Cyberwar- Probleme für die internationale Politik

Bachelorarbeit im 2-Fächer-Bachelor-Studiengang
Kernfach Politikwissenschaften
an der Universität Osnabrück

vorgelegt am 28.11.2011 in Osnabrück
von Florian Grunert

Inhaltsverzeichnis

1. Einleitung.....1

2. Analyse des Begriffs Cyberwar.....5
2.1 Der Einfluss von Kybernetik auf das Militär und seine Technik.....7
2.2.Was ist Krieg im klassischen Sinne des Rechts?.....11
2.3 Versuch einer Verknüpfung von Kybernetik und Krieg.....13

3. Was ist eine Domäne des Krieges?.....14
3.1 Eine engere Definition von Cyberwar.....17

4. Cyber Konflikte im Hinblick auf jus ad bellum.....18
4.1 Spionage im virtuellen Raum am Beispiel Titan Rain.....18
4.2 Sabotage mit Bits und Bytes am Beispiel Stuxnet.....22
4.3 Kriminalität im Usernet am Beispiel vom Kneber-Botnet.....27
4.4 Aktivismus im Netz am Beispiel von Cryptome.....29

5. Cyberwar im Hinblick auf jus in bello.....31
5.1 Georgien Russland Konflikt 2008.....31
5.2 Israel-Syrien Konflikt – Operation Orchard.....33

6. Die Dimension der Cyberkonflikte.....35
6.1 Bytes und Platinen- Differenzierungsprobleme für die internationale Politik.....35
6.2 NON-Attribution als Hauptproblem in Cyberkonflikten.....40
6.3 Institutionen in internationalen Cyberkonflikten.....41

7. Zusammenfassung.....42

8. Literaturverzeichnis.....44

9. Abbildungsverzeichnis.....51

Florian Grunert
Matrikelnummer: 933896

Cyberwar- Probleme für die internationale Politik

1. Einleitung

Zu Beginn der 90er Jahre wurden die verschiedenen Cyberangriffsszenarien nur theoretisch in politischen und militärischen Thinktanks diskutiert, denn die Vernetzung der Computer war noch nicht so komplex und fortgeschritten. Es ging zunächst nur um die theoretische Einbettung des Cyberwar auf staatlicher Ebene. Jedoch startete zum Beginn des 21. Jahrhunderts eine massive Ausbreitung von Informationstechnologien auf ziviler und militärischer Ebene, sodass ein Cyberspace[1] entstanden ist.

In dieser Arbeit geht es um Computer, Sicherheitspolitik, Cyberkonflikte und deren Interaktion. Der Cyberspace ist der Raum, in dem die genannten Aspekte zusammenfließen. Die Probleme ergeben sich aus diesem gemeinsamen Raum. Sowohl Begrifflichkeiten als auch reale Konflikte müssen aufgrund der neuen Bedingungen entwirrt werden. Eine Folie mit dem Titel *Cyberspacemodel*[2] soll die Thematik darstellen und eine klare Übersicht liefern.

Grundlegend kann der Cyberspace so beschrieben werden. Als Vorbedingung der ganzen Diskussion steht der Computer, welcher aus Software[3] und Hardware[4] besteht. Ein Computer verbunden mit anderen Computern ergibt ein Netzwerk. In diesem Netzwerk können die Computer Informationen austauschen. Jeder Computer ist ein Knotenpunkt in diesem Netzwerk. Wenn viele Netzwerke dieser Computer miteinander verbunden werden, entsteht ein größeres Netzwerk. Das Größte wird Internet[5]

1 Cyberspace refers to the electronic space created by computers connected together in networks like the Internet. http://www.techdictionary.com (kurz TD)
2 siehe Abbildung 1
3 Software is the program or set of programs that tell a computer what to do. TD
4 Hardware: The set of physical components that combine to make up a computer system (i.e., CPU, monitor, keyboard, or other mechanical, magnetic, or electronic devices) TD
5 A network of networks; a group of networks interconnected via routers. The Internet (with a capital I) is the world's largest internet. The biggest internet in the world. This worldwide information highway[the Internet] is comprised of thousands of interconnected computer networks, and reaches millions of people in many different countries. TD

genannt. Im Cyberspace selbst kann man heutzutage verschiedene Aktivitäten sehen wie Spionage, Sabotage, Aktivismus und Kriminalität. In dieser Arbeit wird geprüft, ob klassische Kriterien für Krieg, auch für den Krieg im Cyberspace gelten. Denn der Cyberspace hat mittlerweile eine Wichtigkeit in der Gesellschaft erlangt, sodass ihm eine politische und militärische Bedeutung zu gesprochen werden kann.

Die strategische Kriegsführung mit Hilfe von Computertechnologie ist nicht mehr wegzudenken aus der modernen Armee. Infrastruktur, Information und Identität gelten als potentielle Ziele für solche Angriffe. Als Infrastruktur kann alles bezeichnet werden, was das gesellschaftliche Leben ermöglicht (Wasser-, Strom- und Gasnetze z.B.). Informationen können sabotiert und ausspioniert werden. Identitäten können geklaut werden, um in Infrastrukturen einzudringen oder an Informationen zu gelangen. Der Einzug der Informationstechnologien in die Gesellschaft schafft neue Möglichkeiten der Kriegsführung in vielerlei Hinsicht.

Die vergangenen 12 Monate waren stark geprägt durch den Begriff Cyberwar. Dieser wurde über die Medien verbreitet. Doch die Aufarbeitung des Begriffes Cyberwar und die als solche deklarierten Geschehnisse wurden nicht immer durch wissenschaftliche Kriterien verifiziert. Dies hatte zur Folge, dass viele Aspekte wie Kriminalität und Aktivismus fälschlicherweise als Cyberwar bezeichnet worden sind. Zum Nachteil für Juristen, Wissenschaftler und Politiker, die durch schlechte Aufarbeitung des Begriffs meist keine fundierten Aussagen treffen konnten. Diese Arbeit soll den Begriff des Cyberwar analysieren, die wesentlichen theoretischen und praktischen Probleme aufzeigen und kritisch diskutieren.

Es soll eingangs versucht werden historische Merkmale der Entwicklung von Cyberwar hervor zu heben und diese in einen diskursiven Zusammenhang zu stellen. Die historische Betrachtung soll ein Grundverständnis des Begriffs liefern. Die Begriffe Kybernetik und Krieg, aus denen Cyberwar besteht, sollen geklärt und im Verhältnis zu den heutigen Szenarien betrachtet werden. Am Ende sollen die Begrifflichkeiten Kybernetik und Krieg zusammengeführt werden. Die Analyse des Begriffs Cyberwar ist

ein wichtiger Teil dieser Arbeit.

Der nächste Analysepunkt sind die Domänen des Krieges. Als die Domänen des Krieges werden der Krieg zu Land, auf Wasser, in der Luft und im Weltall bezeichnet. Ein Vergleich der klassischen Domänen des Krieges mit der neuen Domäne Cyberwar scheinen sinnvoll für den Diskurs zu sein. Es soll gezeigt werden, dass eine korrekte Kategorisierung der Domäne Cyberwar notwendig ist. Der Begriff der *nullten Domäne* soll den Begriff fünfte Domäne Cyberwar ersetzen. Aus der neuen Perspektive soll in Punkt Drei eine engere Definition von Cyberwar entwickelt werden.

Anschließend werden Vorkommnisse im Cyberspace aus den letzten Jahren beschrieben. Die beiden rechtlichen Grundprinzipien *jus ad bellum*[6] [lat. Recht zum Krieg] und *jus in bello*[7] [lat. Recht im Krieg] sollen als roter Faden für die Erläuterung der Vorkommnisse dienen. Cyberwar kann aus rechtlicher Perspektive sinnvoll in diese zwei Bereiche eingeteilt werden.

Cyberkonflikte, die die hypothetischen Kennzeichen für das *Recht zum Krieg* liefern könnten, sollen Spionage, Sabotage, Kriminalität und Aktivismus sein. Hypothetische Kennzeichen sind die Gefährdung kritischer Infrastrukturen, diplomatische Konflikte und geopolitische Interessen. Es soll an konkreten Präzedenzfällen gezeigt werden, welche Auswirkungen diese auf die internationale Politik haben. Spionage, Sabotage, Kriminalität und Aktivismus werden im Zusammenhang mit Cyberwar häufiger genannt, jedoch nicht differenziert betrachtet.

Der nächste Abschnitt soll sich dem *jus in bello* widmen. Hier sollen Möglichkeiten erläutert werden, die Staaten und Militärs in einem Cyberwar nutzen können. Das erste Beispiel ist der konventionelle Krieg zwischen Georgien und Russland im Jahre 2008. Es soll gezeigt werden wie Cyberangriffe auf informationstechnische Infrastrukturen das Kriegsgeschehen beeinflussen können. Anonyme Gruppierungen können militärische Interventionen des Militärs über das Internet unterstützen und begleiten.

6 Paul Christopher, *The Ethics of War and Peace*, (Prentice Hall, 2nd Ed. 1999) at chap. 6, pp. 81-91
7 Michelle Maiese *Fighting Well and Limited War* 2003

Die Unterstützung des Militärs durch die Bevölkerung ist keine neue Tatsache, jedoch bekommt sie durch das Internet eine neue Dimension. Die Einbeziehung der Bevölkerung in Kriegssituationen ist durch *„Informationskrieg"*[8] in einer vernetzen Informationswelt immer wichtiger geworden.

Der zweite Cyberkonflikt, der im *jus in bello* beschrieben werden soll, ist der Konflikt zwischen Israel und Syrien im Jahre 2007. Anhand dieser Beispiele soll das kriegerische Handlungsspektrum im Cyberspace gezeigt werden. Auf der einen Seite kann über das Internet das Kriegsgeschehen manipuliert und beeinflusst werden und auf der anderen Seite können Cyberangriffe konventionelle Kriege tragen.

Darauf folgend wird auf die Problematik hingewiesen, dass die zugrunde liegenden technischen Voraussetzungen um Cyberwaffen zu bauen, für alle Akteure äquivalent sind. Somit wird die Differenzierung aus rechtlicher, politischer und theoretischer Perspektive erschwert. Im Zusammenhang mit Cyberwaffen soll auf die *Non-Attribution*[9] eingegangen werden, da dies mit der gemeinsamen technischen Voraussetzung, die größte rechtliche Problematik ergibt. Attribution ist die Identifizierung und Lokalisation eines Angreifers oder des angreifenden Computers. Die Grundlage für alle Akteure im Cyberspace ist die *Non-Attribution,* sodass ihr beim Thema Cyberwar eine gesonderte Stellung zu kommt. Es soll herausgestellt werden, dass die meisten Versuche, technische Attribution gegen staatliche Angreifer zu betreiben, gescheitert sind.[10] Es sollen keine Methoden wie Footprinting[11], Tracerouting[12] oder DNS Spoofing[13] konkret diskutiert werden, da diese vielleicht gegen schwächere Angriffe funktionieren, aber gegen Angriffe mit militärischer Präzision völlig unzureichend sind. Die militärische Präzision muss nicht notwendig von Staaten ausgehen. Sowohl im *jus ad bellum* als auch im *jus in bello* gilt die Non-

8 Information as Power– Edited by J. L. Caton, J. H. Greenmyer, J. L. Groh, and W.O. Waddell (2010)
9 "*Attribution scheint vielmehr der Non-Attribution gewichen.*" vgl. S.Gaycken -Internet als Kriegschauplatz, S.81 2.Abs.
10 A Conversation on Cybersecurity With William J. Lynn III, US Deputy Secretary of Defense
11 vgl. S.56 3.Abs; S.216; S.222-S.229 S.Gaycken -Internet als Kriegschauplatz
12 vgl. S.222 S.Gaycken -Internet als Kriegschauplatz
13 vgl. S.81 S.Gaycken -Internet als Kriegschauplatz

Attribution.

So macht die *Non-Attribution*[14] den Cyberspace zu einem hervorragenden Mittel um Interessen von Gruppen, Staaten und Individuen zu verstärken. Nicht nur Cyberwaffen kommen strategische Relevanz zu, sonder auch der Rückhalt in der Bevölkerung während militärischer Konflikte ist im Zeitalter der modernen Kommunikationsmedien immer wichtiger geworden. Die Bevölkerung hat immer eine strategische Relevanz in solchen Konflikten gehabt, so auch im Cyberspace.[15] [16] [17]

Am Ende der Arbeit soll kurz auf relevante Institutionen eingegangen werden, die sich an der internationalen Cyberwar Debatte beteiligen sollten. Die Arbeit versucht daher den Begriff Cyberwar und die damit implizierten politischen, technischen, rechtlichen und sprachlichen Probleme zu analysieren. Die Analyse des Begriffes Cyberwar scheint Priorität zu haben, da es die Grundlage für den Rechtsrahmen in der internationalen Politik bilden wird. Der Rechtsrahmen ist notwendig, um die steigende Gefahr des Cyberwar einzudämmen.

2. Analyse des Wortes Cyberwar – eine kritische Betrachtung

In der Literatur wird die Definition von Cyberwar oft mit dem Hinweis begonnen, dass zu den klassischen vier Domänen, eine fünfte Domäne hinzugekommen ist, welche sich Cyberwar nennt und im Cyberspace stattfindet.[18] Dies scheint auf den ersten Blick konsequent zu sein, da man additiv einfach zu den bekannten Domänen eine neue

14 vgl. Fußnote 8
15 DARPA Seeks To Learn From Social For Warfare by Elizabeth Montalbano via http://informationweek.com
16 So, Why Does the Air Force Want Hundreds of Fake Online Identities on Social Media? By Erik Sherman via http://www.cbsnews.com/
17 The Political Power of Social Media by Clay Shirky via http://www.foreignaffairs.com/
18 Cyberwar - War in the fifth domain via http://www.economist.com/ u. Cyberwar is going? By Niels Werber via http://www.heise.de/ (10/2001)

hinzufügt, um eine Kategorisierung zu schaffen. Doch bei genauerer Betrachtung bemerkt man, dass diese Kategorisierung nicht hinreichend ist, um den Sachverhalt zu beschreiben.

Im Laufe der letzten 18 Monate wurde das Signalwort Cyberwar für Wikileaks[19], Stuxnet[20], DDOS Attacken, Botnetze[21] und anderes benutzt. In einem Blogbeitrag[22] habe ich auf die Problematik hingewiesen, Wikileaks als Cyberwar zu bezeichnen. Der Umgang mit dem Begriff Cyberwar sollte kritisch betrachtet werden, da schon die kontroverse Diskussion um die Bezeichnung des Afghanistaneinsatzes zeigt, was für ein Maß an Sensibilität bei der Verwendung des Begriffs Cyberwar notwendig ist.[23]

Die Unklarheit des Begriffs Cyberwar muss untersucht werden, damit Missverständnisse reduziert werden können. Diese Problematik behindert eine angemessene Diskussion. Das gab Juristen, Politikern, Politologen und anderen Wissenschaftlern die Aufgabe den Begriff zu klären. Ein Konsens über eine Definition des Wortes ist zurzeit nicht in Sicht, jedoch erscheint ein einheitlicher Begriff wichtig für die weitere Arbeit in der internationalen Politik zu sein.

