Florian Flögel

Cyberwar – Systematisierung und Kategorisierung einer „neuen“ Bedrohung

Kieler Analysen zur Sicherheitspolitik Nr. 35
Januar 2014

ISPK.org

Institut für SicherheitsPolitik an der Christian-Albrechts-Universität zu Kiel

Inhalt:

Florian Flögel, B.A.

Cyberwar – Systematisierung und Kategorisierung einer „neuen“ Bedrohung
Kieler Analysen zur Sicherheitspolitik Nr. 35
Kiel, Januar 2014

Lektorat:
Kira Frankenthal

Impressum:

Herausgeber:
Prof. Dr. Joachim Krause (Direktor)/Stefan Hansen, M.A. (Geschäftsführer)

Institut für Sicherheitspolitik
an der Christian-Albrechts-Universität zu Kiel
Westring 400
24118 Kiel

***ISPK*.org**

1 Einleitung und Definitionen

Die Idee vom Cyberkrieg, nachfolgend als Cyberwar bezeichnet, wurde bereits seit den späten 1980er Jahren in Militärkreisen und der Wissenschaft diskutiert. Die Auseinandersetzung mit dem Thema Sicherheit und Risiken in Netzwerken und im Cyberspace nahm nach dem Jahrtausendwechsel signifikant zu, parallel zur voranschreitenden technischen Entwicklung der IT- und EDV-Branche sowie der zunehmenden Vernetzung in geradezu allen privaten, wirtschaftlichen und staatlichen Strukturen in den entwickelten Ländern wie auch den Schwellenländern. Die Debatte erreichte 2010 ihren vorläufigen Höhepunkt mit dem Bekanntwerden der Sabotage an iranischen Atomanlagen in Natanz durch die Schadsoftware *Stuxnet*.[1] Die aktuellen Enthüllungen des *Whistleblowers Edward Snowden* über die Spähprogramme der amerikanischen NSA (PRISM) und des britischen GCHQ (TEMPORA) haben die Debatte erneut angeheizt.[2] Traditionell wurden in westlichen Staaten vor allem Russland und China als Hochburgen der offensiven staatlich gelenkten Cyberaktivitäten gehandelt. Fälle wie *Stuxnet* oder PRISM verdeutlichen, dass der Westen ebenfalls in Offensivmaßnahmen und Werkzeuge investiert hat, allen voran die USA.

Die politische und wissenschaftliche Debatte der vergangenen Jahre – und die daraus gewonnenen Einschätzungen über das tatsächliche Bedrohungsszenario sowie damit einhergehende Unsicherheitsfaktoren für die Internationalen Beziehungen – zeichnet sich durch eine ausgesprochen diffuse Gemengelage an Beurteilungen aus. Dies ist auch der Tatsache geschuldet, dass es relativ schwierig ist, valide Informationen über militärische Cyberkapazitäten oder Sicherheitsvorkehrungen zu erhalten, da diese Informationen i.d.R. staatlicher Geheimhaltung unterliegen. Dadurch entsteht viel Raum für Spekulation. Diese bewegt sich zwischen der Erkenntnis einer unmittelbar bevorstehenden globalen Katastrophe für die digitalen Informationsgesellschaften, bis hin zu einer herunterspielenden Beurteilung eines paranoiden „Cyber-Hypes“, der vor allem Sicherheitsunternehmen, Anti-Viren-Software Anbietern und politischen Kräften nutzt, die eine umfassendere Überwachung der Bürger auch in freiheitlich-demokratischen Systemen anstreben. Weitere Merkmale sind die zum Teil inflationäre Benutzung von Begriffen, die weder einheitlich noch eindeutig definiert sind, geschweige denn als international gültig und rechtskräftig angesehen werden können. Viele solcher Begriffe werden auch in dieser Arbeit Verwendung finden. Bereits der Begriff Cyberwar ist umstritten. Die Verwendung dieser teilweise fragwürdigen Begriffe lässt sich nicht vermeiden, daher ist es Absicht dieser Arbeit jene Begriffe kritisch zu hinterfragen. Diese Analyse verfolgt das Ziel, das Phänomen Cyberwar zu kategorisieren und zu systematisieren. Dazu werden die verschiedenen Ausprägungsformen, die als Cyberwar oftmals zusammengefasst sind, herausgearbeitet und ein Blick auf die beteiligten Akteure und ihre Einzelinteressen geworfen. Es wird eine kritische Abwägung der verschieden Einschätzungen und gängigen Begrifflichkeiten vorgenommen, die der Fragestellung folgt: Wobei handelt es sich im Detail beim Phänomen Cyberwar, wie gestaltet sich die bisherige politische und wissenschaftliche Diskussion und als wie gefährlich ist das Bedrohungsszenario tatsächlich einzuschätzen?

Wie bereits angemerkt existieren keine einheitlichen Definitionen der zentralen Begriffe. Aus der Schnittmenge der von den Verfassern bestehender wissenschaftlicher Abhandlungen formulierten Begriffsbestimmungen lassen sich nachfolgende Arbeitsdefinitionen erfassen:

Cyber: Wird als Präfix für alle Begriffe genutzt, die sich auf automatisierte und informationsverarbeitende Prozesse beziehen. Etymologisch lässt sich der Begriff vom griechischen *kybernetes* (zu Deutsch: Steuermann) herleiten und tritt erstmals 1948 bei Norbert Wiener im Zusammenhang mit Konzepten zu Kontrollmechanismen und Kommunikation auf.[3]

[1] Vgl. Sanger, David E.: „Obama Order Sped Up Wave of Cyberattacks Against Iran“, 01.06.2012, www.nytimes.com, (02.07.2013).

[2] Vgl. Hopkins, Nick: „UK gathering secret intelligence via covert NSA operation“, 07.06.2013, www.guardian.co.uk, (02.07.2013).

[3] Vgl. Luiijf, Eric: Understanding Cyber Threats and Vulnerabilities, in: Lopez, Javier/Setola, Roberto/

Cyberspace: Setzt sich aus allen elektronischen Geräten und Medien zusammen, die mit der Erschaffung, Speicherung, Übertragung und Verarbeitung von digitalen Daten zu tun haben. Hervorzuheben ist, dass es sich nicht ausschließlich um die Geräte und Netzwerke handelt, die mit dem Internet verbunden sind. Der Cyberspace umfasst alle Einzelteile des digitalen Raums, d.h. jede Hard- und Software, alle Netzwerke, im Prinzip alles was zur elektronischen Datenverarbeitung jeglicher Art verwendet wird, egal ob on- oder offline.[4]

Informationsbasierte Gesellschaften: Die Industriegesellschaften der entwickelten Staaten verwandeln sich zunehmend in informationsbasierte Gesellschaften (*Third-Wave-Societies)*. Diese technologisch hochentwickelten Gesellschaften sind politisch, wirtschaftlich und gesellschaftlich stark vom Funktionieren ihrer vernetzten Infrastruktur abhängig. Die Vorteile sind gesteigerte Effizienz und Effektivität durch Prozessoptimierung in Produktion, Verwaltung und Dienstleistung. Diese Entwicklung geht einher mit einer zunehmenden Privatisierung auch in sensiblen Bereichen wie kritischer Infrastruktur. Die Abhängigkeit vom Funktionieren des Gesamtkonstrukts aller Bestandteile der Infrastruktur birgt jedoch Risiken. Der Ausfall einzelner Elemente, durch Fehler oder Fremdeinwirken, kann Folgen für das gesamte System haben und zu erheblichen Unsicherheiten führen.[5]

Kritische Infrastruktur: „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“[6] Die wichtigsten Struk-turen sind die Energie- und Wasserversorgung, Telekommunikation, IT- und Transportdienstleistungen, Nahrungsmittelversorgung und das Gesundheits- und Finanzsystem.[7]

Zur Abgrenzung von zwischenstaatlichen Auseinandersetzungen im Cyberspace sollen auch die Phänomene Cyberkriminalität und Cyberterrorismus knapp definiert werden.

Cyberkriminalität: Die *Cybercrime Convention* des Europarats stellt den Begriff in einen Zusammenhang mit Straftaten durch Datenmissbrauch und Urheberrechtsverletzungen.[8] Weitere Tatbestände sind unter anderem der illegale Zugang zu Computersystemen, das Abfangen von Daten, die Manipulation von Daten und Systemen, sowie alle Verstöße bezüglich der Herstellung und Verbreitung von Kinderpornographie.[9] Das Bundeskriminalamt definiert Cyberkriminalität in einem Satz: „Der Begriff *Cybercrime* umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden.“[10]

Cyberterrorismus: Zurzeit lassen sich keine Fälle feststellen, die sich eindeutig als Cyberterrorismus einstufen lassen. Das Konzept wird aber regelmäßig in Literatur und Presse als Bedrohung kommuniziert. Entsprechend vielfältig und uneindeutig sind die jeweiligen Definitionen. In der Quintessenz kann Cyberterrorismus als „deliberate act or threat with illegal actions [...] against the integrity, confidentiality and/or availability of information, and of information processing systems and

Wolthusen, Stephen D. (Hrsg.): Critical Infrastructure Protection. Information Infrastructure Models, Analysis, and Defense, 1. Aufl., Heidelberg u.a. 2012, S. 53.

[4] Vgl. ebd., S. 54.

[5] Vgl. Beer, Thomas: Cyberwar. Bedrohung für die Informationsgesellschaft, Marburg 2005, S. 5.

[6] Bundesministerium des Inneren: Nationale Strategie zum Schutz Kritischer Infrastruktur (KRITIS), 2009, http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf, S. 4.

[7] Vgl. ebd.

[8] Vgl. o.V.: „Was ist Cyberkriminalität“, Webseite des Anti-Viren-Programm Anbieters Norton (Symantec), http://de.norton.com/cybercrime-definition, (02.07.2013).

[9] Vgl. Europarat: Convention on Cybercrime, Budapest 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, (02.07.2013).

[10] Bundeskriminalamt: Cybercrime Bundeslagebild 2011, Wiesbaden 2011, http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true, (02.07.2013), S. 5.

networks”[11] bezeichnet werden, welche(r) folgende Konsequenzen auslöst: Leiden, Verletzung/Mord von Personen, ernsthafte psychologische Effekte auf die Bevölkerung, gesellschaftliche und ökonomische Störung, Beeinträchtigung der ökologischen Sicherheit sowie eine Beeinträchtigung der politischen Stabilität und Kohäsion.[12]

2 Das Phänomen „Cyberkrieg“

Um sich dem Phänomen Cyberwar zu nähern und zu verstehen warum die öffentliche und wissenschaftliche Debatte ein teilweise hysterisches Bild der gegenwärtigen Situation und Zukunft zeichnet, sollen einige Grundlagen des Wesens und der Beschaffenheit unserer modernen IT und EDV dargestellt werden. Vorwegnehmen lässt sich, dass systemisch bedingte Schwächen und Fehlerpotentiale in der Technologie existieren, die sich nicht ohne weiteres beheben lassen.
Die Multifunktionalität der IT ermöglicht es völlig unterschiedliche Maschinen, Sensoren und komplexe Systeme miteinander zu vernetzen. Dies liegt in der Funktionsweise der IT, die mathematischen und physikalischen Gesetzen unterliegt. IT benutzt den universellen Binärcode zur Verarbeitung von Daten. Diese Daten werden in unterschiedlichen Protokollen bereitgestellt, welche durch die IT in den Binärcode „übersetzt“ wird und so die „Verständigung“ verschiedenartiger Geräte ermöglicht.[13] Der Mensch „kommuniziert“ mit den Geräten um ihnen bestimmte Handlungsanweisungen zu erteilen durch die Programmiersprache. Dieses System ist in sich unendlich, d.h. alle Programmcodes sind grundsätzlich veränderbar. Daher kann jeder Passwortschutz, jedes Anti-Viren Programm, jede Programmzeile verändert also auch „gehackt“ werden. Ein Betriebsystem wie *Windows* besteht aus 80 Millionen Zeilen Programmcode, dadurch gibt es unzählige Möglichkeiten Schwächen auszumachen und Abschnitte zu manipulieren. Die durchschnittliche Fehlerquote wird auf 1,5–5% geschätzt, da die Programmierer schlichtweg Fehler machen.[14] Natürlich wird das Risiko durch diverse Vorkehrungen minimiert, z.B. werden Programmcodes maschinell überprüft. Einhundertprozentige Sicherheit gibt es allerdings nicht. IT ist also grundsätzlich angreifbar durch unbekannte Nutzungsvarianten.[15]
Weitere Unsicherheitsfaktoren kommen durch die breite Verwendung von sogenannten *Commercial off-the-shelf* (COTS) Produkten hinzu. Hierbei handelt es sich um Soft- und Hardware Produkte der global tätigen Unternehmen wie *Microsoft*, *Apple*, *Cisco*, *IBM*, *SAP*, *Intel* u.v.a., die in vielen Bereichen genutzt werden, auch bei dem Militär und Geheimdiensten, in der Verwaltung oder in Bereichen, die direkt oder indirekt mit kritischer Infrastruktur zu tun haben. Aus diesen Produkten ist auch die Telekommunikations-Infrastruktur aufgebaut. COTS-Produkte werden trotz ihrer bekannten Sicherheitsmängel auch in sensiblen Bereichen genutzt, weil sie universell einsetzbar und kostengünstig sind, da sie keine Entwicklungskosten verursachen. IT-Hersteller leisten vor allem betriebswirtschaftlichen Prämissen Folge und priorisieren die Effizienz gegenüber der Sicherheit.[16] Des Weiteren herrschen auf dem IT-Markt in bestimmten Bereichen Monopole respektive Oligopole, d.h. die Auswahl an Produkten und Herstellern ist sehr begrenzt. Ein weiteres Problem sind die globalen Lieferketten, die sich nur unzureichend kontrollieren lassen. Hier gibt es diverse Gelegenheiten zur Manipulation der Hardware.[17] Ein aktuelles Beispiel sind die Anschuldigungen der US-Regierung gegenüber dem chinesischen Elektronikhersteller *Huawei*, der bezichtigt wird Spionagewerkzeuge in seine Produkte implementiert zu haben.[18]

[11] Vgl. Luiijf, Understanding Cyber Threats and Vulnerabilities, S. 54.
[12] Vgl. ebd.
[13] Vgl. Beer, Cyberwar, S. 13.
[14] Vgl. Gaycken, Sandro: Cyberwar. Das Wettrüsten hat längst begonnen, München 2012, S. 40.
[15] Vgl. ebd. S. 37.
[16] Vgl. Beer, Cyberwar, S. 20.
[17] Vgl. ebd., S. 21–22.
[18] Vgl. Rogers, Mike/Ruppersberger, Dutch: Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, 08.10.2012, http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf, (03.07.2013).

