung von Hacker-Experimenten sowie zur Konstruktion des Selbstbildes von Hackern. Interessant wird sie dann, wenn diskutiert werden soll, ob terroristische Gruppen *Hacker* rekrutieren oder zur eigenen Ausbildung nutzen können.

Während die Abwehr von Script-Kiddie-Attacken vergleichsweise einfach ist, ist es wesentlich schwerer einen guten *Hacker* oder *Cracker* abzuwehren, da diese über höhere technische Handlungskompetenz verfügen. Ein Beispiel dafür befindet sich weiter unten im Text, mit *Mafiaboys* Stacheldraht-Attacke auf *Amazon* und *eBay*.

9 Raymond, The Cathedral and the Bazaar.
10 Vgl. Levy, Steven: Hackers: heroes of the computer revolution, New York 1984.
11 Vgl. Chaos Computer Club (Hg.): „Hackerethik", o.D., http://www.ccc.de.

Neben *Script Kiddies*, Hackern und Crackern kann man Akteure auch nach ihrer formalen Qualifikation klassifizieren. Ein typisches Kennzeichen von Hackern et. al. sind die non-formalen und informellen Lernprozesse, in denen die Handlungskompetenz erworben wird.

Die Diskussion um derartige Lernprozesse entstammt der Berufsbildungsforschung bzw. dem Forschungsfeld „Lebenslanges Lernen" bzw. der Anerkennung von Kompetenzen, die außerhalb der formalen Bildungssysteme erworben wurden. Diese ist notwendig, um zum einen formale und non-formale Kompetenzen und Qualifikationen abzugrenzen (Dipl.-Inf. vs. *Hacker*), zum anderen aber auch um die potenzielle Nachwuchsgewinnung und Ausbildung und damit den Kenntnisstand terroristischer oder krimineller Gruppen sowie von Sicherheitsbehörden zu untersuchen und abzugrenzen.
Die Kommission der Europäischen Gemeinschaften[12] (2000, S. 9f) definiert daher wie folgt:

- Formales Lernen findet in Bildungs- und Ausbildungseinrichtungen statt und führt zu anerkannten Abschlüssen und Qualifikationen.
- Nicht-formales Lernen findet außerhalb der Hauptsysteme der allgemeinen und beruflichen Bildung statt und führt nicht unbedingt zum Erwerb eines formalen Abschlusses. Nicht-formales Lernen kann am Arbeitsplatz und im Rahmen von Aktivitäten der Organisationen und Gruppierungen der Zivilgesellschaft (wie Jugendorganisationen, Gewerkschaften und politischen Parteien) stattfinden. Auch Organisationen oder Dienste, die zur Ergänzung der formalen Systeme eingerichtet wurden, können als Ort nicht-formalen Lernens fungieren (z. B. Kunst, Musik- und Sportkurse oder private Betreuung durch Tutoren zur Prüfungsvorbereitung).
- Informelles Lernen ist eine natürliche Begleiterscheinung des täglichen Lebens. Anders als beim formalen und nicht-formalen Lernen handelt es sich beim informellen Lernen nicht notwendigerweise um ein intentionales Lernen, weshalb es auch von den Lernenden selbst unter Umständen gar nicht als Erweiterung ihres Wissens und ihrer Fähigkeiten wahrgenommen wird.

Formales Lernen ist damit beispielsweise die in Deutschland mögliche Berufsausbildung zum Fachinformatiker oder ein Studium der Informatik oder verwandte Studiengänge (Elektrotechnik, Mathematik etc.). Auch Polizisten oder Soldaten werden in der Regel formal im Bereich IT oder IT-Sicherheit ausgebildet.

*Hacker*, *Cracker* und in geringerem Maße auch *Script Kiddies*, erwerben ihre Handlungskompetenz in der Regel durch informelles und non-formales Lernen. Dieses Lernen erfolgt entweder auf eigenes Bestreben hin und ist intrinsisch motiviert oder wird in nicht-formalen Vereinigungen und Lernsettings vermittelt. Beispiele hierfür sind der *Chaos Computer Club* und seine Konferenzen, *Hackerspaces*, Anwendervereinigungen wie die *German Unix User Group* oder Veranstaltungen wie die Chemnitzer Linux-Tage. Diese

12 Kommission der Europäischen Gemeinschaften (Hrsg.): „Memorandum für Lebenslanges Lernen", 30.10.2000, bologna-berlin2003.de.

nicht-formalen Organisationen sind mitunter wesentlich flexibler als eine Universität oder das Berufsbildungssystem und können daher auch allerneueste Entwicklungen berücksichtigen bzw. bringen diese erst hervor. Dabei schließen sich diese Lernformen aber nicht gegenseitig aus, ein *Hacker* kann durchaus ein Diplom-Informatiker sein. Ein Fachinformatiker kann auch in einem *Hackerspace* aktiv sein.