Um eine tragfähige Argumentation zu erreichen, sollen zunächst die Geschichte der Kybernetik und die Ideen der Kybernetik dargestellt werden, da im Begriff Cyberwar das griechische Präfix *Cyber* vorhanden ist, was sich auf Kybernetik zurückführen lässt. Der zweite Teil des Begriffs Cyberwar ist *war (zu dt. Krieg)* und liefert so den zweiten Basisbegriff des Wortes. Krieg hat eine rechtliche Definition, die durch das Völkerrecht geregelt ist, wodurch es eine enorme Relevanz für die Diskussion hat.

19 WikiLeaks cyberwar: hackers planning revenge attack on Amazon by Andy Bloxham via http://www.telegraph.co.uk/
20 vgl. S.175 ff. S.Gaycken -Internet als Kriegschauplatz
21 vgl. Botnets: 10 Tough Questions by Editor: Dr. Hogben, Authors: D. Plohmann, E. Gerhards-Padilla, F. Leder
22 Wikileaks – Cyberwar ? by Florian Grunert via http://www.alios.org/
23 Wortgefechte um "Krieg" und "Frieden" by Professor Girnth der Philipps via http://www.theeuropean.de/

2.1 Einfluss von Kybernetik[24] auf die militärisch-industrielle Entwicklung

-Die Kybernetik im Wort Cyberwar-

Der Begriff Kybernetik entstammt dem griechischen und wird meist mit dem Begriff "*Kunst des Steuerns-, Regelns Oder- Lenkens*" übersetzt. Schon Platon, Homer und andere haben diesen Begriff benutzt, um verschiedene Prozesse zu beschreiben, die sich mit der Regelung oder Steuerung von etwas oder jemanden befassen. Der Ansatz ist, dass eine Einheit wie z.B. eine Maschine, ein Staat oder eine Gruppe durch Einwirken von Außen gesteuert werden kann.

Eine Arbeitsdefinition für die folgende Beschreibung liefert WIKIPEDIA *[Version vom 23.11.2011]*[25]:

"In den 1940er Jahren entstanden die Wurzeln der Wissenschaft Kybernetik, als man Gemeinsamkeiten und Schnittstellen verschiedener Einzeldisziplinen, die Themen wie menschliches Verhalten, Nachrichtenübertragung, Regelung, Entscheidungs- und Spieltheorien-und statistische Mechanik betrachten, erkannte."

Der Begriff der Kybernetik war bis in die frühen 1950er Jahre ein allgemeiner Begriff, der erst durch den Wiener Kreis[26] und die Macy Konferenzen[27] zwischen 1946 und 1953 eine komplett neue Konnotation bekommen hat. Erste Gedanken über die Vernetzung von Maschinen untereinander und die Vernetzung und Verschmelzung von biologischen- und nicht-biologischen Objekten wurden diskutiert. Sowohl durch das Modell der Turingmaschine[28] als auch durch ein neues Kommunikationsmodell (siehe

24 Cybernetics: The study of communication and the control of complex systems, especially concerned with comparing automatic control systems such as computers and the human nervous system. TD

25 Trotz sich ständig ändernder Wikipedia Artikel kann in der Versionsgeschichte genau diese Version gefunden werden

26 The Vienna Circle was a group of early twentieth-century philosophers who sought to reconceptualize empiricism by means of their interpretation of then recent advances in the physical and formal sciences. Their radically anti-metaphysical stance was supported by an empiricist criterion of meaning and a broadly logicist conception of mathematics. http://plato.stanford.edu/ Stanford Encyclopedia of Philosophy (Kurz. SEP)

27 Summary of Macy Conferences http://www.asc-cybernetics.org/foundations/history/MacySummary.htm

28 Turing machines, first described by Alan Turing in (Turing 1937), are simple abstract computational devices intended to

Abb.3) manifestierten sich die Ideen der Kybernetik in der Wissenschaft. Der Einfluss von kybernetischen Ideen veränderte auch militärische Strukturen. So wurde am 7. Februar 1958 die DARPA[29], ursprünglich ARPA von Dwight D. Eisenhower gegründet und war eine Reaktion auf den Sputnikschock[30] und die Veränderung in kriegerischen Konflikten.

Die DARPA hat zunächst das ARPA/DARPANet[31] geschaffen, um dezentrale Kommunikationsstrukturen im Falle eines Atomkrieges zu besitzen.[32] Das ARPA/DARPANet wurde später als ziviles Netz weitergeführt und 1983 hat das Militär das MILNET[33] vom ARPA/DARPANET getrennt.[34]

Unter der Führung des US Militärs und deren Wissenschaftlern begann man ,in verschiedenen Forschungsbereichen, an neuen Projekten zu arbeiten. Unter diesen Umständen ist das Transmission Control Protocol/Internet Protocol (kurz: TCP/IP)[35] entstanden, welches die Vernetzung von Wissenschaftsstandorten, mit Hilfe von Software und Hardware ermöglicht hat. Insbesondere die ersten wissenschaftlichen Netzwerke wie das BITNET[36], CSNET[37] und später das CERN, bilden bis heute die Basis für das Internet und nutzen das TCP/IP. Nicht umsonst wird es auch die *Internetprotokollfamilie*[38] genannt.

---

help investigate the extent and limitations of what can be computed. SEP

29 Defense Advanced Research Projects Agency. The Federal agency that began as ARPA, and began the Internet. It became ARPA again in 1990. TD

30 Der Sputnik war ein ungeheurer Schock für den Westen, der bis zu diesem Zeitpunkt dazu tendierte, die sowjetische techn. Kapazität als niedrig einzustufen. Dies prägte den Beginn des "space race" zwischen den Vereinigten Staaten und der Sowjet-Union. (Universität des Saarlandes – virtuelles Handbuch Informationswissenschaft)

31 vgl. S.38 unten ff. PD Dr. Dr. K. Saalbach Policy Making and Analysis Wintersemester 2009/2010 – Paper

32 vgl. Fussnote 31

33 The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. via http://usacac.leavenworth.army.mil

34 Arte Beitrag Mit offenen Karten - Internet und Geopolitik

35 vgl. S.39 PD Dr. Dr. K. Saalbach Policy Making and Analysis Wintersemester 2009/2010

36 Because It's Time Network. An academic computer network originally connecting IBM mainframes and VAX systems via leased lines, providing electronic mail, file transfer, electronic mailing lists, and other services. TD

37 Computer and Science Network. A large computer network, including universities, research labs, and some commercial enterprises. It originated in the United States, and has some members in other countries. TD

38 vgl. S.8ff Network Security C. Kaufmann, R. Perlman, M. Speciner

Um in diesem weltweiten Maschinensystem mit jeder einzelnen Maschine kommunizieren zu können, braucht man Adressen, sodass jede Maschine eine individuelle Adresse hat, über die sie erreichbar ist. Es funktioniert ähnlich wie beim Postversand vom Sender zum Empfänger. Das TCP/IP lieferte die Basis der Kommunikation. TCP und IP befinden sich auf verschiedenen Ebenen der Kommunikation, welche vom *OSI-Modell*[39] beschrieben werden. Die Infrastruktur eines Netzwerkes wird über verschiedene Ebenen(*Layer*) organisiert. Die verschiedenen Ebenen beschreiben wie ein Netzwerk funktioniert und welche notwendigen Informationen geliefert werden müssen, um die Daten zum richtigen Empfänger zu transportieren. Das Internet Protokoll[40] erfüllt die notwendigen Bedingungen, um die Informationen zu versenden.

Man ist zunächst davon ausgegangen, dass 2^{32} (~4,3 Milliarden) Adressen, die durch das Internet Protocol Version 4 (kurz: Ipv4)[41] zur Verfügung gestellt worden sind, ausreichen, um die Maschinen mit genügend Adressen zu versorgen. Jedoch hat die fortschreitende Vernetzung dazu geführt, dass Ipv4 nicht mehr ausreichend Adressblöcke zur Verfügung stellt.[42] Die Grenze der Vernetzung ist auf die vorhandenen Adressen beschränkt, sodass eine andere Version des Protokolls benötigt wird, um dem wachsenden Bedarf an Adressen gerecht zu werden.

Es wurde ein neues Protokoll mit dem Namen Internet Protocol Version 6(kurz: Ipv6)[43] erfunden. Das Internet Protocol Version 6 stellt 2^{128} (~340 Sextillionen) Adressen zur Verfügung, was den Bedarf für die Zukunft decken wird. Auch die Bundeswehr hat die Relevanz der Vernetzung erkannt und hat sich ~4,7 Trillarden[44] Adressen aus dem Ipv6-Adressraum bei der RIPE Network Coordination Center (kurz: RIPE NCC)[45]

39 vgl. S.7f. Network Security C. Kaufmann, R. Perlman, M. Speciner
40 vgl. Fußnote 39
41 vgl. S.427-431 Network Security C. Kaufmann, R. Perlman, M. Speciner
42 IPv4: Der Countdown läuft ab via http://www.heise.de/ (01/2011)
43 Introduction to Ipv6 by Hubert Feyrer 5/24/2001 oder vgl. S.427-431 Network Security C. Kaufmann, R. Perlman, M. Speciner
44 Lava's IPv6 Subnet Prefix Reference Chart via http://digitalfreaks.org/
45 RIPE NCC (Réseaux IP Européens) is an open and voluntary organization of European Internet service providers. RIPE

gesichert.[46] Diese Information soll ein Beweis für die Wichtigkeit der Vernetzung bei den Streitkräften sein. Cyberwar wird durch die immer fortwährende Vernetzung der Streitkräfte relevanter. Das Weißbuch des Bundesministeriums der Verteidigung aus dem Jahre 2006 geht auf die Notwendigkeit der Vernetzung ein:

„Die vernetzte Operationsführung ermöglicht Führung und Einsatz von Streitkräften auf der Grundlage eines allen Führungsebenen übergreifenden und interoperablen Informations-und Kommunikationsverbundes.“[47]

So wird die immense Anzahl von Erfindungen und Ideen im Bereich der technischen Militärforschung dazu führen, dass es eine noch stärkere Vernetzung von Daten[48] ,Informationen[49] und Wissen[50] über die Netzwerke der modernen Streitkräfte geben wird.

Das militärische Denken und Handeln wird vom Vernetzungsgedanken der Kybernetik dominiert. Die ‘‘*Command and Control*”[51] Struktur hat sich vollkommen verändert. Alle Entscheidungen bei Einsätzen sind mit informationstechnischen Geräten unterstützt und stellen so neue Ansprüche an Menschen und Waffen. Speziell das C4ISR[52] beim US Militär oder das NetOpFü[53] der Bundeswehr zeigt die Veränderung von Strukturen bei den Militärs in den letzten 60 Jahren. Sandro Gaycken beschreibt es mit diesen

NCC is the Regional Internet Registry for Europe, the Middle East and parts of Asia.The services provided ensure the fair distribution of global Internet resources in the RIPE NCC service region required for the stable and reliable operation of the Internet. This includes the allocation of Internet (IP) address space, interdomain routing identifiers (currently BGP autonomous system numbers), and the management of reverse domain name space (currently in-addr.arpa, ip6.arpa and ip6.int) http://itlaw.wikia.com/wiki/RIPE (kurz: ITLAW)

46 Bundeswehr meldet hohen IPv6-Adressbedarf beim RIPE an by Monika Ermert via www.heise.de/

47 vgl, BMVg, Weißbuch 2006 S.107

48 vgl. Ottis and Lorents Conference on Cyber Conflict Proceedings 2010 Knowledge Based Framework for cyber weapons and conflict S.131 ff

49 vgl. Fußnote 48

50 vgl. Fußnote 48

51 Command, control, communications, computers, and intelligence (C4I) systems are a key element in facing the broad range of missions and operations envisioned for a post-Cold War future. C4I systems have traditionally been viewed as the combination of communications, warning, intelligence, command, and information systems necessary for military decisionmaking and force management. These systems provide the command and control (C2) foundation for optimal effectiveness of the forces.

52 vgl. S.228 Conference on Cyber Conflict Proceedings 2010 Benier - Understanding Cyber Operations in a Canadian Strategic Context More than C4ISR, More than CNO oder Secretary of the Air Force Michael W. Wynne Remarks as delivered to the C4ISR Integration Conference

53 Prinzip der vernetzten Informationsführung (engl. *Network Centric Warfare*) Vgl, BMVg, Weißbuch 2006 S.106

Worten:

"*Das Ergebnis ist die „vernetzte Operationsführung" (Network Centric Warfare) […] Sie ist ein neues technostrategisches Paradigma intensiver und organisatorischer und informationstechnischer Vernetzung aller Streitkräfte miteinander.*"[54]

So können Entscheidungsträger beim Militär im Ernstfall, wenn die Technik nicht manipuliert worden ist[55], viel mehr Informationen und Daten in ihr Handeln einbeziehen. Das Militär konnten ihre Waffen zu Land, im Wasser, in der Luft und im Weltraum durch die Ideen der Kybernetik besser synchronisieren und somit effektiver und effizienter gestalten. Der Cyberspace hat an militärischer Bedeutung gewonnen.

2.2 Was ist Krieg im klassischen Sinne?

Dieser Abschnitt soll kurz die grundlegenden Ideen hinter Krieg und kriegerischen Handlungen erläutern, sowie rechtliche Aspekte erwähnen, sodass im nächsten Abschnitt eine Zusammenführung von Kybernetik und Krieg vollzogen werden kann. Einen Einstieg zum Begriff Krieg liefert die Bundeszentrale für politische Bildung.[56]

54 vgl. S.40- 4.Abs; S.Gaycken Cyberwar das Internet als Kriegsschauplatz.