2.1 Cyberangriffsformen

Zur Erreichung eines bestimmten Ziels, z.B. dem Ausspähen von Daten oder dem Lahmlegen von Systemen oder Diensten, wird ein Angriffswerkzeug für das Zielcomputersystem bzw. Netzwerk benötigt. In der Regel werden dafür zunächst konventionelle Hackertools benutzt, deren Grundbausätze sogar als Freeware im Internet zu beschaffen sind.[19] Je nach Ziel kann diese Malware entsprechend modifiziert und angepasst werden. Alle öffentlich bekannt gewordenen Cyberangriffe haben sich weitestgehend dieser Mittel bedient. Es gibt verschiedene Möglichkeiten sich zu einem fremden Computer oder Netzwerk Zugang zu verschaffen. Meistens werden Sicherheitslücken der Software ausgenutzt, die auf einem PC, Server, Netzwerk oder sonstigen Geräten installiert ist. Diese Möglichkeit nennt man *Exploit*. Es gibt unterschiedliche Arten von *Exploits*, die sich entweder Schadsoftware (Malware) oder eigentlich unzulässiger Befehlsfolgen bedienen.[20] Bei einem lokalen *Exploit* wird versucht auf dem Zielgerät eine Schadsoftware z.B. einen Trojaner (Remote Administration Tool – RAT), der einem vielfältige Zugriffsmöglichkeiten verschaffen kann, zu installieren bzw. ihn durch Zielpersonen vor Ort ohne ihr Wissen installieren zu lassen. Das Schadprogramm kann an eine unauffällig erscheinende Datei im E-Mail Anhang angeheftet werden und installiert sich sobald der Benutzer die Datei öffnet.[21] In diesem Zusammenhang spricht man auch von *Spear-Phishing*. Wenn eine bestimmte Person in einer Einrichtung, die evtl. auch über strenge Sicherheitsvorkehrungen verfügt, gezielt attackiert werden soll, bedienen sich Angreifer auch an *Social-* und *Human-Engineering* Methoden um eine möglichst authentische „Falle“ auszulegen.[22] Es gibt diverse Formen von *Exploits*, die aufwendigste Variante ist ein *Zero-Day Exploit*, hierbei wird eine bisher völlig unbekannte Lücke genutzt.[23] Solche *Zero-Day*-Lücken zu finden erfordert hohen Aufwand und ggf. Insider-Informationen, z.B. Quellcodes einer Software oder eines Betriebssystems. Darüber hinaus ist auch ein Computerwurm ein äußerst probates Mittel, um möglichst viele Rechner zu infizieren. Ein Wurm gehört ebenfalls in die Kategorie Malware. Er verhält sich allerdings um einiges aggressiver, da er selbständig in Systeme eindringt, sich selbst kopiert und weiterverschickt, auch über Wechseldatenträger wie USB-Sticks.[24] Eine etwas abweichende Variante einer Cyberattacke ist eine DoS- oder DDoS-Attacke. Eine *(Distributed) Denial of Service* Attacke macht sich die begrenzten Kapazitäten eines Webseitenbetreibers zunutze. Der Angreifer hat im Vorfeld mehrere tausend Privatcomputer gekapert und lässt dieses sogenannte Botnetz aus gekidnappten PCs nun synchronisiert auf einen bestimmten Dienst oder eine bestimmte Website Anfragen verschicken. Diese Flut an Aufrufen überlastet die Kapazitäten der Server und führt zu einem temporären Ausfall des Webdienstes.[25] Unter Rückgriff auf diese und einige spezifischer Unterarten der hier vorgestellten Malware wurden bis dato alle bekannten Cyberangriffe durchgeführt. Bei komplexen Operationen werden diese Hackertools variiert und kombiniert eingesetzt, um in Teilschritten das oftmals besser geschützte Primärziel zu kompromittieren.

Stuxnet ist als eine Zäsur zu betrachten, da der Wurm präzise auf die iranische Atomanlage in Natanz zugeschnitten war und eine Reihe technischer Finessen aufwies. Das Hacken einer komplexen Industrieanlagensteuerung (*Industrial Control System* – ICS), sogenannten SCADA-Systemen (*Supervisory Control and Data Acquisition System*) oder DCS (*Distributed Control Systems*), ist grundsätzlich mit viel

[19] Anmerkung: Einsteiger-trojaner-Baukästen sind z.B. Poison Ivy oder Bifrost, http://www.poisonivy-rat.com/, (04.07.2013).

[20] Vgl. Siller, Helmut: Exploit, Gabler Wirtschaftslexikon, http://wirtschaftslexikon.gabler.de/Definition/exploit.html, (04.07.2013).

[21] Vgl. ebd.

[22] Vgl. o.V.: Spear Phishing, IT Wissen Online-Lexikon, http://www.itwissen.info/definition/lexikon/Spear-Phishing-spear-phishing.html, (04.07.2013).

[23] Vgl. Siller, Exploit.

[24] Vgl. Siller, Helmut: Wurm, Gabler Wirtschaftslexikon Online, http://wirtschaftslexikon.gabler.de/Definition/wurm.html, (04.07.2013).

[25] Vgl. Siller, Exploit.

größeren Schwierigkeiten verbunden, im Vergleich zu Systemen die ausschließlich mit COTS Produkten gesteuert werden. Dabei sind die Schäden, die durch eine erfolgreiche Manipulation verursacht würden viel weitreichender, da SCADA nicht nur in der Industrie sondern auch in vielen Bereichen der kritischen Infrastruktur genutzt wird. Das Risiko vergrößert sich insbesondere dann, wenn SCADA-Systeme zunehmend mit COTS-Produkten vernetzt werden. Ursprünglich arbeiteten SCADA-Systeme isoliert, ohne Verbindung zu Netzwerken oder externen Geräten. Betriebswirtschaftliche Bedürfnisse nach Effizienzsteigerung und technologischem Fortschritt haben dazu geführt, dass SCADA-Systeme auch in Netzwerke integriert wurden um z.B. Möglichkeiten zur Fernsteuerung und Fernwartung von Anlagen von einer zentralen Stelle aus zu ermöglichen.[26] Selbst wenn SCADA-Systeme nicht direkt mit dem Internet oder einem Netzwerk verbunden sind, also eine sogenannte *air gap* besteht, wird über Funk- und *Wireless*-Verbindungen oder durch anschließen eines externen Gerätes mit ihnen kommuniziert. Dazu finden COTS-Produkte Verwendung und es wird i.d.R mit dem üblichen Protokoll TCP/IP mit den SCADA-Systemen korrespondiert.[27] Durch die Verbindungen von SCADA zu potentiell unsichereren COTS-Produkten und die Verwendung standardisierter Protokolle entsteht ein Sicherheitsrisiko, selbst wenn Verbindungen nur temporär bestehen.[28] Mit diesen Verbindungen lässt sich theoretisch schädliche Software auf Industrieanlagen und somit auch auf kritische Infrastruktur übertragen – wie bei *Stuxnet*. Solch ein Sabotageakt ist allerdings alles andere als simpel durchzuführen und lässt sich mit den eingangs vorgestellten Angriffsformen nicht vergleichen. Unter Zuhilfenahme der simplen Angriffsformen lassen sich aber auch komplizierte Operationen durchführen, denn das erste „Einfallstor“ für feindselige Hacker ist immer ein erster, oft simpler *Exploit*.

2.3 Cybersabotage

Als Sabotageakt wird nach allgemeinem Verständnis ein gezielter Angriff bezeichnet, der einen maschinellen Prozess durch eine schädigende Einwirkung unterbricht bzw. eine ganze Einrichtung durch Beschädigung (gar Zerstörung) einzelner Komponenten davon abhält ihren Aufgaben im gewünschten Maße nachzukommen, um ein politisches oder militärisches Ziel zu erreichen. Da im Zuge einer breiten Digitalisierung von Prozessen mittlerweile in allen staatlichen und wirtschaftlichen Bereichen IT und EDV-Technik eingesetzt wird, steigt auch das Risiko gezielter Angriffe. Drei Bereiche sind, ungeachtet der Wahrscheinlichkeit und technischen Umsetzung eines Cyberangriffs, als besonders sensibel anzusehen und deswegen als mögliche Angriffsziele denkbar. Erstens verfügt das Militär der entwickelten Staaten über einen hohen Grad an integrierter z.T. unverzichtbarer IT und EDV, vor allem im Bereich Kommunikation, Koordination und Hightech-Waffensysteme. Dieses Zusammenspiel wird als *Network Centric Warfare* bezeichnet und ist ein zentraler Faktor für die hohe Schlagkraft und Effizienz moderner Armeen, insbesondere der US-amerikanischen Streitkräfte.[29] Die Sabotage der Kommunikations- und Koordinationszentren, der Kommandostrukturen sowie einzelner Waffensysteme könnte die effektive Durchführung von Operationen beeinträchtigen. Zweitens wäre kritische Infrastruktur ein attraktives Ziel für Sabotage, da eine Destabilisierung der Lage durch direkten Einfluss auf die zivile Bevölkerung im Konfliktfall den Vorteil zugunsten des Angreifers verschieben würde. Ein dritter Bereich wäre die Sabotage von Schlüsselindustrien, wie beispielsweise die Ölförderung und Verarbeitung. Doch wie realistisch sind diese Bedrohungsszenarien einzuschätzen und welche empirisch belegba-

[26] Vgl. Alcaraz, Cristina/Fernandez, Gerardo/Carvajal, Fernando: Security Aspects of SCADA and DCS Environments, in: Lopez, Javier/Setola, Roberto/Wolthusen, Stephen D. (Hrsg.): Critical Infrastructure Protection, Heidelberg u.a. 2012, S. 120–121.

[27] Vgl. ebd., S. 121.

[28] Vgl. ebd.

[29] Vgl. Hinkens, Hartmut: Die Mausefalle, ADLAS Magazin für Außen- und Sicherheitspolitik 2/2011, S. 41.

ren Fälle von Cybersabotage sind bis dato zu konstatieren?

Gerade in der US-amerikanischen Diskussion wird bezüglich der genannten Bereiche ein verheerendes Bild der Sicherheitslage aufgezeigt. Dieses Bild wird durch offensichtliche Investitionen vieler Nationen in militärische Cyberkapazitäten und einem Zuwachs hackaktivistischer Gruppen wie *Anonymous* genährt. Hinzu kommt die deutliche Anklage, dass die Volksrepublik China offensiven Cyberaktivitäten gegen die USA nachgehe.[30] Der US-amerikanische Terrorismusexperte und ehem. Sonderberater für Cybersecurity unter Präsident George W. Bush, Richard Alan Clarke, bezieht dazu in seinem 2010 erschienen Werk *World Wide War* (Originaltitel: *Cyber War: The Next Threat to National Security*) deutlich Stellung. In Clarkes Ausführungen ist der Cyberwar Realität. Es geht um die Vorherrschaft im Cyberspace. Daher begrüßt er die offensive Haltung der USA, bemängelt allerdings die Maßnahmen zum Schutz gegenüber feindlichen Cybernagriffen.[31] Die drei Kategorien Sabotage, Spionage und Subversion trennt er nicht eindeutig voneinander. Clarke erklärt, neben feindlicher Spionage, die Sabotage an kritischer Infrastruktur zu einem enormen Risiko, da die amerikanische Bevölkerung unmittelbar gefährdet würde und auch militärische Optionen eingeschränkt wären. Seine Argumentation stützt sich auf „denkbare“ zukünftige Szenarien, die sich dadurch legitimieren, dass es heute schon empirische Beweise für Cyberangriffe gibt, welche laut Clarke nur ein „Vorgeschmack“ auf die Ereignisse und Konflikte seien, die den USA noch bevorstünden. Unter diesen Beispielen befinden sich *Stuxnet* und die DDoS-Angriffe auf Estland.

