

# Cyberwar

## Grundlagen-Methoden-Beispiele

Version 3.0 vom 12.01.2011

### **Zusammenfassung**

Die Diskussionen um die Computer- und Internetsicherheit haben in den letzten Monaten an Intensität zugenommen und der Cyberspace wird wegen der zunehmenden Bedeutung des Internets und der Informationstechnologie inzwischen als fünfte militärische Dimension neben Boden, See, Luftraum und Weltall betrachtet. Die folgende Arbeit unternimmt eine aktuelle Bestandsaufnahme und geht auf die theoretischen und praktischen Probleme des Cyberwars ein. Es wird zudem ein aktueller Überblick über Cyberwar-Aktivitäten seit 1998 gegeben und die Sicherheitsarchitektur im Cyberspace vorgestellt. Abschließend werden exemplarisch die Cyberwar-Strategien der USA und Chinas und die Cyberpolitik der Europäischen Union besprochen.

## Inhalt

1. Grundlagen.....	3
1.1 Einführung .....	3
1.2 Hintergrund.....	3
1.3 Definitionen .....	5
1.4 Die Cyberwar-Konzeption der USA.....	6
2. Methoden .....	8
2.1 Klassifikation .....	8
2.1.1 Physische Zerstörung von Computern und ihren Verbindungen.....	8
2.1.2 Elektromagnetischer Puls EMP .....	8
2.1.3 Der Angriff auf und die Manipulation von Computern und Netzwerken.....	8
2.2 Der Angriff auf Computer .....	8
2.2.1 Angriffsschema .....	8
2.2.2 Zugang erlangen.....	9
2.2.3 Schadprogramme installieren.....	10
2.2.4 Cyberwar führen .....	11
3. Cyberwar in der Praxis.....	13
3.1 Einführung .....	13
3.2 Cyberwar von 1998-heute.....	13
3.2.0 Vorgeschichte: Pipeline-Explosion in der Sowjetunion .....	13
3.2.1 Moonlight Maze 1998-2000 .....	13
3.2.2 Jugoslawienkrieg 1999.....	13
3.2.3 Der Hainan- oder EP3-Zwischenfall von 2001.....	14
3.2.4 Grossangriffe auf westliche Regierungs- und Industrie-Computer .....	14
3.2.5 Der Angriff auf Estland im Jahre 2007.....	15
3.2.6 Der Angriff auf Syrien 2007 .....	15
3.2.7 Der Angriff auf Georgien 2008.....	15
3.2.8 Eindringversuche in das amerikanische Stromnetz 2003-2009 .....	16
3.2.9 Eindringen in amerikanische Kampfdrohnen 2009 .....	16
3.2.10 Der ‚digitale Erstschatz‘ durch Stuxnet 2009-2010.....	16
4 Die Sicherheitsarchitektur im Cyberspace.....	19
4.1 Grundlagen.....	19
4.2 Die Bundesrepublik Deutschland .....	19
4.3 Die Cyberwarstrategien der USA und Chinas .....	21
4.4 Die Cyberpolitik der Europäischen Union.....	25
4.5 Die Cyberabwehr der NATO .....	28
5 Literaturquellen.....	29
6 Literaturhinweis .....	36

# 1. Grundlagen

## 1.1 Einführung

Die Diskussion um die Computer- und Internetsicherheit haben in den letzten Monaten an Intensität zugenommen und der Cyberspace wird wegen der zunehmenden Bedeutung des Internets und der Informationstechnologie inzwischen als fünfte militärische Dimension neben Boden, See, Luftraum und Weltall betrachtet<sup>1</sup>. Die folgende Arbeit unternimmt eine aktuelle Bestandsaufnahme und geht auf die theoretischen und praktischen Probleme des Cyberwar (Cyberkrieges) ein. Es wird zudem ein aktueller Überblick über Cyberwar-Aktivitäten seit 1998 gegeben und die Sicherheitsarchitektur im Cyberspace vorgestellt. Abschließend werden exemplarisch die Cyberwar-Strategien der USA und Chinas und die Cyberpolitik der Europäischen Union besprochen.

## 1.2 Hintergrund

Die wachsende Abhängigkeit von Computern und die zunehmende Bedeutung des Internets durch die wachsende Zahl an Nutzern und verfügbaren Informationen sind allgemein bekannt. Hinzu kommt jedoch, dass die immer intensivere Nutzung netzabhängiger Technologien die Anfälligkeit von Staaten für Angriffe in den letzten Jahren gesteigert hat.

Technologien, die die Angriffsfläche für Angriffe erheblich vergrößern, sind:

- Das Next oder **New Generation Network NGN**, bei dem Fernsehen, Internet und Telefon über das Internetprotokoll (**Triple-Play**) mit paketweiser Verschickung von Daten arbeiten
- Das **Internet of Things IoT**, bei dem Gegenstände Internetadressen erhalten, was in Zukunft ihrer Nachverfolgung, Lokalisation und der Übermittlung von Zustandsmeldungen dienen kann bzw. soll. Im IoT kommunizieren Maschinen und mit **Radiofrequency Identification (RFID)**-Chips versehene Gegenstände mit Computern und auch miteinander<sup>2</sup>. Eine erhebliche geplante Erweiterung ist auch die Vernetzung von Kraftfahrzeugen zur car-to-car-communication<sup>3</sup>.
- Die Fernwartung und –steuerung von Industriemaschinen über speicherprogrammierbare Steuerungen, auch als Industrial Control Systems ICS bzw. **Supervisory Control and Data Acquisition SCADA**

---

<sup>1</sup> vgl. USAF 2010a

<sup>2</sup> Die EU schätzte 2009, dass von den ca. 50-70 Milliarden für die machine-to-machine (M2M)-communication geeigneten Maschinen erst 1% vernetzt sind vgl. EU 2009a, S.2

<sup>3</sup> vgl. Quirin 2010, S.2f.

- bezeichnet. SCADA-Systeme ermöglichen die Kommunikation mit Maschinen über das Internet.
- Die Vernetzung von Waffen und Geräten in der **vernetzten Kriegführung** schafft bis dahin unbekannte Probleme, z.B. die Absicherung und Stabilisierung fliegender Computernetzwerke in der Luftwaffe<sup>4</sup>
  - Weitere geplante Erweiterungen des Netzes sind intelligente Haushaltsgeräte und Stromzähler (**smart grid**) und die Nutzung externer Rechenzentren über das Internet anstelle der Vorhaltung eigener Kapazitäten (**cloud computing**)<sup>5</sup>
  - Die Einführung internetfähiger Mobiltelefone (smartphones), die nun auch die Funktionen von Navigationsgeräten (Global Positioning System GPS-Standortangaben) integrieren.

Aus all dem resultiert eine deutlich gestiegene Verwundbarkeit und informationstechnische Abhängigkeit kritischer Infrastrukturen (KRITIS)<sup>6</sup>. Auf der anderen Seite ist die Durchführung eines Angriffs erheblich vereinfacht<sup>7</sup>.

- Dank des Netzes können die Angriffe nun auch aus großer Entfernung erfolgen. Sie erfordern ein gewisses technisches Know-How, aber wesentlich weniger materiellen und logistischen Aufwand als konventionelle Angriffe
- Dadurch sind auch asymmetrische Angriffe von kleinen Gruppen auf große Ziele wesentlich leichter möglich
- Sowohl die Erkennung eines Angriffes als auch die Identifizierung der Angreifer ist bei guter Vorbereitung des Angriffs wesentlich schwieriger als bisher (sog. **Attributionsproblem**), so dass auch die Abschreckung durch Bestrafung oder Gegenwehr erschwert wird.

---

<sup>4</sup> vgl. Grant 2010

<sup>5</sup> vgl. Postinett 2008, S.12, Knop 2010, S.14. Risiken der Cloud bestehen u.a. darin, dass sich die Daten nicht nur auf fremden Rechnern befinden, sondern auch in fremden Rechtsräumen, wo sie zumindest dem Grundsatz nach auch politischen Einflüssen ausgesetzt sind, vgl. FAZ 2010f, S.17. Der Cloud computing-Anbieter selbst stellt eine für die auslagernde Firma schwer kontrollierbare zusätzliche Eintrittspforte für Angriffe dar, vgl. Menn 2010, S.H12-H13.

<sup>6</sup> Quelle BSI: „Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. In Deutschland zählen folgende Sektoren zu den Kritischen Infrastrukturen: Transport und Verkehr (Luftfahrt, Bahn, Straße, Wasserwege), Energie (Elektrizität, Atomkraftwerke, Mineralöl, Gas), Gefahrenstoffe (Chemie- und Biostoffe, Rüstungsgüter), IT und Telekommunikation, Finanz-, Geld- und Versicherungswesen, Versorgung (Notfall- und Rettungswesen, Wasserversorgung, Entsorgung), Behörden, Verwaltung und Justiz (einschließlich Polizei, Zoll und Bundeswehr), Sonstiges (Medien, Großforschungseinrichtungen, Kulturgut) In den genannten Infrastrukturen sind aufgrund der Abhängigkeit von der Informationstechnik u. a. folgende Systeme als besonders kritisch einzustufen: Leitstellen, Prozessleittechnik, Management- sowie Kommunikationssysteme.

<sup>7</sup> vgl. Megill 2005

Die Autoren sind sich nicht einig, wann der erste Cyberwar stattgefunden hat, aber die ersten Aktivitäten, die man in diesem Kontext diskutierte, begannen schon im Jahr 1998 mit der Operation **Moonlight Maze**.

### 1.3 Definitionen

Der Begriff **Cyberwar** (auch *cyber warfare*) ist aus den Begriffen War und Cyberspace zusammengesetzt und bezeichnet die kriegerische Auseinandersetzung mit den Mitteln der Informationstechnologie. In der Praxis meint dies den Angriff auf Computer und die in ihnen enthaltene Information, die Computernetzwerke und die von den Computern abhängigen Systeme<sup>8</sup>.

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<sup>9</sup>.

Jedoch gehen die meisten Autoren davon aus, 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.

Allgemein werden Angriffe auf Computer, Informationen, Netzwerke und computerabhängige Systeme auch als **Cyberattacken** bezeichnet.

