Rheinische
Friedrich-Wilhelms-
Universität Bonn

Institut für Politische Wissenschaft und Soziologie
Proseminar VMIB
Neue Entwicklungen und Herausforderungen in der internationalen Politik
Dozent: Dr. Kai Hirschmann
Wintersemester 2010/2011

Krieg 4.0 - Auswirkungen und Folgen virtueller Bedrohungen

von
Thomas Liebe

„Jeder kann ein Cyber-Krieger sein.“

Shivshankar Meno

Nationaler Sicherheitsberater Indien

Münchener Sicherheitskonferenz 2011

1. Einleitung

Der im November 2010 erfolgte, virtuelle Erstschlag auf die iranische Urananreichungsanlage in Natanz ist eine neue, aber nicht unbekannte Stufe des Cyberwar. Der zum Einsatz gebrachte Stuxnet-Wurm ist nach angaben eines IT-Sicherheitsunternehmens, der „*erste Computervirus, der verheerende Schäden in der realen Welt verursachen kann*“[1]. Israelische Kampfflugzeuge zerstörten im September 2007 unbehelligt von der zuvor virtuell ausgeschalteten syrischen Luftabwehr eine geheime, im Bau befindliche, Atomforschungsanlage in Syrien.[2] Aber auch Israel selbst wurde bereits mehrfach digital attackiert. Während des vergangenen Gaza-Krieges wurde versucht, Regierungsseiten in mehreren Wellen mit bis zu 15 Millionen Email pro Sekunde außer Kraft zu setzen.[3] Doch nicht nur Staaten drehen derzeit an der digitalen Rüstungsspirale.[4] Auch Hacktivisten[5], wie beispielsweise die Anhänger der Enthüllungsplattform Wikileaks oder Demokratiebewegungen von Tripolis bis Teheran üben mit den gleichen digitalen Waffen Druck aus, um ihren Forderungen Nachdruck zu verleihen, wie Terroristen oder Staaten. Nach den Wikileaks-Veröffentlichungen mussten die Betreiber der Server von Amazon, Paypal, Mastercard und Visa derzeit die teilweise koordinierten Distributed-Denial-of-Service-Attacken der Wikileaks-Unterstützer abwehren.[6] Aber auch Einzelpersonen können sich die neuen Möglichkeiten zu Nutze machen. Besonderes Potential bietet das Internet rechts- wie linksgerichteten und fundamentalistischen Terroristen. Ein wenig Computerkenntnis und Technologie zum Discountpreis sind ausreichend, um die äußerst sensiblen Strukturen der industrialisierten Welt anzugreifen und damit mehr Schaden anzurichten, als mit Sprengsätzen.

Die Brisanz des Themenkomplexes Cyber-Bedrohungen ist deutlich zu erkennen und wird zukünftig an Intensität zunehmen. Unser ökonomisches, militärisches, medizinisches und teilweise das soziale Leben spielt sich überwiegend innerhalb hochvernetzter Informationstechnologien ab. Mobilfunkgeräte der neusten Generation ermöglichen uns die Teilnahme am Internet an nahezu jedem Ort und zu nahezu jedem

[1] Symantec Jahresbericht 2010.
[2] Herwig 2010; Politik.de .
[3] Rößler 2010; FAZ.net.
[4] Vertiefend dazu: Birt, Michael P. 2006: Net Effect: How Technology Shapes the World.
[5] Hacktivismus als virtuelle Protestform, Vgl. Weimann 2004, S.4f.
[6] Patalong, Frank 2010; Spiegel Online.

Zweck. In einigen Staaten, wie z.B. Estland ist sogar die Partizipation am demokratischen System mittels Online-Wahl möglich. Diese informationstechnische Entwicklung der vergangenen Jahre hat eine Vielzahl positiver Optionen für jeden Einzelnen mit sich gebracht. Die Bedrohung, welche mit elektronischen Mitteln generiert werden kann, wurde lange Zeit sträflich vernachlässigt. Zwar reagiert die IT-Sicherheitsindustrie derzeit auf die neue Bedrohungslage, doch stehen hier ganz klar wirtschaftliche Interessen im Vordergrund. Solange es keine wissenschaftlichen, sachlichen und neutralen Auseinandersetzungen zu diesem Thema gibt, können auch keine geeigneten Schutz- und Abwehrmaßnahmen ausgearbeitet werden.

Ziel der vorliegenden Hausarbeit ist es, die unterschiedlichen Aspekte von virtuellen Bedrohungen im Hinblick auf die sicherheitspolitischen Notwendigkeiten hin zu untersuchen und zusammen zuführen. Die relevanten Teilbereiche Kriminalität, Terrorismus und zwischenstaatliche Kampfhandlungen müssen dabei zusammenhängend betrachtet werden. Bisherige Untersuchungen beschränken sich oft nur auf jeweils einen der Teilaspekte. Dabei wird aber vergessen, dass sich alle drei derselben Mittel und Methoden bedienen, wenn auch auf unterschiedlichen Ebenen. Dafür müssen zunächst im zweiten Kapitel die Begriffe und Technologien erörtert und voneinander abgrenzt werden, bevor ihr Bedrohungspotential in Kapitel 3 diskutiert werden kann. Das besondere Augenmerk liegt dabei auf den Punkten Terrorismus und Information Warfare.

Die zu untersuchende Forschungsfrage lautet daher: Worin liegt die besondere Brisanz der Cyber-Bedrohungen begründet? Es wird hypothetisch angenommen, dass die Grenzen zwischen den untersuchten Bedrohungsarten fließend sind. Das gewonnene Wissen soll eine Diskussionsgrundlage für zukünftige Betrachtungen sein. Aufgrund des festgelegten, formalen Umfangs der Ausarbeitung wird in Kauf genommen, dass die Darstellung nicht umfassend beantwortet werden und sich im Hinblick auf die vielen einzelnen elektronischen und digitalen Systeme der Realität nur annähern kann. Aus dem gleichen Grund kann auch auf die Hard- und Software spezifischen IT-Besonderheiten nicht eingegangen werden. Rechtliche Aspekte werden nicht vertiefend dargestellt. Privat- und wirtschaftliche Rechtsprechung – sofern es sie schon gibt (sic) – werden nur am Rande betrachtet.

Die vorliegende Hausarbeit basiert ausschließlich auf Sekundärliteratur. Eine Erhebung von neuen Primärdaten, beispielsweise mittels Fragebögen unter Politikern und Militärs hinsichtlich ihrer Einschätzung der Bedrohungslage, würde enormen Aufwandes bedeuten. Die Literatur zum Thema deckt ein breites Spektrum ab und ist hochaktuell. Als wichtigste Literaturquelle zur Klärung der Forschungsfrage diente vor allem die Dissertation von Maximillian Dornseif, dessen Arbeit sehr ausführlich die verschieden Formen von IT-Delinquenz untersucht. Des weiteren waren die Arbeiten von Oliver Minkwitz von der Stiftung Politik und Wissenschaft und Publikationen des HSFK sehr bedeutsam für die Untersuchung des Forschungsgegenstandes.

2. Virtuelle Bedrohungen

Cyber-Bedrohungen gewinnen zunehmend sicherheitspolitische Bedeutung. Kriminalität, Terror und Krieg in ihren digitalen Formen treffen im Cyberspace auf ideale Bedingungen. Die Informationsnutzung erfolgt eben nicht nur im Bereich von Wissenschaft und Forschung. Neben Umweltschutzorganisationen, die ihre Aktivitäten koordinieren, nutzt Al-Quaida ebenfalls das virtuelle Terrorcamp um seine Kämpfer auszubilden.[7]

IT-Vergehen und Cyber-Angriffe richten sich neben Akteuren gegen Kritische Infrastruktur, also Strukturen und Einrichtungen, die von maßgeblicher Bedeutung für das reibungslose Funktionieren des Staates und der Gesellschaft verantwortlich sind. Problematisch ist die „*zunehmende Verlagerung von gesellschaftlichen Funktionen vom Menschen auf vernetzte Techniksysteme.*“[8] Der Europäische Rat versuchte im Juni 2004 eine umfassende Strategie für den Schutz Kritischer Infrastrukturen zu erarbeiten. Die Richtlinie des Rates versteht unter Kritischer Infrastruktur, diejenige, welche „*die in einem Mitgliedstaat gelegene Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind*“[9]. Einer ähnlichen Definition folgt das Bundesamt für Sicherheit in der Informationstechnik, das unter Kritischer Infrastruktur „*Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche*

[7] Vertiefend dazu: Holtmann 2010 und Musharbash 2006.
[8] Kamin 2002, S.13.
[9] EG Richtlinien 2008/114/EG Online unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=-OJ:L:2008:345:0075:0082:DE:PDF, Stand k. A. / Zugriff 24.02.2011.