55 Perspectives - June 2008 by Alan Cameron via www.gpsworld.com (08/2008)

56 „*Spez.: 1) Nach den Ursachen werden religions- und ideologisch begründete K., Kolonial-, Wirtschafts- und Unabhängigkeits-K. etc. unterschieden. 2) Nach den Zielen wird zwischen Angriffs-, Interventions-, Sanktions-, Verteidigungs- und Befreiungs-K. etc. unterschieden. 3) Nach den Formen werden z.B. regulärer, Partisanen-, Volks-, Miliz- und Guerilla-K. unterschieden. 4) Entsprechend den eingesetzten Waffen(gattungen) wird z.B. zwischen konventionellem, Atom-, bakteriologischem, chemischem K., ferner zwischen Land-, See- und Luft-K. unterschieden. 5) Räumlich wird z.B. zwischen lokal begrenztem, regionalem oder Welt-K. unterschieden. Während früher der K. als Schicksal und als Bewährungsprobe angesehen, als "Fortsetzung der Politik mit anderen Mitteln" akzeptiert und zwischen gerechtem und ungerechtem K. differenziert wurde, gilt heute aufgrund der Gefahr einer Selbstvernichtung der Menschheit (z.B. durch ABC-Waffen) der K.-Ursachenforschung, der Friedens- und Konfliktforschung, den Deeskalations- und Vermittlungsbemühungen in der Außenpolitik, der K.-Vermeidung und den internationalen Abrüstungsverhandlungen oberste politische Priorität. Vielfältige politische und militärisch-organisatorische Bemühungen dienen z.Z. dazu, internationale militärische Einheiten aufzustellen, die (z.B. im Rahmen der OSZE oder der Vereinten Nationen) zur Begrenzung und Eindämmung regionaler kriegerischer Auseinandersetzungen eingesetzt werden können - letztlich mit dem Ziel, die (früher kriegerisch getroffenen) Entscheidungen auf friedlichem Wege zu suchen.*"Definition von Krieg aus dem Lexikon der Bundeszentrale für politische Bildung

Klaus-Peter Saalbach zeigt in seiner Arbeit *Cyberwar- Grundlagen- Methoden- Beispiele*, welche Grenzen dem Begriff Cyberwar aus klassischer Kriegsdefinition gesetzt sind:

„Da Krieg im klassischen Sinne die Auseinandersetzung zwischen 2 Staaten ist, wird zuweilen bezweifelt, ob es überhaupt schon Cyberwars gegeben hat und ob Cyberwar als eigenständige Konfliktform überhaupt denkbar ist.“[57]

Cyberwar spielt bei modernen Kriegen eine Rolle, jedoch sollte neu diskutiert und überprüft werden, inwiefern die Rahmenbedingungen, unter denen der Begriff Krieg genutzt wird, bei Cyberwar geltend gemacht werden kann. Saalbach argumentiert,

„[..]dass groß angelegte und komplexe Cyberangriffe wegen der benötigten Ressourcen und der möglichen Folgen nicht ohne Rückendeckung staatlicher Organisationen stattfinden, so dass eine Reihe von Vorfällen, bei denen sich der Urheber nicht klären ließ, in der Literatur dem Cyberwar zugeordnet werden.“[58]

Die entscheidenden Kriterien, ob einige internationale Vorfälle als Krieg im Cyberspace bezeichnet werden können, liefert das Völkerrecht.[59] Es sollte untersucht werden, ob das Völkerrecht genügend Informationen liefert, um Cyberwar zu identifizieren. Speziell die Genfer- Konvention[60] und die Haager Landkriegsordnung[61] sollten in diesem Kontext erwähnt werden, da eine kriegerische Handlung im Cyberspace, unter Beachtung dieser Rechtsgrundlagen, erstmal geprüft werden muss. Bei der Diskussion

57 vgl. S.5 Saalbach, Cyberwar- Grundlagen- Methoden- Beispiele, 2011

58 vgl. Fussnote 57

59 *„Völkerrecht ist ein Sammelbegriff für alle Rechtsnormen, die das Verhältnis der (unabhängigen) Staaten untereinander und die Beziehungen zwischen den einzelnen Staaten und den internationalen Organisationen regeln. Im Gegensatz zum Recht kann das V. nicht von einer zentralen Gewalt durchgesetzt werden, sondern ist von der Anerkennung der jeweiligen Staaten abhängig. V. entsteht durch Verträge (Abkommen, Konventionen, Pakte etc.), die sich mit der Anerkennung fremder Staatsgebiete, Beschränkung kriegerischer Handlungen, dem diplomatischen Austausch und Verkehr, der Schlichtung von Streitigkeiten, Fragen des internationalen Handels etc. beschäftigen. Von zentraler Bedeutung sind die Verfassung der Vereinten Nationen (UN-Charta) von 1945, die Menschenrechtserklärung der Vereinten Nationen, die Konventionen und Abkommen des Europarates.“*[Völkerrecht] Bundeszentrale für politische Bildung

60 *„Bezeichnung für internationale, von nahezu allen Staaten der Welt unterzeichnete Abkommen über grundlegende humanitäre Regeln bei kriegerischen Auseinandersetzungen“* Bundeszentrale für politische Bildung

61 *1) H.A., H.K. werden verschiedene völkerrechtliche Verträge genannt, die in Den Haag abgeschlossen wurden, insbesondere: das Haager Kulturgüterschutzabkommen von 1954 (das Kulturgüter im Kriegsfall schützt), die Haager Landkriegsordnung von 1899 und 1907 (die definiert, wer Kriegsführender ist, die Stellung von Kriegsgefangenen bestimmt, die Verwendung bestimmter Waffen etc. einschränkt und die Rechte auf besetztem Gebiet festlegt; sie wird durch die Vereinbarungen von Genf von 1929 und 1949 ergänzt) und das Haager Luftpiraterieübereinkommen von 1970 (das Luftpiraten weltweiter Verfolgung aussetzt)*. Bundeszentrale für politische Bildung

des Begriffes Cyberwar sollte stets die rechtliche Grundlage beachtet werden. Ohne die schon vorhandenen Regeln des Krieges und ihre rechtliche Einordnung würde die Diskussion eine falsche Konnotation bekommen. Bruce Schneier[62], ein Sicherheitsforscher und Kryptograph machte auf dieses Problem aufmerksam:

„*The biggest problems in discussing cyberwar are the definitions. The things most often described as cyberwar are really cyberterrorism, and the things most often described as cyberterrorism are more like cybercrime, cybervandalism or cyberhooliganism--or maybe cyberespionage.*“[63]

Bevor nicht eine Definition des Begriffs sich durchgesetzt hat, sollte der Begriff Cyberwar mit Sorgfalt gewählt werden. Einer solchen Definition kommt eine große rechtliche, politische und militärische Bedeutung zu. Im nächsten Punkt verschmelzen Kybernetik und Krieg, mit Hinblick auf die letzten beiden Punkte, wieder zu Cyberwar.

2.3 Versuch einer Verknüpfung von Kybernetik und Krieg

In den zuvor beschriebenen Punkten wurde versucht eine Vorstellung zu schaffen, warum Kybernetik eine große neue Variable im Krieg ist und wieso es wichtig ist, die klassischen Rechtsgrundlagen des Krieges zu betrachten.

Cyber[64] als griechisches Präfix und Krieg ergeben zusammen Cyberwar. Jedoch ist der Begriff nicht in allen Aspekten definiert. Es ist nicht sicher, welche Bedeutung dem Begriff Cyberwar in Zukunft zugerechnet werden kann. Viele rechtliche, gesellschaftliche und wissenschaftliche Diskussion müssen noch geführt werden, damit der Begriff an schärfe gewinnt.

Cyberwar ist ein Begriff, der die technostrategische Veränderung des Krieges in einer

62 Bruce Schneier is an internationally renowned security technologist and author. Described by *The Economist* as a "security guru," he is best known as a refreshingly candid and lucid security critic and commentator.

63 Cyberwar: Myth or Reality? by Bruce Schneier via www.schneier.com/

64 The prefix cyber- comes from the Greek word kybernan, which means to steer or govern, and is used with words related to cybernetics TD

neuen Domäne bezeichnet. Diese Veränderung findet im Cyberspace statt. Der Cyberspace ist ein Konstrukt aus physikalischen Faktoren und menschlichen Entwicklungen, die auf diesen basieren. Wir können mit Hilfe von technischen Geräten wie Computern diesen Cyberspace akkommodieren[65] , assimilieren[66] und verändern. Eine anfängliche Begriffsklärung wie diese, soll vorerst genügen, da im Punkt *3 eine engere Definition von Cyberwar* vorgenommen werden muss.

3. Was ist eine Domäne des Krieges?

Schon immer haben Menschen Kriege zu Land, zu Wasser, in der Luft und im Weltraum geführt. Dies sind die klassischen vier Domänen des Krieges. Jeder dieser Domäne hat spezielle Eigenschaften, die den Menschen dazu bringen neue Lösungen zu erarbeiten, um sich in diesen Domänen zu bewegen und zu verteidigen. Man könnte sagen, dass man im Cyberspace einen Computer als Schnittstelle benötigt und dazu einige Kenntnisse über die Bedingungen, um sich in diesem Raum fortzubewegen. Dies korreliert mit einem Schiff auf dem Wasser oder einem Flugzeug in der Luft. Diese Eigenschaften unterliegen den physikalischen Gesetzen, wie der Geschwindigkeit von Licht durch das weltweite Glasfaserkabelnetz.[67] Es ist anzumerken, dass dieses weltweite Netz nicht nur zivile Strukturen hat, sondern, dass das Militär ihre eigenen Subnetze wie das *Joint Worldwide Intelligence Communications System*[68] unterhält. Es existieren also Subnetze und anderen

65 Akkommodation im kognitiven Bereich im Sinne vonb Piaget: Anpassung, Erweiterung bzw. Veränderung der kognitiven Organisationsstruktur (Schemata) in Richtung auf eine Angleichung an die Umweltanforderungen.

66 Im Gegensatz zu Akkommodation im kognitiven Bereich handelt es sich bei Assimilation um denjenigen Prozeß, in dem das Kind die Wirklichkeit an seine aktuelle kognitive Organisation anpaßt.

67 Vgl Abb. 4 Abbildungsverzeichnis

68 The Joint Worldwide Intelligence Communications System [JWICS] is JWICS is a 24 hour a day network designed to meet the requirements for secure (TS/SCI) multi-media intelligence communications worldwide. JWICS replaces the DDN DSNET3 as the Sensitive Compartmented Information (SCI) component of the Defense Information System Network (DISN). It provides DODIIS users a SCI level high-speed multimedia network using high-capacity communications to handle data, voice, imagery, and graphics.

Systeme, die nicht an das Internet angeschlossen sind, jedoch indirekte Schnittstellen zu diesem haben.

Cyberwar ist bis jetzt nicht im Internet lokalisiert worden, da dort noch keine Angriffe durchgeführt worden sind, die einen Wirkungsgrad erreicht haben, der die Bezeichnung kriegerische Handlung rechtfertigen würde. Am Beispiel Estland soll eine solches Missverständnis beschrieben werden.. Sandro Gaycken sagt dazu:

„*Die Einstufung der Aktion als kriegerische Handlung (vor allem durch die Presse) ist mit Sicherheit nicht gerechtfertigt. Weder konnten Kombattanten nachgewiesen werden, noch war ein benennenswerter Schaden zu beziffern.*“[69]

Wobei hier auch andere Meinungen existieren, was aus den ungenauen Definitionen der Begriffe Cyberwar und Cyberspace resultiert. Der Verteidigungsminister von Estland beschreibt seine Einstellung zu einem solchen Angriff wie folgt:

„*Estonia is also a proponent of the principle that there should be no distinction between a cyber-attack and a physical attack. The early warning, deterrence and defence capabilities of countries in Cyberspace must be comparable to the ability of the countries doing the same in the physical world.*”[70]

Viele haben den Cyberwar als die neue fünfte Domäne bezeichnet[71], aber die Begründung blieb meist undifferenziert. Sind die Subnetze des Militärs der Ort an dem Cyberwar stattfindet oder wo greift der Begriff Cyberwar. Beachtet man die einzigartige, domänentranszendierende Natur eines Cyberangriffes, so ist es offensichtlich, dass Cyberwar nicht in den klassischen Domänenkategorien begriffen werden kann. Er ist eine neue Domäne, aber in einer anderen Ebene(*layer)*, welche alte Attribute bedient und neue mit sich bringt. Im Grunde hat die Entwicklung von ICT[72] die Art der Kommunikation in den einzelnen Domänen des Krieges grundlegend verändert. Es können Drohnen ferngesteuert werden. Roboter können Minen auslösen lassen. Es kann auf die Millisekunde genau eine verteilte Operation ausgeführt

69 S. Gaycken S.170 2.Abs. In Cyberwar -Das Internet als Kriegsschauplatz

70 Estonian Defence Minister: A cyber-attack is no different than an ordinary attack via http://www.defpro.com/ (06/2011)

71 Mobilizing in the Fifth Domain by Michael Scott Moore via www.miller-mccune.com/ (10/2010) und Pentagon declares the Internet a war domainBy John T. Bennett http://thehill.com/ (07/2011)

72 Information and communication technologies (ICT) is an umbrella term that includes all technologies for the manipulation and communication of information.

werden. Kriegsschiffe werden von zentralen Computersystemen gesteuert. Der Einfluss von Technologie in den letzten 60 Jahren auf die vier Domänen war groß. Hinzu kam die Vernetzung von Luft, Wasser, Land und Weltraum durch den Cyberspace zum *Network Centric Warfare*. Cyberwar hat nicht die wesentlichen Eigenschaften der anderen Domänen gemeinsam. Er teilt viele Aspekte der anderen Domänen, jedoch kommen einige Aspekte hinzu, sodass meines Erachtens Cyberwar eine bessere Kategorisierung benötigt. Cyberwar findet über den Cyberspace statt, welcher gleichzeitig auch die Basis der anderen Domänen des Krieges ist. Und um diese Verkettung zu verstehen, muss kurz skizziert werden, was der Cyberspace für das Militär ist. Das US-Militär beschreibt den Cyberspace so:

„[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers“[73]

Operationen Im Cyberspace haben für das US Militär folgende Definition:

„The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid.“[74]

Der Cyberspace ist nur das Mittel zum Zweck im Falle eines Krieges. Zur Veranschaulichung ein Beispiel aus der Seekriegsführung: Ein Cyberangriff richtet sich nicht gegen das Schiff an sich, sondern gegen dessen Computersysteme. Ein erfolgreicher Angriff zerstört also das Schiff nicht zwangsweise, schränkt aber seine Operationsfähigkeit massiv ein. Man muss zu dem Schluss kommen, dass die Domäne Cyberwar allen übrigen Domänen transzendiert.[75] Dieser kategorische Unterschied ist wichtig, da die vernetzte Operationsführung die Handlungsbasis aller Domänen ist. Cyberwar sollte aufgrund dieser speziellen Eigenschaften *"Domäne Null"* genannt werden. Ebenso wie die Null ihre Bedeutung im Zahlensystem erst durch Bezugnahme auf die natürlichen Zahlen erhält, so kann auch Cyberwar erst durch die

73 vgl Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms S.92 cyberspace
74 vgl. Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities Seite 16
75 vgl. Abbildung 2

Transzendenz der klassischen vier Domänen seine Wirkung entfalten.

3.2 Eine engere und übersichtlichere Definition von Cyberwar

Um die Arbeit im Bereich des internationalen Rechts, der Kriegsrechtskonventionen und der wissenschaftlichen Arbeit zu erleichtern, sollte der Begriff Cyberwar anders definiert werden. Die bisher vorgenommenen Untersuchungen des Begriffs Cyberwar lässt nun folgende Definitionseckpunkte zu.

1. Cyberwar ist die Ausnutzung von Sicherheitslücken in der vernetzten Technologie der klassischen Domänen

2. Cyberwar ist eine eigene, neue, transzendentale Domäne.

3. Cyberwar ist die Gesamtheit aller Angriffe über den Cyberspace mit den Vektoren Zerstörung, Manipulation und Spionage während einer kriegerischen Handlung.

Diese drei Punkte können als Ecksteine und Grundlage für weitere differenzierte Theoriebildung betrachtet werden. Bevor jedoch eine massive Veränderung des internationalen Rechts ratifiziert wird, sollte man mit den vorhandenen rechtlichen Grundlagen arbeiten, damit zunächst eine einheitliche Diskussion geführt werden kann. Diese Grundlagenforschung ist wichtig, damit ein Konsens auf internationaler Ebene über der Begriff Cyberwar gefunden werden kann.
Als Beitrag zur Begriffsbildung kann an dieser Stelle zusammenfassend Folgendes festgehalten werden: Cyberwar kann nur im Kontext einer kriegerischen Auseinandersetzung mit Mitteln einer oder mehreren der klassischen Domänen betrachtet werden. Als *Nullte Domäne* ist er diesen nicht beigeordnet, sondern transzendiert sie und wirkt damit stets in die Auseinandersetzungen hinein. Im Umkehrschluss bedeutet dies allerdings auch, dass Cyberwar im hier gewählten Sinne niemals autonom geführt werden kann, da Cyberwar stets militärische Ziele verfolgt

und seine kinetischen Effekte nur in Auseinandersetzungen mit Erscheinungsformen der klassischen Domänen generieren kann. Der letzte Punkt grenzt damit den Cyberwar klar von verwandten Begriffen wie beispielsweise Cybersabotage o.ä. ab. Um diese Abgrenzung soll es auch im folgenden Kapitel gehen, in welchem artverwandte, aber nicht synonyme Phänomene diskutiert werden sollen.