Cyberattacken können auch privater, kommerzieller oder krimineller Natur sein, wobei bei allen Angriffen dieselben technischen Methoden zum Einsatz kommen, was die Identifikation des Urhebers und des Angriffsmotivs mitunter schwierig bis unmöglich macht. Hat die Attacke einen terroristischen Hintergrund, spricht man vom **Cyberterrorismus**, zielt der Angriff auf die Gewinnung von Informationen ab, spricht man von **Cyberspionage**. Natürlich sind auch Cyberterrorismus und Cyberspionage illegal, zumeist wird der Begriff der Cyberkriminalität aber nur für konventionelle Straftaten wie den Diebstahl von Geld über den Zugriff auf fremde Onlinebankingdaten verwendet<sup>10</sup>.

Im Unterschied zum Cyberwar erfolgt die Cyberspionage in der Regel *passiv*, d.h. es findet keine Sabotage oder Zerstörung des angegriffenen Systems statt, da dies ja auch den Informationsfluss an den Angreifer unterbrechen und den Angriff aufdecken würde<sup>11</sup>. Großangelegte Spionageangriffe können jedoch auch zu Computer- und Netzwerkstörungen führen und werden dann mitunter in der Literatur ebenfalls dem Cyberwar zugerechnet.

---

<sup>8</sup> vgl. Wilson 2008, S.3ff.

<sup>9</sup> vgl. auch CSS 2010, Libicki 2009, S. XIV

<sup>10</sup> vgl. auch Mehan 2008, CSS 2010

<sup>11</sup> vgl. Libicki 2009, S. 23

Fazit: Die Begriffe sind fließend und die Einordnung eines Vorfalls kann insbesondere dann, wenn der Urheber unbekannt ist, schwierig sein. Schuldzuweisungen an Staaten sollten daher ohne konkrete Indizien unterbleiben.

#### **1.4 Die Cyberwar-Konzeption der USA**

Die Vernetzung von Computern in einer besonders geschützten Internetumgebung bildet zusammen mit der Verbesserung von Verschlüsselungen zum Schutz der Kommunikation, generellen Verbesserungen der Mustererkennung und dem Global Positioning System (GPS) die technische Grundlage für eine Vielzahl technischer und strategischer Neuerungen, die in den USA unter dem Begriff **Revolution in Military Affairs (RMA)** zusammengefasst werden<sup>12</sup>.

Dazu gehört neben bereits etablierten Anwendungen

- wie dem Radarflugzeugsystem **Airborne Early Warning and Control System (AWACS)**, das der großräumigen Radarüberwachung aus der Luft dient,
- der Einsatz der vernetzten Kriegführung (**Network based warfare NBW**), bei der die **C4ISR** (Command, Control, Computers, Communications, Information for intelligence, surveillance, and reconnaissance) im Zentrum steht, d.h. die Vernetzung aller Führungs-, Informations- und Überwachungssysteme zur Gewinnung eines genauen Lagebildes und zur Verbesserung der Entscheidungsfindung und Führungsfähigkeit
- der Einsatz von **Lenkwaffen** wie smart bombs (intelligente Bomben)
- der Einsatz unbemannter Systeme wie der **Drohnen** (Unmanned Aerial Vehicles UAV) oder auch Bombenentschärfer (PackBots<sup>13</sup>)
- und die **integrierte Kriegführung**.

Die **Drohnen** dienen nicht mehr nur der Aufklärung, sondern können auch zur Terroristenbekämpfung eingesetzt werden, wie schon in Afghanistan und Pakistan erfolgreich geschehen<sup>14</sup>. Der operative Erfolg der Drohnen hat die Nachfrage so steigen lassen, dass die Produktion inzwischen den Bedarf nicht mehr decken kann<sup>1516</sup>.

Bei der **integrierten Kriegführung** werden zivile Ziele und Organisationen in die Planung und Durchführung des Krieges mit eingebunden und die Informationsführung während des Krieges systematisch geplant und ausgeführt.

---

<sup>12</sup> vgl. Neuneck/Alwardt 2008

<sup>13</sup> vgl. Hürther 2010, S.33-34

<sup>14</sup> Rüb 2010, S.5

<sup>15</sup> vgl. FAZ 2010b, S.6

<sup>16</sup> Zunehmend geht der Trend zur Miniaturisierung, wie z.B. beim Modell Rabe, das nur noch Spielzeuggröße hat, vgl. Singer 2010

Die gezielte Einbettung der Medien in den politisch-militärischen Kontext soll den Informationsfluss und die -politik in einer für den Einsatz günstigen Weise lenken. Dieser ganzheitliche Ansatz wird auch als **Effects based operations EBO** bezeichnet und zielt auf die Erringung der **Informationsüberlegenheit** ab, die in Krieg und Frieden auf alle Akteure, also auch auf die Freunde eine Einflussnahme ermöglichen soll.

Mittlerweile hat das US-Verteidigungsministerium die Inhalte und Ziele der **informationellen Kriegsführung (Information Operations IO)** genauer klassifiziert.<sup>17</sup> Ziel der IO ist die Erlangung und Optimierung von 5 Kernfähigkeiten (core capabilities), nämlich

- der erfolgreichen psychologischen Kriegsführung (**psychological operations PSYOP**) zur Erringung der Informationsüberlegenheit, wobei man noch die Gegenspionage (**Counterintelligence CI**), Gegenpropaganda und öffentliche Information (**Public Affairs PA**) abgrenzen kann<sup>18</sup>
- der Irreführung des Gegners (**military deception MILDEC**), z.B. der gegnerischen Luftabwehr wie während des Irakkrieges<sup>19</sup>
- der Sicherung der eigenen Operationen (**Operation Security OPSEC**), z.B. durch Verhindern des versehentlichen Ins-Netz-Stellens militärisch verwertbarer Informationen
- dem Cyberwar im engeren Sinne als **computer network operations (CNO)**, der sich in drei Gruppen gliedern lässt: Angriffe auf Computer, Informationen, Netzwerke und **computerabhängige Systeme (computer network attacks CNA)** bezeichnet<sup>20</sup>, die Entwendung von Informationen als **computer network exploitation (CNE)** und die Schutzmassnahmen gegen beides als **computer network defence (CND)**<sup>21</sup>
- die klassische elektronische Kampfführung (**electronic warfare EW**) mit Hilfe der Schädigung des Gegners durch Störsignale und ähnliche Maßnahmen.

---

<sup>17</sup> vgl. Wilson 2007

<sup>18</sup> vgl. USAF 2010b, S.5

<sup>19</sup> vgl. USAF 2010b, S.32

<sup>20</sup> vgl. Wilson 2008

<sup>21</sup> vgl. CSS 2010

## 2. Methoden

### 2.1 Klassifikation

Im Grundsatz werden vor allem drei Angriffsarten erörtert, nämlich die physische Zerstörung von Computern und ihren Verbindungen, die Zerstörung der Elektronik mit Hilfe eines elektromagnetischen Pulses und der Angriff auf und die Manipulation von Computern und Netzwerken mit Hilfe von Schadprogrammen (Malware).<sup>22</sup>

#### 2.1.1 Physische Zerstörung von Computern und ihren Verbindungen

Die geschieht durch Zerstören, Sabotage, Ausschalten von Hardware sowie Kabel-, Antennen- und Satellitenverbindungen. Die Vorstellung, dass z.B. durch einen Atomschlag die Kommandostrukturen der USA zerstört werden könnten, war der Auslöser zur Bildung des dezentralen Computernetzwerks ARPANET, das die Keimzelle des späteren Internets bildete. Da solche Zerstörungen aber auch unbeabsichtigt durch Brände oder Überschwemmungen entstehen können, ist es heute üblich, Grossrechneranlagen besonders zu sichern und ggf. ein Reservesystem (Back-Up) vorzuhalten.

#### 2.1.2 Elektromagnetischer Puls EMP

Moderne Elektronik, also nicht nur Computer, kann durch starke elektromagnetische Wellen, die auch als **elektromagnetischer Puls EMP** bezeichnet werden, zerstört werden. Ein solcher Puls tritt z.B. als Begleiteffekt einer Atombombenexplosion auf. Die Abschirmung (Härtung) der Elektronik gegen den EMP ist möglich, aber sehr teuer, so dass sie in der Praxis nur auf Teilsysteme beschränkt sein kann.

#### 2.1.3 Der Angriff auf und die Manipulation von Computern und Netzwerken

Computer und Netzwerke können auf verschiedene Weise angegriffen werden, wobei dies technisch durch heimliche Platzierung von Programmen (Computerbefehlen) auf dem angegriffenen Computer oder durch Störung der Kommunikation zwischen den Computern geschieht. Angriffe im Cyberwar werden in aller Regel auf diese Weise durchgeführt.