Gemeinwesen“ versteht, bei deren „*Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.*“[10] Dazu zählen Teilsysteme, wie Transport und Verkehr, Energie, Gefahrstoffe, Informationstechnik und Telekommunikation, Finanz-, Geld- und Versicherungswesen, Versorgung, Behörden, Verwaltung und Justiz. Eine Gewichtung der ausgezählten Systeme ist schwierig, da diese interdependent miteinander verflochten und untereinander abhängig sind. Durch die informationstechnologische Vernetzung und die weitgehend computergestützten Steuerungs-, Überwachungs- und Managementprozessen sind diese Systeme ein Hochwertziel für großflächige elektronische Angriffe.

2.1. Cyber-Kriminalität

Weite Teile der Bevölkerung nehmen derzeit die unmittelbare Bedrohung durch Informations- und Kommunikationstechnik als ein rein kriminelles Phänomen zur Kenntnis. Das Bundeslagebild des Bundeskriminalamtes führt für das Jahr 2009 50.254 Fälle in seiner Statistik auf. Gegenüber dem Vorjahr ist dies ein Anstieg von 33 Prozent (12.354 Fälle).[11] Der Schaden beläuft sich auf 36,9 Millionen Euro. Dazu kommt, dass es bei der Erfassung der Straftaten eine sehr hohe Dunkelziffer gibt, da ein Großteil der Geschädigten gar nicht mitbekommt, dass sie Opfer ein Straftat wurden oder diese aus Reputationsgründen nicht offenlegen möchten. Die Einordnung einer kriminellen Handlung wird ebenfalls durch die zeitliche Dimension erschwert, weil zwischen Tat und Auswirkung ein beliebig steuerbarer Zeitraum liegen kann. Auch hier zeigt sich infolge einer zunehmenden Professionalisierung eine quantitative und qualitative Steigerung der eingesetzten Mittel. Für Privatpersonen ist der Diebstahl digitaler Identitäten das zentrale Problem. Die BKA-Statistik erfasst insgesamt 6800 Fälle – ein Plus von 64% gegenüber dem Vorjahr[12] – die durch Phishing und dem damit einhergehenden Missbrauch von Zugangsdaten entstehen. Das können neben Email-Accounts auch Bankkonten und Zugangsdaten von Vertriebsplattformen, wie beispielsweise eBay oder von sozialen Netzwerken, wie Facebook sein.[13]. Die angesprochene Professionalisierung auf der einen Seite, aber auch das zunehmend kritischere und vorsichtigere Verhalten der Nutzer hat dazu geführt, dass ein Großteil

[10] Siehe Bundesamt für Sicherheit in der Informationstechnik: Definition Kritische Infrastruktur.
[11] BKA 2009, S.6.
[12] Vgl. Ebd. S.8.
[13] Vgl. Ebd. S.7.

der dafür notwendigen Software nicht mehr via Email verbreitet wird, sondern zunehmend der Aufruf von Webseiten zur Gefahr wird. Besonders problematisch für den Nutzer und auch im Hinblick auf die zu untersuchende Forschungsfrage ist es, wenn der private Rechner mittels eines Bot-Netzes zur Waffe wird, ohne dass der Täter identifiziert werden kann. Ist die dafür notwendige Schadsoftware auf dem Rechner installiert, wird dieser im Verbund mit anderen zum „*Zombie-PC*“[14]. Die infizierten Rechner können in diesem Fall ohne Wissen des Nutzers ferngesteuert werden, So können gezielte Angriffe auf Webseiten geführt werden und die betreffenden Server nachhaltig ausgeschaltet werden. Bei wettbewerbsintensiven Portalen können so schnell Schäden in Millionenhöhe entstehen. Die Gefahr für eGovernment-Anwendungen, beispielsweise elektronische Steuererklärungen, Online-Wahlsysteme, oder die Server von Betreibern von kritischer Infrastruktur ist ungleich höher. Das Prinzip dieser DDoS-Attacken taugt zur Waffe, wie die Beispiele aus Israel und die erwähnten Aktivitäten der Wikileaks-Unterstützer zeigen. Damit bekommt Cyberwar auch eine „private“ Dimension.

Die Intentionen für Cyber-Kriminalität lassen sich in drei grobe Kategorien einteilen: persönliche, politische und ökonomische Anreize zur kriminellen Handlung. In vielen Fällen ist ein Motiv-Mix der Anlass für kriminelle Handlungen. Neugier und Ärger sind nur zwei persönliche Motive. Bereicherungsmotive bilden einen Mix aus persönlichen und ökonomischen. Interessant ist die politische Dimension, da hierunter neue soziale Formen des digitalen Widerstands[15] als auch Spionage und Terrorismus fallen.

2.2. Cyber-Terrorismus

Die Informationstechniken des Internetzeitalters und die daraus resultierende Vernetzung der industrialisierten Gesellschaften sind ein Grund für wirtschaftlichen Wohlstand und Entwicklung. Daher ist es nicht verwunderlich, dass diese nicht nur für gesetzeswidrige Handlungen Einzelner und Akteure aus dem Bereich der organisierten Kriminalität genutzt werden, sondern auch für terroristische Aktionen. Nach Timothy L. Thomas, Professor am US Army Eurasian Institute, profitieren Terroisten vom Internet, weil es sie„*...with anonymity, command and control resources, and a host of other*

[14] Vgl. Ebd. S.101.

[15] Beispielsweise das bereits erwähnte Verhalten der Wikileaks-Anhänger im Zuge der Veröffentlichungen zahlreicher Depeschen oder der Versuch der iranischen Opposition, Informationen via Social Media an die Öffentlichkeit zu bringen (Anm. d. Verf.).

measures to coordinate and integrate attack options"[16] versorgt. Das Internet und die eingesetzte Informationstechnik sind zugleich Waffe sowie mögliches Ziel terroristischer Aktivitäten. In der Literatur besteht, im Gegensatz zum Begriff des Terrorismus, weitestgehend Einigkeit darüber, wie Cyber-Terrorismus definiert werden sollte.[17] Nach einer Studie des Center for the Study of Terrorism and Irregular Warfare von 1999 ist Cyber-Terrorismus „*the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological.*"[18] Die Attraktivität den Cyberspace für terroristische Zwecke zu nutzen basiert auf einer Vielzahl von Gründen. Cyber-Terrorismus ist kostengünstiger als konventioneller Terrorismus, wesentlich anonymer und bietet eine Vielzahl von verwundbaren und ungeschützten Zielen. Dazu kommt, das Cyber-Terrorismus mit „*less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorist*"[19] verbunden ist.

In der Studie der „Naval Postgraduate School" werden drei Grundtypen von eTerroristen, die hinsichtlich ihrer technischen, analytischen und organisatorischen Fähigkeiten unterschieden werden können, charakterisiert. Relativ einfach zu erreichen ist die Stufe „*Simple-Unstructured*"[20], für die im Prinzip der Zugang zum Internet ausreichend ist. Dieser Typus zeichnet sich durch aus, das die Gruppe nur über einen sehr schwachen Organisationsgrad verfügt und auf Sekundärsoftware aus dem Internet zurückgreifen muss, da die Mitglieder nur über Computergrundkenntnisse verfügen. Das für die Steuerung der Hackersoftware nötige Wissen kann in relativ kurzer Zeit angeeignet werde. Dadurch das dieses Wissen und die Software im Netz relative leicht zugängig sind, ist diese Art des Cyber-Terrorismus sehr akut, unter taktisch-strategischen Gesichtspunkten betrachtet, verringert sich die Brisanz, da diese Art der Net-Attacke aufgrund der kurzen Verweildauer im Netz und der unmodifizierten Software nicht geeignet sind, eine nachhaltige Störung oder Schädigung von Kritischer Infrastruktur zu erzeugen. Bedrohlicher wird die Attacke einer Terrorgruppe, die sich hinsichtlich ihrer Organisation und der Ausbildung ihrer Mitglieder im Bereich der Informatik ihrer Mitglieder weiterentwickelt hat. Der höherer Organisationsgrad, der

[16] Thomas 2003, S.112.
[17] Vgl. Diskussion in Hirschmann 2006 und Hoffman 2006, S.21ff., S. 72ff.
[18] Nelson 1999, S.9.
[19] Weimann 2004, S.6.
[20] Nelson 1999. S.14.