*Hacker* verfügen oftmals über Zugang zu neueren Erkenntnissen über IT-Sicherheitsprozesse, sind intrinsisch motiviert sich weiterzubilden und verfügen aufgrund der informellen Prozesse auch über eine gut entwickelte Methodenkompetenz, mit der sie sich unterschiedliche Lernbereiche *selbständig* erschließen können.

Wollte eine terroristische Gruppe einzelne Mitglieder für Angriffe auf IT-Systeme ausbilden, würden diese mutmaßlich zuerst formal ausgebildet werden (Informatikstudium, o. ä.), um anschließend in die Hackerszene eintauchen zu können und sich dort selbständig neue Handlungskompetenzen anzueignen. Allerdings bleibt hierbei fraglich, ob ein derartiger Perspektivterrorist in seinem terroristischen Weltbild verhaftet bleibt, wenn er über längere Zeit mit der Hackerszene in Kontakt ist. Fraglich ist auch, ob Salafisten aufgrund Ihres Weltbildes Zugang zur Hackerkultur finden und diese akzeptieren. Mit der Hackerszene enger verbandelte Gruppierungen wie *Anonymous* haben schon eher Zugang zu Gruppierungen aus der Szene oder überschneiden sich dabei bereits.

## 3. Angriffsziele, Angriffsvektoren und deren Schadenspotenziale

In der Informatik bezeichnet man einen möglichen Angriffsweg bzw. die dabei genutzte Methode als Angriffsvektor. Möchte man ein System angreifen oder absichern, ist es notwendig, alle möglichen Angriffsvektoren zu finden und zu identifizieren. Der Angreifer kann einen Angriffsvektor dann ausnutzen um ein System unter seine Kontrolle zu bringen, der Verteidiger muss den Angriffsvektor schnellstmöglich schließen.

Für die Analyse von Cyber-Terrorismus ist es notwendig, potentiell anzugreifende Systeme und deren potenzielle Angriffsvektoren zu identifizieren sowie deren Schadenspotential zu bestimmen.

Ob es „Gewaltakte“ gegen Computer- oder Netzwerksysteme geben kann ist unklar, schließlich bezeichnet § 303 StGB den Vorgang als Sachbeschädigung, bzw. präziser in §§ 303a und 303b StGB als Datenveränderung und Computersabotage. Dennoch kann man auch diese Vorkommnisse als Gewalt gegen Sachen bezeichnen. Außerdem besteht immer die Möglich-

keit, durch Datenveränderung und Computersabotage IT-Systeme derart zu manipulieren, dass Menschen in ihrer körperlichen Unversehrtheit eingeschränkt werden.

Angriffe auf IT-Systeme, die über die Fähigkeiten eines primitiven *Script Kiddies* hinausgehen, werden in der Regel systematisch vorbereitet, geplant und durchgeführt. Derartige Angreifer agieren meistens in Gruppen, die gemäß obiger Definition temporär oder dauerhaft zusammengesetzt sind. Die Abgrenzung zur elektronischen Kampfführung von Streitkräften müsste vorwiegend über die Zusammensetzung der Gruppe erfolgen. Sind die Angreifer Angehörige der Streitkräfte oder anderer staatlicher Organisationen im Sinne des Kriegsvölkerrechtes und handeln im staatlichen Auftrag, handelt es sich um einen kriegerischen Akt. Sind die Angreifer keine Angehörigen der staatlichen Organe, handelt es sich entweder um Kriminelle oder Terroristen. Terroristen verfolgen, anders als Kriminelle, keine (reine) Gewinnerzielungsabsicht, sondern die bereits erwähnten (z.B. religiös motivierten) politischen Ziele, insb. die Abschaffung der bestehenden Herrschaftsverhältnisse.

Die Analyse gestaltet sich schwierig, da dies bisher nur in Gedankenexperimenten möglich ist. Dazu muss aus technischer Sicht bzw. als Technikfolgenabschätzung geklärt werden, ob die Herrschaftsverhältnisse tatsächlich wie avisiert abgeschafft werden können, indem Gewaltakte im Internet durchgeführt werden. Dazu dient im Folgenden die technische Gefährdungsanalyse der potenziellen Opfersysteme.