## 2.2 Der Angriff auf Computer

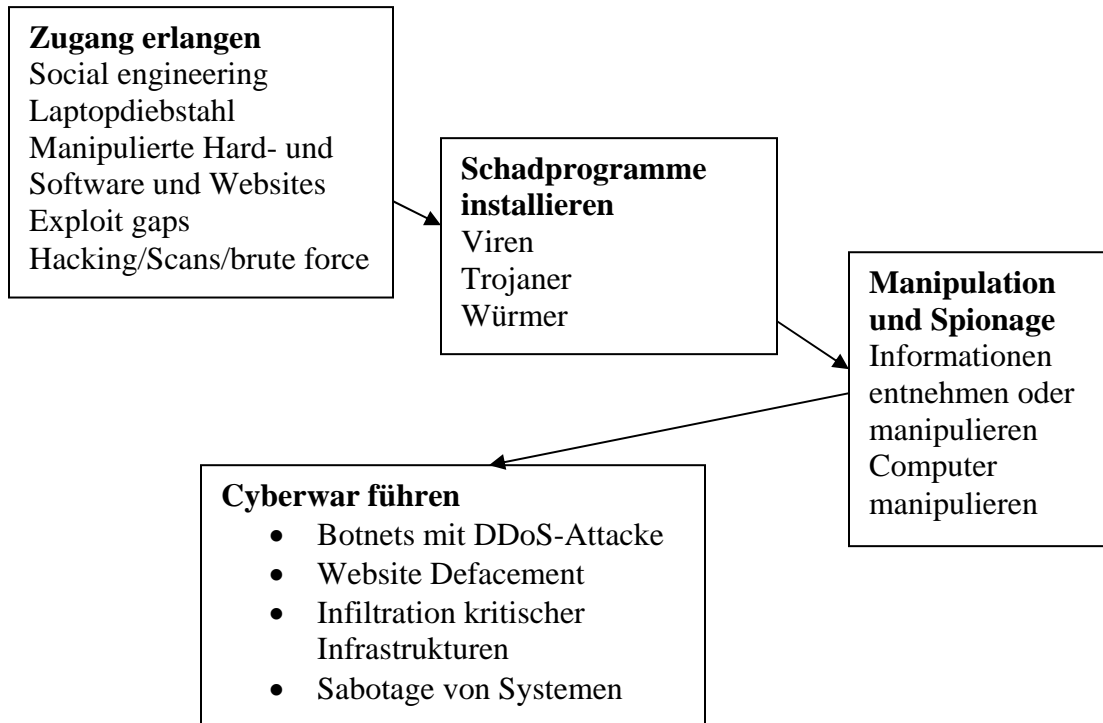
### 2.2.1 Angriffsschema

Das Muster der Angriffe ist im Grundsatz ähnlich. Zunächst geht es darum, Zugang zu den Computern und dem Netzwerk zu erlangen.

---

<sup>22</sup> vgl. Wilson 2008, S.11

Danach wird dieser Zugang ausgenutzt, um Schadprogramme auf dem/den Computern zu installieren. Mit Hilfe dieser Programme können dem Computer Informationen entnommen und/oder die Informationen und/oder der Computer in irgendeiner Form manipuliert werden. Dadurch können wiederum weitere unerwünschte Aktionen eingeleitet werden, wobei hier die für den Cyberwar praktisch bedeutsamen Aktionen vorgestellt werden<sup>23</sup>.



## 2.2.2 Zugang erlangen

Der Zugang kann auf verschiedenste Weise erlangt werden, insbesondere durch

- Ausnutzung von Sicherheitslücken in Computerprogrammen und Betriebssystemen wie z.B. Windows oder Adobe, man spricht auch vom **Exploit-Problem** (exploit = ausbeuten, ausnutzen), wobei die Überprüfung von Computern auf Schwachstellen auch automatisiert über Portscans<sup>24</sup> erfolgen kann
- durch Ausprobieren (**Hacken**) von Passwörtern, wobei dies inzwischen auch automatisiert unter Einsatz großer Rechnerkapazitäten (**brute force**) erfolgt

<sup>23</sup> vgl. Northrop Grumman TASC 2004

<sup>24</sup> Ein Portscanner überprüft, welche Dienste ein System über das Internetprotokoll anbietet, und welches Antwortverhalten es zeigt.

- durch Irreführung von Computernutzern durch **social engineering**, bei denen man den Nutzern unter einem Vorwand Zugangsdaten wie das Passwort entlockt
- Immer häufiger versucht man, das Opfer durch manipulierte e-Mails mit präparierten Anhängen oder Internetseiten hereinzulegen. Beim **Phishing** lockt man Verbraucher per E-Mail auf eine Website und überredet sie, die PIN etc. einzugeben, beim komplizierter durchzuführenden **Spoofing** wird der Computer der Nutzer trotz richtiger Adresseingabe auf die falsche Website geleitet. Beim **Cross-site-scripting** wird der Nutzer unbemerkt auf eine andere Seite weitergeführt, beim **drive-by download** werden unbemerkt Schadprogramme von einer scheinbar seriösen Website auf den Rechner geladen
- Die Platzierung von Schadprogrammen kann aber auch durch das Einlegen **infizierter Datenträger** (früher Disketten, heute insbesondere infizierte USB-Sticks) geschehen
- Es gibt immer wieder Debatten wegen schon vorher eingebauter Hintertüren (**'backdoors'**), durch die sich Geheimdienste an allen Sicherungen vorbei Zugriff zum Rechner verschaffen können. Microsoft bestätigte 2007 offiziell eine Zusammenarbeit mit dem amerikanischen Geheimdienst National Security Agency NSA bei Windows Vista, verneint aber die Existenz von Hintertüren<sup>25</sup>. Microsoft hat das Government Security Program GSP ins Leben gerufen, bei denen Regierungen zumindest in 90% des Quellcodes (des Programmcodes) Einsicht nehmen dürfen, wovon bereits viele Staaten Gebrauch gemacht haben. Jedoch fürchten die USA selber Hintertüren, z.B. als versteckte Funktionen in Chips, weshalb keine asiatischen Chips mehr in sicherheitsrelevanter US-Technologie verwendet werden sollen. Aus demselben Grunde will das US State Department auch keine chinesischen Computer mehr verwenden<sup>26</sup>. Gleichwohl lässt sich die Nutzung kommerzieller Produkte, englisch **commercial off-the-shelf (COTS) technology**, in sicherheitsrelevanten Bereichen trotz der dadurch erhöhten Anfälligkeit nicht ganz vermeiden. Nicht nur Hersteller, sondern auch die globalen Lieferketten bilden mögliche Angriffspunkte<sup>27</sup>.

### 2.2.3 Schadprogramme installieren

Während es bei der Computerspionage, die private, kommerzielle, kriminelle, politische oder militärische Gründe haben kann, um Versuche geht, in Computer

---

<sup>25</sup> Die Welt 10 Januar 2007

<sup>26</sup> Die USA und Indien haben 2010 den großen chinesischen Netzausrüster Huawei und dessen Wettbewerber ZTE beschuldigt, Spionagesoftware in ihren Produkten installiert zu haben, Huawei konnte jedoch zumindest die indische Regierung durch Offenlegung des Quellcodes und Zusicherung von Inspektionen von der Sicherheit seiner Produkte überzeugen, vgl. Mayer-Kuckuck/Hauschild 2010, S.28

<sup>27</sup> vgl. USAF 2010a, S.5

einzudringen, um Passwörter, persönliche Identifikationsnummern (PINs), kurz ‘Geheimzahlen’, oder sonstige Informationen einzusehen, geht es beim Cyberwar in der Regel um aktive Manipulation von Computern, d.h. man versucht den Computer zu Handlungen zu bewegen, die nicht im Sinne des eigentlichen Besitzers sind. Hierzu dienen Schadprogramme, die auf einem oder mehreren unzureichend geschützten Computern installiert werden.

Schadprogramme (**malware**) werden allgemein in Viren (Programme, die sich im Computer festsetzen), Trojaner (Programme, die Vorgänge auf dem Computer nach draußen melden) und Würmer (Programme, die sich selbsttätig im Netz verbreiten können) unterteilt. In der Regel bestehen die Schadprogramme aus einem Teil, der die Installation im Computer bewerkstelligt und weiteren Teilen, die dann die vom Angreifer gewünschten Aktionen durchführen.

Beispiele für solche Schadprogramme sind Tastendruckmeldeprogramme (**keylogger**), die jeden Tastendruck weitermelden und so eine komplette Übersicht über die Aktivitäten am Computer geben, wobei natürlich nach und nach sämtliche Passwörter anfallen<sup>28</sup> und **Rootkits** (Programme, die dem Angreifer das heimliche Einloggen und Steuern des Computers ermöglichen).

#### 2.2.4 Cyberwar führen

Eine zentrale Rolle im Cyberwar spielen sogenannte **Distributed Denial of Service (DDoS)**-Angriffe.

Beim Denial of Service (DoS) verweigern (denial) Computer(systeme) durch gezielte Überlastung, z.B. mit sinnlosen Anfragen von außen, ihren Dienst (service). Bei Distributed Denial of Service-Angriff wird ein Computer(system) von mehreren Rechnern koordiniert angegriffen, was selbst leistungsfähige oder gut gesicherte Computersysteme funktionsunfähig machen kann.

Das Werkzeug, um mit einer DDoS-Attacke anzugreifen, ist das **Botnetz**.

Man kann Computer mit Hilfe eingeschleuster Programme<sup>29</sup> als Arbeitscomputer (**‘Bot’** abgeleitet von Robot) verwenden, wobei diese Programme im Hintergrund laufen können. Die koordinierte Nutzung der Rechenleistung derart manipulierter Computer wird dann als Botnetz bezeichnet. Botnetze werden genutzt, um die Rechenleistung zahlreicher, mitunter tausender Computer gegen ein anderes System zu richten und spielen im Cyberwar eine große praktische Rolle. Illegale Botnetze können inzwischen auch ‘gemietet ‘ werden<sup>30</sup>.

Die Dominanz der Botnetze hat mit folgendem zu tun:

---

<sup>28</sup> vgl. Stark 2009, Schmitt 2009, S.83

<sup>29</sup> Manchmal gebiert Gutes auch Böses. Das erste große Botnetz bestand aus Freiwilligen, die sich ein Programm auf den Rechner luden, um dem **SETI** (Search for Extraterrestrial Intelligence)-**Projekt** bei der Suche nach ausserirdischem Leben zu helfen. Die Rechner werteten nebenher Signale aus dem All aus. Das brachte andere dann auf dunkle Ideen.

<sup>30</sup> vgl. FAZ 225/2009, 5 Dollar kosten Rechner im Tausenderpack in Fernost, um dann für hundert Dollar weiterverkauft zu werden. Das Botnet Conficker hatte angeblich 5 Millionen Computer in 122 Ländern unter Kontrolle, vgl. Wegner 2009.

1. befinden sich die Botnetze nicht unbedingt im selben Land wie der Computer, der sie steuert. Das erschwert die Lokalisation des Angreifers und macht in der Praxis einen direkten Gegenschlag praktisch unmöglich<sup>31</sup>.
2. liefern Botnetze die großen Rechnerkapazitäten, die man für einen Angriff benötigt
3. können Botnetze gezielt gegen ein anderes System gerichtet werden. Viren und Würmer können sich unkontrolliert verbreiten und mitunter auch die eigenen Systeme in Mitleidenschaft ziehen
4. die Botnetze können sich theoretisch in *jedem* Computer befinden, so dass es nicht möglich ist, sich von vornherein gegen bestimmte Computer zu wappnen.