4. Cyber Konflikte im Hinblick auf jus ad bellum

Dieser Teil der Arbeit soll vom Begriff Cyberwar, wie er in den letzten Abschnitten diskutiert worden ist, abgetrennt werden, da in den hier besprochenen Fällen andere rechtliche Grundlagen greifen. Spionage, Sabotage, Kriminalität und Aktivismus sind Formen des Konfliktes, welche zwar Einfluss auf das aktuelle politische und militärische Geschehen haben, jedoch nicht als Cyberwar bezeichnet werden dürfen. In der vernetzen Welt hat sich dies nicht geändert, sondern es hat neue Facetten bekommen. Vor allen genannten Begriffen kann die Präfix *Cyber* verwendet werden. Auch hier gilt wieder ein Paradigmenwechsel auf ganzer Ebene. Das Internet hat einen neuen Raum für solche Aktivitäten erschlossen.

4.1 Spionage im virtuellen Raum am Beispiel Titan Rain

Titan Rain war eine der ersten großen Spionageaktionen, die außerhalb der Nachrichtendienste und Militärs bekannt geworden ist. Es wurden sensible Einrichtungen aus Forschung und Militär infiltriert.[76]

Einer guter Artikel kommt aus dem Times Magazine vom 29. August 2005.[77] Der Artikel

76 vgl. S.100 1.Abs. Gaycken, Sandro Cyberwar- Das Internet als Kriegsschauplatz
77 The Invasion of the Chinese Cyberspies by Nathan Thornburgh via www.time.com

hat Aufsehen erregt, da er zeigte, dass die Angreifer mit einer gewissen Präzision gearbeitet haben, die sonst ungewöhnlich war. Normalerweise hatten Angreifer bis dato persönliches Interesse US-amerikanische Netze zu infiltrieren.

Unter dem Decknamen *Spiderman* war ein Mitarbeiter des *Sandia National Laboratory*[78] vom Militärgeheimdienst beauftragt worden diese Vorkommnisse in verschiedenen Netzwerken zu untersuchen. Zunächst wurde *Spiderman*, mit richtigem Namen Carpenter, auf die Angreifer aufmerksam, als 2003 versucht worden ist, geheime Informationen von *Lockheed Martin*[79] zu erlangen. Nach etlichen Vergleichen weiterer Attacken gegen kritische Netzwerke anderer Firmen wurde schnell klar, dass die Angreifer ähnliche Methoden verwendeten und es einen gemeinsamen Ursprung geben könnte. So entstand der Name Titan Rain in den Ermittlerkreisen. Es wurde versucht in die verschiedenen Netzwerke einzudringen, die Daten als Zip-Format[80] zu komprimieren und diese Daten dann über Süd-Korea, Hong Kong oder Taiwan zu routen. Danach wurden die Daten sofort weiter auf das chinesische Festland nach Guangdong weitergeleitet. Interessant ist, dass die Attacken in einem Zeitraum von 10-30 Minuten vollzogen worden sind. Es wurden keine Spuren hinterlassen, die für forensische Arbeiten hilfreich gewesen wären. Die Angreifer haben sich die Option offen gehalten wieder in die Rechner einzudringen, sodass solche kurzen und schnellen Abgriffe der Daten wieder möglich waren. Carpenter selbst beschreibt es im Times Artikel so:

„Most hackers, if they actually get into a government network, get excited and make mistakes," Not these guys. They never hit a wrong key."[81]

Hierbei muss erwähnt werden, dass Carpenter alias *Spiderman* angeklagt worden ist

78 Sandia is a multiprogram engineering and science laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the US Department of Energy's National Nuclear Security Administration. Sandia's enduring mission is to provide engineering and science support for America's nuclear weapons stockpile.

79 Lockheed Martin Corporation, an advanced technology company, was formed in March 1995 with the merger of two of the world's premier technology companies, Lockheed Corporation and Martin Marietta Corporation.and is principally engaged in the research, design, development, manufacture and integration of advanced technology systems, products and services.

80 *.zip* is the file extension for the ZIP file format, which is a data compression and archive format.

81 vgl. Fußnote 77

illegale Aktivitäten auszuführen, da er als freier Mitarbeiter gearbeitet hat. Er selbst hat nämlich einen der drei Router in Guangdong mit einer Software ausgestattet, die bei jeder Aktivität der Angreifer einen Alarm an ein anonymes Email-Konto bei Yahoo gesendet hat. Über diese, nach amerikanischem Gesetz, illegale Handlung, fand er heraus, dass hinter diesen drei Routern zwischen Zehn und Sechs Arbeitsplätze waren. Da China selbst viele infizierte Computer im eigenen Land hat, was einmal durch das hohe Aufkommen von Computern im Land selbst zu begründen ist und auch oft an den raubkopierten Betriebssystemen liegt, welche oft schon mit großen Sicherheitslücken illegal aus dem Internet geladen werden, kann hier keine genaue Aussage getätigt werden, ob die Informationen von dort weitergesendet worden sind. James A. Lewis beschreibt es in seinem Bericht *Computer Espionage, Titan Rain and China* das Problem der Zurückverfolgung deutlich:

„*While it is believed China was responsible, there is no certainty that the data was not further routed to another location. Foreign states wishing to use cyber warfare against the US may recognise the focus being placed on China and use Chinese computers to conduct their own reconnaissance and attacks by using botnets or proxies based there.“*[82]

Im Fall Titan Rain ist jedoch gezeigt worden, dass die Informationen in ein lokales Netzwerk geladen worden sind, was China hier als direkten Angreifer identifizieren soll. Inwiefern diese Informationen fundiert sind, lässt sich nicht mehr überprüfen. China selbst hat die Vorwürfe abgestritten und sich klar gegen solche Attacken ausgesprochen, jedoch keine Ermittlungshilfe geleistet, sodass die US-Amerikanischen Behörden diesen Fall hätten aufklären können. Das *State Council Information Office* der Volksrepublik China äußerte sich nach Times Magazine Aussagen wie folgt:

„ ... charges about cyberspying and Titan Rain are "totally groundless, irresponsible and unworthy of refute.“[83]

In höheren Regierungskreisen war man sich nicht sicher, ob die chinesische Regierung

82 vgl. Computer Espionage, Titan Rain and China by James A. Lewis S.2
83 vgl. Fußnote 77

hinter den Attacken als Urheber stand. Jedoch waren sich Netzwerkanalysten und Behörden einig über diesen Sachverhalt. Der Chef der Spionageabwehr des FBI äußerte sich im TIME-Magazine Artikel wie folgt:

„When it comes to advancing their military by stealing data, "the Chinese are more aggressive" than anyone else, David Szady, head of the FBI's counterintelligence unit, told TIME earlier this year. "If they can steal it and do it in five years, why [take longer] to develop it?"[84]

Titan Rain war jedoch nicht nur eine Attacke gegen US-amerikanische Netzwerke, sondern auch gegen Netzwerke anderer Länder. Die Problematik bei der Ermittlung solcher Vorfälle liegt klar auf der Hand. Wenn ein amerikanischer Bürger mit Kontakten zu Behörden, während einer offensiven Täterverfolgung, ertappt wird, wie er chinesische Rechner infiltriert, kann aus diesem Fall eine internationale Krise auf diplomatischer Ebene entstehen, die nachhaltige Konsequenzen auf die Beziehung zweier Länder hat. Es wird deutlich, wie das Attributionsproblem eine Rolle im Cyberspace spielt. Die Möglichkeit vollkommen unentdeckt zu bleiben ist da, jedoch ist dies ein schmaler Grad auf dem sich der Angreifer und der Verteidiger bewegt, da die Anonymität durch kleine Fehler aufgehoben werden kann.

Interessant ist der Aspekt, dass Staaten einfach inoffizielle Abkommen mit Computerexperten haben, welche dann die fremden Netze infiltrieren und die Informationen über inoffizielle Kanäle weitergeben. Wenn jedoch der Angreifer entdeckt wird, kann der Staat offiziell sagen, dass er solche Angriffe verurteilt und nicht duldet. Die Problematik kriegerischer Handlungen im Internet ist die Auflösung des Kombattanten Status. In diesem Zusammenhang ist häufiger von sogenannte *Proxywars*[85] die Rede. Der Begriff *Proxywars* in der Cyberwar-Debatte ist in Anlehnung an das Routen über *Proxyserver*[86] entstanden, sodass ein Angriff nicht zum Angreifer zurückverfolgt werden kann. Dies könnte vielleicht ein weiterer Schritt in Richtung der

84 vgl. Fußnote 77

85 *Proxywars* sind eigentlich bekannt aus dem Kalten Krieg, da die UdSSR und die USA in einigen Ländern stellvertretend Kriege geführt haben.

86 Proxyserver: Proxy servers sit between a client program (typically a Web browser) and an external server (typically another server on the Web) to filter requests, improve performance, and share connections. TD

Privatisierung von Spionage und Sabotage sein. Abschließend ist zu sagen, dass der Begriff Cybewar im Falle von Titan Rain nicht angebracht ist.

4.2 Sabotage mit Bits und Bytes am Beispiel Stuxnet

Einführung

Dieser Abschnitt soll den Sachverhalt um die Schadsoftware Stuxnet erläutern. Da die Schadsoftware nicht nur auf technischer Ebene, sondern auch auf Ebene der internationalen Politik eine Komplexität hat, welche in einer umfassenden Arbeit untersucht werden könnte, wird in diesem Abschnitt überwiegend der Artikel[87] von Kim Zetter, die bald ein Buch zum Thema veröffentlichen wird, als Basis für die Beschreibung des Sachverhalts benutzt.

Politische Vorgeschichte

Stuxnet soll in Iran für die Sabotage von Uran Zentrifugen genutzt worden sein. Normalerweise ist die Fehlerquote bei Zentrifugen Zehn Prozent. Die Zentrifugen arbeiten in sogenannten Kaskadensystemen, um Uran anzureichern. Normalerweise wird Uran mit geringem Anreicherungsgrad für den Betrieb von Reaktoren und für medizinische Experimente benötigt. Der Verdacht besteht, dass die iranische Regierung nicht nur ein ziviles Atomprogramm unterhält, sondern auch versucht genug uranhaltiges Material(>90%), mit diesen Kaskadensystemen von Zentrifugen, anzureichern, um eine Atombombe zu bauen.[88] Deswegen ist die internationale Politik, und speziell Israel und die USA am iranischen Atomprogramm interessiert. Israel und die USA haben die Befürchtung, dass Iran durch die Herstellung und den Besitz einer Atombombe das Machtverhältnis im Nahen Osten und auf der Welt zum negativen für sie verändert.

87 How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History by Kim Zetter via www.wired.com/ (07/2011)

88 Security Council tightens sanctions against Iran over uranium enrichment via www.un.org/ (2007)

Der Stuxnet-Fall

Mitarbeiter der Internationalen Atom Energie Organisation (IAEO) haben im Frühjahr 2010 festgestellt, dass wesentlich mehr Zentrifugen, als die üblichen Zehn Prozent, in wenigen Monaten ausgetauscht worden sind. Da die Inspektoren der IAEA jedoch nur für die Kontrolle des angereicherten Materials zuständig sind, konnten und durften sie keine weiteren Untersuchungen zu der Beobachtung anstellen. Bis zum Juni 2010 war die Information über die übermäßige Anzahl von zerstörten Zentrifugen nur teilweise bekannt, sodass bis zum Juni 2010 keine weiteren Vermutungen in Richtung einer Sabotage angestellt worden sind.

Die Wende im Stuxnet -Fall gab das kleine weißrussische IT-Security Unternehmen namens VirusBlokAda, was zum damaligen Zeitpunkt nur eine normale Schadsoftware(Stuxnet) untersucht hat und nicht wusste, dass sie Stuxnet obduzieren. Es stellte sich jedoch heraus, dass die gefundene Software mit viel Sorgfalt programmiert worden ist. VirusBlokAda nahm Kontakt zu Microsoft auf, welche aus der Kombination der Dateinamen *.stub* und *MrxNet.sys,* den Namen *Stuxnet* machten. Analysen ergaben, dass Stuxnet im Grunde aus zwei Teilen besteht, welche in den folgenden Abschnitten diskutiert werden sollen.

Der Windowsteil

Der erste Teil besteht aus der Software, welche sich auf Windows Systemen jeder Art(XP,7,Vista,Win2k,Server2003,Server2008/R2)[89] verbreitet. Stuxnet selbst wurde wahrscheinlich über USB-Sticks auf die Zielsysteme übertragen. Hier nutze die Software zum Beispiel Zertifikate von *Realtek Semiconductor* und *Jmicron Technology Corporation*, um unentdeckt auf die Systeme zu kommen.[90] Stuxnet beinhaltet viele Sicherheitslücken, sowohl auf Windowsebene als auch auf industrieller Kontrollsystemebene, welche von Ralph Langner in einem Beitrag[91] zusammengefasst

89 vgl. N. Falliere, L. O Murchu and E. Chien (Symantec) W32.Stuxnet Dossier S.16
90 vgl. N. Falliere, L. O Murchu and E. Chien (Symantec) W32.Stuxnet Dossier S.4
91 Enumerating Stuxnet's exploits by Ralph Langner via www.langner.com (07/2011)

worden sind. Einen guten Überblick[92] über die den Windowsteil von Stuxnet, welche sozusagen für den Transport der Zentrifugen-Schadsoftware zuständig war, gaben *Bruce Dang* und *Peter Ferrie* auf dem *Chaos Computer Kongress 2010*. Der erste Teil der Software unterscheidet sich im Grunde nicht von herkömmlicher Schadsoftware, die von Kriminellen geschrieben und genutzt wird, um Geld damit zu verdienen.