Derartige Gefährdungsanalysen kann man zum einen als Organisation selbst durchführen, beispielsweise in dem man die ISO 27001 anwendet.[13] Vereinfacht ausgedrückt werden dazu eine Übersicht möglicher Angriffsziele aufgestellt und mögliche Schadensfälle sowie deren Eintrittswahrscheinlichkeit berechnet. Anschließend gewichtet man die Abhängigkeit bzw. Wichtigkeit des Angriffsziels und priorisiert entsprechende Schutzmaßnahmen. Die zentrale Frage ist daher: „Wie hoch ist die Wahrscheinlichkeit, dass ein *Asset* ausfällt und was passiert wenn es ausfällt?“ bzw. „Kann ein ausgefallenes oder manipuliertes *Asset* Menschen schädigen?“.

Eine weitere gängige Möglichkeit einer Gefährdungsanalyse 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.

13 Vgl. Feyrer, Hubert: Eine DIN für IT-Sicherheit? Ein Fallbeispiel, 2012, S. 191–214; vgl. Kudrass, Robert: Datenschutz, IT-Sicherheit, Betriebsschutz: Unternehmensentscheidungen zwischen gesetzlichem Zwang und betrieblicher Notwendigkeit, 2012, S. 171–190.

Dieses Vorgehen ist die praktikabelste Möglichkeit um die Sicherheit eines Systems zu überprüfen. Zudem besteht in der Theorie noch die Variante die Sicherheit oder Fehlerfreiheit eines technischen Systems mathematisch zu berechnen, also zu verifizieren. Jedoch bestehen Systeme nicht nur aus technischen Anlagen, die noch verlässlich berechenbar wären, sondern auch aus Menschen bzw. Interaktionen von und mit Menschen. Diese sind dann kaum mehr sicher berechenbar.[14] Auch die Komplexität eines technischen Systems ist nur bedingt berechenbar, da der Rechenaufwand sehr hoch ist. Man kann theoretisch 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 Belastungstests 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 Schwachstellen aufzuspüren.

Um einen Pen-Test durchzuführen einigt man sich mit dem Auftraggeber auf ein Ziel. Im Rahmen der vorliegenden Analyse ist die Frage ob man beispielsweise gegen Deutschland einen „Krieg im Internet“ führen kann. Dazu werden zunächst alle notwendigen Assets identifiziert, die dazu genutzt werden können dieses Ziel zu erreichen. Diese Assets werden dann auf sogenannte Angriffsvektoren hin untersucht. Wie bereits angedeutet ist ein Angriffsvektor ein „Einfallstor“ für einen Angreifer um Rechte auf einem System zu erlangen. Waren in mittelalterlichen Städten beispielsweise Schwachstellen in der Stadtmauer, die Stadttore oder die Wasserversorgung Angriffsvektoren, so sind dies in modernen IT-Systemen in der Regel Authentifikationsmechanismen (Passwörter, PINs, ID-Karten und ähnliches) oder Sicherheitslücken in Anwendungsprogrammen.[15] 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.

14 Vgl. Schumacher, Stefan: „Die psychologischen Grundlagen des Social Engineerings“, Magdeburger Journal zur Sicherheitsforschung, 2011(b).

15 Vgl. Hofmann, Frank: Sichere Benutzer-Authentifikation an sensiblen IT-Systemen, Magdeburger Journal zur Sicherheitsforschung, Band 2(2012), S. 103–118; vgl. Kohl, Michael: Penetrationstests mit Metasploit, Magdeburger Journal zur Sicherheitsforschung, Band 2(2012), S. 137–152.

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

Mögliche Angriffsvektoren für die vorliegende Analyse, welche auf ihre Sicherheit hin untersucht werden sollen, sind:

- 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)
- Steueranlagen in der Luft-und Raumfahrt, Drohnensteuerung

Nachdem eine solche Liste erstellt ist, können die identifizierten Assets gewichtet und priorisiert werden. Beispielsweise ist ein 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 werden die Assets systematisch auf Schwachstellen hin untersucht, welche dann wiederum selbst gewichtet und priorisiert werden sowie idealerweise geschlossen werden. Leider können in der Praxis nicht alle bekannten Sicherheitslücken in akzeptabler Zeit geschlossen werden; einige aus verschiedenen Gründen 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 „von außen“ einzuschätzen und verlässlich zu bestimmen. Hier sind empirische Detailuntersuchungen notwendig.

Fakt ist aber auch, dass die IT-Sicherheit ein vorrangig technisches und organisatorisches Problem ist und von den Betreibern der IT-Anlagen gelöst werden muss. Die beste Abwehrmaßnahme gegen Angriffe jedweder Art ist eine Absicherung der Anlagen nach dem gegenwärtigen Stand der Technik.