Kurzum: In Übereinstimmung mit den Forderungen von Clausewitz an ein ideales Manöver können mit Hilfe der Botnetze massive, überraschende, effiziente, leicht und zentral koordinierbare Angriffe geführt werden<sup>32</sup>.

Weitere tatsächlich praktizierte Methoden sind

- das **Website Defacement**, bei dem man das Aussehen (face) einer Internetseite zu propagandistischen Zwecken verändern
- die Infiltration und Manipulation **kritischer Infrastrukturen** wie Radarsysteme, Stromnetze und Steuerungen von Kraftwerken
- und die **Sabotage** von Computersystemen, wobei dies oft als Begleiterscheinungen massiver Computerspionage und nachfolgenden Systemstörungen auftritt.

Wichtig ist jedoch, dass durch technische Entwicklungen bisherige Strategien quasi über Nacht wertlos werden können, so dass die Vergangenheit des Cyberwars nur begrenzte Prognosekraft für zukünftige Angriffe hat<sup>33</sup>. Gleichwohl ist zumindest vorläufig davon auszugehen, dass der Einsatz von Botnetzen vorerst ein Kernelement massiver Angriffe bleiben wird.

---

<sup>31</sup> Um den wachsenden staatlichen Kontrollfähigkeiten auszuweichen, wurde inzwischen das Konzept der DRDoS (Distributed-Reflected-Denial-of-Service)-Attacken entwickelt, bei denen der Angreifer wie bei einer Art Billiard unter der Internetadresse des Opfers Anfragen an Internetdienste schickt, die dann dem ahnungslosen Opfer haufenweise Antworten schicken. Wegen der falschen Internetadresse ist der wahre Ursprung des Angriffs für den Angegriffenen kaum noch ermittelbar

<sup>32</sup> WhiteWolfSecurity 2007

<sup>33</sup> vgl Gaycken 2009

## 3. Cyberwar in der Praxis

### 3.1 Einführung

In der Literatur werden *Cyberattacken mit Sabotagewirkung, bei denen man wegen ihrer Komplexität zumindest von der Unterstützung oder Duldung durch staatliche Stellen ausgehen muss*, als Cyberwar geführt.

Die Besonderheit beim Cyberwar ist, dass anders als bei einem herkömmlichen Konflikt die Informationen in aller Regel *nur von einer Seite* stammen, meistens dem Opfer, in Ausnahmefällen jedoch auch nur vom Angreifer. Dies erschwert die Beweisführung und insofern auch die Überprüfung des tatsächlichen Geschehens.

### 3.2 Cyberwar von 1998-heute

#### 3.2.0 Vorgeschichte: Pipeline-Explosion in der Sowjetunion

Russland versuchte, an US-Hochtechnologiesysteme zur Steuerung der eigenen Pipelines zu gelangen, die ihnen die USA wegen des kalten Krieges nicht überlassen wollten. Die USA ließen die Entwendung dennoch zu, bauten aber in die Software ein Schadprogramm ein, das dazu führte, dass der Druck in der Pipeline über den zulässigen Höchstwert gebracht wurde. Es folgte eine Explosion von ca. 3 Kilotonnen Stärke, immerhin einem Fünftel der Hiroshima-Bombe<sup>34</sup>. Russland widersprach dieser Darstellung der Ereignisse.

#### 3.2.1 Moonlight Maze 1998-2000

Im Zuge der ca. 2 Jahre andauernden Aktion **Moonlight Maze** wurden Computer des Pentagon, der NASA, des Energieministeriums und anderen Akteuren systematisch auf Schwachstellen abgeprüft und zehntausende von Dateien gestohlen, das Verteidigungsministerium vermutete Russland hinter dem Angriff, das jedoch dementierte<sup>35</sup>.

#### 3.2.2 Jugoslawienkrieg 1999

Als erste dem Cyberwar nahekommende Maßnahme zählen manche Autoren die Sabotage jugoslawischer Telefonnetze im Jahre 1999 durch die NATO im Zuge des Kosovo-Krieges<sup>36</sup>. Als Reaktion auf die versehentliche Bombardierung der chinesischen Botschaft in Belgrad wurden Webseiten der US-Regierung von chinesischen Hackern angegriffen, u.a. die Website des Weißen Hauses<sup>37</sup>.

---

<sup>34</sup> vgl. Falliere 2010, Herwig 2010

<sup>35</sup> vgl. Vistica 1999

<sup>36</sup> vgl. Hegmann 2010

<sup>37</sup> vgl. Hunker 2010, S.3

### 3.2.3 Der Hainan- oder EP3-Zwischenfall von 2001

Im zeitlichen Zusammenhang mit dem Zusammenstoß einer US-Aufklärungsflugzeugs vom Typ EP-3 mit einem chinesischen Jet, dem sogenannten Hainan-Zwischenfall, wurden mutmaßlich von patriotischen chinesischen Hackern die Würmer *Code Red* und *Code Red II* auf amerikanische Computer losgelassen, die dann ca. 600.000 Computer infizierten und 2 Mrd. Dollar Schaden anrichteten. Es kam zu Computerabstürzen und Website defacements, bei denen u.a. der Slogan „hacked by Chinese“ platziert wurde<sup>38</sup>.

### 3.2.4 Grossangriffe auf westliche Regierungs- und Industrie-Computer

Neben militärischen Netzwerken sind aber auch zivile Netzwerke von Behörden und Rüstungsfirmen interessant; auf dem Sektor konstatieren US-Beobachter bereits eine Art **kalten Cyberkrieg** mit China<sup>39</sup>, so soll China im Jahre 2007 mindestens 10-20 Terabytes an Daten aus entsprechenden US-Netzwerken abgezogen haben, zudem wurden im selben Jahr 117.000 Internet-Angriffe auf die Server des Heimatschutzministeriums Homeland Security gemeldet. Diese Aktivitäten folgten einer mehrjährigen systematischen Angriffswelle, die von den USA **Titan Rain** getauft wurde<sup>40</sup>. Auch die Bundesregierung beklagte in der Zeit den Angriff auf ihre Computersysteme.

Das aus Titan Rain abgeleitete Angriffsmuster sah wie folgt aus: Teams von ca. 6-30 Hackern dringen in Computer ein, kopieren ihren gesamten Inhalt in ca. 30 Minuten, senden die Daten zu einem Botnetz in Südostasien und von dort weiter in die chinesische Provinz Guangdong, wobei sich letzteres aber nicht sicher nachweisen ließ<sup>41</sup>.

Es gibt auch zahlreiche Medienberichte zu russischen und chinesischen Eindringversuchen in das Pentagon und das Weisse Haus in den Jahren 2007-2008. ArcSight berichtet von 360 Millionen Eindringversuchen in das Pentagon-Computersystem im Jahre 2008<sup>42</sup>. Nach einem erfolgreichen Eindringen in das Email-System des Verteidigungsministers mussten 1.500 Pentagon-Systeme abgeschaltet werden. Ein erfolgreicher Eindringversuch in das Pentagon erfolgte über einen infizierten USB-Stick, den ein Soldat im Nahen Osten unwissentlich in einen Pentagoncomputer steckte<sup>43</sup>.

Weitere Angriffe waren **GhostNet** und die **Operation Aurora** aus dem Jahr 2009. Bei **GhostNet** wurden laut BBC News durch ein Virus offenbar gezielt Computer von Botschaften attackiert, u.a. von Indien, Südkorea, Indonesien, Thailand,

---

<sup>38</sup> vgl. Fritz 2008 und Nazario 2009, der in seinem Papier einen Überblick über politisch motivierte DoS-Attacken gibt.

<sup>39</sup> vgl. Hegmann 2010, S.5. ‚Kalt‘ deshalb, weil es ‚nur‘ um Spionage geht, aber nicht um Sabotage. Dieser Begriff zeigt jedoch auch die Probleme, genau zu sagen, was Cyberwar ist, vgl. auch Herwig 2010, S.61

<sup>40</sup> Fischermann/Hamann 2010

<sup>41</sup> Fritz 2008, S.55 und auch Stokes 2005

<sup>42</sup> ArcSight 2008, S.2

<sup>43</sup> vgl. Glenny 2010, S.23

Taiwan, Deutschland und Pakistan sowie in den Außenministerien u.a. des Iran, Bangladesch, Indonesien, Brunei und Bhutan. China wurde verdächtigt, weil auch der Computer des Dalai Lama infiziert wurde, aber der sichere Beweis ließ sich wieder nicht führen. Das Virus konnte in den befallenen Computern die eingebaute Kamera und die Tonaufzeichnungsfunktionen zur Raumüberwachung in Gang setzen.

Bei der **Operation Aurora** versuchten mutmaßlich chinesische Angreifer, Zugang zu den Computerprogrammen, genauer gesagt den Quellcodes, von Firmen aus der IT-Branche (allen voran Google, aber auch Adobe) sowie von Hochtechnologiefirmen der Sicherheits-, Computersicherheits- und der Verteidigungsbranche zu erlangen<sup>44</sup>.

### 3.2.5 Der Angriff auf Estland im Jahre 2007

Es kam zu einem computertechnischen Großangriff auf Estland 2007, nachdem Estland ein russisches Kriegerdenkmal abgebaut hatte, das für die Russen die Opfer bei der Befreiung Estlands von Hitler darstellte, den Esten jedoch als Besatzungssymbol erschien<sup>45</sup>. Estlands Netz wurde daraufhin von Russland aus mit gewaltigen Datenmengen bombardiert, wobei dies nicht vom russischen Staat ausging, sondern 'nur' von nationalistisch gesinnten Kreisen<sup>46,47</sup>. Die Zahl der Anfragen auf bestimmte Computer stieg von 1.000 pro Tag auf 2.000 pro Sekunde an und die gesamte Attacke dauerte insgesamt Wochen<sup>48</sup>.