Kommando- und Kontrollfunktionen mit sich bringt, versetzt Gruppen, die mit „*Advanced-Structured*“[21] klassifiziert werden, in die Lage, mit eigener Hacking-Software anspruchsvollere Angriffe gegen System und Netzwerke zu führen. Reale und virtuelle Ziele könnten zeitgleich anzugreifen werden. Eine ernsthafte Bedrohung für Kritische Infrastruktur geht von Terrororganisationen aus, die ihre konventionellen Aktivitäten vollends in den Cyberspace übertragen können. Die Klassifizierung „*Complex-Coordinated*“[22] erhalten Vereinigungen, die in der Lage sind, koordinierte Angriffe von verschiedenen Orten, auch gegen stark geschützte heterogene Netzwerkziele, zu fahren. Voraussetzung dafür ist ein hoher Organisationsgrad mit entsprechend hohen Führungs- und Leitsystemen. Die Spezialisten für Programmierung und Informationsversorgung arbeiten auf technologisch höchstem Stand und beziehen auch die sekundären und tertiären Effekte ihres Cyber-Anschlags in ihrer Planungen mit ein. Für den Aufbau einer digitalen Terrorzelle der Stufe „*Advanced-Structured“* und „*Complex-Coordinated*“ sind zwei Aspekte ausschlaggebend: nicht unerhebliche finanzielle Ressourcen und Zeit.[23] Vor diesem Hintergrund wird Outsourcing zu einem probaten Mittel, diese Hürden in kurzer Zeit zu überwinden und sich schnell in die Lage zu versetzten, effektiven Cyber-Terror auszuführen.[24] Es ist daher besser, den Begriff Cyber-Terrorismus um den Begriff des „*Cyberplanning*“[25] zu umschreiben, da Cyber-Terroristen – das gilt auf für Cyber-Kriminelle – zwar das Internet zur internen wie auch externen Kommunikation nutzen, allerdings aufgrund der derzeit noch relativ hohen Hürden für komplexere Aktivitäten, nicht das gesamt Spektrum ausführen können.

2.3. Informationskriegsführung

Die Kapazitäten, das gesamte Spektrum an Cyber-Aktivitäten, ausführen zu können, besitzen derzeit nur staatliche Akteure. Allen voran das Militär und die Geheimdienste. Hier zeichnete sich in den vergangenen zwanzig Jahren eine beispiellose Entwicklung im Bereich der militärisch genutzten Informations- und Kommunikationstechnologien ab. Die „Revolution in Military Affairs“ ist das „*Resultat der Anpassung des militärischen Instrument an politische Zwecke*“[26] und setzt dabei auf die

[21] Vgl. Ebd. S. 16.
[22] Vgl. Ebd. 16f.
[23] Bei „Advanced-Structured“-Zellen dauert der Aufbau mindestens ein, eher zwei bis vier Jahre, bei „Complex-Coordinated“-Zellen mindestens zwei, eher 6 bis zehn Jahre. Vgl. Nelson 1999, S.96f.
[24] Vgl. Ebd. S. 99ff.
[25] Thomas 2003, S. 113ff.
[26] Minkwitz, Oliver 2003, II.

Informationskriegsführung (IW) oder die vernetzte Operationsführung, welche aktuelle Technologietrends in die jeweilige Strategie einbettet. Zukünftige Konflikte werden eher von niedriger Intensität sein und dürften auch schon zu Friedenszeiten von Informationsoperationen begleitet werden.[27] Führt man der Argumentation des deutsch-amerikanischen Medienwissenschaftlers Gundolf S. Freyermuth konsequent weiter, ist die Bezeichnung Krieg 4.0 zutreffend, wenn es um die Beschreibung des Cyberwar geht.[28] In dieser sehr speziellen Form der zwischenstaatlichen Gewaltanwendung[29] in Datennetzen geht es darum, dass eine „*Militärorganisation nicht funktionieren kann, wenn ihre Informationsströme vom Gegner kontrolliert werden.*“[30] Der Begriff wurde erstmals in den 1990er Jahren von John Arquilla und David Ronfeld benutzt, die im Cyberwar „*not simply a set of measures based on technology*“[31] sehen, sondern es als eine Form der Informationsüberlegenheit verstehen. Für beide ist Cyberwar eine „*innovation in warfare, we anticipate that cyberwar may be to the 21st century what blitzkrieg was to the 20th century.* “[32] Betrachtet man „*Information Warfare*“ als offensive oder defensive Nutzung von Informationen und Informationssystemen, so kann Cyberwar als der Kampf im elektronischen System angesehen werden.[33] Information Warfare oder Informationskriegsführung umfasst alle Informationsoperationen in Friedens- wie in Konfliktzeiten, die geeignet sind, spezifische Ziele gegenüber einem Gegner durchzusetzen.[34] Das Spektrum umfasst nach Martin Libicki „*command-and-control warfare, intelligence-based warfare, electronic warfare, psychological operations; hackerwar software-based attacks on information systems; information economic warfare, war via the control of information trade and cyberwar.*“[35] Die Joint Doctrine Information Warfare der US-Streitkräftekennt nennt neben den von Libicki angeführten Elementen noch den Business Information War, der

[27] Vgl. Ebd. 2003, II.
[28] Vgl. Freyermuth, G.S. 2005: Krieg Version 3.0, in NZZ-Folio 01/05 – Thema Bomben, Online unter http://www.nzzfolio.ch/www/d80bd71b-b264-4db4-afd0-277884b93470/showarticle/95caf6c1-d2e2-429e-81b6-8a7cd5cfe52f.aspx. Stand 2005 / Zugriff 24.02.2011.
[29] IT-Experten streiten darüber, ob die Bezeichnung Cyber-Krieg richtig gewählt ist, da eine direkte Bedrohung derzeit im Schadensausmaß nicht mit den Folgen direkter Kampfhandlungen vergleichbar sind. Vgl. dazu McAffee 2009: Bericht zum Thema Virtuelle Kriminalität 2009, Virtueller Internetkrieg wird zur Wirklichkeit, Online unter: http://www.mcafee.com/de/resources/reports/rp-virtual-criminology-report-2009.pdf. Stand 2009 / Zugriff 24.02.2011.
[30] Dornseif 2005, S. 85.
[31] Arquilla/Ronfeld 1990, S. 33.
[32] Ebd. S. 31.
[33] Vgl. Dornseif, S. 85f.
[34] Minkwitz 2003, S .8.
[35] Libicki 1995, S. 1.

auf die wirtschaftliche Schwächung des Gegners abzielt.[36] Die Doktrin fasst Cyberwar als „*Mißbrauch und(Zer-)Störung öffentlicher elektronischer Informations- und Kommunikationssystem[e] sowie IT-abhängige[r] nationale[r] und internationale[r] Strukturen*“[37] und schließt offensive Informationsoperationen in Friedenszeiten ausdrücklich ein.[38]

3. Auswirkungen und Folgen virtueller Bedrohungen

Bernhard Hutter kritisiert zu Recht, dass „*in weiten Teilen der öffentlichen Diskussion (...) Cyber-Gefahren zu eng gesehen (...) und auf die Begriffe Internet, Hacking, Viren*“[39] reduziert werden. Asymmetrische Terroranschläge aus dem Cyberspace sind selbstverständlich ein mögliches Szenario, da es nicht primär um eine möglichst hohe Opferzahl geht. Terror ist eine „*Kommunikationsstrategie*“[40], welche auf eine möglichst hohe psychologische und politische Folgewirkung setzt. Die Verletzlichkeit der Infrastrukturen und Informationsinfrastrukturen lädt dazu geradezu ein. Eine grundlegende Maxime des Terrors ist es, mit „*so wenig Aufwand wie möglich, so viel Aufmerksamkeit wie möglich*“[41] zu erzielen. Ein weiteres Phänomen der asymmetrischen Kriegsführung liegt in dem David-gegen-Goliath-Mythos begründet, der Schwachstellen des Gegners zum eigenen Vorteil nutzt. Aus diesen drei Aspekten lässt sich eine einfache Regel ableiten: Es gibt keine. Virtuelle wie reale asymmetrische Kriegsführung „*kennt weder geografische noch moralische Grenzen*“[42]. Der leichte Zugang, das geringe Entdeckungsrisiko, sowie die Verletzlichkeit des Systems machen den Cyberspace für Terroristen zu einem sehr interessanten Medium. Derzeit wird es überwiegend für den Informationsaustausch in Foren und mittels Online-Magazinen sowie für Propaganda-Aktionen genutzt.[43] Terroristische Information Warfare Aktivitäten konnten bislang noch nicht nachgewiesen werden.[44]

3.1. Unkontrollierter Rüstungswettlauf

[36] Vgl. Pohl, Hartmut 2000, S.1f.
[37] Geiger, Gebhard 2002, S. 11.
[38] Vgl. Joint Doctrine for Information Operations
[39] Hutter, Bernhard 2002, S. 31.
[40] Fitschen, Patrick 2004, S. 81.
[41] Musharbash, Yassin 2006, S. 130.
[42] Fitschen, Patrick 2004, S. 1.
[43] Vgl. Musharbash 2006, S. 100ff.
[44] Lau, Thorsten 2003, S. 7.