## 4. *Distributed-Denial-of-Service*-Angriffe als Beispiel

Eine *Denial-of-Service*-Attacke ist eine Angriffsform, bei der ein Server, der einen bestimmten Dienst anbieten soll durch Überlastung „außer Gefecht“ ge-

setzt 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, indem er beispielsweise mit seinem eigenen Rechner den angebotenen Dienst (zum Beispiel eine Netzseite) immer wieder abruft. Da heutzutage ein einzelner Rechner mit einer Endkunden-Internetanbindung nicht mehr ausreicht um einen groß 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.

Hinsichtlich der Strafverfolgung ist hier die Herrschaft über einen Rechner, der ggf. ein Zombie ist, problematisch. Selbst wenn es gelingt den Angreifer (also Zombierechner) zu identifizieren, ist noch nicht sichergestellt, dass 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 Probleme der Rückverfolgung einer Tat existieren.

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 Jahre 2000, als ein 15-jähriger kanadischer Schüler mit dem Alias *Mafiaboy* mehrere US-Amerikanische Server mit dem deutschen dDoS-Tool *Stacheldraht*[17] lahmlegte und nach Medienberichten einen Schaden in Höhe von 1,7 Milliarden kanadischen Dollar anrichtete. Bei *Mafiaboy* handelt es sich übrigens nicht um einen Hacker, sondern um ein *Script Kiddie*.

16 Vgl. Ruef, Marc: „Labs: LOIC-Attacken abwehren – DDoS im Umfeld von Wikileaks“, 19.12.2010, scip.ch.

17 Vgl. Cheng, Geoffrey: „Malware FAQ: Analysis on DDOS tool Stacheldraht v1.666“, sans.org, o.D.

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

Interessant ist hierbei vor allem die wahrscheinliche Verbindung von Banden der Organisierten Cyber-Kriminalität und politischen Akteuren. So wird aufgrund verschiedener Indizien gemutmaßt, dass die *Putin*-nahe Jugendorganisation *Naschi* in Russland ansässige Cyber-Kriminelle damit beauftragt und dafür bezahlt hat, estnische und georgische Webseiten anzugreifen. Dies wäre eine politisch motivierte Tat von (teilweise) nichtstaatlichen Akteuren, die darauf abzielte die Herrschaftssverhältnisse in dem angegriffenen Land zu destabilisieren.

## 5. Verdeckte Kommunikation durch Terroristen

Vor allem islamistische terroristische Gruppen sind vorwiegend in losen Netzwerken statt in starren Hierarchien organisiert. Dies ermöglicht ihnen größere Flexibilität in der Planung und Durchführung von Attentaten und höhere Resilienz bei der Aufdeckung oder Ausschaltung von Teilen der Organisation.[20]

Flexible Netzwerkstrukturen zeichnen sich durch die genannten Eigenschaften positiv aus, erfordern aber einen höheren und vor allem komplexeren Kommunikationsaufwand als klassische Organisationsformen.[21] Daher sind gerade terroristische Netzwerke darauf angewiesen, sicher und verdeckt zu kommunizieren.

Baehr[22] beschreibt die Möglichkeiten salafistischer Propaganda im Internet. Dazu nutzen salafistische Gruppen offene Kommunikationsformen zur Nachwuchsgewinnung und Propaganda, beispielsweise Diskussionsforen, Mailinglisten, Netzseiten oder Videoplattformen, um professionell aufberei-

18 Vgl. Anderson, Nate: „Massive DDos attacks target Estonia, Russia accused“,14.05.2007, arstechnica.com.

19 Vgl. Moses, Asher: „Georgian Websites Forced Offline in Cyber War“, 12.08.2008, smh.com.

20 Vgl. Ritzmann, Alexander: „Strukturen des Terrors: Wie al-Qaida und Hisbollah sich organisieren und was der Tod Osama Bin Ladens für al-Qaida bedeutet, BIGS Policy Paper“, 17.06.2011, wordpress.com.; vgl. Sageman, M.: Leaderless Jihad: Terror Networks in the Twenty-First Century, Pennsylvania 2011; vgl. Steinberg, G.: Der nahe und der ferne Feind: Die Netzwerke des islamistischen Terrorismus, München 2005.

21 Vgl. Davidow, W/Malone, M.: The virtual corporation: structuring and revitalizing the corporation for the 21st century, New York 1992; vgl. Raymond, The Cathedral and the Bazaar.