### 3.2.6 Der Angriff auf Syrien 2007

Bei dem Angriff auf eine mutmaßliche Atomanlage in Ostsyrien am 06.09.2007 mussten israelische Flugzeuge den gesamten syrischen Luftraum durchfliegen. Um dies zu ermöglichen, hatten die Israelis den Computern der syrischen Luftabwehr einen leeren Himmel vorgegaukelt, so dass die Flugzeuge unbehelligt einfliegen und angreifen konnten. Dies ist ein klassisches Beispiel für die Idee des Cyberwars als operativer Ergänzung zu konventionellen Maßnahmen<sup>49</sup>.

### 3.2.7 Der Angriff auf Georgien 2008

Schon im Vorfeld des Krieges zwischen Russland und Georgien begannen mutmaßlich aus Russland kommende Angriffe gegen georgische Computersysteme, wobei auch kritische Infrastrukturen und Webseiten von Medien, Banken und Transportunternehmen betroffen waren<sup>50</sup>. Schon Wochen vorher wurde die Internetseite des georgischen Staatspräsidenten am 20. Juli 2008

---

<sup>44</sup> vgl. Markoff/Barbosa, 18.02.2010

<sup>45</sup> vgl. Busse 2007

<sup>46</sup> Später bekannte sich die russische patriotische Jugendorganisation **Naschi** (die Unsrigen) zu dem Angriff, vgl. Frankfurter Allgemeine Zeitung 11.03.09

<sup>47</sup> vgl. Koenen/Hottelet 2007, S.2

<sup>48</sup> vgl. Wilson 2008, S.7ff.

<sup>49</sup> vgl. Herwig 2010, S.60

<sup>50</sup> vgl. die Stellungnahme der georgischen Regierung von 2008

durch einen Distributed Denial of Service (DDoS)-Angriff lahmgelegt. Außerdem kam es zum Website defacement, bei dem auf georgischen Internetseiten neben Fotos des georgischen Präsidenten solche von Adolf Hitler positioniert wurden. Der Hauptangriff bestand aus einer großangelegten DDoS-Attacke einen Tag vor dem Beginn des russischen Vormarsches und schwächte die Computersysteme Georgiens massiv.

### **3.2.8 Eindringversuche in das amerikanische Stromnetz 2003-2009**

Schon beim großen Stromausfall von 2003 war der Verdacht aufgekommen, dass dieser durch ein Computervirus verursacht worden sein könnte<sup>51</sup>.

Schon im August 2003 konnte der Internetwurm *Slammer* für einige Stunden in das zum Glück abgeschaltete Atomkraftwerk in David-Besse in Ohio eindringen<sup>52</sup>. Seit 2006 mussten zweimal Atomkraftwerke nach Cyberangriffen abgeschaltet werden<sup>53</sup>. Im April 2009 gelang es Hackern, in die Stromnetzkontrolle der USA vorzudringen<sup>54</sup> um dort Programme zu hinterlassen, mit denen das System bei Bedarf unterbrochen werden könnte, wobei China, das umgehend dementierte, und Russland verdächtigt wurden.

### **3.2.9 Eindringen in amerikanische Kampfdrohnen 2009**

2009 wurde berichtet, dass irakische Aufständische mit einer Software in die Videosysteme unbemannter US-Drohnen eindringen und so die Videos dieser Drohnen mit ansehen konnten<sup>55</sup>.

### **3.2.10 Der ‚digitale Erstschlag‘ durch Stuxnet 2009-2010**

Fernwartungs- und -steuerungsfunktionen (**Industrial Control Systems ICS**) wie die Supervisory Control and Data Acquisition SCADA<sup>56</sup>) über IP-Adressen für Maschinen ermöglichen die Kommunikation mit Maschinen über das Internet.

Der erste großangelegte Angriff auf Industrieanlagen erfolgte im 2009 durch den Stuxnet-Wurm und zielte primär auf Siemens-Steuerungssysteme<sup>57</sup>.

Stuxnet ist ein Wurm, also ein Programm, das sich, wenn es erstmal auf einem Computer platziert hat, von dort eigenständig in andere Computer ausbreiten kann<sup>58</sup>.

Stuxnet wurde mit Hilfe von infizierten USB-Sticks in Computer eingebracht. In Windows existierte eine Schwachstelle in LNK-Dateien, die als Eintrittspforte

---

<sup>51</sup> vgl. Gaycken 2009 mit Abbildung des großen Stromausfalls in Northeast USA 2003

<sup>52</sup> vgl. Wilson 2008, S.22

<sup>53</sup> vgl. ArcSight 2009

<sup>54</sup> vgl. Goetz/Rosenbach 2009, Fischermann 2010, S.26

<sup>55</sup> vgl. Ladurner/Pham 2010, S.12

<sup>56</sup> vgl. Shea 2003

<sup>57</sup> Welt online 2010b. Siemens baut daher seine Cyberwarforschung aus, vgl. Werner 2010, S.7

<sup>58</sup> Da Stuxnet sehr viele (Dutzende) Funktionen hat, wird es in der Literatur auch als Trojaner oder als Virus bezeichnet, vgl. auch FAZ2010a.

genutzt wurde<sup>59</sup>. Gefälschte Sicherheitszertifikate (digitale Signaturen) von den zwei Herstellern Realtek und Semiconductor, die mit der Sache aber nichts zu tun hatten, gaukelten dem Betriebssystem Windows 7 Enterprise Edition Vertrauenswürdigkeit vor<sup>60</sup>.

Die im Simatic S7-System von Siemens enthaltenen speicherprogrammierbaren Steuerungen (SPS) laufen unter dem Betriebssystem Windows, ebenso die Software für die Visualisierung von Parametern und die Steuerung der SPS, unter dem Kürzel WinCC<sup>61</sup>. Stuxnet sucht in Computern gezielt nach WinCC und der Step 7-Software in Simatic S7, wobei nur die Versionen S7-300 und S7-400 befallen werden und zwar auch nur dann, wenn eine bestimmte Netzwerkkarte des Typs CP 342/5 daran angeschlossen ist<sup>62</sup>. Stuxnet arbeitet also hochselektiv. Nach dem Befall beginnt Stuxnet, Informationen ins Internet zu schicken, u.a. an zwei Server in Malaysia und Dänemark. Stuxnet enthält und unterstützt Rootkits, also Programmsätze zur Kontrolle des Computers<sup>63</sup>.

Zudem sucht Stuxnet auch nach weiteren geeigneten Systemen zur Infektion unter Ausnutzung der sogenannten *Autorun*-Funktion von Windows. Stuxnet löscht sich nach einer bestimmten Zahl von erfolgreichen Infektionen selbst<sup>64</sup>. Es kamen Vermutungen auf, dass dadurch möglicherweise zum Atombombenbau benötigte Uran gaszentrifugen im Iran geschädigt wurden, da ihre Zahl 2009 aus unerfindlichen Gründen rückläufig war und die Internationale Atomenergiebehörde IAEA auch 2010 über Stillstände berichtete<sup>65</sup>, die daraufhin vom Iran auch bestätigt wurden<sup>6667</sup>.

Aus diesen Informationen und dem Umstand, dass Stuxnet gleich mehrere bis dahin gänzlich unbekannte Schwachstellen (**Zero-Day-Exploits**) nutzte und geschätzten Entwicklungskosten von ca. 1 Million US-Dollar<sup>68</sup> ergab sich in den Medien das Bild einer gezielten Superwaffe, die möglicherweise von Geheimdiensten konstruiert wurde, um das iranische Atomprogramm zu sabotieren<sup>69</sup>.

---

<sup>59</sup> Am 13.10.2010 gab Microsoft deshalb 16 Updates heraus, die insgesamt 49 Sicherheitslücken schlossen, vgl. Handelsblatt 2010, S.27.

<sup>60</sup> vgl. Rieger 2010, S.33, der auch den Begriff des digitalen Erstschlags prägte.

<sup>61</sup> vgl. Krüger/Martin-Jung/Richter 2010, S.9

<sup>62</sup> vgl. Schultz 2010, S.2

<sup>63</sup> vgl. Kaspersky 2010

<sup>64</sup> vgl. Falliere 2010

<sup>65</sup> vgl. FAZ2010c, S.6

<sup>66</sup> vgl. FAZ2010e, S.5. Laut derselben Meldung kam am 29.11.2010 Irans führender Cyberwarexperte und Leiter einer Stuxnet-Arbeitsgruppe, Madschid Schariari, bei einem Anschlag ums Leben.

<sup>67</sup> Das Institute for Science and International Security (ISIS) vermutete aufgrund entsprechender Befehle im Stuxnet-Code und der phasenweise rückläufigen Zentrifugenzahl, dass möglicherweise ca. 1000 Uran gaszentrifugen vom Typ IR-1 von Stuxnet betroffen waren, bei denen Stuxnet die Rotationsfrequenz anstelle der nominalen Frequenz von 1064 Hertz auf 1410 Hertz erhöhte oder nur 2 Hertz drosselte, wodurch diese Brüche erlitten; wobei diese Zentrifugenbrüche bei diesem Bautyp jedoch auch im Normalbetrieb recht häufig vorkommen; vgl. ISIS 2010.

<sup>68</sup> vgl. Schultz 2010, S.2

<sup>69</sup> vgl. Ladurner/Pham 2010, S.12

Es gibt jedoch einige Ungereimtheiten zu bedenken.

Erstens waren auch andere Staaten betroffen, insbesondere Indonesien, Indien, Aserbeidschan und Pakistan, und neben einem Dutzend weiterer Staaten auch die USA und Großbritannien, wenngleich der Iran das Primärziel war<sup>70</sup>.

Zweitens hat Stuxnet auch im Sinne des Angreifers Fehler gehabt. Stuxnet war auf ein bestimmtes Zeitfenster programmiert; da aber bei manchen Computern die Uhren verstellt sind, um das Ablauf von Lizenzen zu verhindern, ließ sich die geplante Befristung nicht aufrechterhalten, d.h. der Angriff wurde im Bezug auf die Software sehr präzise ausgeführt, nicht jedoch im Bezug auf Zeitpunkt und Ort<sup>71</sup>.