China spielt als Großmacht im Pazifikraum eine besondere Rolle, da sich Konflikte zwischen China und den Verbündeten der USA im Südchinesischen Meer bereits abzeichnen. Das China im Konfliktfall offensive Cybersabotage gegen US-Einrichtungen auch an der „Heimatfront“ vornehmen würde, entnimmt Clarke den Aussagen des Generalmajors *Wang Pufeng*, dem Leiter der Strategieabteilung der chinesischen Militärakademie, der Chinas Ziel der „Informationsdominanz“ formuliert.[32] Diese Dominanz soll laut Generalmajor *Dai Qingmin* durch einen Präventivschlag im virtuellen Raum erreicht werden, woraus sich das chinesische Konzept des „integrierten elektronischen Netzkriegs“ ergibt, das dem amerikanischen *Network Centric Warfare* teilweise ähnelt.[33] Des Weiteren liest Clarke die feindlichen Absichten der Chinesen in dem 1999 erschienenen Strategiepapier *Unrestricted Warfare* der chinesischen Militärexperten *Qiao Liang* und *Wang Xiangsui* ab. Das Strategiepapier sagt aus, dass China die Technologien des Gegners stehlen und auf Mängel prüfen solle. Mit dem Ziel eigene sicherere Versionen zu entwickeln und im Kriegsfall Schäden an der Heimatfront des Gegners anzurichten. Die Strategie zielt darauf ab den technologischen Vorsprung der US-Armee auszugleichen.[34] Diese Darstellungen dienen Clarke als Argumente für seine These, dass die Infrastruktur gefährdet sei und z.B. das amerikanische Stromnetz bereits im Vorfeld von möglichen Konflikten mit Cybersabotage-Werkzeugen bestückt wurde. Die Chinesen sollen sogenannte „logische Bomben“ im amerikanischen Stromnetz versteckt haben, die im Konfliktfall großflächige Stromausfälle auslösen, um so die USA zur Kapitulation zu zwingen.[35] Diese These vertritt Clarke nicht nur in seinen schriftlichen Ausführungen. Seine Erkenntnisse sind offizieller Gegenstand sicherheitspolitischer Erwägungen der USA.[36] Als Beispiel gibt Clarke einen Zwischenfall aufgrund des SQL-Wurms „Slammer“ von 2003 an, der zu temporären Störungen der Stromversorgung in Ohio führte.[37] Besonders

[30] Vgl. Cooper, Charles: „House hearing: U.S. under cyber attack“, 24.04.2012, www.news.cnet.com, (08.07.2013).

[31] Vgl. Clarke, Richard A./Knake, Robert K: World Wide War, 1.Aufl, Hamburg 2011, S. 57–58.

[32] Vgl. ebd., S. 80.

[33] Vgl. ebd. 80–81.

[34] Vgl. ebd. S. 85.

[35] Vgl. ebd. S. 86.

[36] Vgl. McCaul, Micheal T.: “America is Under Cyber Attack: Why Urgent Action is Needed“, offizielles Statement vor dem US Homeland Security Komitee vom 24.04.2012, http://homeland.house.gov/sites/homeland.house.gov/files/04-24-12%20McCaul%20Open.pdf, (09.07.2013).

[37] Vgl. Clarke/Knake, World Wide War, S. 138–139.

beunruhigend waren die Probleme im Atomkraftwerk (AKW) Davis-Besse. Hier fiel die computergesteuerte Überwachung der Anlage aus, das unternehmensinterne Netzwerk war durch den Wurm beeinträchtigt und auch SCADA-Systeme waren betroffen.[38] Allerdings kam es zu keinem physischen Schaden, die Lage konnte durch ein *Back-up* unter Kontrolle gebracht werden. Die Sicherheitslücken der computergestützten Systeme bei amerikanischen Stromversorgern waren schon 1997 in einem offiziellen Bericht der Regierung festgestellt worden. Der Zwischenfall im AKW erhöhte den Druck auf die Unternehmen, verbesserte Sicherheitskonzepte vorzulegen.[39] Die Willkürlichkeit des Angriffs lässt keine Rückschlüsse auf den Urheber zu. Natürlich ist die These, dass es sich bei solchen Zwischenfällen um Testläufe staatlicher Hackaktivitäten handelt, durchaus nachvollziehbar. Sie bleibt allerdings hoch spekulativ. Das großflächige Sabotageszenarien durch logische Bomben als unwahrscheinlich beurteilt werden können, zeigen die wenigen Hinweise, welche die Empirie heute bietet. Denn logische Bomben müssten, um die Infrastruktur nachhaltig zu beschädigen, die SCADA-Systeme der angegriffenen Anlagen z.B. Umspannwerke oder Wasserwerke beeinträchtigen. Wie ein erfolgreicher Angriff auf solche Anlagentechnik funktioniert, hat *Stuxnet* gezeigt. Allerdings werden hier bei näherer Betrachtung auch die Schwierigkeiten und der enorme Aufwand deutlich, was Clarkes prognostizierte Szenarien unverhältnismäßig erscheinen lässt.

Die Sabotage der iranischen Atomanlage in Natanz durch *Stuxnet* ist der einzige bekannte Fall, bei dem mit Schadcodes eine physische Beeinträchtigung einer Industrieanlage nachzuweisen ist, da Sicherheitsexperten die Beschaffenheit der Schadsoftware weitgehend entschlüsseln konnten. Dabei wurde deutlich, dass *Stuxnet* hochentwickelt und ganz gezielt auf diese eine Atomanlage und ihre *Siemens* Software-Konfiguration sowie spezifische Anordnung der Komponenten ausgerichtet war.[40] Aus diesem einzelnen erfolgreichen Angriff die Schlussfolgerung zu ziehen, dass solche Angriffe nun eine alltägliche Bedrohung für alle modernen Industrieanlagen darstelle, wäre falsch. Denn ein solcher Angriff ist mit erheblichem Aufwand verbunden und nicht direkt auf andere Anlagen und ihre SCADA-Systeme übertragbar. Die mutmaßlich amerikanischen und israelischen Urheber dieser Operation hatten eine Menge Hürden und Einzelschritte zu bewältigen, bevor der tatsächliche Sabotageakt gestartet werden konnte. Die Sabotageoperation begann schon 2005 unter dem Codenamen *Olympic Games*, die Hauptattacke wurde zwischen 2009 und 2010 durchgeführt.[41] Das Ziel war die Schadsoftware in das Steuerungssystem der Urananreicherungsanlage einzuschleusen. Die Steuereinheiten sind durch eine *air gap* geschützt (wie in sensiblen Bereichen üblich). Zur Wartung werden diese Steuereinheiten mit sogenannten *Programmable Logic Controller* (PLC)[42] verbunden, d.h. die Urheber mussten zunächst einmal den Wurm in die Nähe des Ziels bringen, damit er ein Gerät befallen konnte, das direkten Kontakt mit den Kontrollsystemen hatte.[43] *Stuxnet* infizierte über 100.000 Geräte weltweit, davon 60% im Iran. Auf diese Weise erreichte der Wurm letztendlich sein Ziel über einen infizierten Computer eines Mitarbeiters der Atomanlage. Kollateralschäden an anderen Anlagen wurden vermieden, da der Wurm zwar andere Anlagen infizierte, allerdings nur bei der Konfiguration der Anlage in Natanz seine Wirkung entfachte.[44] Die Urheber verfügten also über ein hochdetailliertes Bild der Lage vor Ort und Konfigurationspläne der Atomanlage. Der Fall *Stuxnet* verdeutlicht, dass ein erfolgreicher Cyberangriff ein erhebliches Maß an Vorbereitungszeit, Know-how und finanziellen Mitteln erfordert. Die Urheber von *Stuxnet* brauchten vier *Zero-Day Exploits*, mehrere gestohlene

[38] Vgl. Poulsen, Kevin: Slammer worm crashed Ohio nuke plant network, 19.08.2003, www.security focus.com, (11.07.2013).
[39] Vgl. ebd.
[40] Vgl. Langner, Ralph: Stuxnet knacken, eine Cyber-Waffe des 21. Jahrhunderts, März 2011, www.ted.com, (11.07.2013).
[41] Vgl. Rid, Thomas: Cyberwar Will Not Take Place, 1. Aufl., London 2013, S. 43.
[42] Anmerkung: PLCs sind spezielle Notebooks zur Wartung von Siemens Anlagentechnik.
[43] Vgl. Rid, Cyberwar Will Not Take Place, S. 43–44.
[44] Vgl. ebd., S. 44.

Sicherheitszertifikate und *Rootkits*[45]. Die Kosten der Beschaffung und Entwicklung des Schadcodes waren hingegen vermutlich überschaubar in Relation mit konventionellen Rüstungsgütern. Den größten Kostenaufwand dürfte die Informationsbeschaffung aller Details, die zur Durchführung dieser Operation nötig waren, erzeugt haben. Denn um diese sensiblen Informationen zu sammeln und die Operation auch erfolgreich durchzuführen, muss ein großer geheimdienstlicher Aufwand betrieben worden sein.[46]

Ein weiteres Beispiel aus dem Nahen Osten zeigt, dass die technischen Möglichkeiten, bzw. der bloße Besitz einer Schadsoftware nicht ausreicht, um physischen Schaden anzurichten. Das Ziel der Cyberattacke war das nationale saudi-arabische Ölförderunternehmen *Saudi Aramco*. Am 15. August 2011 stürzten weite Teile der Computer innerhalb des Firmennetzwerkes durch den Virus *Shamoon* ab, es kam zu Datenverlusten und das interne Netzwerk musste temporär stillgelegt werden, um die Verbreitung des Virus zu unterbinden. Als Urheber halten die US-Geheimdienste den Iran für wahrscheinlich.[47] Die SCADA-Systeme der Ölförderungsanlagen waren weder infiziert noch nachhaltig beschädigt worden. Die IT-Spezialisten brauchten zwar über zehn Tage, um die Betriebsbereitschaft des internen Netzwerks komplett wiederherzustellen, die Förderungsanlagen und Raffinerien waren aber nicht beeinträchtigt.[48] Das bedeutet, hier liegt zwar eine gezielte Beeinträchtigung der Verwaltung und Wartung der Anlagen vor, aber ob solch eine Attacke schon als Angriff oder kriegerischer Akt bezeichnet werden kann, ist äußerst fraglich.

Ähnlich verhält es sich mit den sogenannten DoS- oder DDoS-Angriffen, von denen die Privatwirtschaft regelmäßig betroffen ist. Auch Staaten wie Estland (2007)[49] und Georgien (2008) haben Erfahrungen mit dieser Form der Cybersabotage gemacht. In beiden Fällen wurde Russland beschuldigt für die Angriffe verantwortlich zu sein, der Kreml dementierte diesen Vorwurf und beteuerte, dass die Regierung keinen Einfluss auf patriotische (vigilantische) Hacker habe. Eine Verbindung zwischen russischen Hackaktivisten und der russischen Regierung konnte nicht bewiesen werden. Rein technisch betrachtet war die schädliche Wirkung sehr begrenzt, da es nur zu einer temporären Überlastung der angegriffenen Webseiten kam. In Estland wurden sowohl die Seiten von Banken als auch der Regierung temporär lahmgelegt. In Georgien gingen die Cyberattacken einher mit den russischen Truppenbewegungen in Südossetien.[50] Insgesamt waren über 50 Webseiten in den Bereichen Kommunikation, Finanzwesen und Regierung betroffen. Auch eine Untersuchung des *Small Wars Journal* kommt zu dem Schluss, dass die Synchronisierung der Cyberattacken mit den russischen Truppenbewegungen eine weitere Domäne auf taktisch operationeller Ebene implementiert. Der Fall Georgien legt nahe, dass Russland (wahrscheinlich auch China) über ein Netzwerk von „patriotischen Hackern“ verfügt, welches direkte Verbindung zu Geheimdiensten der Regierung haben muss. Solche Cyberoperationen benötigen Vorbereitungen im Vorfeld eines Konflikts, um die Malware im Zielland zu verbreiten. Daher sollte ein potentiell gefährdeter Staat schon im Vorfeld mit Gegenaufklärung (Counterreconnaissance, Counterintelligence) für die Sicherheit seiner Netzwerke sorgen.[51]

[45] Anmerkung: *Rootkits* sind betriebssystemähnliche Software, die unautorisiert Administratorrechte auf einem System zur Verfügung stellen und mit Funktionen z.B. versteckten Zugängen (Backdoors) erweitert werden können.

[46] Vgl. Rid, Cyber War Will Not Take Place, S. 45–46.

[47] Vgl. Perlroth, Nicole: „In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back“, 23.10.2012, www.nytimes.com, (12.07.2013).

[48] Vgl. Rid, Cyber War Will Not Take Place, S. 56.

[49] Vgl. Traynor, Ian: Russian accused of unleashing cyberwar to disable Estonia, 17.05.2007, www.guardian.co.uk, 12.07.2013. Anmerkung: Auslöser der diplomatischen Verstimmungen zwischen Estland und Russland war der Umzug einer Bronzestatue einer russ. Kriegsgedenkstätte aus dem Zentrum Tallinns auf einen Soldatenfriedhof.

[50] Vgl. Hollis, David: Cyberwar Case Study: Georgia 2008, Artikel zur Studie des Small Wars Journal vom 06.01.2011, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008,12.07.2013.