22 Vgl. Baehr, „Salafistische Propaganda im Internet: Von der reinen Mission bis zum globalen Jihad – Die wesentlichen ideentheoretischen Unterschiede unter den salafistischen Strömungen in Deutschland“.

tete Videos und Magazine zu verbreiten. Derartige Angebote sind vergleichsweise öffentlich und daher relativ einfach aufzuklären und zu infiltrieren oder abzuschalten.

Daneben nutzen terroristische Gruppen aber auch elektronische Kommunikation zur Steuerung der Zellen und zur Planung von weiteren Anschlägen. Diese Kommunikation aufzuklären und zu infiltrieren ist daher eines der wichtigsten Ziele der Terrorismusbekämpfung und zumindest in der offiziellen Darstellung Hauptzweck der globalen Überwachungssysteme Echelon[23], PRISM[24], Tempora und Co.

Theoretisch ist es für Jedermann – auch Terroristen – möglich, elektronische Kommunikation zu schützen. So gibt es die Möglichkeiten, sich unerkannt im Internet zu bewegen, in dem man Anonymisierungsdienste wie TOR oder *Remailer* über sogenannte Mixkaskaden nutzt.[25] Außerdem können Dateien, Festplatten oder E-Mails verschlüsselt werden, um sie vor unbefugtem Mitlesen oder gar Manipulation zu schützen.[26] Die dazu notwendige Software steht meist als *Open-Source-Software* bereit und kann daher sehr einfach beschafft und eingesetzt werden. *Duncan Campbell* hat dazu auf der *DeepSec* 2011, einer jährlichen IT-Sicherheitskonferenz in Wien, die *Keynote* gehalten. Der britische Journalist hat dazu Unterlagen der britischen Sicherheitsbehörden ausgewertet und überprüft, wie Terroristen verschlüsseln[27]. Er beschreibt darin die sogenannte *Encyclopedia of the Afghan Jihad*, einem Handbuch mit Anweisungen zu Waffen, Sprengstoffen, militärischen Taktiken und Strategien sowie Formen der Aufklärung. Dieses Handbuch zirkuliert seit der Zeit der Besatzung Afghanistans durch die Sowjetunion in gedruckter Form vor allem in Afghanistan und Pakistan. Mitte der 1990er-Jahre erweiterten in den USA aufgewachsene Dschihadisten das Handbuch um IT-Sicherheitstechniken, vor allem PGP zur E-Mailverschlüsselung. Campbell beschrieb in seiner *Keynote*, wie unbedarft al-Qaida bezüglich IT-Sicherheit vorgeht. Anstatt E-Mails verschlüsselt und anonymisiert zu versenden, wurden E-Mails einfach als Entwurf gespeichert und mehrere Terroristen teilten sich den Benutzernamen und das Passwort zum *Account*. Sie hofften dadurch nicht aufzufallen, weil der Text nie als E-Mail durch das Netz ging. Als weitere „Sicherungsmaßnahme" nutzten die Terroristen Codewörter – statt von Wasserstoffperoxid sprachen sie eben von *Aftershave*.

23 Vgl. vor allem die Echelon-Papiere von Heise, die in die 1990er Jahre zurückreichen: Heise online (Hrsg.): „Echolon", heise.de, o.D.

24 Vgl. o.V.: „Friedrich lässt sich von Prism überzeugen", 13.07.2013, stern.de..

25 Vgl. Kubieziel, Jens: Anonymität im Internet, Magdeburger Journal zur Sicherheitsforschung, Band 1(2012), S. 79–90.

26 Vgl. Schumacher, Stefan: „Timeo Danaos et dona ferentes: Zur Funktionsweise von Schadsoftware", 2012(a), S. 45–78.

27 Vgl. Campbell, Duncan: „How Terrorists Encrypt: Threatscape Overview", 09.08.2012, privacy-pc.com. Videomitschnitt unter: 06.08.2013, http://www.youtube.com.

Die ausschnittartige Analyse zeugt nicht eben von technischem Know-how oder gar von tiefergehendem Verständnis von IT-Sicherheit oder Überwachungsstrukturen. Dies verleitet zu der Annahme, dass zumindest al-Qaida nicht „in der Breite" über Mitglieder oder Sympathisanten verfügt, die in der Lage sind erfolgreiche Angriffe im Internet durchzuführen.