Drittens muss aber auch der Schaden betrachtet werden, den Stuxnet für die Zukunft anrichtet. Wenn Stuxnet einfach nur Überlegenheit demonstrieren sollte, dann hätte der Erschaffer sich und anderen vielleicht einen Bärenienst erwiesen, denn mit Stuxnet wurde auch das Know-How allgemein preisgegeben, und es könnte daher vielleicht nur eine Frage der Zeit sein, bis Stuxnet-Verwandte auftreten<sup>72</sup>.

Die Stuxnet-Berichterstattung weist übrigens eine Art ‚Lücke‘ auf. Die breite Berichterstattung begann erst Mitte September 2010, obwohl Stuxnet schon im Juni 2010 von einer Weißrussischen Firma entdeckt wurde und eine kommerzielle Antivirussoftware schon am 22. Juli 2010 verfügbar war, Bloomberg Businessweek hatte den Vorgang dann am 23. Juli 2010 gemeldet. Der Iran hat schon am 26. Juli 2010 in *Iran Daily* den Angriff durch Stuxnet bestätigt<sup>73</sup>. Siemens bestätigte, dass Anlagen von 15 Kunden betroffen seien, davon 60% im Iran. Mögliche Gründe für diese fast zweimonatige Medienlücke sind das nachträgliche Aufkommen der Vermutung geheimdienstlicher Beteiligung, ein offiziell nicht bestätigter Befall des iranischen Reaktors in Buschehr und die Debatte über den Cyberspace im Rahmen der neuen NATO-Strategie<sup>74</sup>.

---

<sup>70</sup> vgl. Handelsblatt 2010, S.27, Symantec 2010, S.5-7

<sup>71</sup> Gaycken 2010, S.31 erklärt dies jedoch damit, dass die Uhr von Stuxnet von den Angreifern weiter vorgestellt wurde, laut Symantec (2010, S.14) zuletzt auf den 24.06.2012

<sup>72</sup> vgl. Rosenbach/Schmitz/Schmundt 2010, S.163

<sup>73</sup> Iran Daily 26 July 2010

<sup>74</sup> vgl. Knop/Schmidt 2010, S.20

## 4 Die Sicherheitsarchitektur im Cyberspace

### 4.1 Grundlagen

Grundsätzlich ist die Sicherheitsarchitektur in drei Bereiche aufgeteilt, den zivilen Bereich, der den Schutz von kritischen Infrastrukturen organisiert, den nachrichtendienstlichen, der für die Analyse der Kommunikation und Datenströme (**Signals Intelligence SigInt**) zuständig ist und den militärischen Bereich. In militärischen Bereichen sind auch zumindest jene Offensivkapazitäten auf dem Gebiet des Cyberwar angesiedelt, die offiziell zugegeben werden.

### 4.2 Die Bundesrepublik Deutschland

Im **zivilen Sektor** spielt das Bundesministerium des Innern BMI und das ihm nachgeordnete Bundesamt für Sicherheit in der Informationstechnik BSI die führende Rolle.

Das **Bundesamt für Sicherheit in der Informationstechnik BSI** ist seit 1991 als Behörde des Bundesministeriums des Inneren BMI für alle Aspekte der IT-Sicherheit zuständig, insbesondere alle Arten der Abhörsicherheit und der Abwehr von Computerattacken für staatliche Einrichtungen. Das BSI fördert hierzu entsprechende Technologien. Es ist historisch aus der Abteilung für Chiffrierwesen des Bundesnachrichtendienstes BND hervorgegangen. Mit dem Aufkommen des Internets und dem nahenden Ende des kalten Krieges setzte sich die Auffassung durch, dass man eine Behörde benötigt, die die IT-Strukturen der Bundesrepublik schützt und der modernen Technik gerecht wird. So entstand 1989 im BND erst das ZSI (Z=Zentralstelle), aus dem dann 1991 das BSI wurde. Das neue BSI-Gesetz BSIG von 2009 hat die zentrale Stellung der Behörde im Paragraphen 5 „Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes“ nochmals gestärkt<sup>75</sup>.

Die Aufgaben der Behörde sind unter anderem<sup>76</sup>:

- Mitarbeit im Arbeitskreis KRITIS zum Schutz **Kritischer Infrastrukturen** vor Angriffen<sup>77</sup>
- Schutz der Regierungskommunikation, u.a. durch Kryptohandys für die Regierung, aber auch im **Informationsverbund Bonn-Berlin IVBB** und

---

<sup>75</sup> Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes mit BSI-Gesetz vom 14. August 2009, im BGBl 2009 Teil I Nr. 54, S.2821-2826

<sup>76</sup> vgl. BSI Jahresberichte 2005, 2006-2007 und 2008-2009

<sup>77</sup> Im Rahmen des „Nationalen Plans zum Schutz der Informationsinfrastrukturen“ (NPSI) hatten BMI und BSI im Jahr 2005 den Auftrag erhalten, einen Plan für den Bereich „Kritische Infrastrukturen“ auszuarbeiten. An der Erstellung des Umsetzungsplans KRITIS (UP KRITIS)

- dem **Informationsverbund Bundesverwaltung IVBV**, der vom BSI seit 2009 regelmäßig auf Schadsoftware gescannt wird<sup>78</sup>
- Schutz von Behörden beim elektronischen Dokumentenverkehr, der durch das **eGovernment** immer mehr zunimmt
  - Schutz der NATO-Kommunikation unter anderem durch Verschlüsselungs-Technologien, wie dem System **Elcrodat 6.2**
  - Mitarbeit an der **SINA** (Sichere Internetwerk-Architektur) –Technologie
  - Arbeit auf dem Gebiet der Kommunikationssicherheit (**Comsec**), zu der auch die Gebäudeabschirmung gehört<sup>79</sup>
  - Arbeit an stabilen und resistenten Computertechniken wie der Hochverfügbarkeit<sup>80</sup> oder der **Mikrokerntechnologie**, bei der Rechnerbereiche intern noch mal gegeneinander abgeschottet werden usw.
  - Für 2011 diskutiert die Bundesregierung die Errichtung eines nationalen „Cyber-Abwehr-Zentrums“ am BSI<sup>81</sup>

Im **nachrichtendienstlichen Sektor** gibt es das **Bundesamt** und die **Landesämter für Verfassungsschutz BfV/LfV** für die zivilen Angelegenheiten, während sich der **Militärische Abschirmdienst MAD** um den Schutz der Bundeswehr kümmert. Der **Bundesnachrichtendienst BND** ist für das Ausland zuständig. Das Bundesamt für Sicherheit in der Informationstechnik BSI darf im Rahmen der gesetzlichen Möglichkeiten die Geheimdienste technisch unterstützen.

Im **militärischen Sektor** gab es zwischenzeitlich das **Zentrum für Nachrichtenwesen in der Bundeswehr ZnBW**, das sich zu einem militärischen Auslandsgeheimdienst zu entwickeln begann, aber dann zwischen dem BND und dem 2002 gegründeten **Kommando Strategische Aufklärung KSA** (KdoStratAufkl) aufgeteilt wurde<sup>82</sup>. Das KSA, das seit 2008 den Kern des Militärischen Nachrichtenwesens der Bundeswehr (MilNWBw) bildet, hatte 2010 eine Stärke von ca. 6.000 Mann<sup>83</sup> und ist zuständig für die

- für die Elektronische Kampfführung (EloKa), d.h. die Störung feindlicher Kommunikation und

---

<sup>78</sup> vgl. Steinmann 2010, S.10

<sup>79</sup> um Probleme wie das Abfangen von vom Computer abgestrahlten Informationen zu bewältigen, vgl. Schröder 2008

<sup>80</sup> Hochverfügbarkeit umfasst u.a. die Ausfallssicherheit. Ein Unterproblem ist hier die Resistenz gegen einen **elektromagnetischen Puls EMP**, wie er z.B. bei einer Atombombenexplosion entstehen könnte und der die Elektronik nachhaltig zerstört.

<sup>81</sup> vgl. FAZ 2010g, S.4

<sup>82</sup> vgl. Eberbach 2002

<sup>83</sup> vgl. Bischoff 2009

- seit 2007 gehört dem KSA auch die Einheit **Computer- und Netzwerkoperationen CNO**<sup>84</sup> an, die auch für den Cyberwar zuständig ist, d.h. den Kampf im Internet gegen mögliche Angreifer<sup>85</sup>
- und für die Aufklärungssatelliten des Typus Synthetic Aperture Radar (SAR-Lupe)<sup>86</sup> und die Kommunikationssatelliten COMSATBW1 und 2.

Auf dem IT-Sektor arbeitet die Bundeswehr an einer grundlegenden Modernisierung ihres IT-Netzes, dem Projekt **Herkules**, das vom mit Siemens und IBM gehaltenen Joint Venture BWI IT betrieben wird. Herkules gilt (noch) als relativ anfällig<sup>87</sup>.

### 4.3 Die Cyberwarstrategien der USA und Chinas

Medienberichten zufolge wird die Zahl der Staaten, die versuchen, Cyberwarkapazitäten aufzubauen, auf mehr als 100 geschätzt. Nach US-Schätzungen versuchen ca. 140 ausländische Nachrichtendienste in Computer der Regierung oder von US-Firmen einzudringen<sup>88</sup>.

Die USA und China werden hier als die in Literatur und Medien meistdiskutierten Akteure näher vorgestellt. Es geht hier aber nicht um eine Neuauflage eines Ostwestkonfliktes. So fühlen sich beispielsweise die Inder von der Entwicklung insgesamt sehr bedroht<sup>89</sup>.

Das Primärziel aller Akteure ist die Erringung der **elektromagnetischen Dominanz** und insbesondere der **Überlegenheit im Cyberspace**<sup>90</sup>, d.h. der Beherrschung des Cyberspace im Konfliktfall.

Die USA betonen jedoch den defensiven Charakter ihrer Cyberwarstrategie, die auf der **Cyber-Triade** aus *resilience* (Hochverfügbarkeit von Computersystemen auch während eines Angriffs), *attribution* (möglichst rasche und sichere Identifikation des Angreifers) und *deterrence* (Abschreckung potentieller Angreifer durch die Fähigkeit zum Gegenschlag) beruht. Mittlerweile wurde die **Comprehensive National Cybersecurity Initiative (CNCI)** gestartet, bei der u.a.