Gegenwärtig investieren alle Regierungen in großem Stil in virtuelle Geschütz und Waffensysteme. Allein die Volksrepublik China hat im vergangen Jahr rund 55 Milliarden US$ in den Aufbau von Cyber-Militärtechnologie gesteckt.[45] Selbst der Iran hat 2010 mit 10 Milliarden US$ mehr für die digitale Aufrüstung ausgegeben als die Vereinigten Staaten, die nur 7 Milliarden US$ investierten.[46] Militärtechnologisch betrachtet lohnt dich die Aufrüstung in jedem Fall. Die benötigten IT-Systeme sind in der Anschaffung und im laufenden Betrieb günstiger als konventionelle Großkampfsysteme. Außerdem unterliegen die dafür benötigten Technologien keinen rüstungspolitischen Restriktionen, wie bei ABC-Waffen, so das Schwächen der eigenen konventionellen Streitkräfte schnell und vergleichsweise kostengünstig kompensiert und die Schlagkraft erhöht werden können. Strategische Computernetzwerkangriffen bieten die Option, Sicherheitslücken in C^4ISR der gegnerischen Streitkräfte präemptiv und prophylaktisch auszuschalten und den Gegner durch den Verlust seiner elektronischen Führungsmöglichkeiten blind zu machen.

3.2. Bedrohungen durch Information Warfare

IW und damit auch Cyberwar dient nicht nur dem Schutz der eigenen Kräfte sondern minimiert theoretisch auch die Risiken für die Zivilbevölkerung auf dem gegnerischen Territorium. Dabei wird allerdings vergessen, dass die „*Verletzlichkeit der Informationssysteme*“[47] durch die Wechselwirkungen zwischen einzelnen vernetzten Kritischen Infrastrukturen verschärft wird. Neben militärischen Zielen geraten auch zivile Informations- und Kommunikationsnetzwerke ins Fadenkreuz. Beabsichtig oder unbeabsichtigt, viele digitale Informationsoperationen weisen ungeahnte sekundäre oder tertiäre Nebenwirkungen auf. Gerade dieser wertvolle politische Umstand – militärische Effektivitätssteigerung bei reduzierter ziviler Opferzahl – führt in demokratisch legitimierten Staaten dazu, dass militärische Gewalt wieder zu einem brauchbaren Mittel wird. Kurze und erfolgreiche Konflikte schonen politische, gesellschaftliche und wirtschaftliche Ressourcen. Militärische Gewalt wird so den von Demokratien gesetzten Normen gerecht.[48]

Nicht nur die Hemmschwelle für Gewaltanwendung wird dadurch herabgesetzt, auch verschwimmt bei Computernetzwerkangriffe und Information Warfare die Grenze

[45] Gaycken / Talbot, TechnologyReview 2010.
[46] Ebd.
[47] Geiger 2002, S. 10.
[48] Vgl. Ebd. 2003, S. 17f.

zwischen Krieg und Frieden. IW-Aktivitäten müssen schon vor einer möglichen Konfliktphase eingeleitet werden, um den gesamten militärischen Vorteil zu nutzen.[49] Diese Grauzone führt zum Versagen der institutionell gesetzten Schranken für Gewaltanwendung und ist mit einem Waffeneinsatz vergleichbar, ohne an herkömmliche oder rechtliche Regeln gebunden zu sein.[50] Aus der Tatsache, dass sich Informationsoperationen nur schwer nachverfolgen und entdecken lassen, resultiert ein weiteres Absenken der Hemmschwelle für Gewaltanwendung.[51] Die der Unsichtbarkeit und Nichtstrafbarkeit geschuldeten Vorteile können sogar den Kant´schen Grundsatz vom Demokratischen Frieden außer Kraft setzten. Auch die von Günter Joetze[52] daran anknüpfende „*Unmöglichkeit klassischer Krieg*“ [53] zwischen vernetzten Staaten, muss dahingehend erweitert werden, dass IuK-Technologien ein ideales Mittel sind, Machtrivalitäten und politische Konflikte unkontrolliert und nicht sanktionierbar austragen. Denn das Verhältnis der zu erwartenden Vorteile und der geringen Entdeckbarkeit begünstigt auch eine kriegerische Handlung unter Demokratien, um bestimmte wirtschaftliche oder politische Forderungen durchzusetzen.

Die völkerrechtliche Unterscheidung zwischen Kombattanten und Nichtkombattanten wird in dem Moment aufgehoben, wo einzelne zivile Teilsysteme, wie der Energiesektor, einen militärischen Charakter bekommen und stellen damit ein Hochwertziel dar.[54] Günther Öttinger, EU-Kommissar für Energie, betonte auf der diesjährigen Münchener Sicherheitskonferenz, dass die Energieversorgung die Achillesferse Europas sei.[55] Neudefinitionen von restriktiven Bestimmungen des Kriegsvölkerrechts im Hinblick auf dessen, was als Waffe, Krieg oder Nicht-Kombattant gilt, sind langwierig und werden mittelfristig nur schwer umsetzbar sein.[56] Auch vielfach geforderte Selbstrestriktionen unter Vermittlung international anerkannter und geachteter Organisationen versprechen keine Abhilfe.[57] Forderungen nach mehr Transparenz sind ebenfalls nicht durchsetzbar, da Transparenz in letzter Konsequenz Transparenz nach sich zieht. Und gerade in sensiblen und

[49] Vgl. Joint Doctrine Information Warfare 1998, S.40.
[50] Vgl. Geiger 2002, S. 8.
[51] Vgl. Minkwitz 2003, S. 23.
[52] Ehemaliger Präsident der Bundesakademie für Sicherheitspolitik
[53] Joetze, Günter 1999, S. 5.
[54] Vgl. Minkwitz 2003, S. 24.
[55] Vgl. Harbig, Cornelia 2011.
[56] Vgl. Minkwitz S. 21ff.
[57] Stichwort No-First-Use-Doctrine, Vgl. Minkwitz 2003, S. 35ff., Geiger 2002 S. 20ff.

sicherheitsrelevanten Systembereichen ist dies weder gewollt noch durchsetzbar. Auch traditionelle rüstungspolitische Instrumente, wie Inspektionen und Verifikationsmechanismen, greifen aufgrund des Dual-Use-Charakters und der angesprochenen Definitionsschwierigkeiten den neuen Informationskriegsstrategien nicht.[58]Eine Implementierung des Cyberspace in die internationale Rechtsprechung ist allerding dringend von Nöten.[59] Die Unklarheiten des internationalen Rechts erlauben derzeit den Einsatz dieser Mittel und profitieren von der Nichtsanktionierbarkeit im rechtsfreien Raum. Sollte es dennoch gelingen, die neuen militärtechnologischen Entwicklungen im internationalen Recht zu etablieren, bedeutet das aber noch lange nicht das Ende von offensiver IW. Staaten haben in diesem Fall die Möglichkeit, ihre Cyber-Aktivitäten an Dritte auszulagern. Privatpersonen oder Unternehmen, aber auch Terroristen können diese Aufgaben auf ihrer Ebene übernehmen, ohne selbst dafür belangt werden zu können. Beispielhaft hierfür ist der Man-in-the-middle-Angriff, des tunesischen Regimes im Vorfeld der Revolution 2010.[60] Jeffrey Hunker vom NATO Research Defence College fasst diese Tatsache, welche die Multidimensionalität von virtuellen Bedrohungen belegt, wie folgt zusammen: „*Since the technical skills required for cyber attack are similar or equivalent to those of sophisticated cyber criminals and hackers, it may be that cyber attacks, trough sanctioned or supported by the attacking state, use cyber criminals or hackers resources in part or whole*."[61]

Hier verdeutlicht sich, dass ein Problem wie Information Warfare nicht nur auf der internationalen Ebene beheben lässt, sondern direkte Implikationen auf die nationale, ja sogar bis auf die private Ebene hat. Bis heute ist jeder Versuch gescheitert Internetkriminalität zu vereinheitlichen.[62]

3.3. Aktuelle Regulierungsversuche

Der Schutz vor Bedrohungen aus dem Cyberspace führte in den letzten Jahren zu einer Vielzahl von Regulierungsversuchen auf den unterschiedlichen politischen Ebenen. So zielt der 2005 vom Bundesministerium des Inneren veröffentlichte Nationale Plan zum Schutz der Informationsinfrastrukturen (NPSI) auf die Implementierung von drei

[58] Vgl. Minkwitz 2003, S. 32ff.
[59] Vgl. Lau 2004, S. 23f. und Geiger 2002, S. 21f.
[60] Vgl. Spiegel Online 2011: Revolte-Instrument Internet. Online unter: http://www.spiegel.de/-netzwelt/web/0,1518,742961,00.html. Stand 02.02.11, Zugriff: 24.02.2011.
[61] Hunker, Jeffrey 2010, S. 6.
[62] Vgl. Geiger S. 20.