Da Anti-Viren Firmen jeden Monat viele solcher Schadsoftware sehen, ist Stuxnet zunächst nur durch seine Größe(500kb) und durch die vielen Sicherheitslücken, die es in Windowssystemen ausnutzt, aufgefallen. Eine *normale* Schadsoftware hat durchschnittlich die Größe von 10kb bis 15kb und nutzt meist nur eine Sicherheitslücke in der Software aus, sodass auch vermutet werden könnte, dass Stuxnet mehrere Aktualisierungen erhalten hat. Andere glauben, dass der Quellcode gewisse Ähnlichkeiten mit Conficker[93] hatte und dadurch ein Verdacht aufkam.[94]

Der Industrielle Kontrollsysteme(ICS)-Teil

Nach langem *Disassemblen*[95] der Software kam der zweite Teil von Stuxnet in die Öffentlichkeit. Dieser Teil versucht ICS, der Firma Siemens zu manipulieren. Die Entwicklung dieses Teils war eine große Herausforderung für die Entwickler der Software und wird von Experten als Indiz für staatliche Akteure gesehen. Alleine um solch eine Software für Zentrifugen, wie sie auch in Iran stehen, zu schreiben und zu testen, braucht man viele Informationen über die Systeme von Siemens. Des Weiteren viel Geld[96], um solch ein Testgelände aufzubauen. Solche Informationen sind nicht einfach zu bekommen, wobei ein Passwort(2WSXcder), welches in die Hardware von

92 Adventures in analyzing Stuxnet von Bruce Dang und Peter Ferrie via http://media.ccc.de (12/2011)

93 A computer worm targeting the Microsoft Windows operating system that was first detected in November 2008. It has also been called Downup, Downadup and Kido. The worm uses a group of advanced malware techniques in combination, which has made it unusually difficult to eliminate. It spread through removable storage devices and network shares, disabling security software and installing fake antivirus software. Conficker infected millions of computers, in businesses, hospitals, governments, and military institutions, even forcing aircraft to be grounded. The worm's unknown authors have periodically released new variants to counter efforts to eradicate it. There are five known variants: Conficker A, B, C, D and E. Microsoft has released a removal guide for the worm. TD

94 Why the Stuxnet worm could be Conficker's cousin by Byran Acohido via http://content.usatoday.com/

95 Building Custom Disassemblers by FX via www.youtube.com

96 vgl. S. Gaycken, Cyberwar- Das Internet als Kriegsschauplatz S.175

Siemens zum Warten der Geräte, fest eingeschrieben war, schon seit 2008 in Internetforen bekannt war. [97]

Der ICS-Teil von Stuxnet griff einmal die Zentrifugen selbst an und veränderte die Frequenz der Zentrifugen, welche wahrscheinlich den hohen Schaden an Zentrifugen hervorgerufen hat. Der andere Angriff war eine *man-in-the-middle-attack*[98] welche der Experte Joel Langill so beschreibt:

„The other payload is less known, less understood, and scarier. In essence, this payload performs a Man-in-the-Middle (MITM) attack INSIDE the PLC. It takes the inputs coming from the PLC's I/O modules and fakes them so that the logic works off of incorrect information. It then tells the PLC's outputs to do what it wants, not what the logic says"[99]

Dies hatte zur Folge, dass der Mitarbeiter, der die Zentrifugen überwacht, die Änderung der Frequenz nicht wahrgenommen hat und die Software unentdeckt bleibt. Ralph Langner berichtete auf der *International Conference on Cyber Conflict 2011* (ICCC) in seinem Vortrag[100] über die genaue Wirkungsweise der Schadsoftware. Der Iran selbst bestätigte die Attacke erst einige Monate nach bekannt werden der Software.[101]

Was bedeutet Stuxnet für die internationale Politik?

Es stellt sich die Frage, ob Stuxnet die erste Cybersabotage mit Hilfe einer Cyberwaffe war, die bekannt geworden ist. Da keine Menschen gestorben sind und wahrscheinlich nur der Plan des iranischen Atomprogramms behindert worden ist, sollte man Stuxnet nicht als Massenvernichtungswaffe bezeichnen. Stuxnet fällt in die Kategorie Cybersabotage, was die Gefahr ähnlicher Software nicht mindert. Sabotage industrieller Kontrollsysteme kann einen ähnlichen Schaden anrichten wie eine konventionelle Waffe, somit ist nicht ausgeschlossen, dass solch eine Software auch

97 vgl. Fußnote 96
98 vgl. S. Gaycken, Cyberwar- Das Internet als Kriegsschauplatz S.231 unten
99 Summing up Stuxnet in 4 Easy Sections by Eric Byres via http://scadahacker.blogspot.com/
100 The first deployed cyber weapon in history: Stuxnet's architecture and implications" by R. Langner auf ICCC der CCDCOE (07/2011)
101 Iran confirms Stuxnet attack on nuclear site by Rupert Goodwins via www.zdnet.co.uk

mit Massenvernichtungswaffen konkurrieren kann. Ralph Langner bezeichnet Stuxnet in seinem Vortrag bei der CCDCOE und TED fälschlicherweise als „*cyberweapon of massdestruction!*“[102], was nach jetzigen Diskussionen nicht bewiesen werden konnte. Ein weiterer Punkt ist die Attribution des Angriffes zu einer Quelle des Ursprungs, was bis heute nur auf Vermutungen basiert, die sich nie erhärtet haben.

Ein wichtiger Aspekt für die Politik und das Militär ist der vergleichsweise niedrige Aufwand für einen Staat, solch eine Software herzustellen, was aus der Sicht von Industrieländern gewisse strategische Vorteile gegenüber kleineren Staaten mindern könnte, jedoch diesen auch die Möglichkeit gibt, Interessen ohne konventionelle Mittel zu vertreten. Speziell auf politischer Ebene könnte man schneller eine Zustimmung für solche Manöver bekommen, da keine Soldaten, Maschinen oder andere wertvolle Dinge riskiert werden müssen. Hinzu kommt die mögliche Non-Attribution, die solch einer Operation gewisse diplomatische Probleme nimmt. Jedoch könnte ein Angriff auf kritische Infrastrukturen, wenn es zu ähnlichen Verlusten wie bei einem konventionellen Angriff kommen würde, ausreichen, um einen Krieg zu rechtfertigen.

Des Weiteren bringt ein Einsatz solcher Software auch noch andere Gefahren mit sich, denn Stuxnet hat sich auch auf andere Hardware auf der ganzen Welt installiert. Die Verbreitung betraf den ganzen Globus.[103] Ist eine Schadsoftware wie Stuxnet erstmal im Cyberspace, hat der Urheber nur noch über *Command and Control Server*[104] wie bei Stuxnet die Möglichkeit auf die Schadsoftware Einfluss zu nehmen. Hierbei kann der Angreifer jedoch enttarnt werden, was die Operation gefährden würde. Ein anderer wichtiger Punkt sind die Sicherheitslücken, die die Software in Windows ausgenutzt hat. Nach bekannt werden der Sicherheitslücken durch die Hersteller, werden diese Lücken sofort geschlossen (*es wird ein Patch eingespielt*), was der Schadsoftware nur eine gewisse Lebensdauer verschafft. Zwar ist eine Software wie Stuxnet vergleichsweise günstig und einfach herzustellen, dafür jedoch unkontrollierbarer und

102Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon via www.ted.com (05/2011)
103vgl. N. Falliere, L. O Murchu and E. Chien W32.Stuxnet Dossier S.5-S.10
104vgl. S.GayckenCyberwar- Das Internet als Kriegsschauplatz S.177

nicht immer erfolgssicher. Stuxnet wird jedoch als die erste evolutionäre Veränderung in der Schadsoftwaregeschichte eingehen. Diese Entwicklung hat Mikko Hyponnen in *From Brain to Stuxnet*[105] historisch aufgearbeitet hat.

4.3 Kriminalität im Internet am Beispiel vom Kneber-Botnet

Ein weiterer Bericht, der einen dauerhaften Konflikt im Cyberspace darlegt, ist die Kriminalität, welche immer größeres Ausmaß annimmt und von Computerexperten als größte Gefahr für die Zukunft des globalen Internets gesehen wird.[106]

In diesem Abschnitt soll gezeigt werden, dass die Kriminalität sich zunehmend an Schadsoftware bedient, um Gewinne zu erzielen. Um diese Gewinne zu erzielen, wird oft auf Botnetze zurückgriffen. Der Anreiz für die Investition in solche Botnetze ist ganz unterschiedlicher Natur. Die eine Gruppe von Kriminellen möchte gerne ihr Botnetz an zahlenden Kunden vermieten, die andere Gruppe will direkt an die Daten der infizierten Computer heran, um diese zu verkaufen, oder um durch den Besitz der Daten Betrug zu begehen. Da es sehr viele verschiedene Botnetze gab und gibt, soll in diesem Abschnitt anhand eines bekannten Botnetz erklärt werden, wie diese funktionieren. Es soll deutlich werden, dass solche Botnetze auch eine militärische Relevanz[107] haben, welche jedoch nicht als hoch eingestuft werden sollte.

Dieser kurze Bericht über das Kneber-Botnet wird sich hauptsächlich auf den Bericht[108] von Netwitness[109] beziehen. Netwitness ist ein Unternehmen was Software für die

105 From Brain to Stuxnet: Mikko Hyponnen on Malware and Security Preparedness by Dennis Fisher via http://threatpost.com/

106 How international cyber crime threatens national security by Kathleen Hickey via http://gcn.com/ (07/2011) und Strategy to Combat Transnational Organized Crime via www.whitehouse.gov (07/2011)

107 Air Force Colonel Wants to Build a Military Botnet by Kevin Poulsen via http://www.wired.com/ (05/2008) Carpet bombing in cyberspace Why America needs a military botnet by COL. Charles W. Williamson III via www.armedforcesjournal.com/

108 Vgl A. Cox and G. Golomb The "Kneber" botnet

109 NetWitness® is a revolutionary network monitoring platform that provides enterprises a precise and actionable

Überwachung von Firmennetzen verkauft.

Kneber hatte eine Größe von 74,126 Hostrechnern[110], welche sich aus den einzelnen Ip-Adressen der angemeldeten Hostrechner zusammensetzen. Das Botnetz war über 196 Länder dieser Erde verteilt und hatte fast die Hälfte der infizierten Hostrechner in Ägypten, Mexiko und Saudi-Arabien. Alle infizierten Systeme benutzten Windows Software, welche mit einem Marktanteil von ungefähr 90%[111] mit Abstand den größten Anteil hat. Netwitness zeigt in ihrem Bericht, dass innerhalb von vier Wochen 68,000 Anmeldeinformationen von Sozialen-Netzwerken, Email und anderen Diensten wie Facebook, Hi5 oder Yahoo entwendet worden sind. Wenn man die Daten der IP Adressen mit denen von großen Unternehmen vergleicht, stellt man fest, dass 374 Unternehmen aus den USA und 2411 Unternehmen aus der ganzen Welt von diesem Botnetz betroffen waren. Die Unternehmen waren in Bereichen wie Energie, Finanzen, Technologie und Internet Service beteiligt, was dieses Botnetz zu einem gefährlichen Werkzeug macht.

Da ein infizierter Computer häufig mit verschiedener Schadsoftware manipuliert worden ist, schien es zunächst nicht unnormal, dass es Überschneidungen mit dem *WALEDAC*[112] Botnetz gab. Jedoch schien die Verknüpfung zwischen den beiden Bot-Netzen so ausgelegt worden zu sein, dass das eine Netz das Andere über deren *Command and Control Server* steuern kann, falls eines der beiden Netze durch Aktionen von Anti-Viren Herstellern oder anderen Kriminellen gestört wird.

Auch hier spielt die Attribution eine große Rolle, da es bei Botnetzen schwierig ist, die Urheber zu finden. Beim Kneber-Botnetz führte die Spur zu einer Mail mit dem Namen *hilarykneber@yahoo.com* die zu vielen Domains führte, auf denen Schadsoftware abgelegt wurde. Danach hat Netwitness zeigen können, dass die meisten Server in

understanding of everything happening on the network.

110 A computer connected to a network, that provides data and services to other computers. TD

111 Top Operating System Share Trend

112 W32.Waledac is a worm that spreads by sending emails that contain links to copies of itself. It also sends spam, downloads other threats, and operates as part of a botnet.

China stehen, was jedoch bei der hohen Anzahl von Nutzern und der hohen Anzahl von Nutzern mit *gecrackter* Software(siehe Titan Rain) in diesem Land nicht unnormal ist. Kriminelle Banden arbeiten im Netz zusammen, um sich gegenseitig zu schützen. Sie nutzen Software oft für viele verschiedene Zwecke wie Bankbetrug oder Datendiebstahl und organisieren sich über das ganze Internet.

Für die internationale Politik impliziert das eine notwendige Zusammenarbeit auf verschiedenen Ebenen, da die finanziellen Verluste durch Kriminalität im Internet die Volkswirtschaften belasten.[113] Auch auf internationaler Ebene existiert bereits seit 2001 ein Vertrag[114] über die Bekämpfung von Cyber-Kriminellen, wobei erwähnt werden sollte, dass dieser Vertrag oft in der Kritik stand, da er Kriminelle nicht davon abhält Straftaten über Länder zu leiten(*routen*), die nicht diesen Vertrag unterschrieben haben. In Zukunft werden ähnliche Verträge unabdingbar werden, um den wachsenden Cyber-Kriminellen Vereinigungen entgegenzuwirken, sodass die Volkswirtschaften weniger Verlust durch Kriminalität im Internet hat.

Abschließend scheint die Relevanz solcher Botnetze auch in zwischenstaatlichen Konflikten relevant zu sein. Denn sowohl in Estland 2007[115] als auch in Georgien 2008[116] wurden Angriffe über Botnetze gemacht, die zu einem *denial-of-service*[117] geführt haben. Ob diese Zusammenschlüsse nun Botnetze waren, die nur von wenigen *Command and Control Servern* gesteuert worden sind, oder durch die Aktivität vieler Individuen, ist für das erreichen eines *denial-of-service* irrelevant. Abschließend ist zu erwähnen, dass Angriffe mit Botnetzen nicht hinreichende Eigenschaften haben, um vom Recht zum Krieg gebrauch zu machen.

113 Commission proposes new EU cybercrime law via http://www.theregister.co.uk/ (10/2010)
114 Convention on Cybercrime via ITLAW
115 vgl. S.14- 34 E. Tikk, K. Kaska and L. Vihul in International Cyber Incidents: Legal Considerations
116 vgl. S.66- 88 E. Tikk, K. Kaska and L. Vihul in International Cyber Incidents: Legal Considerations
117 When action(s) result in the inability to communicate and/or the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of a signal or operational capability (JCS 1997)

4.4 Aktivismus im Netz am Beispiel von Cryptome

Cryptome ist die erste Enthüllungsplattform, die das Internet hervorgebracht hat. Der 1930 geborene Aktivist John Young startet das Projekt 1996 in den USA und veröffentlicht seit dem Informationen von Staaten, die nicht öffentlich sein sollten. Die Plattform gibt allen Menschen mit einem Internetanschluss die Möglichkeit diese Daten abzugreifen und zu lesen. Young setzt sich für volle Informations- und Meinungsfreiheit ein. Oft werden Informationen auf der Webseite veröffentlicht, welche geheim sind. Für die internationale Politik können solche Veröffentlichungen viel Wirkung erzeugen, da sich Diplomaten, Geheimdienste und Militärs so der Öffentlichkeit aussetzen müssen. Dies ist meist von den Betroffenen nicht gewünscht. Auf diplomatischer Ebene können solche Aktionen zu Problemen führen. Das Vertrauen unter den einzelnen Regierungen kann dadurch verloren gehen. Auf der anderen Seite schaffen solche Plattformen eine Transparenz für die Bürger, die so ihren Regierungen bei der Arbeit zu schauen können. Ob jemals eine Veröffentlichung solcher Informationen zu einem schwerwiegenden Konflikt mit kriegerischer Handlung zwischen Staaten führen wird, ist fraglich. Da die Informationen auch für andere Staaten interessant sind, sehen Staaten wie die USA, eine große Gefahr in solchen Plattformen, da so wertvolle Informationen, die man vor anderen Staaten geheim halten wollte, nun jedem zugänglich sind. Zu erwähnen ist, dass andere Staaten anonym über solche Plattformen Informationen verteilen können.