[51] Vgl. Hollis, David: Cyberwar Case Study: Georgia 2008, Studie des Small Wars Journal vom

Ein zentraler Punkt unterscheidet Sabotage im Kontext von *Stuxnet* gegenüber DoS-Attacken, *Shamoon* und weiteren bekannten Zwischenfällen. *Stuxnet* war gegen Hardware gerichtet. Das Ziel des Wurms war die Zerstörung der Zentrifugen zur Urananreicherung. DoS-Attacken oder *Shamoon* richteten sich nur gegen Software, es wurde kein physischer Schaden herbeigeführt, sondern lediglich Webdienste temporär unterbrochen. Daraus lässt sich extrahieren, dass ein Angreifer der nachhaltigen Schaden anrichten möchte sich SCADA-Systeme und DCS als Ziel vornehmen muss. Da das Sabotieren solcher Industrieanlagen besonders kompliziert und ressourcenaufwändig ist, kann ein Szenario wie ein landesweiter Stromausfall – wie Clarke es befürchtet – als unwahrscheinlich angesehen werden. Das Dilemma für Staaten entsteht selbst bei Cyberangriffen mit begrenzter Wirkung aus dem sich erhöhenden innenpolitischen Handlungsdruck auf Regierungen – und dies ohne Beweise für den Urheber zu besitzen. Estland hat Hilfe von der NATO angefordert und das *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) wurde 2008 in Tallinn errichtet.

2.3 Cyberspionage

Big Data ist heute zu einem Schlagwort geworden: Das Ausspähen und gezielte Filtern von Daten kann ein umfangreiches Lagebild ermöglichen. Auch der Staat, das Militär und Geheimdienste speichern vertrauliches und sensibles Material innerhalb ihrer Netzwerke. Informations- und Kommandostrukturen sind zentralisiert und haben ihre Kommunikationskanäle über den gesamten Globus gestreut, das kann von entschiedenem Vorteil sein. Spionage ist ein Phänomen, das so alt ist wie der Krieg selbst. In einer komplexen multipolaren Weltordnung, die von globalisierter Wirtschaft, asymmetrischen Konflikten, Revolutionen und der Erhebung Chinas zur Großmacht geprägt ist, sind Informationen der Schlüssel zur Wahrnehmung nationaler Interessen, Stabilität und Sicherheit.

Sensible Informationen durch Spionage zu erlangen kann also ein entscheidender Vorteil sein. Der technische Fortschritt und die globale Vernetzung stellen den Geheimdiensten und dem Militär eine neuerliche Quantität an Informationen zur Verfügung, deren Zugänglichkeit mit weniger Risiken der Entdeckung verbunden ist als die herkömmliche Spionagetätigkeit der *Human Intelligence* (HUMINT), aufgrund des Attributionsproblems. Die Überwachung jeglicher Telekommunikation, *Signal Intelligence* (SIGINT), ist zur wichtigsten Aufgabe von Geheimdiensten geworden. Cyberspionage nimmt in Staaten, wie die USA, Russland und China, einen großen Teil der finanziellen Ressourcen und Cyberkapazitäten ein.[52] Gerade die USA bauen ihre Spionagekapazitäten massiv aus. Beispielhaft ist die Errichtung eines neuen Rechenzentrums der NSA in Bluffdale, Utah. Ein Großteil der weltweiten Datenströme passiert Server in den USA, aufgrund der Omnipräsenz von amerikanischen Unternehmen in der Computer- und Internetbranche. Dass diese Unternehmen scheinbar auch eng mit den Sicherheitsbehörden zusammenarbeiten geht aus NSA-Informationen, welche die *Washington Post* veröffentlichte, eindeutig hervor.[53] Diese Zusammenarbeit passt in das Paradigma der USA betreffend ihres Konzepts von *Cyber Defence* zur Erhaltung der nationalen Sicherheit. Denn wie Richard Clarke eindeutig fordert, müssen die USA, da die kritische Infrastruktur inklusive der Telekommunikation Privatunternehmen gehört, wieder mehr Einfluss durch staatliche Regulierung und Überwachung gewinnen um die Sicherheit der US-Bürger zu gewährleisten.[54] Natürlich verfügen auch Russland und China über weitreichende Kapazitäten in diesem Bereich. Die Informations- und Quellenlage ist diesbezüglich allerdings deutlich schlechter.

Technisch betrachtet, bedienen sich Cyberspione ähnlichen Werkzeugen, die auch bei der Cybersabotage benutzt werden (Trojaner,

06.01.2011, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf, S. 5–7.

[52] Vgl. Rid, Cyber War Will Not Take Place, S. 81–82.

[53] Vgl. o.V.: „NSA slides explain the PRISM data-collection program“, 06.06.2013, www.washingtonpost.com, (13.07.2013).

[54] Vgl. Clarke/Knake, World Wide War, S. 325–327.

Backdoors, Rootkits etc.). Eine Unterscheidung ist durch die verschiedenen Zielsetzungen möglich: „[C]yberspionage [...] refers to the clandestine collection of intelligence by intercepting communications between computers as well as breaking into [...] computer networks in order to exfiltrate data. Cyber sabotage, by contrast, would be the computer attack equivalent of covert operations [...] in order to create a desired physical effect[...].“[55] Professionelle Attacken bleiben oft unentdeckt, dennoch sind einige Zwischenfälle veröffentlicht worden. Die USA berichteten 2003 von einer Reihe von Cyberspionagefällen, die unter dem Namen *Titan Rain* zusammengefasst wurden. Die Angreifer verschafften sich Zugang zu Netzwerken von US-Einrichtungen wie dem *State Department*, dem *Department of Homeland Security*, dem Pentagon und dem Rüstungsunternehmen *Lockheed Martin*. Insgesamt wurden 10 bis 20 Terabyte Datenvolumen aus dem NIPRNET (*Non-classified Internet Protocol Router Network*) des Pentagons ausgespäht. Das SIPRNET (*Secret Internet Protocol Router Network*) konnte nach Angaben von General William Lord nicht ausgespäht werden. Die Computerforensiker der *US-Airforce* verfolgten die digitalen Spuren nach China. Ob China der Urheber ist und die chinesischen Geheimdienste beteiligt waren, ist nach wie vor unklar.[56] Einer der bemerkenswertesten Cyberspionagefälle ist unter dem Namen *Flame* bekannt geworden. *Flame* war mit umfassenden Spionagewerkzeugen ausgestattet und im Nahen Osten seit März 2010 für zwei Jahre vor allem im Iran aktiv. Die Malware konnte Screenshots machen, Webcams und Mikrofone abhören, sowie gespeicherte Daten stehlen. *Kaspersky* stufte *Flame* als eine hochwertige Cyberwaffe ein, weil die Software hochentwickelt war, spezifische Sicherheitslücken ausnutzte, komplex programmiert wurde und sich selbstständig verbreitete, was auf einen staatlichen Urheber hinweist. Des Weiteren ließen sich Parallelen zu *Stuxnet* aufzeigen.[57]

Ein weiterer wichtiger Teilbereich ist die Industriespionage durch das Ausspähen der IT von Unternehmen. Aus Image- und Datenschutzgründen sprechen Unternehmen nur ungern über dieses Problem, dennoch gibt es bekannte Fälle und anonyme Studien um die Tragweite des Problems zu ermessen. In den USA sind die Cyber-Industriespionage-Vorfälle namens *Operation Aurora* und *Shady Rat* veröffentlicht worden. In beiden Fällen wurden internationale Großunternehmen ausgespäht. Bei *Operation Aurora* waren neben IT-Unternehmen wie *Adobe*, *Google*, *Yahoo* und *Symantec*, auch Rüstungskonzerne und die Finanzbranche betroffen, z.B. *Northrop Grumman* und *Morgan Stanley*.[58] *Shady RAT* war zwischen den Jahren 2006 und 2008 aktiv und spähte über 70 internationale Unternehmen, Regierungen und NGOs weltweit aus. Technisch ist der Vorfall gewöhnlich, die Schadsoftware wurde durch *Spear-Phishing* gezielt verteilt. Bemerkenswerter sind hingegen die Ziele, die auch außerhalb der Industrie angesiedelt waren, z.B. das Internationale Olympische Komitee und die UN.[59] Im Bereich Industriespionage sind auch die EU und insbesondere Deutschland betroffen, daher forderte der ehem. Innenminister Peter Friedrich, wie auch einige andere Politiker auf EU-Ebene, eine Meldepflicht für Hackangriffe einzuführen, im Idealfall für die ganze EU.[60] Denn ein Hauptproblem bei der Bewertung der Bedrohung durch Cyberspionage ist das relativ unklare Lagebild. Die Unternehmen äußerten Bedenken gegenüber den Vorschlägen der EU, auch der Bundesverband der deutschen Industrie befürchtet Mehraufwand und Imageschäden.[61] Ein aktuelles Lagebild der Cyber-Industriespionage in Deutschland zeigt eine repräsentative Studie aus dem Jahr 2012 von

[55] Rid, Cyber War Will Not Take Place, S. 82.
[56] Vgl. ebd., S. 85–86.
[57] Vgl. o.V.: „Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat“, 28.05.2012, www.kaspersky.com, (13.07.2013).

[58] Vgl. Gaycken, Cyberwar. Das Wettrüsten hat längst begonnen, S. 112.
[59] Vgl. Alperovitch, Dimitri: Revealed: Operation Shady RAT, McAfee White Paper, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf, (14.07.2013).
[60] Vgl. Sawall, Achim: „Hackerangriffe sollen meldepflichtig werden“, 17.08.2012, www.golem.de, (14.07.2013).
[61] Vgl. o.V.: „Cyberangriffe: Hacker-Meldepflicht für Unternehmen offenbar vor dem Aus“, 05.06.2013, www.spiegel.de, (14.07.2013).

Corporate Trust in Zusammenarbeit mit dem TÜV an der über 6.000 deutsche Unternehmen teilnahmen. Die Fallzahl von Industriespionage ist um 2,5 % gestiegen im Vergleich zu 2007. 21,4% der befragten Unternehmen gaben zu, Opfer von mindestens einem Fall geworden zu sein, zum Vergleich im Jahr 2007 waren es 18,9%. Der Mittelstand ist am häufigsten betroffen, insgesamt entstand ein Schaden von 4,2 Milliarden Euro. In ca. 70% der Fälle sind Mitarbeiter mutwillig oder unbewusst durch *Social Engineering*[62] Strategien involviert. Interessant ist auch die Tatsache, dass nur etwa 20% der geschädigten Unternehmen den Verfassungsschutz oder Polizeibehörden alarmierten.[63] Des Weiteren wurden erhebliche Mängel bei den Sicherheitsvorkehrungen festgestellt. Zwar verfügt die Mehrzahl der Unternehmen über technische Sicherheitsvorkehrungen wie Passwortschutz und Anti-Viren Software, allerdings gibt es große Lücken bei der verschlüsselten Kommunikation und der Schulung der Angestellten gegen *Social Engineering*.[64] Dabei gibt es moderne Verschlüsselungstechniken, die mit geringem technischen Aufwand zum Schutz sensibler Daten eingesetzt werden können. Als unknackbar gilt aktuell der AES-Verschlüsselungsalgorithmus der mit bis zu 256 Bit verschlüsselt.[65] Daher sollte davon auszugehen sein, dass alle Regierungen, Unternehmen und Organisationen geheime Daten entsprechend absichern. Diese Erkenntnis schmälert die Glaubwürdigkeit der Stimmen, die behaupten der Einbruch von Schadsoftware in sensible Netzwerke wäre ein ernsthafter Schaden per se, weil selbst wenn Daten z.B. aus dem SIPRNET gestohlen würden, könnte der Datendieb die verschlüsselten Daten nicht ohne weiteres auswerten.

Zusammenfassend lässt sich feststellen, wenn ein Teilbereich des Cyberwar einen großflächigen Wirkungsgrad erreicht, dann ist es der Bereich Spionage. Dieser wird aber auch weiterhin durch HUMINT angereichert werden müssen, denn die Geheimdienste stehen bei Cyberspionage vor neuen Herausforderungen. Erstens ist die Selektion der relevanten Daten und Quellen in den riesigen Datenmengen anspruchsvoll. Zweitens erfordert der Prozess der Analyse und Interpretation, um aus „rohen“ Daten praktikable *Intelligence* zu gewinnen einen erheblichen Aufwand. Die rein virtuelle Aufklärung (*remote reconnaissance*) kann einem wichtige Insiderinformationen vorenthalten.[66] Eine Operation wie *Stuxnet* wäre ohne HUMINT nicht möglich gewesen und auch bei geheimdienstlicher Aufklärung und Industriespionage werden Agenten vor Ort benötigt um Hindernisse wie *air gaps* zu überwinden oder Malware gezielt in ein Netzwerk einzuschleusen.

2.4 Cybersubversion

Der Begriff Subversion leitet sich vom lateinischen Wort *subvertere* (umdrehen, umstürzen) ab und wird in vielen wissenschaftlichen Disziplinen benutzt. Im politischen Kontext ist die Untergrabung der bestehenden politischen Ordnung oder der Machtinhaber unter Zuhilfenahme subversiver Mittel gemeint. Diese subversiven Mittel schwanken in ihrer Intensität zwischen Terrorismus, Propaganda, Befehlsverweigerung und sozialem Ungehorsam. Gerade die Verwendung des Begriffs Subversion im Zusammenhang mit politischen Protesten ist fraglich und insbesondere in autoritären Staaten mit Blick auf die Menschenrechte problematisch.[67] Subversion ist konzeptionell von *Insurgency* und Terrorismus zu unterscheiden, wobei die Grenzen im Falle von Gewaltanwendung fließend sein können.

[62] Ausspionieren über das persönliche Umfeld, [...] durch zwischenmenschliche Beeinflussung, meist unter Verschleierung der eigenen Identität [...]. Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen, vgl. Schaaf, Christian u.a.: Corporate Trust Studie: Industriespionage 2012, http://docs.dpaq.de/703-120423_-_studie_industriespionage_2012.pdf, (14.07.2013).