strategischen Zielen ab: Prävention, Reaktion und Nachhaltigkeit.[63] Eine konkrete Ausarbeitung ist der Umsetzungsplan KRITIS, der 2007 verabschiedet wurde und eine Reihe von Maßnahmen vorschlägt, die als Grundlage für die künftige Zusammenarbeit gilt.[64] Die Strategie setzt auf das Herausbilden einer Risikokultur, die Zusammenarbeit mit der Wirtschaft und auf eine Selbstverpflichtung der Infrastrukturbetreiber. Die enge Kooperation mit der Wirtschaft ist zum einen der enormen Innovationskraft und zum anderen einem paradoxen Umstand geschuldet. Die Privatisierungsvorgänge der vergangen Jahre haben dazu geführt, dass Sicherheit vielerorts nicht mehr der staatlichen Kontrolle unterliegt, obwohl der Staat für eben diese zuständig ist.[65] Die aus dem Public Privat Security basierenden Schutzkonzepte verdeutlichen, dass eine Trennung zwischen Defence und Security nicht länger möglich ist.[66] Im Februar 2011 verabschiedete die Bundesregierung eine neue Cyber-Sicherheitsstrategie, die auch die Einrichtung eines Nationalen Cyber-Abwehrzentrums beinhaltet.[67]Auf europäischer Ebene forderte die EU-Kommission 2009 eine Verbesserung und erhöhte Robustheit der Kritischen Informationsinfrastruktur und prangert die uneinheitlichen und unkoordinierten nationalen Strategien an. Der vorgeschlagene Aktionsplan fordert die Umsetzung von fünf Handlungsschwerpunkten: Prävention und Abwehrbereitschaft, Erkennung und Reaktion, Folgeminderung und Wiederherstellung, internationale Zusammenarbeit und besondere Kriterien für den IKT-Sektor.[68] Auch auf NATO-Ebene werden seit einigen Jahren Anstrengungen unternommen, die Bedrohung aus dem Internet zu reduzieren. Dazu wurde bereits 2002 die NCIRC ins Leben gerufen, um auf Computerzwischenfälle reagieren zu können. Das seit 2008 in Tallin operierende Cooperative Cyber Defence Centre of Excellence erforscht Methoden der Cyber-Verteidigung.[69]

4. Drei Ebenen – Ein Problem

Die Brisanz von Cyber-Bedrohungen liegt in der Tatsache begründet, dass Kritische Informationsinfrastrukturen nicht nur durch staatliche und terroristische Akteure,

[63] Bundesministerium des Inneren 2005, S. 6.
[64] Vgl Bundesamt für Sicherheit in der Informationstechnik. Definition Kritische Infrastruktur.
[65] Vgl. Kuhn, Jan 2005, S. 27.
[66] Thiele, Ralph 2009, S. 7.
[67] BMI 2011, Online unter: http://www.bmi.bund.de/cln_183/SharedDocs/Pressemitteilungen/DE/2011/-mitMarginalspalte/02/cyber.html. Stand 2011 / Zugriff 24.02.2011.
[68] Vgl. dazu Europäische Kommission, KOM(2006) 786, S. 5f., 8ff.
[69] Weitere Informationen unter http://www.ccdcoe.org/3.html.

sondern auch gleichzeitig durch kriminelle Vereinigung bedroht sind. Unklare rechtliche Bestimmungen auf nationaler wie internationaler Ebene erschweren eine effektive Verfolgung und Aufdeckung der Aktionen ebenso, wie unklare Kompetenzverteilung auf den unterschiedlichen Ebenen. Dabei ist die Bevölkerung nicht nur durch die primären und sekundären Auswirkungen von Cyber-Aktivitäten bedroht, sondern auch aufgrund der vernetzten IT-Systeme und der Teilhabe an der Informationsgesellschaft selbst ein wesentlicher Teil der Bedrohung. Privatpersonen können und werden von Kriminellen, Terroristen oder Staaten für entsprechende Maßnahmen instrumentalisiert.

Die Verwundbarkeit des Systems kann unter realistischen Gesichtspunkten nicht genau ermittelt werden, da viele Strukturzusammenhänge zwischen einzelnen Bereichen noch nicht identifiziert worden sind und sich auch nur schwer simulieren lassen. Das macht es schwierig einen geeigneten Weg zum Schutz Kritische Infrastrukturen zu finden. Schwierig deshalb, weil sich die zu erwartenden Schäden und die finanziellen und personellen Aufwendungen nicht beziffern lassen. Erschwert wird dieser Umstand zudem noch dadurch, dass die Gefährdung sich nicht allein dadurch beseitigt werden kann, indem „*nicht alle bekannten Schwachstellen mit bekannten Maßnahmen geschlossen werden können [und] es grundsätzlich eine hundertprozentige technische Sicherheit nicht geben kann*“[70]. Das Bedrohungspotential wird dabei von „*enorm*“[71], „*exorbitant hoch*“[72] und „*für die nationale Sicherheitspolitik von herausragender Bedeutung*“[73]. Seymour M. Hersh konstatiert, dass eine seriöse Einschätzung durch den „*Kampf der Bürokratien*“[74] eingeschränkt wird. Eine OECD-Studie aus dem Jahr 2011 schlussfolgert, dass nur wenige „*cyberbedingte Ereignisse*“[75] geeignet sind, einen globalen Schock auszulösen.

Die im vorangegangen Kapital skizzierten virtuellen Cyber-Problematiken haben eine gravierende Gemeinsamkeit. Die angewendeten Waffensysteme sind in allen drei Bereichen nahezu identisch. Schwachstellen und Sicherheitslücken in IT-Systemen können mittels Hacking angegriffen werden um Daten und Informationen zu

[70] Hutter, Gebhard 2000: Lage und Prognose.
[71] Möckli, Daniel 2010, S. 2.
[72] Lau 2003, S. 6
[73] Bundesministerium des Inneren NPSI, S. 3
[74] Hersh, Seymour 2011, S. 48.
[75] Tagesschau Online: "Die große Katastrophe ist unwahrscheinlich". Online unter: http://www.tagesschau.de/inland/cyberwar106.html. Stand 2011 / Zugriff 24.02.2011.

manipulieren oder zu zerstören. Dazu zählen die Sabotage von SCADA-Systemen[76] mit einem ökonomischen oder militärischen Hintergrund oder die Programmierung und Bereitstellung solcher Software, in Form von Würmern, Trojanern, Viren und logischen eBomben. Informationsbeschaffung wird je nach Motiv-und Interessenlage entweder Spionage oder Hacking bezeichnet. Distributed-Denial-of-Service-Attacken beinträchtigen für eine bestimmte Zeitspanne IT-Ressourcen ohne diese jedoch grundsätzlich zu zerstören und werden von Privatpersonen und auch von Staaten ausgeführt, wie die Beispiele des Hacktivismus und der israelische Angriff auf die syrische Nuklearanlage zeigen. Kommunikationsdelikte, wie Spam oder missbilligende Kommunikationsinhalte[77] sind zwar überwiegend im privaten und kriminellen Bereich vorzufinden, bieten aber auch motivierten Terroristen und staatlichen Geheimdiensten eine Reihe von Möglichkeiten, ihre Ziele zu verwirklichen. Allein die zur Verfügung stehenden wirtschaftlichen und finanziellen Ressourcen entscheiden über die Wahl der Mittel. Militär und Geheimdienste können daher auf das größte Repertoire an Mitteln zurückgreifen. Frustrierten Jugendlichen und religiösen Fanatikern bleiben oftmals nur die günstigen Softwarelösungen die im Netz zur Verfügung stehen.

Die Informationsrevolution des digitalen Zeitalters und die daraus folgende Störanfälligkeit des Gesamtsystems führt zur Beschleunigung eines seit den Terroranschlägen vom 11. September 2001 schleichenden Prozesses. Innere und Äußere Sicherheit werden zunehmend und unaufhörlich miteinander verschmelzen. Kriminelle Aktivitäten enden nicht an der Staatsgrenze und fügen einer Volkswirtschaft beträchtliche Schäden zu, unabhängig davon, ob die Gefahr von Privatpersonen, Banden oder staatlicher Seite erzeugt wird. Das Hauptproblem, liegt nach Gebhard Geiger, in der „*Verletzlichkeit der Informationsgesellschaft*“[78] und in der Tatsache, dass die globale Vernetzung zu einem Kontrollverlust in den Bereichen Sicherheit und Verteidigung führt.[79] Die fließenden Grenzen bei der Wahl der Waffensysteme und IT-Technologien und die mangelnde Sanktionierbarkeit ermöglicht es den Akteuren, zwischen den Ebenen zu wechseln. Die Bedeutsamkeit liegt also darin begründet, dass keine geeigneten Schutzmaßnahmen generiert werden können, wenn nicht gleichzeitig auch die beiden anderen Ebenen an die Bedrohung angepasst werden. Internationale

[76] Supervisory Control and Data Acquisition
[77] Z.B. Cyber-Mobbing und Stalking oder Bombenbauanleitungen, Vgl. Dornseiff 2005, S. 378ff.
[78] Geiger, Gebhard 2001.
[79] Ebd.

Abkommen werden wirkungslos, wenn staatliche Akteure ihre IW-Tätigkeiten an nichtstaatliche Akteure aus dem kriminellen oder terroristischen Bereich umdisponieren können.