Zusammenfassung der vier Bereiche Spionage, Sabotage, Kriminalität und Aktivismus

Alle vier Bereiche wurden in den Medien[118] gelegentlich als Cyberwar bezeichnet, obwohl diese nicht die Kriterien eines Cyberwar, nach der Definition in dieser Arbeit, erfüllen. Es lässt sich feststellen, dass Höchsten massive Spionage und Sabotage

118 Threat of 'cyberwar' has been hugely hyped by Bruce Schneier http://edition.cnn.com/ (07/2010)

ausreichende rechtliche und politische Wirkung haben könnte, um den Eintritt in einen Krieg zu rechtfertigen. Die Beispiele haben jedoch auch gezeigt, dass die Gefahr zum Krieg(*jus ad bellum*) durch Cyberspionage, Cybersabotage, Cyberkriminalität und Cyberaktivismus bis jetzt klein war. Viel wichtiger werden zukünftige Verträge gegen Cyber-Kriminalität sein. Diese Verträge werden jedoch von einigen Interessengruppen wie Geheimdiensten und Militärs als kritisch betrachtet, da Staaten relevante Informationen zu eigenen Strukturen offenlegen müssen, was als strategischer Nachteil gesehen werden kann. An diesem Dilemma der Kooperation sollte in Zukunft mehr gearbeitet werden.

5. Cyberwar im Hinblick auf jus in bello

In diesem Abschnitt soll anhand des Krieges zwischen Georgien und Russland im Jahre 2008 gezeigt werden, wie Cyberattacken in einem Krieg genutzt werden können, um das politische System und die Bevölkerung zu destabilisieren. Ein anderes Beispiel von Cyberangriffen ergänzend zu konventionellen Angriffen soll der Cyberangriff der israelischen Streitkräfte auf die syrischen Radaranlagen sein. Hier wurde ein Cyber-Angriff im klassischen Sinn des Krieges genutzt.

5.1 Georgien Russland Konflikt 2008

Im Jahre 2008 haben Russland und Georgien in den Provinzen Abchasien und Südossetien Krieg geführt. Ergänzend zum konventionellen Krieg wurde das Internet für Cyberangriffe genutzt. Der politische Kontext war ein bewaffneter Konflikt zwischen den beiden Staaten.

Georgien hatte zu diesem Zeitpunkt eine sehr geringe Anzahl(~7%)[119] an Bürgern, die

119 vgl. E. Tikk, K. Kaska and L. Vihul in International Cyber Incidents: Legal Considerations S.68, zweite Spalte, 1. Abs.

effektiv das Internet genutzt haben. Die Vernetzung in Georgien war sehr niedrig zu dieser Zeit. Hinzukommt, dass die Hauptanbindung ans Internet über Russland kommt. Die Attacken wurden von einer Forschungsgruppe der CCDCOE der NATO im *International Cyber Incidents: Legal Considerations*[120]gut dokumentiert.

Einen weiteren guten Beitrag zur Aufklärung über die Angriffe gab das *Project Grey Goose*[121]. Es soll die Zusammenfassung der CCDCOE genutzt werden. Die Methoden[122] des Angriffs waren DoS, DDoS, SQL Injections und die Verteilung von Schadsoftware über georgische Webseiten. Des Weiteren wurden Webseiten *defaced*[123] und Email-Adressen mit *Spam* penetriert. Die Ziele[124] dieser Angriffe waren Seiten des Präsidenten, der Ministerien, von Zeitungen, von Foren und Banken.[125]

Der Ursprung[126] der Attacken lag wahrscheinlich bei russischen Hacker-Gruppen, die diese Attacken vollzogen haben. Es gab keinen Beweis, dass russische Behörden oder andere russische Institutionen direkt in diese Attacken involviert waren. Außer der Verdacht auf die russische Jugendorganisation *Nashi.* Es gibt bis heute keinen Anhaltspunkt, wer das *defacement* oder die DDoS -Attacken organisiert hat.

Der Effekt[127] war, dass georgische Behörden in ihrer internen Kommunikation und in der Kommunikation mit ihren Bürgern eingeschränkt waren. Des Weiteren sind gewisse Knotenpunkte unter der Last zusammengebrochen, sodass einige Kommunikationsmedien nicht mehr funktioniert haben.

120This book features four national-scale cyber incidents (Estonia, Georgia, Lithuania and Radio Free Liberty) which demonstrate unique dependencies resulting from the widespread use of information society. These incidents raise questions to policymakers, diplomats, the intelligence community, military, information technology managers, and economists, as well as the general citizenry. E. Tikk, K. Kaska and L. Vihul in International Cyber Incidents: Legal Considerations 2010 CCDCOE S.66-90

121Project Grey Goose is, in technology terms, a pure play Open Source Intelligence (OSINT) initiative launched on August 22, 2008 to examine how the Russian cyber war was conducted against Georgian Web sites and if the Russian government was involved or if it was entirely a grass roots movement by patriotic Russian hackers

122vgl. E. Tikk, K. Kaska and L. Vihul in International Cyber Incidents: Legal Considerations S.89

123vgl. Fußnote 123

124vgl. Fussnote 123

125Coordinated Russia vs Georgia cyber attack in progress by Dancho Danchev via www.zdnet.com/ (08/2008)

126vgl. Fussnote 123

127vgl. Fussnote 123

Die Gegenmaßnahmen[128] wurden vom georgischen CERT(*Computer Emergency Response Team*) und CERTs aus anderen Ländern ausgeführt und koordiniert. Russische Webseiten wurden geblockt, um den Datenverkehr wieder unter Kontrolle zu bringen. Einige Webdienste wurden gespiegelt und in sogenannten *Mirrors*[129] hinterlegt, um den Zugriff auf wichtige Dienste wieder zu ermöglichen.

Während dieser Angriffe wurde klar, dass das internationale Recht für bewaffnete Kriege keine Möglichkeit gibt, solche Angriffe zu kategorisieren. Georgien hatte keine Möglichkeit die Angriffe gegen ihre Netze vor einem Gericht untersuchen zu lassen, da es keine Beweise für staatliches Handeln gab.

Jedoch kann man behaupten, dass diese Angriffe in ihrer Koordination einen Akt des Krieges darstellen könnten. Somit ist im Fall Georgien die Komponente *Cyber* im Krieg ein Präzedenzfall, welcher dem internationalen Völkerrecht neue Probleme aufgezeigt hat. Es muss deutlich gesagt werden, dass Georgien keinen großen wirtschaftlichen Schaden davon getragen hat, da viele Bürger moderne Kommunikationsmedien nicht benutzen. Auch ist kein Bürger durch diese Angriffe physisch zu Schaden gekommen. Eine ähnliche Attacke hätte jedoch in einem hoch vernetzen Land ganz andere Schäden angerichtet.

5.2 Israel-Syrien Konflikt – Operation Orchard

Am sechsten September 2007 flog die israelische Luftwaffe einen Angriff auf ein angebliches syrisches Atomkraftwerk, was vermutlich zur militärischen Nutzung vorgesehen war.[130] Im Jahre 2009 bestätigte die IAEA die Vermutungen Israels, dass diese Anlage illegal dort gebaut worden ist und wahrscheinlich militärisch genutzt

128 vgl. Fussnote 123

129 To create a site on a network which is a duplicate of another site, so more users can access a busy site. The closest mirror site to the user will provide the fastest access. TD

130 Syrien baute offenbar geheimen Atomreaktor via www.tagesschau.de

werden sollte.[131] Die *Operation Orchard* wurde in der Region *Deir ez-Zor* vom israelischen Militär präzise ausgeführt. Die Operation in Syrien dauert nur wenige Minuten, sodass syrische Boden- und Lufteinheiten nicht schnell genug reagieren konnten. Dieser Angriff scheint einer der wenigen Angriffe in den letzten Jahren gewesen zu sein, den man Cyberwar nennen könnte.

In diesem Konflikt wird vermutet, dass die israelische SIGINT[132] Einheit *Unit-8200*[133] die syrischen Radaranlagen gestört und manipuliert hat. Das syrische Militär benutze veraltete russische Radaranlagen, welche wahrscheinlich durch einen ähnlichen Angriff wie es das US-amerikanischen Suter-Program[134] kann, ge*hackt* worden sind.[135]

Hier kann abschließend gesagt werden, dass offensive Cyberkapazitäten den Erfolg dieser Operation ausgemacht haben.

Zusammenfassung

Im Georgien Beispiel war die Cyberattacke nur eine Begleiterscheinung zum regulären Krieg. Sie war nicht kriegsentscheidend und hatte keine hohe strategische Priorität. Wobei beim Angriff auf das syrische Atomprogramm die Komponente *Cyber* eine entscheidende Rolle gespielt hat.

Diese beiden Beispiele sollen nur exemplarisch die Situation auf internationaler Ebene darstellen. Sandro Gaycken hat vor zwei Jahren auf der SIGINT in Köln einen guten Überblick gegeben, was Staaten in solche Kapazitäten investieren, um sich einen strategischen Vorteil zu verschaffen.[136]

131 IAEA finds graphite, further uranium at Syria site by Mark Heinrich via www.reuters.com/ (02/2009)und IAEA inspects nuclear research reactor in Syriavia by AFP via http://www.google.com/hostednews/afp/ (11/2009)

132 Signals intelligence (SIGINT) is intelligence-gathering by interception of signals, whether between people (i.e., communications intelligence (COMINT)) or between machines (i.e., electronic intelligence (ELINT)), or mixtures of the two.

133 Unit 8200 ist die operative Einheit im Cyberspace der Israelischen Armee . Geschichte zur Truppe unter: http://dover.idf.il/IDF/English/News/today/2008n/09/0101.htm

134 Both L-3 Communications' Network-Centric Collaborative Targeting (NCCT) system and operational versions of the BAE Systems-developed Suter communications network exploitation system are being rushed to support Iraq operations via http://www.aviationweek.com

135 Israel used electronic attack in air strike against Syrian mystery target by David A. Fulghum and Douglas Barrie via http://www.aviationweek.com/

136 SIGINT 2009: Sandro Gaycken über Cyberwarfare by Christian Scholz via http://mrtopf.de/

6. Die Dimension der Cyberkonflikte

6.1 Bytes und Platinen- Differenzierungsprobleme für die internationale Politik

Für Software und Hardware gelten grundsätzlich ähnliche Eigenschaften. Sie sind die Universalien aus denen Computer bestehen. Damit bilden sie für alle Staaten, Gruppen und Individuen die Basis im Cyberkonflikt. Es soll kurz erläutert werden, dass die Angriffsmöglichkeiten für alle Akteure ähnlich sind. Sowohl Software als auch Hardware lassen Spielraum für Manipulation und Sabotage. Aus diesem Grund werden Staaten daran interessiert sein, solche Sicherheitslücken zu besitzen, um sie in einem zukünftigen Konflikt einzusetzen. Dies wird zu einem Wettrüsten führen.[137]

Jede Cyberattacke wird durch eine Cyber*waffe* getätigt werden, welche auf einer Software oder Hardware Sicherheitslücke basiert. Eine kurze Definition von Waffen und Cyber*waffen* liefern Rain Ottis und Peeter Lorents in ihrem Aufsatz *Knowledge Based Framework for Cyberweapons and Conflict.* Die drei Definitionen sollen als grundlegende Beschreibung für Cyber*waffen* dienen.

„[...]A weapon is a system that is designed to damage the structure or operations of some other system(s)"[138]

„[...]An information technology weapon, or shorter IT weapon, is an informationtechnology-based-system(consisting of hardware, software and communication mediu)[Anmerk.[139]*] that is designed to damage the structure or*

137vgl. K. Coleman Cyberwarfare Doctrine Addressing the most significant threat of the 21st century

138vgl. Ottis and Lorents Conference on Cyber Conflict Proceedings 2010 Knowledge Based Framework for cyber weapons and conflict S.139

139Anmerkung: Bei dieser Definition sollte besser ein "*und*" und ein "*oder*" stehen, folglich: "consting of hardware and/or, software and/or communication medium", denn es kann nur eine Software oder Hardware sein, die den Schaden anrichtet.

operations of some other system(s)"[140]

„[...]A cyber weapon is an information technology-based system that is designed to damage the structure or operationsof some other information technology based system(s)"[141] *[Anmerk.]*[142]

Bytes, die Basis der Softwareattacke im Cyberkonflikt

Der Quellcode einer Schadsoftware für Cyberwaffen versucht andere Software oder Hardware zu beeinflussen, was auf der Ebene der Maschinensprache in Bits und Bytes (8Bit sind 1Byte) ausgeführt wird. So wie radioaktives Material zum Bauen einer Atombombe benötigt wird, so wird Quellcode *(Sourcecode)* für den Bau einer Cyberwaffe benötigt. Der Unterschied zur Analogie mit Nuklearwaffen wird deutlich durch die Herstellung der Waffe mit radioaktivem Material. Sspeziell hochangereichertes Uran unterliegt ganz anderen Beschaffungskriterien wie Quellcode, der in jedem herkömmlichen Textverarbeitungsprogramm geschrieben werden kann oder aus dem Internet heruntergeladen werden kann. Sogar der Quellcode für Stuxnet kann ohne großen Aufwand über das Internet heruntergeladen werden. Quellcode kann in winzig kleinen Speichermedien transportiert werden, sodass es unmöglich ist, ein internationales Handelsembargo mit Sanktionen durchzusetzen. In diesem Zusammenhang sollte erwähnt werden, dass schon heute sogenannte *logic bombs*[143] in Software verbaut sind, um strategische Vorteile zu

140 Siehe Fußnote 138

141 Siehe Fußnote 138

142 Anmerkung: Da heute alle kritischen Infrastrukturen, militärisches Gerät und Alltagsgegenstände auf solche *informations-technologisch-basierten* Systemen aufbauen, ist klar, dass die Kausalwirkung im Falle eines Angriffs ähnliche Schäden wie konventionelle Waffen hervorrufen kann oder sogar größere. Die meisten Vergleiche zwischen konventionellen Waffen und Schadsoftware sind jedoch falsch, denn Schadsoftware kann sich selbst reproduzieren, konventionelle Waffen nicht. Schadsoftware kann konventionelle Waffen zerstören, *vice versa* funktioniert das nicht.

143 Code that is hidden in a program or system which will cause something to happen when the user performs a certain action or when certain conditions are met. A logic bomb, which can be downloaded along with a corrupted shareware or

haben. Da Software auf der ganzen Welt meist von privaten Unternehmen geschrieben wird, ist es wahrscheinlich, dass Unternehmen wie Microsoft von US-amerikanischen Geheimdiensten und Militärs genutzt werden, um Hintertüren einzubauen.[144] Hier haben die USA einen klaren strategischen Vorteil durch die hohe Nutzung von Windows auf Computern. Gegen solche Attacken hilft nur die Herstellung eigener Software, welche gewisse Kriterien erfüllen muss. Dies ist sehr teuer und aufwendig, da es nicht viele Programmierer gibt, die auf solch einem Niveau arbeiten können.

Platinen, die Basis der Hardwareattacke im Cyberkonflikt

Schon lange wird vermutet, dass Staaten und Unternehmen, in der Produktion von Hardware, Sicherheitslücken oder auch *logic bombs* einbauen, um in zukünftigen Konflikten einen Vorteil zu haben. Die USA hatten schon vor einigen Jahren festgestellt, dass Hardware von der chinesischen Firma *Huawei* ein Sicherheitsrisiko darstellt.[145] Der „*Cisco Raider*“[146] Vorfall im Jahre 2007 zeigte anschaulich, dass gefälschte Netzwerkkarten der Firma Cisco ein erhebliches Sicherheitsrisiko sind, da die Hardware Hintertüren eingebaut hat, die jederzeit aktiviert werden können. Es muss klar sein, dass egal welche Software auf dem Computer läuft, die Hardwareattacke trotzdem funktioniert. Somit hat die Hardware Hintertür für Staaten klare strategische Vorteile gegenüber der Software Hintertür.