<sup>84</sup> vgl. Bischoff 2009

<sup>85</sup> Goetz 2009, p.34f., von Kittlitz 2010, S.33. Am 01.07.2010 wurde die Gruppe Informationsoperationen (InfoOp), die bislang beim Kommando Strategische Aufklärung (KSA) mit der CNO zusammenarbeitete, dem Zentrum Operative Information organisatorisch unterstellt, das wie der KSA der Streitkräftebasis SKB angehört (Uhlmann 2010). Dadurch wird die Informationspolitik gegenüber Medien und Bevölkerung jetzt einheitlich durch das Zentrum Operative Information gesteuert.

<sup>86</sup> vgl. Bischoff 2009. Nach Bischoff bildet SAR Lupe auch die Grundlage für eine noch engere deutsch-französische Kooperation auf dem Gebiet der Satellitenaufklärung. Gemeinsam mit dem französischen optischen Satelliten Helios II bildet es den Kern des europäischen Satellitenaufklärungsverbundes ESGA.

<sup>87</sup> Scheidges 2010a, S.2-3

<sup>88</sup> vgl. Wilson 2008, S.12

<sup>89</sup> vgl. Kanwal 2009

<sup>90</sup> vgl. USAF 2010a, S.2

verstärkte Kooperation, Stärkung des Problembewusstseins und Weiterbildung zur Erhöhung der Sicherheit beitragen sollen. Während die Nationale Sicherheitsstrategie (**National Strategy to Secure Cyberspace**) die defensiven Elemente betont, konzentriert sich die militärische Cyberstrategie (**National Military Strategy for Cyberspace Operations (NMS-CO)**) mehr auf die operativen Aspekte.

Die USA haben ihre Cyberwarkapazitäten über zwei Jahrzehnte systematisch aufgebaut und koordiniert<sup>91</sup>.

1988 errichtete das US-Verteidigungsministerium (Department of Defence DoD) als Reaktion auf die erste Computerwurminfektion von 60.000 Unix-Computern mit dem Morris-Wurm ein Notfallteam für Computerzwischenfälle (Computer Emergency Response Team CERT) an der Carnegie-Mellon University<sup>92</sup>.

1992 wurde das erste defensiv ausgerichtete Programm zur informationellen Kriegführung ins Leben gerufen, das Defensive Information Warfare Program, dem 1995 ein konkretisierender Management Plan folgte.

Ab 1996 richteten die drei Teilstreitkräfte Luftwaffe, Marine und Heer eigene Zentren zur informationellen Kriegführung ein, so dass das Pentagon 1998 als Koordinationsplattform die Joint Task Force for Computer Network Defense einrichtete.

Mit der wachsenden Bedeutung der Materie folgten eigene Cyber Commands auf der Ebene der Teilstreitkräfte<sup>93</sup>, so dass die USA als logischen Endpunkt der Entwicklung 2010 ein eigenes zentrales **Cyber Command (US CYBERCOM)** errichtet haben, das Ende Mai 2010 mit ca. 1000 Beschäftigten die Arbeit aufnahm und dem Direktor der National Security Agency NSA, General Keith Alexander, unterstellt ist<sup>94</sup>. Das US CYBERCOM ist dem strategischen Kommando US STRATCOM unterstellt, das übergeordnet für die Planung und Ausführung von Operationen im Cyberspace zuständig ist<sup>95</sup>.

Das US CYBERCOM wird jedoch nur die Websites mit der vom US-Militär genutzten Domain ‚mil‘ schützen, während das Heimatschutzministerium Department of Homeland Security DHS weiterhin für die zivile Regierungsdomain ‚gov‘ zuständig sein wird<sup>96</sup>. Die NSA rüstet sich auch zum offensiveren Umgang mit China<sup>97</sup>.

Eine erste große Übung, mit die USA ihre Abwehrbereitschaft getestet hat, war das sogenannte **elektronische Pearl Harbour** der US-Navy aus dem Jahre 2002, bei der erstmals ein Grossangriff auf kritische Infrastrukturen simuliert wurde.

---

<sup>91</sup> vgl. Hiltbrand 1999

<sup>92</sup> vgl. Porteuos 2010, S.3

<sup>93</sup> USAF: 24th Air Force, Army Forces Cyber Command (ARFORCYBER), Fleet Cyber Command (FLTCYBERCOM) und das Marine Forces Cyber Command (MARFORCYBER)

<sup>94</sup> vgl. Hegmann 2010, S.5, The Economist 2010, S.9/22-24, Glennly 2010, S.23

<sup>95</sup> vgl. USAF 2010a, S.21-22

<sup>96</sup> vgl. Porteuos 2010, S.7

<sup>97</sup> vgl. Barnford 2010

Seither wird der Begriff des ‚elektronischen Pearl Harbour‘ häufig als Metapher für drohende Gefahren im Cyberspace verwendet.

Regelmäßige Übungen sind die **Cyber Storm Exercises**, wobei bisher Cyber Storm I-III in den Jahren 2006, 2008 und 2010 unter der Leitung des Department of Homeland Security (DHS) stattfanden, bei denen ebenfalls Grossangriffe auf die IT-Infrastruktur der USA getestet wurden.

Im März 2007 wurde durch die Idaho National Laboratories (INL) der **Aurora Generator test** durchgeführt, bei dem die Sabotage von Stromgeneratoren durch eine Cyberattacke überprüft wurde. Es gelang tatsächlich, den Stromgenerator durch Schadprogramme lahmzulegen.

Auch die chinesische Führung hat sich intensiv mit der Materie auseinandergesetzt und baut wie viele andere Staaten Cyberwar Kapazitäten auf und aus.

Der Cyberwar ist eine relativ kostengünstige Waffe und ermöglicht, zu anderen Staaten weitaus rascher aufzuschließen als durch massive Ausgaben zur Modernisierung konventioneller Waffen („leapfrog strategy“). Das heißt nicht, dass der Cyberwar konventionelle Waffen ersetzen kann oder soll, vielmehr stellt er eine die eigenen Fähigkeiten rasch erweiternde zusätzliche Kampfmethode dar, die sich sehr gut in das Konzept der ‚**aktiven Verteidigung**‘ einbauen lässt, bei dem es um die frühzeitige und gezielte Ausschaltung der möglichen Gegenschlagskapazitäten des Gegners geht<sup>98</sup>.

Außenpolitisch hat China das Problem, von Staaten umgeben zu sein, die China nicht unbedingt positiv gegenüberstehen bzw. mit den USA verbündet sind<sup>99</sup>, wie z.B. Japan, Taiwan und Südkorea, so dass China (noch) nicht ernsthaft in der Lage ist, den USA im Falle eines ersten Konfliktes (z.B. um Taiwan) nachhaltigen physischen Schaden zuzufügen. Der Cyberwar kennt das Entfernungsproblem nicht und erlaubt eine asymmetrische Kriegführung und seine Vorbereitung bzw. das Training im Zuge der Cyberspionage wirft obendrein viele nutzbringende Informationen ab.

Die Analyse der chinesischen Cyberwar-Strategie durch Northrop Grumman hat die Schwachstellen vernetzter Sicherheitseinrichtungen deutlich gezeigt<sup>100</sup>. Man kann im militärischen Sektor drei Bereiche abgrenzen, nämlich als ersten Bereich das normale Netz, dann Netzabschnitte mit gewissen Sicherungen als zweiten Bereich für kritische Infrastrukturen und militärnahe Einrichtungen und als dritten Bereich das militärische Hochsicherheitsnetz<sup>101</sup>. Beim Cyberwar könnte auch ein

---

<sup>98</sup> Kanwal 2009, S.14

<sup>99</sup> vgl. Rogers 2009

<sup>100</sup> vgl. Krekel et al. 2009

<sup>101</sup> In den USA sind dies das mit dem normalen Internet verbundene Non-classified Internet Protocol Router Network NIPRNET, das Secret Internet Protocol Router Network SIPRNET und das Joint Worldwide Intelligence Communication System JWICS; auf deutsche Verhältnisse übertragen, wäre die Datenbank JASMIN im dritten Level, die IT-Plattform der Bundeswehr HERKULES im zweiten Level anzusiedeln.

Schlag gegen den zweiten Bereich die Handlungsfähigkeit der vernetzten Kriegsführung schon erheblich beeinträchtigen<sup>102</sup>.

Der zweite Bereich der USA, das gesicherte **Secret Internet Protocol Router Network SIPRNET**, leidet auch darunter, dass es inzwischen zu groß geworden ist und zu viele Zugangsberechtigte hatte<sup>103</sup>, wie die Debatten nach den aus dem SIPRNET stammenden WikiLeaks-Enthüllungen vom 28.11.2010 gezeigt haben<sup>104</sup>.

Mögliche Gegenmaßnahmen gegen die umfangreiche Entwendung von Daten, sei es von innen wie beim Wikileaks-Vorfall oder durch Cyberangriffe von außen sind z.B. die **Segmentierung** durch ein vertikal nach Dienstgraden und horizontal nach Zuständigkeiten gestuftes System von Zugangsberechtigungen, Blockaden von Druck- und Downloadfunktionen z.B. durch **Dokumentenmanagement-systeme**, und die heute technisch einfach realisierbare Nachverfolgung von Zugriffen und downloads (**tracking**). Auch die Übermittlung von Nachrichten über gesonderte Kanäle trägt dem bewährten **need to know-Prinzip** (jeder bekommt nur die Informationen, die für die Aufgabe notwendig sind) Rechnung<sup>105</sup>. In einem ersten Schritt haben die USA die Zahl der Zugangsberechtigten verkleinert<sup>106</sup>.