Dies kann bei anderen Gruppen jedoch anders sein, vor allem Netzwerke wie *Anonymous* verfügen durchaus über Kontakte zu Personen mit sehr hohem technischen Know-how und mitunter dem Willen auch Straftaten zu begehen. In der seit 2010 laufenden *Operation Payback* werden Server von Strafverfolgungsbehörden, Verwertungsrechteinhabern oder Finanzdienstleistern mit dDoS-Attacken angegriffen. Besonders prominent ist hierbei der Angriff auf Finanzdienstleister, die die Konten von *Julian Assange* oder *Wikileaks* geschlossen haben. Daraufhin riefen Teile des Anonymous-Netzes zu Angriffen gegen *Paypal*, *Postfinanz*, *Visa* und *Mastercard* auf, welche mit dem *Script Low Orbit Ion Cannon* durchgeführt wurden. Das *Script* ist ein einfaches Programm, welches sehr viele Anfragen in sehr kurzer Zeit an einen Server schickt und ihn damit überlasten kann. Im Zuge der Ermittlungen konnten die niederländischen Strafverfolgungsbehörden einen 16-jährigen festnehmen, welcher gestanden hat an den Angriffen beteiligt zu sein.[28] Das Anonymous-Netzwerk war zwar in der Lage mehrere Webserver lahmzulegen, diese sind aber nur für die Bereitstellung der Netzseite verantwortlich und nicht für das Funktionieren der Finanzdienstleistungen. Die Angriffe sind eher primitiv und nicht einmal anonymisiert, so dass einige Angreifer relativ einfach identifiziert werden konnten. Diese lassen sich höchstens als *Script Kiddies* bezeichnen, nicht jedoch als *Hacker* oder Sicherheitsexperten.

## 6. Fazit

Cyber-Terrorismus als neue, andere Form des Terrorismus *sui generis* existiert offenbar nicht. Es ist zumindest bisher nicht möglich, durch Angriffe im Internet bestehende Herrschaftsverhältnisse abzuschaffen und bestehende Herrschaftseliten zu beseitigen. Solange es Alternativen und Ausweichmöglichkeiten zu vernetzten Systemen gibt, können Internet-Angriffe Herrschaftseliten oder Gesellschaften nur begrenzt zu einem gesellschaftlichen Wandel bewegen.

Terroristen nutzen das Internet dennoch als Operationsraum, sei es als „klassischer Nutzer" von Angeboten, indem beispielsweise Propagandavideos veröffentlicht, Diskussionsforen betrieben oder einfach E-Mail-Dienste

28 Vgl. Ihlenfeld, Jens: „16-Jähriger wegen DDoS-Angriffen festgenommen", 10.12.2010, golem.de.

gebraucht werden. Es ist jedoch auch möglich Angriffe gegen IT-Systeme durchzuführen, dann aber vorwiegend zur Unterstützung konventioneller Attacken. Militärisch würde dies als elektronische Kampfführung bezeichnet werden. Möglich sind hierbei Spähattacken zur Aufklärung von Informationen, dDoS-Attacken um Systeme lahmzulegen oder im beschränkten Maße auch Angriffe auf Steuerungtechnik um Industrieanlagen lahmzulegen.

Aus sicherheitspolitischer Sicht ist es weiterhin notwendig, Terroristen zu überwachen und deren Kommunikation, Kenntnisstand sowie Methoden zu analysieren. Terroristische Gruppen gelangen zunehmend an entsprechendes Know-how. Zudem ist vorstellbar, dass sich technisch versierte Gruppen radikalisieren. Auch eine Kooperation beider Gruppentypen kann stattfinden.

Aus technischer Sicht ist die Frage nach dem Cyber-Terrorismus weniger relevant. Mögliche cyber-terroristische Angriffe sind in der technischen Dimension von kriminellen Angriffen oder Geheimdienstoperationen kaum zu unterscheiden. Es ist aus technischer Sicht belanglos ob ein *Buffer Overflow* oder ein schwaches Passwort durch ein *Script Kiddie*, einen Terroristen oder einen staatlichen/militärischen Akteur ausgenutzt wird. Die Schutzmaßnahmen sind von der Intention des Angreifers nicht abhängig.

Hinsichtlich der Identifikation von möglichen Angriffszielen und der Analyse der *Assets* sollten jedoch terroristische Motivationen berücksichtigt und bezüglich der Abwehr Eingang in die jeweiligen Sicherheitsrichtlinien finden.

Zur Abwehr von möglichen Angriffen sind auf der Seite potenzieller Opfer die üblichen technischen und organisatorischen Maßnahmen durchzuführen und die IT-Systeme entsprechend abzusichern. Die rechtstaatliche Überwachung von terroristischen Gruppierungen ist notwendig, um den Aufwuchs technischer Fähigkeiten bei terroristischen und extremistischen Akteuren nachzuverfolgen. Des Weiteren ist anzunehmen, dass terroristische Gruppierungen mittelfristig von kriminellen Gruppen Know-how einzukaufen versuchen, da das vergleichsweise günstige, schnelle und Aufmerksamkeiterregende verüben von Angriffen im *Cyberspace* durchaus dem Handlungsmuster und der Motivation von Terroristen entspricht.