Im November 2011 gab der US-Senat bekannt, dass militärisches Gerät gefälschte Hardware enthielt, was eine immense Sicherheitslücke ist.[147] Gegen solche Attacken kann man sich einigermaßen schützen, wenn die Hardware überprüft wird und

freeware program, may destroy data, violate system security, or erase the hard disk. It is not the same as a virus because the logic bomb executes once, or at periodic intervals, whereas the action of a virus is ongoing. Also known as a Fork Bomb - A resident computer program which, when executed, checks for a particular condition or particular state of the system which, when satisfied, triggers the perpetration of an unauthorized act. TD

144How NSA access was built into Windows by Duncan Campbell via http://www.heise.de/

145Huawei a security risk, claims Minchin *By AAP via* www.zdnet.com.au/ (12/2008)

146vgl. S. Gaycken, Cyberwar- Das Internet als Kriegsschauplatz S.135

147US weapons 'full of fake Chinese parts' by Malcom Moore via www.telegraph.co.uk

vielleicht im eigenen Land produziert wird. Der Aufwand ist extrem hoch, da alleine ein handelsüblicher Computer viele Teile hat, wo solche Attacken theoretisch möglich sind. Hinzu kommt, dass in fast allen kritischen Bereichen herkömmliche Hardware verbaut ist

Hier ist anzumerken, dass ein großer Teil der Hardwareproduktion von chinesischen Unternehmen dominiert wird. Dies lässt folgern, dass der chinesische Staat bei der Hardwareherstellung theoretisch einen Vorteil gegenüber anderen Staaten hat. Sandro Gaycken teilte auf der Handelblatt Konferenz zu Cybersecurity mit, dass im Zuge des Problembewusstseins Vorschläge, wie die Verlagerung der Produktion von Chips für kritische Strukturen zurück nach Deutschland, im Moment politisch diskutiert wird.

Grundsätzlich kann festgestellt werden, dass durch die Technologisierung und massive Vernetzung in kritischen Bereichen wie den Militärs ein großes Interesse darin besteht, solche Cyberwaffen beim Gegner zu haben. Jedoch entsteht hier ein Dilemma. Denn wahrscheinlich haben alle Akteure sich schon gegenseitig ge*hackt*, sodass es am Ende darauf hinausläuft, wer mehr Sicherheitslücken beim anderen kennt oder selbst eingebaut hat. Somit wird derjenige den strategisch größten Vorteil haben, der seine Software und Hardware selbst herstellt. Dies gilt nicht nur für Staaten und ihre Militärs. Für die internationale Politik wird es große Veränderungen geben, da es hier um Risiken geht, die schlecht abzuschätzen sind. Die Implikationen für Wirschaft und Handel im Bereich kritischer Strukturen wie Maschinen und Rüstungsgüter sind kaum abzusehen. Jede normale Software und Hardware kann so verändert oder eingesetzt werden, dass dadurch ein Bedrohungsszenario mit Schaden entsteht. Jeder Staat, jede Gruppe und jede Person ist rein theoretisch in der Lage solche Cyberwaffen herzustellen und zu benutzen. Die Parallele zu zum asymmetrischen Krieg, wie es der Terrorismus ist, ist nicht von der Hand zu weisen. Vorhandene Machtverhältnisse werden dadurch nachhaltig verändert wie Sandro Gaycken feststellt[148] und durch eine These von George Orwell treffend beschreibt,

148vgl. S. Gaycken, Cyberwar- Das Internet als Kriegsschauplatz S.195

„A complex waepon makes the strong stronger while a simple waepon- so long as there is no answer to it- gives claws to the weak“ [Tribune 1945]

Diese These sagt Gaycken stimmt jedoch nur teilweise, zwar kann „*jeder ein Hacker“*[149] sein und jede Gruppe kann die Fähigkeiten erlernen solche Attacken über Computer auszuführen, jedoch zeigt Gaycken, dass diese Einschätzung nicht überbewertet werden sollte.

„Jeder Schaden durch Freizeithacker wird weit opportunistischer und harmloser sein als jener, der durch Militärs verursacht wird“[150]

Ein Vertrag unter den Staaten sollte es trotz der asymmetrischen Problematik geben, da Staaten die größte Gefahr im Zusammenhang mit Cyberwaffen darstellen. Es ist aber eine Illusion, dass dieser Vertrag das staatliche Hacken und Spionieren einschränkt. Die Überprüfung der Einhaltung solch eines Vertrages wird völlig unmöglich sein, sodass die Staaten sich nur vertrauen können. Professor Heintschel von Heinegg sagte auf der Handelsblatt Konferenz für Cybersecurity im Jahre 2011, dass es einen internationalen Cyber-Abrüstungsvertrag nicht geben wird. Aus strategischer Sicht werden Staaten sich misstrauen und versuchen einen Vorteil durch den Bau solcher Waffen zu erlangen. An diesem Punkt sollte erwähnt werden, dass spieltheoretische Ansätze einen guten Überblick geben würden, diese Problematik zu analysieren. Cyberwaffen werden die internationale Politik nachhaltig verändern, sodass eine zukünftige Zusammenarbeit auf internationaler Ebene nicht einfacher wird und deswegen immer notwendiger.

6.2 NON-Attribution als Hauptproblem in Cyberkonflikten

Dieser Abschnitt soll sich mit der Problematik der Attribution beschäftigen. Attribution im Krieg ist die Zurückverfolgung einer Attacke zum Angreifer. Aus politischer,

149vgl. Fußnote 148
150vgl. Fußnote 148

militärischer und rechtlicher Sicht ist dieser Abschnitt eine Herausforderung für die zukünftige Sicherheitspolitik.

Es soll deutlich werden, dass kein Staat und keine Institution ein offizielles Konzept vorgestellt hat, um das Attributionsproblem im Cyberspace zu lösen. Wie am Anfang der Arbeit schon erwähnt worden ist, sind die bekannten Methoden der Attribution in Computernetzen nicht ausreichend, um gut ausgerüstete Geheimdienste und Militärs zu identifizieren. Somit werden Abschreckung und Gegenschlag obsolet. Dies ist ein wirkliches Dilemma für Entscheidungsträger. Sandro Gaycken beschreibt es so:

„Konzeptionell wäre es daher sauberer, sich mit der Unmöglichkeit der Attribution abzufinden und künftig unter dem Label Non-Attribution neue Wege jenseits der Abschreckung zu suchen.“[151]

Da die Lösung des Problems eine technische und rechtliche ist, muss abgewartet werden, ob in Zukunft Fortschritte in der Forschung gemacht und Verträge ausgehandelt werden. Für die internationale Politik wird es Probleme geben, solche Verträge zu ratifizieren. Ein Versuch dem Problem entgegenzuwirken, war die Idee des *„Active Defense“*[152] von Matthew Skelerov. Dieser Vorschlag wurde vom Chef der NSA und des USCYBERCOMMANDS, General Keith Alexander, auf der *InfoWarCon 2011*[153] beschrieben:

„Gen. Keith Alexander, chief of U.S. Cyber Command, called the cloud approach "active defense," adding that "hunting on our networks has got to change."[154]

Er sprach zwar nur von Kriminalität, jedoch ist klar, dass unter den Einbrüchen in militärische Netze der USA auch Staaten beteiligt sind. Auch Jeffrey Carr nimmt diese Idee in seinem Buch *Inside Cyberwarfare – Mapping the Cyber Underworld* auf. Aus Sicht von Sandro Gaycken ist diese Umsetzung irrational, was er in seinem Aufsatz

151 vgl. S. Gaycken, Cyberwar- Das Internet als Kriegsschauplatz S.85 3.Abs.

152 vgl. S. Gaycken Cyberwar – Das Internet als Kriegsschauplatz S.89 unten: *“Skelerov argumentiert darin für eine Anwendung der Safe-Heaven-Regulierung des Kriegsrechts auf nicht staatliche Hackerangriffe. Wenn Cyber-Angriffe nicht staatlicher Akteure aus einem fremden Land nicht von diesem Land selbst gestoppt und aufgeklärt werden können, wird das Land als Unterstützer kriegerischer Aktivitäten angesehen und darf militärisch angegriffen werden.”*

153 This conference will provide a forum for professionals from the military, government, industry, and academia to discuss the issues related to planning, programming, and executing Cyber, EW, OPSEC, and deception operations to achieve IO effects.

154 Defense cyber chief: The cloud is the military's next Internet by Aliya Sternstein via www.nextgov.com/

The Necessity of (Some) Certainty -A Critical Remark Concerning Matthew Sklerov's Concept of "Active Defense[155] widerlegt.

Meist wird die Attribution durch den Kontext versucht herzustellen. Jedoch hat dies in der Vergangenheit zu vielen Vermutungen mit diplomatischen Konsequenzen geführt. Non-Attribution sollte als Status Quo verstanden werden. Die Non-Attribution in Kombination mit fehlenden rechtlichen Rahmenbedingungen stellen für die strategische Folgenabschätzung spieltheoretische Probleme dar.

6.3 Institutionen in internationalen Cyberkonflikten

Institutionen werden in Zukunft eine wichtige Rolle in der Regulierung des Cyberwar spielen. Das Problem ist, dass sich bei Konflikten durch die Komponente Cyber regionale, nationale und transnationale Zuständigkeitsbereiche überschneiden. Durch die hohe Interdependenz, die über den Cyberspace erreicht wird, wird es schwer werden eine spezielle Institution zu beauftragen, das Problem zu lösen. Cyberwar stellt wie der Terrorismus als asymmetrischer Krieg den Institutionalismus in Frage. Zwar sollten die Vereinten Nationen(VN) und die OSZE eine wichtige Funktion in der internationalen Kommunikation im Bereich Cyberwar haben, was sie bis dato nicht haben. Da Militärs auf der ganzen Welt von diesem Phänomen betroffen sind, fallen die zuständigen Kompetenzen meist in die Nationalstaaten zurück. Denn fast alle militärischen Einheiten werden noch von Nationalstaaten geführt und geleitet. Auch die NATO ist nur ein Zusammenschluss von vielen Staaten. Hier ist abzusehen, dass es ein weiteres Dilemma geben wird oder gibt, denn Cyberwar ist ein globales Problem. Es wird abzuwarten sein, ob die Vereinten Nationen versuchen werden die Diskussion zu leiten. Es gab Gespräche über zukünftige Lösungsvorschläge, jedoch scheint die Debatte schwierig zu sein. Auch die OSZE könnte zukünftige Aufgaben in diesem Bereich übernehmen. Auch einzelnen Staaten wie China, USA und Russland haben

155Vgl S. Gaycken The Necessity of (Some) Certainty - A Critical Remark Concerning Matthew Sklerov's Concept of "Active Defense

wichtige Funktionen in der zukünftigen Debatte, da im Moment ein klarer Ton aus den USA gegenüber China in der Cyber-Debatte herrscht.[156] Trotz vieler Bedenken, wie z.B. der Non-Attribution, sollte Cyberpeace[157] in Zukunft erstrebenswert sein und von allen regionalen, nationalen und internationalen Institutionen durch Verträge und gemeinsamen Informationsaustausch gefördert werden.

7. Abschließende Zusammenfassung

Die Bachelorarbeit hat versucht, die Entwicklung und das Verständnis des Wortes Cyberwar anhand einer Begriffsanalyse zu erläutern. Mit dem Versuch mehr Klarheit für den Begriff Cyberwar zu erlangen, wurde die Kybernetik und der klassische Krieg als Grundideen untersucht. Eine Beschränkung der inflationären Nutzung des Begriffs Cyberwar wurde durch die engere Definition des Begriffs erreicht. Die drei Eckpunkte Punkte der Definition für Cyberwar waren, erstens ***die Ausnutzung von Sicherheitslücken in der vernetzten Technologie der klassischen Domänen, zweitens, das Cyberwar eine eigene, neue, transzendentale Domäne ist und drittens die Gesamtheit aller Angriffe über den Cyberspace mit den Vektoren Zerstörung, Manipulation und Spionage während einer kriegerischen Handlung ist.*** Die neue Definition postuliert Cyberwar als *Nullte Domäne*, welche alle anderen Domänen des Krieges **transzendiert**. Eine Neubetrachtung der Situation ist nötig, um zukünftige Gefahren für die Sicherheitspolitik zu antizipieren.

Der Vorteil dieser Definition ist, dass viele Konflikte, wie im Teil jus ad bellum gezeigt, nicht leichtfertig als Cyberwar bezeichnet werden können. Gerade die Vermischung der Bereiche Spionage, Sabotage, Kriminalität und Aktivismus sollten mit der geforderten Definition nicht möglich sein. Die vier Beispiele sollten grob skizzieren, wie schon vorhandene Konflikte kategorisiert werden sollten.

156vgl. C. Bronk Blown to Bits-- China's War in Cyberspace, August-September 2020
157vgl. The Quest for cyberpeace -- International Telecommunication Union -- By Dr Hamadoun I.Touré

Eine Untersuchung von Cyberwaffen hat die beiden Komponenten Software und Hardware und ihre Möglichkeiten als Cyberwaffen aufgezeigt. Es wurde gezeigt, dass die Verschiebung der Machtverhältnisse durch Cyberwaffen vorprogrammiert ist. Es wurden Vorteile für einzelne Staaten wie die USA(Software) oder China(Hardware) ausgearbeitet, da sie durch die Produktion von Komponenten, *logic bombs* nutzen können. Jedoch können Länder mit wenig vernetzter Infrastruktur ohne großen Aufwand, ohne Angst vor Angriffe über den Cyberspace offensive Kapazitäten aufbauen, da sie nicht so massiv vernetzt sind. Dies wird in den nächsten Jahren dafür sorgen, dass die internationale Politik stark durch die Cyber Komponente geprägt werden wird.

Abzuwarten ist die Lösung des Attributionsproblems. Ohne einen Fortschritt in diesem Bereich wird Cyberwar wahrscheinlich gefährlicher werden, da der Cyberspace weiter wachsen wird. Der Vernetzung der Welt steht bis heute nichts entgegen, da der Nutzen für die Nutzer größer ist als die Gefahren. Bürgern, Wirtschaft und Staaten wird durch das Internet eine globale Plattform zur Verfügung gestellt, die so mobil und vernetzt ist, wie noch nie zuvor. Wie lange diese Aussage noch gültig ist, hängt ganz von der Kooperation der einzelnen Staaten im Cyberspace ab, um Cyberwar zu regulieren, Cybercrime zu bekämpfen und freien Zugang zum Internet zu fördern.

8. Literaturverzeichnis

1. Paul Christopher, The Ethics of War and Peace, (Prentice Hall, 2nd Ed. 1999) (259 pages) English

2. Maiese, Michelle. "Jus in Bello." Beyond Intractability. Eds. Guy Burgess and Heidi Burgess. Conflict Research Consortium, University of Colorado, Boulder. Posted: June 2003 http://www.beyondintractability.org/bi-essay/jus_in_bello/

3. Sandro Gaycken Cyberwar Das Internet als Kriegsschauplatz 1. Auflage November 2010 ISBN 978-3-941841-23-9 dt., 248 S brosch.