5. Fazit

Die substanzielle Dringlichkeit von Cyber-Bedrohungen liegt in einer Mixtur aus technologischen, intentionalen und regulativen Gründen Die technische Komplexität des Cyberspace, die interdependente Abhängigkeiten zwischen den einzelnen Teilsystemen, verbunden mit der leichten Verfügbarkeit, produzieren einen gefährliche Basis. Diese Lücke kann jedoch kurzfristig mit technischen Innovationen geschlossen werden. Anders verhält es sich bei den intentionalen Gründen. Eine Vielzahl von Akteuren ist heute in der Lage, die sensiblen Strukturen der vernetzten Welt zu bedrohen. Die Kommunikationsinfrastrukturen werden von „Script-Kiddies“, kriminelle und terroristische Einzeltäter und Organisationen wie auch Staaten offensiv wie defensiv genutzt. Die Grenzenlosigkeit des Internet sorgt für die angesprochene Aufhebung zwischen innerer und äußerer Sicherheit bzw. Rechtsprechung. Kriminalität und Terrorismus muss sowohl auf nationalstaatlicher, als auch auf internationaler Ebene verfolgbar und sanktionierbar sein. Diese Entwicklung ist kurzfristig nicht umsetzbar, obwohl es dringend von Nöten wäre. Für die durch den Terrorismus generierte Bedrohung gibt es keinen hundertprozentigen Schutz. Hier hilft nur die Reduzierung der Bedrohungslage durch den physischen Ausbau der Infrastrukturen um etwaige Angriffsmöglichkeiten zu minimieren. Die wohl größte Bedrohung für die modernen Gesellschaften geht vom Information Warfare aus. Hier helfen nur übergeordnete, klare Richtlinien, denen die Staaten unterworfen sein müssen. Die anzustrebende Neuausrichtung und Aktualisierung des Völkerrechts wird wohl auch mittelfristig – und in der gebotenen Geschwindigkeit – nicht umsetzbar sein.

Die politische, ökonomische, ökologische und kulturelle Vernetzung der komplexen Gesellschaften nach innen und außen begünstigen symmetrische und asymmetrische - Bedrohungen. Die besondere Brisanz ist der Tatsache geschuldet, dass die Bedrohung mehrdimensionaler Art ist. Die angesprochene Tatsache, dass es prinzipiell möglich ist, als Akteur zwischen den virtuellen Ebenen Kriminalität, Terrorismus und Information Warfare zu wechseln, ist das wohl gravierendste Problem. Die Gefährdungspotentiale hängen nicht nur von den Intentionen der unterschiedlichen Akteure ab, sondern auch

von deren Ressourcenausstattung. Der Mangel an aktueller und angepasster nationaler und internationaler Rechtsprechung erschwert derzeit eine effektive Verfolgung möglicher Täter. Die Verwundbarkeit der Infrastrukturen, die auf die revolutionären Entwicklungen im kommunikationstechnischen Bereich trifft, sowie die globale Dimension des Untersuchungsgegenstandes ist die zentrale Herausforderung für die nächsten Jahre. Die Debatte über die Ausgestaltung der internationalen Rechtsprechung, der Verschränkung von Innerer und Äußerer Sicherheit und die Herausbildung einer Risikokultur in der Bevölkerung muss dringend geführt werden, um die vielen unterschiedlichen Bedrohungen zu minimieren. Um einen höchstmöglichen Schutz zu erzeugen, müssen die bereits angeregten Strategien und Pläne schnell und konsequent umgesetzt werde.

6. Literaturverzeichnis

Arquilla, John /Ronfeld, David 1990: Cyberwar is coming. In: Athena's Camp: Preparing for Conflict in the Information Age, RAND/MR-880-OSD/RC (1997), Reprint, S. 23-60. Online unter: http://www.rand.org/content/dam/-rand/pubs/reprints/2007/RAND_RP223.pdf. Stand 15. September 2010 / Zugriff 24.02.2011.

Bendrath, Ralf 1999: Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Bittner, Peter / Woinowski, Jens 1999 (Hg.): Mensch - Informatisierung - Gesellschaft, Münster 1999, S. 141-161.

Birt, Michael P. 2006: Net Effect: How Technology Shapes the World. Washingtonpost Newsweek Interactive, Foreign Policy, No. 156 (Sep. - Oct. 2006), Seite 92-93, 95. Online unter: http://www.jstor.org/stable/25462091. Stand 2006 / Zugriff: 24.02.2011.

Bundesamt für Sicherheit in der Informationstechnik, Definition Kritische Infrastruktur, Online unter: https://www.bsi.bund.de/cln_156/ContentBSI/Themen/Kritis/-Einfuehrung/KritisDefinitionen/definitionen.html. Stand 2011 / Zugriff 24.02.2011.

Bundeskriminalamt 2009: IuK-Kriminalität – Bundeslagebild 2009, Pressefreie Kurzfassung, 11 S. Online unter: http://www.bka.de/lageberichte/zk/-bundeslagebild_zk_2009.pdf. Stand 2010 / Zugriff 24.02.2011.

Bundesministerium des Inneren 2005: Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI), Online unter: http://www.bmi.bund.de/-SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf?__blob=publicationFile. Stand 2009-2012 / Zugriff 24.02.2011.

Dornseif, Maximillian 2005: Phänomenologie der IT-Delinquenz. Computerkriminalität, Datennetzkriminalität, Multimediakriminalität, Cybercrime, Cyberterror und Cyberwar in der Praxis. Inauguraldissertaion zur Erlangung des Grades eines Doktors der Rechte durch die Rechts- und Staatswissenschaftliche Fakultät Rheinischen Friedrich-Wilhelms-Universität Bonn, Bonn 2005, 630 Seiten.

Europäische Kommission 2006: Mitteilung der Kommission über ein europäisches Programm für den Schutz kritischer Infrastrukturen, KOM(2006) 786, 13 Seiten. Online unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=-COM:2006:0786:FIN:DE:PDF. Stand k. A. / Zugriff 24.02.2011.

Fitschen, Patrick 2004: Gelesen, in: Die Politische Meinung 2004 (10/2004), S. 79 bis 82. Online unter: http://www.kas.de/wf/doc/kas_5440-544-1-30.pdf?041028112635. Stand 15. Januar 2011 / Zugriff 24.02.2011.

Freyermuth, Gundolf S. 2005: Krieg Version 3.0, in NZZ Folio 01/05 – Thema Bomben. Online unter: http://www.nzzfolio.ch/www/d80bd71b-b264-4db4-afd0-277884b93470/showarticle/95caf6c1-d2e2-429e-81b6-8a7cd5cfe52f.aspx. Stand 2010 / Zugriff 24.02.2011.

Gaycken, Sandro / Talbot, David 2010: Aufmarsch im Internet, in Technology Review, Online unter: http://www.heise.de/tr/artikel/Aufmarsch-im-Internet-1102301.html. Stand 08.10.2010 / Zugriff 24.02.2011.

Geiger, Gebhard 2001: Sicherheit im Informationszeitalter. Information zur Politischen Bildung, Heft 274, Bundeszentrale für Politische Bildung, Bonn, Online unter:

http://www.bpb.de/die_bpb/73GFRE,0,0,Sicherheit_im_Informationszeitalter.html#art0. Stand 2001 / Zugriff 24.02.2011.

Geiger, Gebhrad 2002: Offensive Informationskriegsführung. Die „Joint Doctrine for Information Operations“ der US-Streitkräfte: sicherheitspolitische Perspektiven. Stiftung Wissenschaft und Politik, SWP-Studie 2/2002, 29 Seiten. Online unter: http://www.swp-berlin.org/fileadmin/contents/products/studien/S2002_02_ggr.pdf. Stand 2010 / Zugriff 24.02.2011.

Harbig, Cornelia 2011: Der Cyberspace stellt die Welt vor komplexe Herausforderungen. Münchener Sicherheitskonferenz 2011. Online unter: http://www.securityconference.de/Artikel-Details.57+M54066947697.0.html?&L=-0%2F.php%3Fid%3D%27. Stand 05.02.2011 / Zugriff 24.02.2011.

Hersh, Seymour M. 2011: Cyberwar: Die neue Front, in: Blätter für deutsche und internationale Politik 1/2011, S. 45-56, Online unter: http://www.blaetter.de/archiv/jahrgaenge/2011/januar. Stand 2011 / Zugriff 24.02.2011.

Herwig, Malte 2010: Die Furcht vor einem "elektronischen Pearl Harbor", Politik.de, Online unter: http://www.politik.de/forum/aussenpolitik/225716-hackerangriffe.html. Stand 2010 / Zugriff 24.02.2011.

Hirschmann, Kai 2006: Internationaler Terrorismus, in: Information zur politischen Bildung, 2006 Heft 291, S.24-30. Online unter: http://www.bpb.de/publikationen/JPDP27,0,Sicherheitspolitik_im_21_Jahrhundert.html. Stand 2006 / Zugriff 24.02.2011.