[63] Vgl. ebd., S. 8.

[64] Vgl. ebd.

[65] Vgl. Laurent Haan, Kristian: Advanced Encryption Standard (AES), Kapitel: Einführung & Schluss, 17.02.2008, www.codeplanet.eu, (16.07.2013).

[66] Vgl. Rid, Cyber War Will Not Take Place, S. 109–110.

[67] Vgl. Ernst, Thomas: Ein Gespenst geht um. Der Begriff der Subversion in der Gegenwart, E-Paper Universität Bielefeld, http://www.gradnet.de/papers/pomo02.papers/subversion.pdf, (15.07.2013).

Subversion kann auch als Vorstufe gelten, die im weiteren Verlauf zu *Insurgency* oder Terrorismus führen kann.[68] Subversion ist also äußerst facettenreich, ebenso verhält es sich mit der Cybersubversion.

Das Internet als globales Kommunikationsmittel bietet umfangreiche Optionen um subversive Ideen zu verbreiten und ihre Umsetzung, wie auch immer geartet, transnational zu organisieren. Auch Plattformen wie *WikiLeaks* beeinträchtigen das Vertrauen in Regierungen, die Motive und Rechtskonformität sollen an dieser Stelle unbewertet bleiben. Der arabische Frühling, der in den Medien oft als „Facebook-Revolution“[69] bezeichnet wurde, ist ein weiteres Beispiel für die zentrale Rolle des Internets und sozialer Medien. Es zeigt sich, dass es diverse Spielarten gibt – ob die Rolle des Internets sich als entscheidender Faktor aufweist ist umstritten.

Es soll im Folgenden ausschließlich um Subversion im direkten Zusammenhang mit dem Internet gehen, dabei sind Bewegungen wie *Occupy Wall Street*, *Anonymous* oder der „arabische Frühling“ gemeint. Das Internet bringt für solche Bewegungen signifikante Vorteile, allerdings auch entscheidende Nachteile. Ein Vorteil ist die erleichterte Verbreitung von subversiven Ideen sowohl regenerativer als auch destruktiver Art. Dadurch vergrößert sich zwar die Diversität der subversiven *Entrepreneurs*, aber gleichzeitig sind die Bewegungen auch Ursachen/Anlassgetriebener (*cause-driven*).[70] Zu erkennen ist dies an neuen Parteien wie der Piratenpartei oder Tierschutzorganisationen, die nur eine spezifische Agenda vertreten. Solchen Bewegungen gelingt es zwar schnell Mitglieder anzuwerben, da im Schutz der Anonymität im Internet die Eintrittskosten gering sind, andererseits führt genau dies zu einem hohen Maß an Mobilität der Mitglieder, was die interne Disziplin einer Organisation schwächt und so ein langfristiges Aufrechterhalten erschwert.[71] Das zeigt sich auch am sog. arabischen Frühling in Ägypten. Die Revolution hat als Jugendbewegungen begonnen und die sozialen Medien eröffneten die Möglichkeit organisierter Proteste trotz des autoritären Regimes. Die ursprünglichen Urheber haben die Kontrolle über die Entwicklungen verloren. Im Umfeld der Unruhen haben die Muslimbrüder und Salafisten die Führung der Protestbewegungen übernommen und den Präsidenten bis zum Militärputsch des 3. Juli 2013 gestellt. Der *modus operandi* von subversiven Aktivitäten ist die soziale Bindung, deswegen soll das Vertrauen in Institutionen gezielt unterwandert werden.[72] Das Internet kann hier als Promoter wirken, die weitere Entwicklung findet dann allerdings oft sprunghaft und offline statt. Die Anonymität des Internets ermöglicht es ebenso Geheimdiensten und dem Militär Propaganda und Falschinformationen großflächig zu verbreiten. *Perception Manangement* ist integraler Bestandteil sogenannter *Psychological Operations* (PSYOPS)[73], um die öffentliche Meinung zu beeinflussen und sich somit strategische Vorteile und Deutungshoheit zu verschaffen. Der Begriff PSYOP wurde mittlerweile verworfen und durch MISO (*Military Information Support Operations*) ersetzt.[74] Die vermeintlichen Vorzüge des „Web 2.0“ durch globale bürgerliche Partizipation und das Austauschen von Informationen über Blogs, sozialen Medien oder Plattformen wie *Wikipedia* sind mitunter leicht manipulierbar, da eine unabhängige Kontrollinstanz fehlt.[75] Welchen Stellenwert das Konzept des Informationskriegs hat und welche Wirkung auf die öffent-

[68] Vgl. Rid, Cyber War Will Not Take Place, S.115; vgl. Agnoli, Johannes: Subversive Theorien, Gesammelte Schriften Band 3, Freiburg 1996, S. 19.

[69] Vgl. Güßgen, Florian: „Mubarak kontert die Facebook Revolution“, 28.01.2011, www.stern.de, (15.07.2013).

[70] Vgl. Rid, Cyber War Will Not Take Place, S. 115.

[71] Vgl. Rid, Cyber War Will Not Take Place, S. 115.

[72] Vgl. ebd., S. 116.

[73] Vgl. Departement of Defense Dictionary of Military and Associated Terms, 12.04.2001, http://books.google.de/books?id=Ap_En_k7r9AC&printsec=frontcover&dq=Dictionary+of+Military+and+Associated+Terms&hl=de&sa=X&ei=_9jjUbGVF4fQOc7EgegK&ved=0CD4Q6AEwAA, (16.12.2013), S. 380.

[74] Vgl. Department of Defense Dictionary of Military and Associated Terms, 08.11.2010, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, (16.12.2013), S. 494.

[75] Vgl. Gaycken, Cyberwar. Das Wettrüsten hat längst begonnen, S. 158; 162.

liche Wahrnehmung Bilder und Pressemeldungen haben, zeigte auch die Berichterstattung während und im Vorfeld des Irakkriegs 2003, wie das Beispiel der sogenannten Brutkastenlüge einer kuwaitischen Lobbyorganisation bewies.[76] Die Manipulation von Bildern und Webseiteninhalten ist heute technisch simpel und „Fakes“ lassen sich schnell über das Netz verbreiten, wie die offiziell veröffentlichten Fotos des Langstreckenraketentests des Iran 2008 zeigten.[77] Subversion, Manipulation und psychologische Kriegsführung unter Zuhilfenahme des Internet sind möglich und bieten Vorteile, dennoch ist die nachhaltige Tragweite begrenzt. In Demokratien können sich *grassroot*-Bewegungen offen über das Internet organisieren und für die Bürger von autoritären Staaten ergibt sich, je nach Grad der Zensur, die Möglichkeit Bürgerrechte wie freie Rede und politische Organisation im Schutz der Anonymität wahrzunehmen.

2.5 Das Attributionsproblem

Den Urheber einer Cyberattacke zu identifizieren, ist aus technischen, justiziellen und politischen Gründen nahezu unmöglich. Physische Spuren wie Fingerabdrücke werden i.d.R. nicht hinterlassen. Daher gehen IT-Forensiker den Datenspuren nach, z.B. durch Ermittlung der IP-Adresse oder dem Inhalt einer Schadsoftware, auch die Programmiersprache kann ein Hinweis sein. Allerdings tun sich an dieser Stelle erneut Probleme auf. Alle Hinweise und Charakteristika, wie ein impliziertes Datum oder die verwendete Sprache, die sich aus dem entschlüsselten Programmcode extrahieren lassen, sind technisch ebenso leicht manipulierbar, d.h. ein Angreifer kann den Forensiker hier gezielt auf eine falsche Fährte locken.[78] Auch die IP-Adresse bringt dem Forensiker keinen stichhaltigen Beweis, höchstens eine Vermutung. Denn IP-Adressen werden dynamisch vergeben und können global über eine beliebige Anzahl von Servern verschleiert werden. Selbst wenn es gelingt die Spur einer bestimmten IP zu einem bestimmten Gerät zu verfolgen, besteht weiterhin die Mensch-Maschine-Lücke. Es lässt sich also letztendlich kaum beweisen wer zu einem bestimmten Zeitpunkt an einem Gerät gearbeitet hat.[79] Hinzu kommen justizielle und politische Hürden, da nicht alle Staaten bei der Herausgabe von Verbindungsdaten kooperieren. Die Verbindungen im Internet werden grenzübergreifend erstellt, selbst wenn das Identifizieren des *Command-and-Control* Servers einer Malware gelingt, liegt dieser in einem nicht verbündeten Drittstaat, ist ein Zugriff nicht möglich.[80] Selbst bei politischen Partnern können Vorbehalte aus Datenschutzgründen auftreten. Auch eine Vorratsdatenspeicherung hilft nicht uneingeschränkt weiter: Die Zugriffsdaten werden zwar temporär gespeichert, allerdings verfügen nicht alle Länder über die Verbindungsdatenspeicherung und würden die Information auch nicht vorbehaltlos herausgeben. Die europaweite Vorratsdatenspeicherung ist ein Mittel zur Bekämpfung von Cyberkriminalität, gegen hochentwickelte Spionage- oder Sabotagesoftware hilft sie jedoch nicht.

Diese Anonymität durch die Non-Attribution ist für Staaten Fluch und Segen zugleich – auch für die Staaten die offensive Cyberstrategien verfolgen. Es ermöglicht ihnen verdeckte Operationen mit weniger menschlichem Einsatz (*boots on the ground*) durchzuführen, andererseits fallen essentielle strategische Prinzipien wie die Abschreckung weg. Martin Libicki erhebt in einer *RAND*-Studie erhebliche Zweifel daran, dass Abschreckung im Cyberspace funktioniert. Da die Wirkungslogik obsolet wird, sobald der Angreifer nicht eindeutig identifizierbar ist, somit keinen unmittelbaren Gegenschlag zu befürchten hat. Der Angegriffene steht zudem vor dem Dilemma, dass er einem Dritten ungerechtfertigt mit Vergeltung drohen könnte, weil dieser im Vorfeld Opfer

[76] Vgl. Gaycken, Cyberwar, S. 161–162.
[77] Vgl. Rötzger, Florian: Iran hat ein Foto vom Raketentest manipuliert, 11.07.2008, www.heise.de, (15.07.2013).
[78] Vgl. Gaycken, Sandro: Die vielen Plagen des Cyberwar, in: Schmidt-Radefeldt, Roman/Meissler, Christine: Automatisierung und Digitalisierung des Krieges, 1 Aufl., Baden-Baden 2012, S. 101–102.
[79] Vgl. Gaycken, Die vielen Plagen des Cyberwar, S. 104.
[80] Vgl. Rid, Cyber War Will Not Take Place, S. 145.

einer *false flag* Operation geworden ist[81], was aufgrund der Manipulierbarkeit der datenforensischen Spuren leicht möglich ist. Dies wiederum bedeutet, selbst wenn ein Angreifer offensichtliche Spuren hinterlässt, um mit seinen offensiven Cyberfähigkeiten abzuschrecken, kann diese Geste missverstanden werden. Es ist auch kaum möglich, Macht zu demonstrieren durch virtuelle Gewaltandrohung, da Staaten ihre Cyberwaffen nicht zur Schau stellen oder einen Warnschuss abgeben können, da die essentiellen Bestandteile eines Cyberangriffs, z.B. die genutzte Lücke dadurch bekannt und behoben würde. Der symbolische und psychologische Wirkungsgrad von Cyberangriffen fällt schlichtweg zu gering aus.[82] Natürlich gibt das Ziel sowie die Art und Weise der Operation Hinweise auf mögliche Motive und Verdächtige, aber eine valide Beweisführung ist unmöglich. Denn ein angeklagtes Land kann auf einen Missbrauch durch Dritte verweisen. Das Abschreckungspotential von Geheimoperationen ist ohnehin gering. Hinzu kommt, dass wirksame Angriffe unsichtbar bleiben müssen, um möglichst lange ihre Wirkung zu entfalten (Sabotage, Spionage etc.). Der Tonfall der Politik bei diesem Thema ist aggressiv, um die eigene Entschlossenheit zu Vergeltungsmaßnahmen gegenüber einem Cyberangriff zu bekräftigen.[83] Unter diesen Umständen entstehen Unsicherheiten, die destabilisierend auf die internationalen Beziehungen wirken können und diplomatische Verhandlungen belasten.[84] Regierungen könnten unter Zugzwang geraten und militärische Maßnahmen trotz Non-Attribution ergreifen. Cyberattacken, die solch ein Szenario ausgelöst haben, sind aber bislang nicht bekannt. Rid stellt hingegen fest, dass im Falle einer wirklich verheerenden Cyberattacke, die (hemmenden) Standards zur Attribution des Urhebers erheblich sinken würden, dadurch könnte sich der bezichtigte Urheberstaat nicht mehr hinter patriotischen Hackern oder Missbrauch verstecken. Der internationale Druck, zur Aufklärung und justiziellen Zusammenarbeit beizutragen, würde dann sehr stark ansteigen. Das lässt den „Wetteinsatz“ für groß angelegte Cyberattacken als sehr hoch erscheinen, da das Risiko eines konventionellen Gegenschlags besteht.[85]