4. A Conversation on Cybersecurity With William J. Lynn III, US Deputy Secretary of Defense
On 15 September 2010, the Security and Defence Agenda hosted William J. Lynn, III, US Deputy Secretary of Defense, to present the US perspective on cybersecurity and discuss NATO's outlook for improving cyber defence networks.
http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=122287

5. INFORMATION AS POWER AN ANTHOLOGY OF SELECTED UNITED STATES ARMY WAR COLLEGE Vol. 5 – Edited by Jeffrey L. Caton, John H. Greenmyer, Jeffrey L. Groh, and William O. Waddell (2010) 261 pages) (English) http://www.carlisle.army.mil/DIME/documents/IAP%20Vol%205%20Complete%20Book%20(21%20Jan%2011).pdf

6. Botnets: 10 Tough Questions by Editor: Dr. Giles Hogben, Authors: Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder (18 pages) (english)

http://www.enisa.europa.eu/act/res/botnets/botnets-10-tough-questions/at_download/fullReport

7. PD Dr. Dr. K. Saalbach Policy Making and Analysis Wintersemester 2009/2010 (49 Seiten) (deutsch)

8. **Network Security: Private Communication in a Public World, 2/E** Charlie KaufmanRadia PerlmanMike Speciner ISBN-10:0130460192 ISBN-13: 9780130460196 Publisher: Prentice HallCopyright: 2002Format: Cloth; 752 pp Published: 04/22/2002Status: Instock

Cyberwarfare Doctrine Addressing the most significant threat of the 21st century – Public Version- Sensitive Security Information Removed by Kevin Coleman 2008 The Technolytics Institute (8 pages9 (English)
http://www.technolytics.com/Cyber_Warfare_Doctrine_Public_Version.pdf

10. Die Struktur wissenschaftlicher Revolutionen (suhrkamp taschenbuch wissenschaft) Thomas S.Kuhn (20. Februar 2001) (239 Seiten) (Deutsch)

11. Conference on Cyber Conflict Proceedings 2010 version 1.0 June 2010 Publisher CCDCOE Publications (245 pages) (English)

12. International Cyber Incidents: Legal Considerations 2010 CCDCOE -- E. Tikk, K. Kaska and L. Vihul Publisher CCDCOE Publications (published 2010)(130 pages) (English)

13. Inside Cyberwar -Mapping the Cyber Underworld by J. Carr – Published by O'Reilly Media Inc. (published 2010) (213 pages) (English)

14. U.S. Cyber Command Fact Sheet May 25, 2010 On June 23, 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish USCYBERCOM. Initial Operational Capability (IOC) was achieved on May 21,2010.
http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf

15. (Symantec) W32.Stuxnet Dossier Version 1.4 Nicolas Falliere, Liam O Murchu and Eric Chien (published February 2011) (69 pages)

16. Computer Espionage, Titan Rain and China by James A. Lewis (2 pages) (English) Published by CSIS http://csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf

17. Blown to Bits -- China's War in Cyberspace, August-September 2020 by Christopher Bronk (20 pages) (English)
http://www.au.af.mil/au/ssq/2011/spring/bronk.pdf

18 Introduction to Ipv6 by Hubert Feyrer 5/24/2001 (6 pages) (English) Published by O'Reilly Media
http://www.elportal.info/ebooks/O'Reilly%20-%20Introduction%20to%20IPv6.pdf

19. Bundesministerium der Verteidigung Weißbuch 2006 Zur Sicherheitspolitik Deutschlands und zur zukunft der Bundeswehr (176 Seiten) (Deutsch) Hrsg. BMVg

20. Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms (Published by the Department of Defense US Army) (549 pages) (English) Hinweis: JP 1-02 is accessible online as a searchable database and in PDF format at

the following Internet address: http://www.dtic.mil/doctrine/dod_dictionary and at the following NIPRNET address: https://jdeis.js.mil. The contents of JP 1-02 are updated on a monthly basis to include any terminology additions, modifications, or deletions made within the previous calendar month in accordance with CJCSI 5705.01.
http://www.fas.org/irp/doddir/dod/jp1_02.pdf

21. Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities 34-35 (GAO-11-75) (July 2011) (79 pages) (English)
http://www.gao.gov/new.items/d1175.pdf

22. The “Kneber” botnet by A. Cox and G. Golomb Published by Netwitness (8 pages) (English) http://www.netwitness.com/resources/downloads/2011-the-kneber-botnet

23. The Necessity of (Some) Certainty - A Critical Remark Concerning Matthew Sklerov’s Concept of “Active Defense” by Dr. Sandro Gaycken – University of Stuttgart (6 pages) (English) in Journal of Military and Strategic VOLUME 12, ISSUE 2, WINTER 2010 Studies

24. The Quest for cyberpeace -- International Telecommunication Union -- By Dr Hamadoun I.Touré and
the Permanent Monitoring Panel on Information Security
World Federation of Scientists
(132 pages) (English) published 2011
http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf

Eine Liste der verwendeten Links zu den Fussnoten:

Fussnote 15
http://informationweek.com/news/government/security/231002112

Fussnote 16

http://www.cbsnews.com/8301-505124_162-43448728/so-why-does-the-air-force-want-hundreds-of-fake-online-identities-on-social-media-update/
Fussnote 17
http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media
Fussnote 18
http://www.economist.com/node/16478792 und http://www.heise.de/tp/artikel/9/9753/1.html
Fussnote 19
http://www.telegraph.co.uk/news/worldnews/wikileaks/8192001/WikiLeaks-cyberwar-hackers-planning-revenge-attack-on-Amazon.html
Fussnote 22
http://www.alios.org/blog/2010/12/wikileaks-cyberwar/
Fussnote 23
Professor Girnth der Philipps-Universität Marburg zu diesem Thema http://www.theeuropean.de/heiko-girnth/604-der-neue-krieg-in-afghanistan
Fussnote 26
http://plato.stanford.edu/entries/vienna-circle/
Fussnote 27
http://www.asc-cybernetics.org/foundations/history/MacySummary.htm
Fussnote 28
http://plato.stanford.edu/entries/turing-machine/
Fussnote 30
http://is.uni-sb.de/studium/handbuch/exkurs1.html
Fussnote 31
http://is.uni-sb.de/studium/handbuch/exkurs1.html
Fussnote 33
http://usacac.leavenworth.army.mil/CAC2/CALL/thesaurus/toc.asp?id=17438&section=j
Fussnote 34
http://www.youtube.com/watch?v=ofbt7A2pEm4 Arte Beitrag Mit offenen Karten - Internet und Geopolitik
Fussnote 42
http://www.heise.de/netze/meldung/IPv4-Der-Countdown-laeuft-ab-1175088.html
Fussnote 44
http://digitalfreaks.org/~lavalamp/CIDR6.html
Fussnote 45
http://itlaw.wikia.com/wiki/RIPE
Fussnote 46
http://www.heise.de/netze/meldung/Bundeswehr-meldet-hohen-IPv6-Adressbedarf-beim-RIPE-an-820590.html
Fussnote 51
http://www.dod.mil/execsec/adr95/c4i_5.html
Fussnote 52
http://www.iwar.org.uk/iwar/resources/cybercommand/speech.htm
Fussnote 55
http://www.gpsworld.com/gnss-system/perspectives-june-2008-7254
Fussnote 56
http://www.bpb.de/popup/popup_lemmata.html?guid=GV0OHL
Fussnote 59
http://www.bpb.de/popup/popup_lemmata.html?guid=7OLVPF
Fussnote 60
http://www.bpb.de/popup/popup_lemmata.html?guid=VWQDF0
Fussnote 61
http://www.bpb.de/popup/popup_lemmata.html?guid=S86L3V

Fussnote 63
http://www.schneier.com/essay-201.html
Fussnote 65
http://www.psychology48.com/deu/d/akkommodation/akkommodation.htm
Fussnote 66
http://www.psychology48.com/deu/d/assimilation/assimilation.htm
Fussnote 68
http://www.fas.org/irp/program/disseminate/jwics.htm
Fussnote 72
http://itlaw.wikia.com/wiki/ICT
Fussnote 70
http://www.defpro.com/news/details/25068/?SID=8f2d3ac8a587be5afceaeae378d3c929
Fussnote 71
http://www.miller-mccune.com/politics/mobilizing-in-the-fifth-domain-24726/ und
http://thehill.com/blogs/hillicon-valley/technology/171531-pentagon-declares-the-internet-a-domain-of-war
Fussnote 77
http://www.time.com/time/magazine/article/0,9171,1098961,00.html
Fussnote 78
Metainformation in html www.sandia.gov
Fussnote 79
Metainformation in html http://www.lockheedmartin.com/
Fussnote 80
http://itlaw.wikia.com/wiki/ZIP
Fussnote 87
http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1
Fussnote 88
http://www.un.org/apps/news/story.asp?NewsID=21997&Cr=Iran&Cr1=
Fussnote 91
http://www.langner.com/en/2011/06/07/enumerating-stuxnet%e2%80%99s-exploits/
Fussnote 92
http://media.ccc.de/browse/congress/2010/27c3-4245-en-adventures_in_analyzing_stuxnet.html
Fussnote 94
http://content.usatoday.com/communities/technologylive/post/2011/01/why-the-stuxnet-worm-could-be-confickers-cousin-/1
Fussnote 95
http://www.youtube.com/watch?v=Q9ezff6LIoI
Fussnote 99
http://scadahacker.blogspot.com/2011/03/summing-up-stuxnet-in-4-easy-sections.html
Fussnote 100
http://vimeo.com/25710852
Fussnote 101
http://www.zdnet.co.uk/news/security-threats/2010/09/26/iran-confirms-stuxnet-attack-on-nuclear-site-40090272/
Fussnote 102
http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html
Fussnote 105
http://threatpost.com/en_us/blogs/brain-stuxnet-mikko-hyponnen-malware-and-security-preparedness-072711
Fussnote 106
http://gcn.com/articles/2011/07/27/international-cyber-crime-threat-to-us.aspx

http://www.whitehouse.gov/administration/eop/nsc/transnational-crime
Fussnote 107
http://www.wired.com/threatlevel/2008/05/air-force-col-w/
http://www.armedforcesjournal.com/2008/05/3375884
Fussnote 109
http://www.netwitness.com/ NetWitness
Fussnote 111
http://www.netmarketshare.com/os-market-share.aspx?qprid=9
Fussnote 112
http://www.symantec.com/security_response/writeup.jsp?docid=2008-122308-1429-99
Fussnote 113
http://www.theregister.co.uk/2010/10/11/eu_new_cybercrime_law/
fussnote 114
http://itlaw.wikia.com/wiki/Convention_on_Cybercrime
Fussnote 117
https://www.iad.gov/ioss/department/opsec-glossary-of-terms-10026.cfm
Fussnote 118
http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/
Fussnote 125
http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670
Fussnote 130
http://www.tagesschau.de/ausland/syrien386.html
Fussnote 131
http://www.reuters.com/article/2009/02/19/us-nuclear-iaea-syria-sb-idUSTRE51I45R20090219 und
http://www.google.com/hostednews/afp/article/ALeqM5h5unOYKKK_uObtyARlvuJiY5jU_w
Fussnote 133
http://dover.idf.il/IDF/English/News/today/2008n/09/0101.htm
Fussnote 134
http://www.aviationweek.com/aw/generic/story_channel.jsp?
channel=defense&id=news/aw011507p2.xml&headline=null&next=10
Fussnote 135
http://www.aviationweek.com/aw/generic/story.jsp?
channel=defense&id=news/aw100807p2.xml&headline=Israel%20used%20electronic%20attack%20in
%20air%20strike%20against%20Syrian%20mystery%20target&next=10
Fussnote 136
http://mrtopf.de/blog/conferences-and-meetings/sigint-2009-sandro-gaycken-uber-cyberwarfare/
Fussnote 135
http://www.crows.org/details/144-maneuvering-in-Cyberspace-and-io.html
Fussnote 144
http://www.heise.de/tp/artikel/5/5263/1.html
Fussnote 145
http://www.zdnet.com.au/huawei-a-security-risk-claims-minchin-339293891.htm
Fussnote 147
http://www.telegraph.co.uk/news/worldnews/northamerica/usa/8876656/US-weapons-full-of-fake-Chinese-parts.html
Fussnote 154
http://www.nextgov.com/nextgov/ng_20111027_3085.php

9. Abbildungsverzeichnis

Abbildung 1 Sebastian Kautz www.study4cyberwar.com/images/cyberspace%20model.jpg

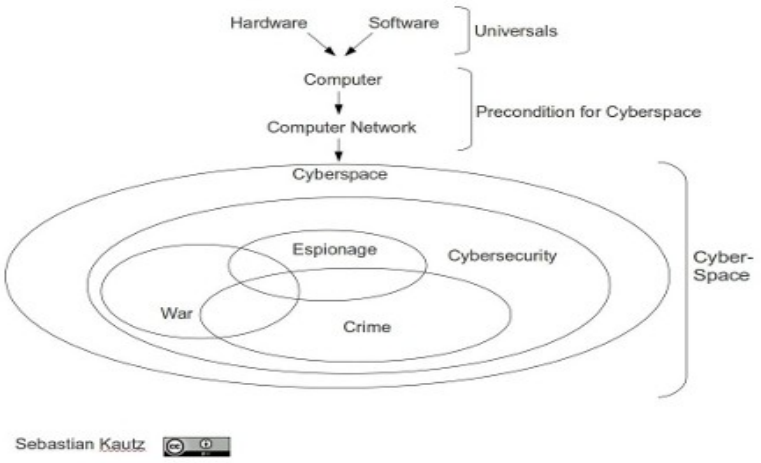

Abbildung 2 von Florian Grunert www.study4cyberwar.com/images/domain01.jpg

Abbildung 3: Communication model(adapted from Shannon and Weaver [1949]) via http://plato.stanford.edu/entries/information-semantic/ (SEP Zugriff 10.10.2011)

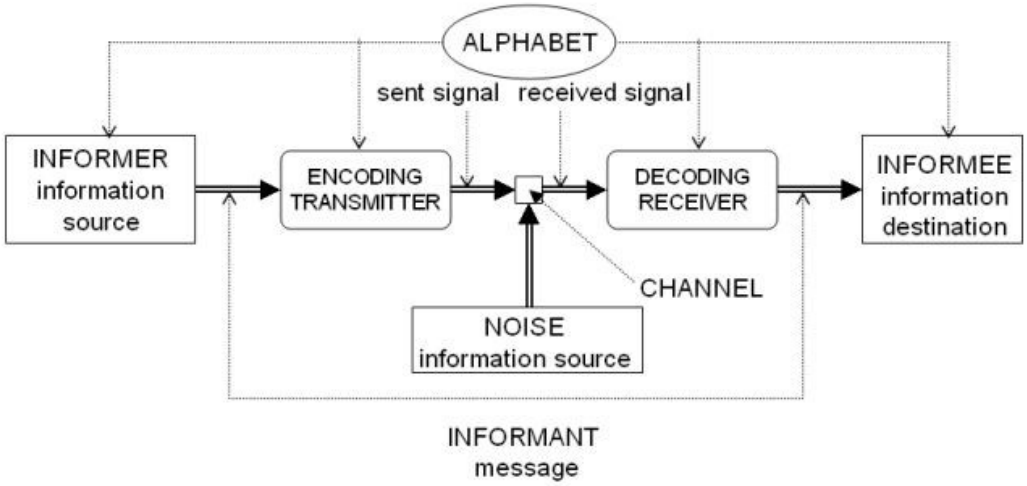

Abbildung 4: The Internet's undersea World in Understanding Internet Infrastructure And Its Prime Element 'Submarine Cable' http://www.goospoos.com/2010/08/understanding-internet-infrastructure-and-submarine-cable-and-isp-hierarchy/ (Zugriff 20.11.2011)