Hoffman, Bruce 2006: Terrorismus – der unerklärte Krieg. Bonn 2006, Schriftenreihe Band 551, Lizenzausgabe für die Bundeszentrale für politische Bildung, 608 Seiten.

Holtmann, Philipp 2010: Virtueller Dschihad: Eine reale Gefahr. Stiftung Wissenschaft und Politik, SWP-Aktuell 48/2010. Online unter: http://www.swp-berlin.org/de/produkte/swp-aktuell-de/swp-aktuell-detail/article/virtueller-dschihad-eine-reale-gefahr.html. Stand 2010 / Zugriff 24.02.2011.

Hunker, Jeffrey 2010: Cyber war and cyber power – Issues for NATO doctrine, in: NATO Research Division, NATO Research Paper Nr. 62/2010, NATO Defence College. Online unter: http://www.ndc.nato.int/download/downloads.php?icode=230, Stand 11. Januar 2010 / Zugriff 24.02.2011.

Hutter, Gebhard 2000: Angriffe auf Informationstechnik und Infrastrukturen, in: Aus Politik und Zeitgeschichte Medienpolitik, 2000 B41-42/2000, Bonn. Online unter: http://www.bpb.de/publikationen/26J9UB,0,0,Angriffe_auf_Informationstechnik_und_Infrastrukturen.html#art0. Stand 6.10.2000 / Zugriff 24.02.2011.

Hutter, Reinhard 2002: „Cyber-Terror“: Risiken im Informationszeitalter, in: Aus Politik und Zeitgeschichte, 2002 B10-11/2002, S. 31-39. Online unter: http://www.bpb.de/publikationen/NVN0CA,0,CyberTerror%3A_Risiken_im_Informationszeitalter.html. Stand 2002 / Zugriff 24.02.2011.

Joetze, Günter 1999: Außen- und sicherheitspolitische Aspekte der Globalisierung. Arbeitspapier zur Tagung Globalisierung als Aufgabe. Handlungsmöglichkeiten und Gestaltungsoptionen der Politik, Expertenkolloquium der Evangelischen Akademie Loccum vom 10. 12. Dezember 1999, Online unter: http://www.loccum.de/material/interpol/globalisierung/joetze.pdf. Stand 2007 / Zugriff 24.02.2011.

Joint Doctrine for Information Operations 1998: Joint Pub 3-13, Online unter: http://www.c4i.org/jp3_13.pdf. Stand k. A. / Zugriff 15. Januar 2011.

Kamin, Thoralf (Hrsg.)/ Mayr, Philipp / Merl, Martin 2002: Cyberwar – Neue Technologie und Rüstungskontrolle. Seminar „Neuere Debatten zur Innovations- und Technikanalyse“, Institut für Sozialwissenschaften, Humboldt-Universität zu Berlin, 29 Seiten. Online unter: http://www.ib.hu-berlin.de/~mayr/arbeiten/cyberwar.pdf. Stand 21.12.2010 / Zugriff 24.02.2011.

Kuhn, Jan 2005: Der Schutz kritischer Infrastrukturen. Unter besonderer Berücksichtigung von Kritischen Informationsinfrastrukturen. Institute für Peace Research and Security Policy at the University of Hamburg, Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle, Working Paper Nr. 5/2005, 36 Seiten. Online unter: http://www.ifsh.de/IFAR/pdf/wp5.pdf. Stand k. A. / Zugriff 24.02.2011.

Lau, Thorsten 2003: Cyber-Crime und Cyber-Crime-Kontrolle. Zum möglichst rationalen Umgang mit weltweiten Bedrohungsszenarien: Cyber-Kriege und Cyber-Terror, Kolloquium SoSe 2003, 28 Seiten. Online unter: http://www.uni-bonn.de/~ujr701/Startseite/Texte/Vonwem/CyberCrime-CyberCrimeKontrolle-SS2003/SammlungCyberCrime/Lau.ppt. Stand 2003 / Zugriff 24.02.2011.

Libicki, Martin C. 1995: What is Information Warfare? Online unter: http://www.dodccrp.org/files/Libicki_What_Is.pdf. Stand k. A. / Zugriff 24.02.2011.

McAffee 2009: Bericht zum Thema Virtuelle Kriminalität 2009, Virtueller Internetkrieg wird zur Wirklichkeit. Bericht zum Thema virtuelle Kriminalität 2009. Online unter: http://www.mcafee.com/de/resources/reports/rp-virtual-criminology-report-2009.pdf. Stand 2003 – 2011 / Zugriff 24.02.2011.

Minkwitz, Oliver 2003: Ohne Hemmung in den Krieg. Cyberwar und die Folgen, Hessische Stiftung für Friedens- und Konfliktforschung, HSFK-Report 10/2003, 42 Seiten. Online unter: http://www.hsfk.de/fileadmin/downloads/report1003.pdf. Stand 2003 / Zugriff 24.02.2011.

Möckli, Daniel 2010: Cyberwar. Konzept, Stand und Grenzen, CSS Analysen zur Sicherheitspolitik, Center for Security Studies (CSS), ETH Zürich, Online unter: http://www.ssn.ethz.ch/Aktuell/CSS-Analysen/Detail/?lng=de&id=114412. Stand 2011 / Zugriff 24.02.2011.

Müller, Harald / Schörnig, Niklas 2001: „Revolution in Military Affairs“ – Abgesang kooperativer Sicherheitspolitik der Demokratien? Hessische Stiftung für Friedens- und Konfliktforschung, HSFK-Report 8/2001. Online unter: http://www.hsfk.de/Publikationen.9.0.html?&no_cache=1&detail=101&no_cache=0&cHash=22825fa11f. Stand 2001 / Zugriff 24.02.2011.

Musharbash, Yassin 2006: Die neue al-Qaida. Innenansichten eines lernenden Terrornetzwerkes. Bonn 2006, Schriftenreihe Band 610, Lizenzausgabe für die Bundeszentrale für politische Bildung, 306 Seiten.

Nelson, Bill (Hrsg) 1999: Cyberterror. Prospects and Implications, White Paper prepared for: Defense Intelligence Agency Office for Counterterrorism Analysis (TWC-1), Center for the Study of Terrorism and Irregular Warfare Monterey, CA, Online unter: http://www.au.af.mil/au/awc/awcgate/nps/cyberterror_prospects.pdf. Stand 9. Dezember 2010 / Zugriff 24.02.2011.

Patalong, Frank 2010: Rache für WikiLeaks – Dauerfeuer aus Ionenkanonen. Spiegel Online. Online unter: http://www.spiegel.de/netzwelt/web/0,1518,733703,00.html. Stand 2010 / Zugriff 24.02.2011.

Pohl, Hartmut 2000: Business Information Warfare – Einige vorläufige Bemerkungen, in: Reinermann, H. (Hrsg.) 2000: Regieren und Verwalten im Informationszeitalter: Unterwegs zur virtuellen Verwaltung, Speyer 2000, Online unter: http://www.fh-brs.de/informatikmedia/Downloads/Personen/pohl/Aufsaetze/Business_Information_Warfare_in_Regieren_000606_.pdf. Stand k. A. / Zugriff 24.02.2011.

Rößler, Hans-Christian 2010: Große Chancen für die Kleinen – Israel im Cyber-Krieg. Faz.net. Online unter: http://www.faz.net/s/RubDDBDABB9457A437BAA85A49C-26FB23A0/Doc~EC38787E3CEA447BF9057A35BA638F12C~ATpl~Ecommon~Scontent.html. Stand 2011 / Zugriff 24.02.2011.

Symantec Jahresbericht 2010 Online unter: http://www.symantec.com/-business/theme.jsp?themeid=threatreport. Stand 2011/ Zugriff 24.02.2011.

Thiele, Ralph 2009: Public Private Security. Möglichkeiten und Grenzen integrierter Konzepte und Projekte. Institut für Strategie-, Politik-, Sicherheits- und Wirtschaftsberatung Berlin. Online unter: http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=106320. Stand 2011 / Zugriff 24.02.2011.

Thomas, Timothy L. 2003: Al Qaeda and the Internet: The Danger of „Cyberplanning“. In: Parameters, The US Army's Senior Professional Journal US Army War College, 2003 Frühling 03, S. 112 bis 123.Online unter: http://www.carlisle.army.mil/-USAWC/parameters/Articles/03spring/thomas.pdf. Stand 2010/ Zugriff 24.02.2011.

Weimann, Gabriel 2004: Cyberterrorisms – How real is he Threat? in: Special Report 119/2004, United States Institute of Peace, 12 Seiten. Online unter: http://www.usip.org/files/resources/sr119.pdf. Stand k. A. / Zugriff 24.02.2011.