2.6 Rechtliche und konzeptionelle Rahmenbedingungen

Es existiert weder eine Art von *Internet Governance* noch verbindliche völkerrechtliche Regelungen für virtuelle zwischenstaatliche Auseinandersetzungen. Es gibt zwar internationale Diskussionsforen wie die *World Conference on International Telecommunications* (WCIT-12) und Organisationen wie die *International Telecommunication Union* (ITU), auf globale Rechtsnormen konnten Staaten sich bisher aber nicht einigen.[86] Bei Cyberkriminalität gelten i.d.R. nationale Gesetze, was das Internet als grenzübergreifendes Medium schwer kontrollierbar macht.
Wie wird im Rahmen des Cyberwar-Konzepts (rechtlich) aus Software ein Gewaltakt und ist der Begriff Cyberwaffe überhaupt legitim? Der Begriff Krieg wird im Zusammenhang mit Cyberaktivitäten sehr inflationär benutzt. Krieg oder der bewaffnete Konflikt wird gemeinhin als eine physisch gewaltsame Auseinandersetzung definiert. Nach Clausewitz ist Krieg „[...] ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen.“[87] Dieser direkte Zusammenhang zwischen Krieg und Gewalt findet sich auch in der völkerrechtlichen Definition wieder: „[...][U]nter Krieg [wird] eine mit Waffengewalt geführte Auseinandersetzung zwischen zwei Gruppen verstanden, von denen wenigstens eine als reguläre Armee oder bewaffnete Streitkraft auftreten muß. [...][D]ie Tätigkeiten dieser Gruppen

[81] Vgl. Libicki, Martin C.: Cyberdeterrence and Cyberwar, Studie der RAND Corp. 2009, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf, S. 41–42.
[82] Vgl. Rid, Cyber War Will Not Take Place, S. 20.
[83] Vgl. o.V.: „USA wollen Hackerangriffe zum Kriegsgrund erklären“, 31.05.2011, www.handelsblatt.com, (16.07.2013).
[84] Vgl. Barnes, Julian E./Page, Jeremy: „Hackerangriffe belasten Beziehungen zwischen USA und China“, 20.02.2013, www.wallstreetjournal.de, (16.07.2013).
[85] Vgl. Rid, Cyber War Will Not Take Place, S.161-162.
[86] Vgl. Skierka, Isabel: Kampf um die Netzherrschaft, ADLAS 1/2013, S. 12.
[87] Von Clausewitz, Carl: Vom Kriege, Berlin 1832.

[sollen] organisiert und zentral gelenkt sein [...]. Des Weiteren sind diese Gruppen jeweils souveräne Vereinigungen meistens mit staatlichem Charakter [...].“[88] Daraus ergibt sich die Kontroverse ob gängige Cyberangriffsformen überhaupt als Waffen bezeichnet werden können. Die bekannten Cyberangriffsformen sind (D)DoS-Angriffe, *Exploits* und Sabotagesoftware wie *Stuxnet*. (D)DoS Attacken können in ihrer Wirkungsweise mit „virtuellen Sitzblockaden“ verglichen werden.[89] Sie nutzen die technische Gegebenheit der begrenzten Rechen- und Speicherkapazität eines Host-Servers aus. Ein (D)DoS-Angriff bewirkt keine physischen Schäden an betroffenen Systemen. Daher ist ein (D)DoS-Angriff als missbräuchliche Verwendung der technischen Möglichkeiten zu bewerten, erfüllt z.B. in Deutschland den Straftatbestand der Computersabotage[90], ist aber keine Waffe. Spionage-Software wie *Flame* erzeugt ebenfalls keinen physischen Schaden, sondern beutet technische Möglichkeiten aus. Die Benutzung von Malware zu Spionagezwecken stellt ebenfalls einen Straftatbestand dar[91], ist aber ebenfalls eindeutig keine Waffe. Im Prinzip verhält es sich bei Sabotage-Software wie *Stuxnet* ähnlich, wobei die nachhaltigen Folgewirkungen physischer Natur sein können. Der Schadcode verändert die Funktionsweise der EDV, dies führt zu einer Fehlfunktion der einzelnen Anlagenkomponenten, welche final einen physischen Schaden oder gewaltsame Wirkung entfalten können. D.h. die Malware löst indirekt Gewalt aus. Da Schadsoftware wie *Stuxnet* generisch ist, kann sie theoretisch auf verschiedenartige Anlagenkomponenten unterschiedliche Wirkungen erzielen, daher kann auch das Ausmaß des Schadens variieren.[92] Durch die indirekte physische Wirkung erfüllt *Stuxnet* tendenziell die notwendige Bedingung der Gewaltausübung, kann also durchaus als waffenähnlich eingestuft werden, obwohl die physikalischen Mittel z.B. Ventile und Zentrifugen eindeutig keine Waffen sind. Rid führt dafür den Begriff *code-caused violence* ein, um den Vorgang der Modifikation eines Gegenstandes in eine Waffe durch den Schadcode zu beschreiben.[93] Das die Gewaltauswirkungen das zentrale Moment ist, lässt sich auch aus dem *Tallinn Manual* der NATO entnehmen. Dort wird eine Cyberattacke als solche definiert sobald sie Schäden an Personen und Objekten verursacht. Interessanterweise gilt dies sowohl für offensive als auch defensive Operationen.[94] Dennoch kann auch *Stuxnet* nicht als kriegerischer Akt gewertet werden, da durch die Non-Attribution keine Kombattanten auszumachen sind, somit die hinreichende Bedingung der völkerrechtlichen Definition, der Partizipation einer zentral organisierten Gruppe mit staatlichem Charakter, nicht erfüllt ist. Einen Höhepunkt erreichte diese Debatte im Mai 2011 als die USA Cyberangriffe als *Act of War* klassifizierten.[95] Legitimiert wird dies durch das Recht auf Selbstverteidigung nach Art. 51 der UN-Charta. Die USA bezeichnen also das Resultat der Cyberattacke als *Act of War*. Als Rückschluss wird, natürlich nicht ganz uneigennützig, der Besitz oder das Ausbringen von Malware nicht als Kriegsakt bewertet. Das wirkt

[88] Vgl. Imbusch, Peter/Zoll, Ralf (Hrsg.): Friedens- und Konfliktforschung. Eine Einführung, 5. Aufl., Wiesbaden 2010, S. 109.

[89] Vgl. Gaycken, Die vielen Plagen des Cyberwar, S. 94.

[90] StGB § 303b Computersabotage, auf: Juris Rechtsportal des BMJ, http://www.gesetze-im-internet.de/stgb/__303b.html, (17.07.2013).

[91] StGB § 202c Vorbereitung des Ausspähens und Abfangens von Daten, auf: Juris Rechtsportal des BMJ, http://www.gesetze-im-internet.de/stgb/__202c.html, (17.07.2013).

[92] Vgl. Langner, Ralph: Stuxnet knacken, eine Cyber-Waffe des 21. Jahrhunderts, März 2011, www.ted.com, (17.07.2013).

[93] Vgl. Rid, Cyber War Will Not Take Place, S. 13.

[94] Vgl. Tallinn Manual on the International Law applicaple to Cyber Warfare, http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf, (18.07.2013), S. 92. Anmerkung: Am 29.04.2013 bezeichnete die Bundesregierung in ihrer Antwort auf eine Kleine Anfrage das Tallinn-Handbuch als eine „rechtlich nicht bindende Darstellung völkerrechtlicher Regeln [...], die nach Ansicht [...] der Sachverständigen, [...] auf Cyberoperationen oberhalb der Schwelle des bewaffneten Konflikts Anwendung findet.“, siehe: Drucksache 17/13357.

[95] Vgl. Gorman, Siobhan/Barnes, Julian E.: Cyber Combat: Act of War, 30.05.2011, www.online.wsj.com, (16.07.2013).

zunächst legitim aus Sicht der oben entwickelten Ableitung, da eine Cyberangriffsform erst als waffenähnlich angesehen werden kann, wenn sie physischen Schaden anrichtet oder zu menschlichen Opfern führt. Dies bedeutet im Umkehrschluss, dass momentan kein Cyberwar stattfindet, da weder massive Schäden an Menschen noch an Gegenständen durch Cyberangriffe nachgewiesen wurden. *Stuxnet* tangierte allerdings schon die Kategorie „physischer Schaden“, erreichte aber nicht die Intensität konventioneller Waffen. Im September 2011 haben Russland und China ein Cyber-Rüstungsabkommen bzw. Cybersicherheitsabkommen auf UN-Ebene vorgeschlagen. Aus drei Gründen kann die Umsetzung und die Wirksamkeit eines solchen Abkommens bezweifelt werden. Erstens lassen sich kriminelle Cyberaktivitäten kaum von staatlichen unterscheiden, da in den überwiegenden Fällen die gleichen Hackertools verwendet werden. Zweitens lassen sich die offensiven Cyberkapazitäten nicht kontrollieren bzw. sind leicht zu verbergen. Drittens löst ein Abkommen das diplomatische Problem der Non-Attribution nicht.[96]

3. Akteure und Interessengruppen

3.1 Staaten, Geheimdienste und Militär

Die Rolle der Staaten, ihrer Geheimdienste und Streitkräfte als zentrale Akteure sind das Hauptaugenmerk der Kontroverse um den Cyberkrieg. Die größten Kapazitäten lassen sich in Russland, China und den USA verorten, gefolgt von Israel, Frankreich, Großbritannien und Estland. Auch Schwellenländer wie Indien und Brasilien arbeiten an dem Aufbau von Cyberkapazitäten. Ebenfalls lassen sich in Nordkorea und dem Iran solche Kapazitäten vermuten. Eine exakte quantitative Einordnung abzugeben, ist schwierig. Die Zahlen variieren je nach Quelle stark und eine einheitliche Definition was einen „Cyberkrieger“ ausmacht fehlt, des Weiteren unterliegen viele Informationen staatlicher Geheimhaltung. Die allgegenwärtige Dokumentation und Spekulation eines vermeintlichen Cyber-Wettrüstens zwischen China und den USA lässt die journalistische und wissenschaftliche Auseinandersetzung mit Russland oft in den Hintergrund geraten. Über Russlands Cyberkapazitäten lassen sich wegen des undurchsichtigen Netzwerks zwischen Militär, Geheimdiensten und kriminellen Organisationen nur Vermutungen anstellen.

Die technologische Entwicklung kann durchaus als *game-changing* für zwischenstaatliche Konflikte und internationale Beziehungen interpretiert werden. Vor allem Big Data und die Non-Attribution geben den Geheimdiensten ein breites Spektrum an neuen, risikoarmen und komfortablen Optionen zur Informationsgewinnung und Durchführung verdeckter Operationen z.B. *Economic Operations* (EcoOps) oder *Information Operations* an die Hand.[97] Dennoch erhöht sich das Risiko einer Verschlechterung des diplomatischen Klimas z.B. durch Enthüllungen oder Vermutungen und Anschuldigungen aus machtstrategischen Erwägungen. Hinzu kommt, dass Bürger- und Freiheitsrechte eingeschränkt werden, denn das Internet lässt die Trennlinie zwischen innerer und äußerer geheimdienstlicher Aufklärung verschwimmen: „[...] it[`s] impossible to identify a specific piece of intelligence as foreign or domestic.“[98] Das Militär profitiert im Konfliktfall von der umfangreichen Aufklärung der Geheimdienste und verfügt durch moderne IT über ein breites Portfolio an Optionen zur elektronischen Kampfführung (EloKa). Die Störung (*Jamming*) von feindlichen Kommunikations- und Aufklärungskanälen existiert zwar schon seit dem Zweiten Weltkrieg, wird aber stets weiterentwickelt und adaptiert zunehmend moderne IT. Letztendlich ist ein Großteil der modernen IT und EDV vom Militär oder ursprünglich für das Militär entwickelt worden, auch das Internet ist eine Schöpfung des US-Militärs. Die aktuelle Debatte vernachlässigt diese Zusammenhänge eindeutig. Viele Publikationen erwecken den Eindruck das Militär hätte den Cyberspace neuerlich für seine Zwecke entdeckt, wie sich an der Rhetorik betreffend der „Fünften Dimension des

[96] Vgl. Rid, Thomas: Think Again: Cyberwar, März/April 2012, www.foreignpolicy.com, (18.07.2013).

[97] Vgl. Gaycken: Cyberwar. Das Wettrüsten hat längst begonnen, S. 144–146; 149; 152.

[98] Vgl. Rid, Cyber War Will Not Take Place, S. 112.

Krieges“ erkennen lässt. Das Militär hat die virtuelle, elektronische Kampfführung weder neu für sich entdeckt, noch hat es diese Domäne nach dem Zweiten Weltkrieg je verlassen. Es war eine neue Unternehmenskultur aus dem *Silicon Valley*, die Technologien des Militärs modifizierte und der Zivilgesellschaft zugänglich machte. EloKa und der Begriff Cyberattacke werden in manchen Quellen auch synonym verwendet. Beispielsweise bezeichnet Clarke die Störung der syrischen Radaranlagen im Zuge der *Operation Orchard* 2007, bei der die israelische Luftwaffe eine illegale Atomanlage in Syrien zerstörte, als Cyberangriff.[99] Mit welcher Methode die Israelis die syrische Luftabwehr sabotierten und ob dabei Hackertools genutzt wurden, ist allerdings unklar. Staaten verfolgen zurzeit vier Hauptinteressen, welche sie mithilfe ihrer jeweilig zur Verfügung stehenden Cyberkapazitäten umsetzen: Erstens sollen eigene Einflussmöglichkeiten über die Gestaltung des Internet erhalten und ausgebaut werden, auch mit Hinblick auf zukünftige Verhandlungen über einen internationalen Rechtsrahmen für das Netz. Zweitens ist das Internet nach wie vor ein umkämpfter Markt, d.h. Staaten haben ein Interesse daran, dass sich ihre Internet- und Dienstleistungsbranche gut positionieren kann. Drittens ist die Überwachung der gegnerischen Datenströme von zentraler Bedeutung, sowie die Informationsgewinnung durch Ausspähen der IT anderer Staaten, deren Industrie und militärischer Strukturen. Viertens ist die Überwachung der nationalen Datenströme unter dem Aspekt der inneren Sicherheit relevant – in autoritären Staaten auch um subversive Bewegungen zu unterbinden. Dem offensiven Nachgehen dieser Interessen sind Grenzen gesetzt. Beispielsweise wird der Vorteil einer verdeckten Operation durch die Non-Attribution bei zu aggressivem Vorgehen obsolet. Interdependenzen durch die globalisierte Weltwirtschaft können ebenfalls als limitierendes Moment hinzugezogen werden.