## Literatur


Anderson, Nate: „Massive DDos attacks target Estonia, Russia accused“, 14.05.2007, http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/, (15.10.2012).

Baehr, Dirk D: „Salafistische Propaganda im Internet: Von der reinen Mission bis zum globalen Jihad - Die wesentlichen ideentheoretischen Unterschiede unter den salafistischen Strömungen in Deutschland“, Magdeburger Journal zur Sicherheitsforschung, Band 2(2012), http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS-016.pdf, (21.10.2013).

Campbell, Duncan: „How Terrorists Encrypt: Threatscape Overview“, 09.08.2012, http://privacy-pc.com/articles/how-terrorists-encrypt-threatscape-overview.html, (13.08.2013).

Campell, Duncan: „How Terrorists Encrypt“, 06.08.2013, http://www.youtube.com/watch?v=IDOtFZDm4F0, (21.10.2013).

Chaos Computer Club (Hrsg.): „Hackerethik“, o.D., http://www.ccc.de/hackerethik, (13.08.2013).

Cheng, Geoffrey: „Malware FAQ: Analysis on DDOS tool Stacheldraht v1.666“, http://www.sans.org/security-resources/malwarefaq/stacheldraht.php, (19.04.2008).

Davidow, W/Malone, M.: The virtual corporation: structuring and revitalizing the corporation for the 21st century, New York 1992.

Feyrer, Hubert: Eine DIN für IT-Sicherheit? Ein Fallbeispiel, in: J. Sambleben, Jörg/Schumacher, Stefan (Hrsg.): Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen? – Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung, Norderstedt 2012, S. 191–214.

Flögel, Florian: Cyberwar – Systematisierung und Kategorisierung einer „neuen“ Bedrohung, (Kieler Analysen zur Sicherheitspolitik Nr. 35), Januar 2014, http://www.ispk.uni-kiel.de/fileadmin/user_upload/Kieler%20Analysen%20zur%20Sicherheitspolitik/KAzS_35_Florian_Floegel_Cyberwar.pdf, (28.02.2014).

Heise online (Hrsg.): „Echolon“, o.D., http://www.heise.de/tp/special/ech/default.html, (23.05.2013).

Hofmann, Frank: Sichere Benutzer-Authentifikation an sensiblen IT-Systemen, in: Sambleben, Jörg/Schumacher, Stefan (Hrsg.): Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen? – Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung, Norderstedt 2012, S. 103–118.

Holze, Jens: Eine Geschichte der Hackerkultur: Subkultur im Digitalen Zeitalter, in: Sambleben, Jörg/Schumacher, Stefan (Hrsg.): Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen? Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung, Norderstedt 2012, S. 263–274.

Ihlenfeld, Jens: „16-Jähriger wegen DDoS-Angriffen festgenommen“, 10.12.2010, http://www.golem.de/1012/80031.html, (13.08.2013).

Kohl, Michael: Penetrationstests mit Metasploit, in: Sambleben, Jörg/Schumacher, Stefan (Hrsg.): Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen? Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung. Norderstedt 2012, S. 137–152.

Kommission der Europäischen Gemeinschaften (Hrsg.): „Memorandum für Lebenslanges Lernen“, 30.10.2000, http://www.bologna-berlin2003.de/pdf/MemorandumDe.pdf, (13.01.2013).

Krüger, Kristin: IT-Sicherheit in der öffentlichen Wahrnehmung, in: Sambleben, Jörg/Schumacher, Stefan (Hrsg.): Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen? Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung, Norderstedt 2012, S. 245–262.

Kubieziel, Jens: Anonymität im Internet, in: Sambleben, Jörg/Schumacher, Stefan (Hrsg.): Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen? –Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung, Norderstedt 2012, S. 79–90.

Kudrass, Robert: Datenschutz, IT-Sicherheit, Betriebsschutz: Unternehmensentscheidungen zwischen gesetzlichem Zwang und betrieblicher Notwendigkeit, in: Sambleben, Jörg/Schumacher, Stefan (Hrsg.): Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen? –Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung, Norderstedt 2012, S. 171–190.

Levy, Steven: Hackers: heroes of the computer revolution, New York 1984.