Glossar & Abkürzungsverzeichnis

Bot-Netz:. Kurzform von „Roboter-Netzwerk“ Darunter versteht man einen Verbund infizierter PCs im Internet, die zentral ferngesteuert werden, um Spam zu senden oder Denial-of-Service Attacken (1)durchzuführen, ohne das die Nutzer wissen, das ihr PC infiziert ist. Die Einbindung erfolgt in de meisten Fällen durch unbedachtes Öffnen von infizierten Dateien oder von E-Mail Anhängen, die Würmer oder Trojaner enthalten. Durch Bot-Netze ist Ihr Rechner nicht mehr nur Opfer, sondern er wird gleichzeitig auch zum Täter. Ist der PC infiziert, fängt dieser selbst an Spam zu versenden oder Denial-of-Service Attacken durchzuführen. Persönliche Daten wie Passwörter und Kreditkarteninformationen sowie Kontonummern können ausgespäht und für illegale Zwecke missbraucht werden. Quelle: Deutschland sicher im Netz e.V., Online unter: https://www.sicher-im-netz.de/wir_ueber_uns-/1339_1637.aspx. Stand 2011 / Zugriff: 24.02.2011.

Business Information War: Auch Economic Warfare, der Angriffe gegen Informationsstrukturen auf wesentliche Teile des Kerngeschäfts von Unternehmen oder gesamten Branchen, mit dem Ziel, die Nutzung einzuschränken, zu verhindern oder auszuspähen. Quelle: Pohl, Hartmut 2000: Business Information Warfare.

C²-Warfare: Command and Control Warfare.

C³-Warfare: Command, Control and Communications Warfare.

C^{4}ISR-Warfare: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.

CCD-CoE: CCD-COE ist eine internationale Militärorganisation, die vollständig vom NATO-Nordatlantikrat am 28. Oktober 2008 akkreditiert wurde. Das CCD-COE ist in Tallinn auf dem Gelände eines estnischen Fernmeldebataillons stationiert. Quelle: http://www.ccdcoe.org/3.html. Stand: 2011 / Zugriff: 24.02.2011.

Cybermobbing: Unter Cyber-Mobbing versteht man das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mit Hilfe moderne Kommunikationsmitte. Cyber-Mobbing findet entweder im Internet (z.B. durch E-Mails, Instant Messenger wie beispielsweise ICQ, in Sozialen Netzwerken, durch Videos auf Portalen) oder per Handy statt. Quelle: Klicksafe.de Online unter: https://www.klicksafe.de/themen/kommunizieren/-cyber-mobbing/cyber-mobbing-was-ist-das.html. Stand: 2011 / Zugriff 24.02.2011.

Cyberplanning: Unter Cyberplanning wird die digitale Koordinierung einer integrierten Planung über geografische Grenzen hinweg verstanden, die für terroristische Zwecke genutzt werden kann. Quelle: Thomas, Timothy L. 2003: Al Qaeda and the Internet: The Danger of "Cyberplanning" Online unter: http://www.carlisle.army.mil/USAWC/parameters/Articles/03spring/thomas.pdf. Stand 2010/ Zugriff 24.02.2011.

DDoS: "Distributed Denial of Service" (DDoS)-Angriffe. Vervielfachung der Schadenswirkung aufgrund einer verteilten Arbeitsweise unter Nutzung einiger weniger Master und einer Vielzahl sog. Agenten, die mehrere einfache DoS-Angriffsvarianten kombinieren. Quelle: Bundesamt für Sicherheit in der InformationstechnikOnline unter: https://www.bsi.bund.de/-cln_156/ContentBSI/Themen/Internet_Sicherheit/Gefaehrdungen/DDoSAngriffe/toolsana.html. Stand 2011 / Zugriff 24.02.2011.

DoS: „Denial of Service"-Angriffe die Schwachstellen in der Implementierung der Netzwerkfunktionalität verschiedener Betriebssysteme ausnutzen, mit zum Teil drastischen Auswirkungen auf die Verfügbarkeit der Zielsysteme – in Verbindung mit einer freien Zugänglichkeit der entsprechende Tools. Quelle: Bundesamt für Sicherheit in der InformationstechnikOnline unter: https://www.bsi.bund.de/cln_156/ContentBSI/Themen/Internet_Sicherheit/Gefaehrdungen/DDoSAngriffe/toolsana.html. Stand 2011 / Zugriff 24.02.2011.

Hacking: Hacking bezeichnet im Kontext von Informationssicherheit Angriffe, die darauf abzielen, vorhandene Sicherheitsmechanismen zu überwinden, um in ein System IT-System einzudringen, seine Schwächen offen zulegen und es gegebenenfalls – bei unethischem Hacking – zu übernehmen. Quelle: Bundesamt für Sicherheit in der Informationstechnik. Online unter: https://-www.bsi.bund.de/cln_156/ContentBSI/Themen/Internet_Sicherheit/Glossar/glossarbegriffe.html#H. Stand 2011 / Zugriff 24.02.2011.

Hacktivismus:. Ziel des Hacktivismus als Form der Gesellschaftskritik und des zivilen Widerstandes via Internet ist es, ein Demonstrationsrecht in Datennetzen auszuüben.

Man-in-the-middle-Angriff: MitM ist ein Angriff auf den Kommunikationskanal zwischen zwei Partnern. Der Angreifer versucht dabei den Kommunikationskanal unter seine Kontrolle zu bringen, und zwar in der Art und Weise, dass die Kommunikationspartner nicht feststellen können ob sie miteinander oder mit dem Angreifer kommunizieren. Quelle: IT Wissen. Das große Onlinelexikon für InformationstechnologieOnline unter: http://www.itwissen.info/definition/lexikon/Man-in-the-Middle-Angriff-man-in-the-middle-attack.html. Stand 2011 / Zugriff 24.02.2011.

NCIRC: NATO Computer Incident Response Capability, NATO Zentrum zur Reaktion auf Computerzwischenfälle Quelle: NATO Computer Incident Response Capability Online unter: http://www.ncirc.nato.int/. Stand 2001-2010 / Zugriff 24.02.2011.

Phishing: Versuch von Betrügern, IT-Anwender irrezuführen und zur Herausgabe von Authentisierungsdaten zu bewegen. Dies wird in den meisten Fällen bei Online-Banking-Verfahren eingesetzt. Quelle: Bundesamt für Sicherheit in der InformationstechnikOnline unter: https://www.bsi.bund.de/cln_156/ContentBSI/-Themen/Internet_Sicherheit/Glossar/glossarbegriffe.html#P. Stand 2011 / Zugriff 24.02.2011.

Revolution in Military Affairs: Die RMA ist die Leitidee amerikanischer Rüstungspolitik seit den frühen neunziger Jahren. Die These der Vertreter der RMA innerhalb des US-amerikanischen Verteidigungsestablishments ist es, dass die Einführung von Computern und Informationstechnologien in den Streitkräften eine Änderung der Kriegsführung, ja der Natur des Krieges mit sich bringen würde. Präzisionslenkwaffen, Computernetzwerke und Echtzeit-Aufklärungssysteme würden eine Kriegsführung von nie gekannter Präzision und Verlustfreiheit, für Freund und Feind, erlauben. Quelle: Universität Innsbruck, Arbeitskreis Wissenschaft und Verantwortlichkeit. Online unter: http://www.uibk.ac.at/wuv/programm/yoda_und_jedis.html. Stand 21.04.2010 / Zugriff 24.02.2011.

Script-Kiddies: Abwertender Begriff für in der Regel Jugendliche, die intensiv Computer nutzen, jedoch ohne ein tiefgreifendes Verständnis der technischen Zusammenhänge. Sie nutzen Programme und Werkzeuge, ohne zu überblicken, welchen Schaden sie damit anrichten können. Quelle: Dornseif, Maximillian 2005: Phänomenologie der IT-Delinquenz, S. 123.

Trojaner: Trojaner oder Trojanische Pferde sind Programme, die neben scheinbar nützlichen auch nicht dokumentierte, schädliche Funktionen enthalten und diese unabhängig vom Computer-Anwender und ohne dessen Wissen ausführen. Diese können sich im Gegensatz zu Computer-Viren nicht selbständig verbreiten. Quelle: Bundesamt für Sicherheit in der InformationstechnikOnline unter: https://www.bsi.bund.de/cln_156/DE/Themen/InternetSicherheit/Gefaehrdungen/TrojanischePferde/trojanischepferde_node.html. Stand 2011 / Zugriff 24.02.2011.

Virus: Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich nach ihrer Ausführung selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Quelle: Bundesamt für Sicherheit in der InformationstechnikOnline unter: https://www.bsi.bund.de/cln_156/ContentBSI/-Themen/Internet_Sicherheit/Glossar/glossarbegriffe.html#V. Stand 2011 / Zugriff 24.02.2011.

Wurm: Selbstständiges, sich selbst reproduzierendes Programm, das sich in einem System (vor allem in Netzen) ausbreitet. Quelle: Bundesamt für Sicherheit in der Informationstechnik Online unter: https://www.bsi.bund.de/-cln_156/ContentBSI/Themen/Internet_Sicherheit/Glossar/glossarbegriffe.html#V. Stand 2011 / Zugriff 03.02.2011