3.2 Privatunternehmen

Das Geschäft mit Cybersecurity ist für viele private Unternehmen einträglich. Sie können von dem alarmierenden Klima in den Medien und der Politik profitieren. Hier sind zunächst die bekannten Anti-Virenprogramm-Anbieter wie *Kaspersky*, *Avast*, *Symantec* etc. zu nennen. Sie verkaufen Sicherheitssoftware an private User und Unternehmen. Diese Anbieter sind mit dem Problem konfrontiert, dass täglich eine erhebliche Anzahl neuer Malware-Varianten erscheint[100], da oft schon geringe Modifikationen der Malware ausreichen um Virenscanner zu umgehen. Ein ethisch fragwürdigeres Geschäftsmodell haben private Sicherheitsfirmen aus der Branche der *Private Military Companies* (PMCs), die ebenfalls den Cybersecurity Markt besetzen. Ihre Geschäfte machen sie mit Staaten, Geheimdiensten, Militär und Großindustrie. Ein Beispiel ist das französische Unternehmen *VUPEN Security*. *VUPEN* verkauft Sicherheitskonzepte für die Industrie, Regierungen und *Computer Emergency Response Teams* (CERTs).[101] Gleichzeitig bietet das Unternehmen auch ein umfangreiches Angebot an offensiven Cyberwerkzeugen für Staaten und ihre Geheimdienste an. Neben Malware lassen sich auch hochentwickelte *Zero-Day Exploits* erwerben. *VUPEN* weist ausdrücklich darauf hin, dass sie Produkte nicht bei Dritten erwerben sondern hauseigen entwickeln und nur an vertrauenswürdige Staaten und ihre rechtstaatlich kontrollierten Agenturen verkaufen, sowie alle internationalen Embargos und restriktiven Maßnahmen der EU gegenüber Drittstaaten einhalten.[102] Problematisch sind diese Geschäfte, da der Verdacht besteht, dass einige Unternehmen ihre Sicherheitslücken nicht nur durch eigene Forschung sondern auch am globalen Schwarzmarkt für Malware und *Zero-Days* beziehen. Es existiert ein Markt für Sicherheitslücken, auf dem autarke Hacker gefundene Schwachstellen an die großen Software-Unternehmen verkaufen. Die höchsten Gewinne lassen sich mit *Zero-Day* Lücken er-

[99] Vgl. Clarke/Knake, World Wide War, S. 22–26.

[100] Vgl. Ziemann, Frank: „Anzahl der Schädlinge nimmt rasant zu“, 24.5.2013, www.pcwelt.de, (18.07.2013).

[101] Vgl. VUPEN Security Homepage, siehe Reiter: Industry Solutions, http://www.vupen.com/english/services/solutions.php, (18.07.2013).

[102] Vgl. ebd., siehe Reiter: Products, http://www.vupen.com/english/services/lea-index.php, (18.07.2013).

zielen. Die Preise für eine Lücke variieren je nach Software und Schweregrad der Schwachstelle zwischen 5000 und 250.000 US-Dollar.[103] Firmen wie *Google* oder *HP* veranstalten auch regelmäßige Live-Hack-Events bei denen Hacker sich Preisgelder verdienen können. Viele Hacker verkaufen aber eher an PMCs, weil deren Kunden um ein vielfaches höhere Preise vor allem für *Zero-Day Exploits* bezahlen.[104] Zudem wächst der Schwarzmarkt stetig, weil neben dem organisierten Verbrechen auch Staaten und PMCs ihre Kapazitäten aus diesem Markt erwerben können. Insidern zufolge treten gerade die USA besonders kaufkräftig auf.[105] Dieses Verhalten von staatlichen Akteuren und PMCs ist äußerst kritisch zu bewerten, da in diesem Preiskampf die Softwarebranche und somit letztendlich auch alle Privatkunden benachteiligt sind. Des Weiteren werden immer lukrativere finanzielle Anreize für die kriminelle Hackerszene und das organisierte Verbrechen geschaffen.

3.3 Hacker und Hackaktivisten

Die Hackerszene kann als äußerst heterogen und intransparent bezeichnet werden. Die bekannteste Hackeraktivistengruppe ist *Anonymous*. Die Strukturen und Hierarchien des Hackerkollektivs sind nebulös. Neben ihren Aktivitäten im Internet treten die Anonymus-Sympathisanten auch bei Demonstrationen regelmäßig in die Öffentlichkeit. Solidarität wird durch die charakteristische *Guy Fawkes* Maske ausgedrückt. Die bekanntesten Aktionen waren z.B. die breite Kampagne gegen Scientology namens *Project Chanology* im Jahr 2008[106] und *Operation Payback* im Jahr 2010, bei der eine Reihe von DoS-Angriffen gegen die Webseiten der Finanzdienstleiter *Mastercard*, *Visa* und *Postfinance* ausgeübt wurden, nachdem diese die Spendenabwicklung der Enthüllungsplattform *WikiLeaks* eingestellt hatten.[107]

Grundsätzlich lassen sich Hacker in drei Kategorien einordnen, die sogenannten *White Hats*, *Black Hats* und *Grey* (Gray) *Hats*. *White Hats* sind „ethische“ Hacker, die ihre Fähigkeiten für rechtschaffende Zwecke verwenden. Sie unterstützen Organisationen und Unternehmen dabei ihre Computersicherheit zu verbessern, indem sie auf Sicherheitslücken aufmerksam machen und *penetration tests* durchführen, bei denen sie unter Absprache der Inhaber in Systeme einbrechen um Schwachstellen zu finden.[108] *Black Hats* sind kriminelle Hacker, die in Systeme einbrechen um persönliche Daten, Kreditkartennummern etc. zu stehlen und kriminell auszubeuten. Wenn *Black Hats* Sicherheitslücken, oder gar eine *Zero-Day*-Schwachstelle entdecken, verkaufen sie diese auch an kriminelle Organisationen. Der Aufbau von Botnetzen fällt ebenfalls unter *Black Hat* Aktivitäten.[109] *Grey Hats* stehen zwischen *White* und *Black Hats*. I.d.R. sind sie nicht kriminell, begehen aber dennoch Straftaten, da sie im Gegensatz zu *White Hats* ohne Wissen der Inhaber in Systeme einbrechen. Sicherheitslücken enthüllen *Grey Hats* meistens öffentlich auf einschlägigen Webseiten.[110] Die DoS-Attacken der *Anonymous*-Aktivisten können ebenfalls in dieser Grauzone verortet werden.

4. Der Krieg im Netz – nur ein Hype ?

4.1 Fragwürdige Analogien

In vielen Beiträgen von Politikern, Journalisten und Wissenschaftlern wird eine regelrechte Endzeitstimmung durch zum Teil überzogene Vergleiche erzeugt. Dazu werden oft Analo-

[103] Vgl. Greenberg, Andy: „Shopping For Zero-Days: A Price List For Hackers’ Secret Software Exploits“, 23.03.2012, www.forbes.com, (19.07.2013).
[104] Vgl. Greenberg, Andy: „Meet The Hackers Who Sell Spies The Tools To Crack Your PC“, 21.03.2012, www.forbes.com, (19.07.2013).
[105] Vgl. Paganini, Pierluigi: Zero-Day Black Market: Governments are the biggest costumers, 21.05.2013, www.hplusmagazine.com, (19.07. 2013).
[106] Vgl. Dahdah, Howard: „’Anonymous’ group declares online war on Scientology“,08.02.2008, www.computerworld.com, (18.07.2013).
[107] Vgl. o.V.: „Operation Payback: Hacker-Großangriff auf Mastercard, Visa & Co“, 08.12.2010, www.spiegel.de, (18.07.2013).
[108] Vgl. o.V.: „Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats“, o.D., www.howtogeek.com, (18.07.2013).
[109] Vgl. ebd.
[110] Vgl. ebd.

gien zu Nuklearwaffen und dem Kalten Krieg herangezogen. Viele Beiträge greifen auf fiktive Szenarien zur Argumentationsführung zurück, da es an eindrucksvollen empirischen Beispielen fehlt. Legitimiert wird dieses Ausweichen auf Fiktion meist mit dem Hinweis, dass die Entwicklung von Cyberwaffen erst am Anfang stünde. Die Analogie zum Kalten Krieg oder Nuklearwaffen stammt aus US-Militärkreisen. Hier wird versucht aus Nuklearwaffenstrategien und der Doktrin des Kalten Krieges Ableitungen zu generieren, die für eine Cyberstrategie nützlich sein könnten, wie es beispielsweise in Libickis Ausführungen zu den begrenzten Abschreckungsmöglichkeiten durch Cyberwaffen deutlich wird.[111] Diese Überlegungen sind grundsätzlich legitim, da sie auf der strategischen Ebene verbleiben. Das Problem ist das Überschreiten der Linie hin zum sachlichen Vergleich. Dieser führt zu fragwürdigen Aussagen wie, *Zero-Day Exploits* seien waffenfähige Lücken, hoch angereicherte Bits und Bytes und ein Grundbaustein von Cyberwaffen, in etwa Äquivalent zu Uranerz beim Bau von Nuklearwaffen.[112] Solche Vergleiche – hier stellvertretend für viele andere – sind sachlich inadäquat. Die Bezeichnung *Zero-Day* beschreibt lediglich, dass die Lücke unbekannt ist, was die Chance erhöht sich unerlaubten Zugang zu verschaffen. Für diesen Zugang muss aber nichts „angereichert“ werden. Hier entsteht der falsche Eindruck die Lücke würde in irgendeiner Weise additiv modifiziert werden, um daraus resultierend als „Waffe“ nutzbar zu sein. Eine martialische Wortwahl und Vergleiche mit konventionellen Waffen sollten vermieden werden, da dies unsachliche und falsche Assoziationen weckt. Denn es lässt sich nach allen Cyberattacken der letzten 20 Jahre nicht ein einziges menschliches Opfer konstatieren. Die zweifelhafte Einordnung der empirischen Lage wird durch öffentliche Aussagen insbesondere der amerikanischen Eliten noch begünstigt. 2012 warnte Leon Panetta vor einem möglichen „Cyber-Pearl Habor“[113], Janet Napolitano gar vor einem „Cyber 9/11“.[114] All diese Analogien sind fehlleitend, weil sie in keiner angemessenen Relation zur Wirklichkeit stehen. In journalistischen und wissenschaftlichen Publikationen wird nicht deutlich genug auf die metaphorische Verwendung von Begriffen und Vergleichen hingewiesen. Daraus resultiert ein relativ unsachliches Diskussionsklima – ein Hype. Dies lenkt von den tatsächlichen Problemen und Risiken, die auch kritische Infrastruktur betreffen, ab.[115] Des Weiteren entsteht der Eindruck, die alarmierenden Szenarien dienen zur Promotion gesellschaftlicher Akzeptanz gegenüber einer „Versicherheitlichung“ des Internets und der Investition in umfassende Überwachungs- und Offensivkapazitäten.[116] An dessen Stelle sollte in Forschung und Entwicklung einer sichereren Infrastruktur und risikoärmerer Prozesse investiert werden.

4.2 Die „Mär“ von den geringen Kosten

Die vergangenen Dekaden zeichnen sich durch asymmetrische Konflikte aus. Die westlichen Alliierten gelten dabei als militärisch überlegen. Einige Experten warnen davor, dass sich diese Asymmetrie in eine Anti-Asymmetrie zu Ungunsten der entwickelten Staaten verkehren könnte, da sich auch schwächer entwickelte Länder Cyberkapazitäten aneignen werden.[117] Begründet wird dies durch die geringeren Kosten im Vergleich zur konventionellen Rüstung, des verminderten Risikos aufgrund der Non-Attribution und der kleineren Angriffsfläche für Cyber-Gegenschläge. Clarke entwickelt diese These am Beispiel Nordkorea.

[111] Vgl. Libicki, Martin C.: Cyberdeterrence and Cyberwar, Studie der RAND Corp. 2009, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

[112] Vgl. Dölling, Stefan: „Das Geschäft mit der Lücke“, ADLAS 3/2012, S. 72.

[113] Vgl. Bumiller, Elisabeth/Shanker, Thom: „Panetta Warns Dire Threat of Cyberattack on U.S.“, 11.10.2012, www.nytimes.com, (20.07.2013).

[114] Vgl. Briand, Xavier/Charles, Deborah: „U.S. homeland chief: cyber 9/11 could happen “imminently““, 24.01.2013, www.reuters.com, (20.07.2013).

[115] Vgl. Rid, Thomas: „The Great Cyberscare“, 13.03.2013, www.foreignpolicy.com, (20.07.2013).