Meier, Ernst-Christoph/Hannemann, Andreas/Meyer zum Felde, Rainer: Wörterbuch zur Sicherheitspolitik: Deutschland in einem veränderten internationalen Umfeld, Hamburg 2012.

Moses, Asher: „Georgian Websites Forced Offline in Cyber War“, 12.08.2008, http://www.smh.com.au/news/technology/georgian-websites-forced-offline-in-cyber-war/2008/08/12/1218306848654.html, (15.10.2012).

O.V.: „Friedrich lässt sich von Prism überzeugen“, 13.07.2013, http://www.stern.de/politik/ausland/us-ueberwachungsprogramm-friedrich-laesst-sich-von-prism-ueberzeugen-2037766.html, (21.10.2013).

O.V.: „The Jargon File (New Hackers Dictionary)”, 01.10.2004, http://www.catb.org/jargon/, (03.01.2005).

Raymond, Eric: The Cathedral and the Bazaar, Sebastopol 1999.

Ritzmann, Alexander: „Strukturen des Terrors: Wie al-Qaida und Hisbollah sich organisieren und was der Tod Osama Bin Ladens für al-Qaida bedeutet“, 17.06.2011, http://ritzmann.wordpress.com/2011/06/17/bin-ladens-nachfolge-gefahrdet-al-qaida/, (21.10.2013).

Ruef, Marc: „Labs: LOIC-Attacken abwehren – DDoS im Umfeld von Wikileaks“, 19.12.2010, http://www.scip.ch/?labs.20101219, (22.04.2011).

Sageman, Marc: Leaderless Jihad: Terror Networks in the Twenty-First Century, Pennsylvania 2011.

Sambleben, Jörg/Schumacher, Stefan (Hrsg.): Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?, Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung, Norderstedt 2012, S. 275–308.

Schumacher, Stefan: „Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil I“, Informationsdienst IT-Grundschutz, 7/2009(a), S. 11–13, http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_7-2009_11_13.pdf, (21.10.2013).

Schumacher, Stefan: „Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil II“, Informationsdienst IT-Grundschutz, 8/2009(b) , S. 8–9, http://grundschutz. info/fileadmin/kundenbereich/Dokumente/Grundschutz_8-2009_8_ 9.pdf, (21.10.2013).

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

Schumacher, Stefan: „Psychologische Grundlagen des Social-Engineering“. Die Datenschleuder: Das wissenschaftliche Fachblatt für den Datenreisenden, #94, 2010(d), S. 52–59, http://ds.ccc.de/pdfs/ds094.pdf, (10.10.2012).

Schumacher, Stefan: „Die psychologischen Grundlagen des Social Engineerings“. Magdeburger Journal zur Sicherheitsforschung, 2011(b)., http://www.wissenswerk.de/index.php/mjs, (31.01.2011).

Schumacher, Stefan: „Sicherheit messen: Eine Operationalisierung als latentes soziales Konstrukt“, in Adorf, Stella/Schaffeld, Jan-Florian/Schössler, Dietmar (Hrsg.): Die sicherheitspolitische Streitkultur in der Bundesrepublik Deutschland: Beiträge zum 1. akademischen Nachwuchsförderpreis Goldene Eule des Bundesverbandes Sicherheitspolitik an Hochschulen (BSH), Magdeburg 2011, S. 1–38.

Schumacher, Stefan: „Timeo Danaos et dona ferentes: Zur Funktionsweise von Schadsoftware“, in J. Sambleben, Jörg/S. Schumacher, Stefan (Hg.), Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?, Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung. Norderstedt 2012(a), S. 45–78.

Schumacher, Stefan S.: „Vom Cyber-Frieden“, in J. Sambleben, Jörg/S. Schumacher, Stefan (Hg.), Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?, Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung. Norderstedt 2012(c), S. 1–26, S. 337–361.

Schumacher, Stefan S.: „Vom Cyber-Kriege“, in: Sambleben, Jörg/Schumacher, Stefan (Hrsg.): Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?, Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung, Norderstedt 2012, S. 1–26.

Schumacher, Stefan: „Vom Cyber-Kriege: Gibt es einen Krieg im Internet?“, in: Magdeburger Journal zur Sicherheitsforschung, 2, 2012(d), S. 285–307.

Schumacher, Stefan: „Vom Cyber-Frieden“, in: Magdeburger Journal zur Sicherheitsforschung, 1, 2013(a), S. 354–369.

Steinberg, G.: Der nahe und der ferne Feind: Die Netzwerke des islamistischen Terrorismus, München 2005.

Von Clausewitz, Carl: Vom Kriege, Berlin 1832.