[116] Vgl. Ludwig, Sören: Mächtige Worte, in: ADLAS 1/2013, http://adlasmagazin.files.wordpress.com/2013/02/adlas-0113.pdf, (20.07.2013), S. 17–19.

[117] Vgl. Clarke/Knake, World Wide War, S. 190–196; vgl. Gaycken, Cyberwar. Das Wettrüsten hat längst begonnen, S. 61ff.

Wenn die Nordkoreaner Cyberangriffe gegen die USA durchführen würden, stünden sie vor einer breiten Auswahl an potentiellen Zielen, hätten durch Non-Attribution und wenige Ziele für amerikanische Gegenschläge im eigenen Land, nur einen kleinen Wetteinsatz zu leisten.[118] Solch ein Kosten-Nutzen Kalkül wäre auch für terroristische Organisationen denkbar, da die Kosten für die Hardware, Internetanschluss und kritische Sicherheitslücken auf dem Schwarzmarkt gering sind. Das Risiko wird allerdings als gering eingeschätzt, weil terroristischen Gruppen die technische/wissenschaftliche Expertise fehlt.[119] Viele Thesen lassen sich auch anhand empirisch belegbarer Cyberangriffe entkräften. Der Fall *Stuxnet* zeigte, dass für einen Angriff mit physischer Schadenswirkung ein enormes Aufgebot an geheimdienstlichen und fachwissenschaftlichen Ressourcen aufgebracht werden muss. D.h. der Anschaffungspreis für die Hardware und Schadsoftware ist in der Tat gering, bildet aber nur einen Bruchteil der tatsächlich benötigten finanziellen und strukturellen Mittel. Eine ergänzende These betrifft die Symbolträchtigkeit. Gerade in Diktaturen müssen Angriffe oder Provokationen gegenüber dem Feind möglichst propagandistisch ausgeschlachtet werden können, verdeckte Cyberoperationen eignen sich dafür nicht. Eine Asymmetrie zum Nachteil der westlichen Staaten ist nur bei der Cyberspionage, insbesondere bei Industriespionage, zu erkennen. In Folge des Ungleichgewichts an Know-how, haben die westlichen Staaten mehr zu verlieren, als sie durch eigene Spionagetätigkeiten gewinnen könnten.[120]

4.3 Gibt es wirksamen Schutz?

Es gibt eine Vielzahl verschiedener Schutzmaßnahmen, allerdings ist es fraglich ob sich ein ganzheitlicher Lösungsansatz entwickeln ließe. Aktuell stützt sich die Sicherheitsarchitektur im IT Bereich vor allem auf präventive Softwarelösungen, z.B. Firewalls, Anti-Virenprogramme etc. Wie jede andere Software hat auch Sicherheitssoftware Lücken. Nachdem eine Lücke bekannt geworden ist, wird diese durch einen Patch oder Update geschlossen, es findet eine ständige Koevolution zwischen Malware und Schutzsoftware statt. Im Falle eines erfolgreichen Angriffs oder eines Systemausfalls können Unternehmen und Behörden auf CERTs zurückgreifen, diese Expertenteams bieten Ad-hoc-Lösungen an, um Computersysteme und Netzwerke zu stabilisieren und wiederherzustellen. Viele Staaten verfügen zudem über defensive Cybereinheiten, die ihre militärischen und geheimdienstlichen Netze schützen sollen. Diese Maßnahmen erscheinen aus Sicht einiger Sicherheitsbehörden nicht mehr ausreichend. Gerade in den USA wird eine stärkere Kontrolle der Datenströme angestrebt. Clarke verdeutlicht in seinen Ausführungen, dass totalitäre Staaten einen defensiven Vorteil bei Cyberangriffen hätten, weil deren Regierungen über umfassendere Mittel verfügen um Datenströme aus dem Ausland zu unterbinden. Dies verdeutlicht er am Beispiel des chinesischen Intranets: der *Great Firewall*. Für die USA schlägt Clarke das Konzept der „defensiven Triade“ vor. Ein Hauptbestandteil seines Konzepts ist die breite Anwendung einer *Deep Packet Inspection* (DPI) an allen amerikanischen Internetknotenpunkten.[121] DPI ermöglicht es alle Datenpakete an Knotenpunkten auf Verbindungsdaten und Inhalt hin zu prüfen und Malware auszufiltern, allerdings ist diese Technik in Bezug auf Datenschutz, Post- und Fernmeldegeheimnis sehr fragwürdig.[122] De facto wenden Provider DPI bereits an und da die amerikanische NSA scheinbar Zugriff auf die Daten der Unternehmen hat, ist die von Clarke geforderte

[118] Vgl. Clarke/Knake, World Wide War, S. 194–196.
[119] Vgl. Gaycken, Sandro: „Sicherheit im Netz“ (Expertengespräch), Stellungnahme in der Enquete-Kommission Internet und digitale Gesellschaft vom 28.11.2011, http://www.bundestag.de/interneten quete/dokumentation/Zugang_Struktur_und_Sich erheit_im_Netz/PGZustrSi_2011-11-28_oeffentlich es_Expertengespraech/PGZuStSi_2011-11-28_Expe rtengespraech_Stellungnahme_DrGaycken.pdf.
[120] Vgl. Gaycken, Cyberwar. Das Wettrüsten hat längst begonnen, S. 112–113.
[121] Vgl. Clarke/Knake, World Wide War, S. 206 ff.
[122] Vgl. o.V.: DPI, Lexikoneintrag auf IT Wissen, www.itwissen.info/definition/lexikon/DPI-deep-packet-inspection.html, (19.07.2013).

staatlich überwachte DPI in den USA bereits umgesetzt. DPI schützt aber kaum vor hochentwickelten Cyberangriffen, da das Problem der Innentäter bleibt und sich Malware auch auf viele Datenpakete stückeln und verbergen lässt. DPI nützt also in erster Linie der staatlichen Überwachung.
Eine weitere Möglichkeit sensible Bereiche zu schützen, wäre die gezielte Entnetzung, vor allem im Bereich kritischer Infrastruktur.[123] Für geheime Informationen wäre theoretisch auch eine Analogisierung denkbar, der russische FSO nutzt angeblich für besonders sensible Dokumente wieder Schreibmaschinen.[124] Letztendlich bietet auch die Komplexität der Systeme an sich Schutz: „Building and deploying Stuxnet required extremely detailed intelligence about the systems it was supposed to compromise, and the same will be true for other dangerous cyberweapons. Yes, convergence, standardization, and sloppy defense of control-systems software could increase the risk of generic attacks, but the same trend has also caused defenses against the most coveted targets to improve steadily and has made reprogramming highly specific installations on legacy systems more complex, not less.“[125]
Zusammenfassend lässt sich festhalten, dass es keine ganzheitliche defensive Lösung gibt. Die IT und EDV in ihrer gegenwärtigen Form birgt ein Grundrisiko, welches sich technisch momentan nicht beseitigen lässt. Gezielte Angriffe bleiben dennoch schwierig aufgrund der Komplexität des Gesamtsystems. Das fortschreitende Integrieren kritischer Infrastruktur in Netzwerke sollte trotz aller betriebswirtschaftlichen Vorteile überdacht werden.

5 Konklusion

An den vorgestellten Kategorien wird deutlich, dass es sich beim Phänomen Cyberwar um kein Novum handelt, auch die Bezeichnung als „fünfte Domäne des Krieges“ ist irreführend und nicht zutreffend. Cyber-Sabotage, Spionage und Subversion eröffnet keine neuartigen *Theatres of War*, denn im Kern greifen Geheimdienste und Militär nur die erweiterten technologischen Möglichkeiten der sich ständig weiterentwickelnden Telekommunikationsmittel und Technologien auf. Alle bekannten Cyberzwischenfälle lassen sich bewährten Kategorien zuordnen: Sabotage und EloKa, sowie Spionage und Subversion. Die Analyse der verschiedenen Cyberangriffsformen zeigt, dass die meisten Cyberangriffe entweder gar kein oder nur indirektes Gewaltpotential aufweisen, somit nur sehr bedingt als Cyberwaffen bezeichnet werden sollten. Das Präfix „Cyber“ ist durchaus zur Orientierung sinnvoll, um die Art und die technischen Mittel von Sabotage- oder Spionageakten zu verdeutlichen. Erschwerend kommt hinzu, dass es keine international verbindlichen Definitionen des Cyberwar gibt, was auch an der konzeptionell fragwürdigen Ausgestaltung des Begriffs selbst liegt. Diese Umstände verleihen der weltweiten Diskussion einen gewissen Grad an Willkürlichkeit. Die Benutzung des Begriffs Cyberwar wäre nur dann eindeutig und unmissverständlich, wenn sich zwischenstaatliche Konflikte ausschließlich in den genannten Bereichen und nur mit virtuellen Mitteln abspielen würden. Solch ein Szenario ist allerdings empirisch nicht festzustellen. Der Begriff Cyberwar wird, wie viele andere Bezeichnungen für digitale Sachverhalte, im metaphorischen Sinne benutzt. Diese übertragende Verwendung wird in den meisten Publikationen oder Pressemeldungen nicht hinreichend deutlich gemacht. Die allgemeinen Assoziationen, die sich in der Öffentlichkeit verständlicherweise beim Begriff Krieg ergeben, wie Gewalt, Angriffe und Waffen, stellen ein verzerrtes Bild der tatsächlichen Lage dar. Das Bedrohungsszenario ist nicht so verheerend einzuschätzen, wie viele Experten, Politiker und Journalisten der Öffentlichkeit glauben machen wollen. Letztendlich ist die Effektivität aller Bereiche des Cyberwar in Frage zu stellen. Der Iran hielt zunächst[126] unverändert an seinem Atompro-

[123] Vgl. Karger, Michael/Gaycken, Sandro: Entnetzung statt Vernetzung, in: MultiMedia und Recht 1/2011, www.it-rechts-praxis.de/files/Entnetzung_Gaycken_Karger_MMR_2011.pdf, (21.07.2013).
[124] Vgl. o.V.: „Hacker Abwehr: Russischer Geheimdienst FSO setzt auf Schreibmaschine“, 11.07.2013, www.spiegel.de, (21.07.2013).
[125] Vgl. Rid, Think Again: Cyberwar.

[126] Durch die erfolgreichen Verhandlungen in Genf vom 24.11.2013 kann vorerst eine Entspannung der diplomatischen Lage gegenüber dem Iran und

gramm fest, obwohl das Regime nach Ansicht der Experten mit der schlagkräftigsten „Cyberwaffe“ bis dato konfrontiert war. Natürlich haben die USA vermutlich Zeit gewinnen können, um Israel zur militärischen Zurückhaltung gegenüber dem Iran zu bewegen. Jedoch sind Cybersabotageakte sehr komplex, zeitraubend und ressourcenaufwändig. Daher ist in naher Zukunft nur vereinzelt mit solchen Ereignissen zu rechnen. Cyberangriffe zu Spionagezwecken sind dagegen lohnenswerter für den Urheber. Die aktuelle Form der Cyberspionage dient vor allem Überwachungszwecken. Dies wiederum kann sich als effektive Waffe gegen Cybersubversion eignen oder im Kontext von Informationskriegen nützlich sein. Cyberüberwachung durch Cyberspionage hilft insbesondere autoritären Staaten, um ihre Bevölkerungen zu kontrollieren und Repressalien gegen Oppositionelle zu ergreifen. Die NSA-Enthüllungen stellen allerdings auch den USA und den demokratischen europäischen Staaten ein erschreckendes, wenngleich nicht überraschendes Zeugnis aus. Die USA werden auch in Zukunft an ihrer Strategie der größtmöglichen Überwachung festhalten, wie aus der Veröffentlichung aktueller Strategiepapiere der NSA hervorgeht.[127] Die Gründe für die diffuse Gemengelage der Diskussion sind folgende: Erstens ist die Interpretierbarkeit der empirischen Lage sehr weitläufig, da viele Details im Verborgenen liegen. Zweitens verfolgen viele Staaten eine eigene Agenda und versuchen zumindest ihren nationalen Diskurs diesbezüglich zu lenken. Dabei liegt es im Interesse des jeweiligen Militärs zusätzliche Haushaltsmittel für Cybersicherheit und Cyber-Offensiv-kapazitäten zu erhalten. Drittens existiert eine breite Anzahl an privaten Nutznießern, wie Sicherheitsunternehmen und Software-Hersteller, denen ein alarmierendes Klima weiterhin gute Geschäfte verheißt. Viertens erfährt das ganze Themenfeld in allen Facetten hohe mediale Aufmerksamkeit, was beispielsweise Journalisten profitieren lässt. Der Cyberwar im engeren Sinne bleibt im Jahr 2014 folglich eindeutig ein Hype, der allerdings Großmächten wie den USA und China dazu dient machtpolitische Räume und Offensivfähigkeiten auszubauen. Das neben den zunehmenden geopolitischen Spannungen im Pazifikraum ein zusätzliches Konfliktfeld eröffnet wurde, kann als weiteres Eskalationspotential bewertet werden. Dieses Konfliktpotential, das sich aufgrund gegenseitiger Anschuldigungen der USA und China verschärfen könnte, fußt allerdings nicht primär auf den neuen Möglichkeiten der Technologien im Cyberspace, sondern vornehmlich auf realpolitischen und geostrategischen Erwägungen der involvierten Staaten.

dem umstrittenen Atomprogramm konstatiert werden.

[127] Vgl. Risen, James: „N.S.A. Report Outlined Goals for More Power“, 22.11.2013, www.nytimes.com, (25.11.2013).