Die chinesische Strategie besteht darin, zunächst das gegnerische Netzwerk zu treffen, um dann die resultierende ‚operative Blindheit‘ des Gegners mit konventionellen Waffen zu überprüfen und ggf. weiter vorzugehen<sup>107</sup>. Natürlich besteht das Risiko, dass der Gegner sein Netz wieder repariert, so dass diese Strategie auf lange Sicht erfolglos sein kann; um so wichtiger ist es, in der Frühphase des Konflikts die Oberhand zu gewinnen und die „elektromagnetische Dominanz“ so lange wie möglich zu behalten. Die Strategie ist natürlich riskant, falls sich der Gegner unerwartet schnell regeneriert oder nicht im gewünschten Ausmaß getroffen werden kann. US-Studien zeigen, dass sich ein solcher Krieg wohl nur über einen sehr begrenzten Zeitraum wirksam führen lässt.<sup>108</sup>

Für die Zukunft der Computer- und Internetindustrie dürfte aber ein ganz anderer Faktor viel ernstere Auswirkungen auf den Westen haben: China besitzt einen 97%igen Marktanteil<sup>109</sup> an seltenen Erden (speziellen Industriemetallen), die für

---

<sup>102</sup> wie man sich so einen Schaden denken kann, zeigte der Internet-Wurm **Conficker**, der zur Jahreswende 2008/2009 sein Unwesen trieb. Dieser traf auch die Bundeswehr und französische Marine schädigte; unter anderem mussten Kampffjets mussten zwei Tage auf dem Boden bleiben, vgl. Leppegrad 2009.

<sup>103</sup> Es handelte sich um 2,5 Millionen Zugangsberechtigte und 280.000 Personen für die höhere Geheimhaltungsstufe; vgl. Schneider 2011, S.9

<sup>104</sup> vgl. Schaaf 2010, S.9

<sup>105</sup> vgl. Sattar et al. 2010, S.3

<sup>106</sup> vgl. Schneider 2011, S.9

<sup>107</sup> vgl. Krekel et al. 2009

<sup>108</sup> vgl. Tinner et al. 2002.

<sup>109</sup> vgl. Büschemann/Uhlmann 2010, S.19

die IT- und Elektronik-Industrie unersetzlich sind und die bisher nicht hinreichend wirtschaftlich recycelt können, und China schränkt vor dem Hintergrund eines wachsenden Eigenbedarfs bei gleichzeitig schwindenden bekannten Vorräten zunehmend das Exportvolumen ein<sup>110</sup>. Der hohe Marktanteil kam durch die zunächst konkurrenzlos billigen Lieferungen aus China zustande, weshalb andere Marktteilnehmer aufgaben; nun wird die Exploration außerhalb Chinas unter Hochdruck wieder aufgenommen<sup>111</sup>.

#### **4.4 Die Cyberpolitik der Europäischen Union**

Im Unterschied zu den USA und China besteht die Europäische Union EU aus 27 Nationalstaaten. Sicherheitslücken in nationalen Computersystemen sind jedoch hochsensitive Informationen; ein Austausch mit anderen offenbart die Schwachstellen, daher überwiegt zwischen den Nationalstaaten trotz allem noch das Misstrauen.

Dies hat mit einem Sicherheitsproblem zu tun. Verschlüsselte Kommunikation kann auch als Plattform für Terroristen dienen, so dass es aus nachrichtendienstlicher Sicht erforderlich ist, Zugriffe auf die Schlüssel oder die Quellcodes der Verschlüsselungssoftware zu haben, um nach Maßgabe der gesetzlichen Regelungen ggf. Zugriff auf diese Daten zu haben. In Deutschland wird dies seit 2002 durch die **Telekommunikations-Überwachungsverordnung (TKÜV)** geregelt, vergleichbare Regelungen gibt es inzwischen praktisch in allen Staaten, so z.B. in den USA, wo die **National Security Agency NSA** Zugriff auf die Quellcodes der Verschlüsselungssoftware hat<sup>112</sup>. Die nationalen Zugriffsrechte haben aber zur Folge, dass man sich mit einer ausländischen oder internationalen IT-Plattform auch die anderen Nachrichtendienste ins Haus holt<sup>113</sup>. Obwohl die Informationstechnologie und die Cyberattacken globale Angelegenheiten sind, fördert die IT-Sicherheit paradoxerweise nationale Lösungen.

In den meisten Staaten gibt es inzwischen Computersicherheitsteams, die bei sicherheitsrelevanten Vorfällen Warnungen herausgeben und Gegenmaßnahmen erarbeiten. Derartige Teams werden als **Computer Emergency Response Team (CERT)** bzw. als **Computer Security Incident Response Team (CSIRT)** bezeichnet. Die europäische **European Government CERT Group EGC** hat aber immer noch nur 10 Mitglieder (Finnland, Frankreich, Deutschland<sup>114</sup>,

---

<sup>110</sup> vgl. Mayer-Kuckuck 2010, S.34-35, vgl. auch Mildner/Perthes 2010, S.12-13, Bardt 2010, S.12 und Schäder/Fend 2010, S.3

<sup>111</sup> vgl. FAZ 2010d, S.12, Bierach 2010, S.11

<sup>112</sup> Scheidges 2010b, S.12-13

<sup>113</sup> Scheidges 2010b, S.12-13

<sup>114</sup> Zur deutschen Gruppe CERT-Bund siehe Website des BSI

Niederlande, Norwegen, Ungarn, Spanien, Schweden, England, Schweiz)<sup>115</sup>. Andererseits sind Cyberattacken ein globales Problem, so dass die Nationalstaaten von einem verbesserten Informationsaustausch profitieren würden, so dass die EU das zentrale Problem der europäischen Cyberpolitik 2010 wie folgt zusammenfasst: „Die Wirkung einer besseren Zusammenarbeit wäre sofort spürbar, doch sind zunächst kontinuierliche Bewusstseinsbildung und Vertrauensaufbau erforderlich.“<sup>116</sup>

Die Hoffnungen der EU ruhen nun ganz auf ihrer Agentur **ENISA (Europäische Agentur für Netzwerksicherheit, European Network and Information Security Agency)**, die 2004 mit der Verordnung 460/2004 mit 33 Mio. Euro Budget und 50 Angestellten errichtet wurde und 2005 die Arbeit aufnahm. Die Agentur befindet sich in Heraklion auf Kreta am äußersten südlichen Rand der EU, was nicht gerade als zweckmäßig gilt<sup>117</sup>.

Die ENISA arbeitete seit 2004 u.a. an Übersichtsstudien zur Netzwerksicherheit und an verbesserten Verschlüsselungsmethoden; die Kryptographieforschung gehört auch zu den Aktivitäten des laufenden Forschungsrahmenprogramms der EU<sup>118</sup>. Das Mandat der ENISA wurde 2008 unverändert bis März 2012 verlängert. Die ENISA, deren neuer Direktor Dr. Udo Helmbrecht, der ehemalige Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist, wird seit 2009 unter anderem mit folgenden Maßnahmen systematisch zum Zentrum der europäischen Cyberpolitik ausgebaut:

- die ENISA soll nach den neuen EU-Plänen gegen Cyberwar die Zusammenarbeit zwischen nationalen/staatlichen Notfallteams (CERT) stärken<sup>119</sup>, u.a. durch die Förderung und Ausweitung bestehender Kooperationsmechanismen wie der ECG-Gruppe
- Die ENISA hat 2009 eine vergleichende Analyse der EU- und EFTA-Staaten veröffentlicht, in der u.a. die sehr unterschiedlich geregelten Zuständigkeiten im Bereich der Netzwerksicherheit, der unzureichende Aufbau von CERTs und deren mangelnde Kooperation sowie unzureichende Prozeduren bei der Berichterstattung sicherheitsrelevanter Ereignisse (*incident reporting*) festgestellt wurden. Es wurden Empfehlungen für verbesserte Prozesse und zu einer verstärkten Kooperation unter Federführung der ENISA gegeben<sup>120</sup>.

---

<sup>115</sup> ECG 2008, Website der ECG Nov 2010. Weitere CERT-Foren, an denen die deutsche CERT-Bund beteiligt ist, sind FIRST (Forum of Incident Response and Security Teams) und TI (Trusted Introducer).

<sup>116</sup> vgl. EU 2010b. Im Rahmen der Zusammenarbeit im Bereich Innere und Justiz wurde zwar schon 2006 ein Europäisches Programm für den Schutz kritischer europäischer und nationaler Infrastrukturen (EPSKI) verabschiedet, jedoch kam erst nach dem Cyberangriff gegen Estland 2007 wirklich Bewegung in die Sache

<sup>117</sup> EU-ISS 2007

<sup>118</sup> ENISA 2007

<sup>119</sup> EU 2007, EU 2009b

<sup>120</sup> vgl. ENISA 2009

- Im Einklang mit den Plan zum Schutz kritischer Infrastrukturen von 2009<sup>121</sup> richtete die ENISA die 2010 die erste europäische Übung **Cyber Europe 2010** aus, an der 22 Länder mit 70 Organisationen aktiv und 8 weitere Länder als Beobachter beteiligt waren und insgesamt 320 Stresstests durchgeführt wurden<sup>122</sup>. Jedoch zeigten sich auch bei dieser Übung die uneinheitlich geregelten Zuständigkeiten innerhalb der EU und die mangelnden Strukturen kleinerer Staaten<sup>123</sup>. Nach der Auswertung sollen in die nächste Übung auch privatwirtschaftliche Akteure miteinbezogen werden.

Zudem will die Kommission eine **europäische öffentlich-private Partnerschaft für Robustheit (EÖPPR)** für eine verbesserte Sicherheit und Robustheit einrichten und ein Europäisches Informations- und Warnsystem (EISAS) schaffen, das sich an Bürger und kleine und mittelständische Unternehmen (KMU) richten soll. Begleitend sollen EU-einheitliche Kriterien für kritische Informationsinfrastrukturen in Europa festgelegt werden<sup>124</sup>.

Großbritannien und Frankreich haben im November 2010 eine umfassende Militärkooperation vereinbart, bei der auch die Kooperation im Bereich des Cyberwars angestrebt wird<sup>125</sup>.

---

<sup>121</sup> vgl. EU 2009b

<sup>122</sup> vgl. ENISA 2010a, ENISA2010b

<sup>123</sup> vgl. Mertins 2010, ENISA 2010a: „There is a lack of pan-European preparedness measures to test. This reflects the fact that many Member States are still refining their national approaches.”

<sup>124</sup> vgl. EU2009b, auch EU 2010b

<sup>125</sup> vgl. Thibaut/Alich 2010, S.15

## 4.5 Die Cyberabwehr der NATO

Die in Mons bei Brüssel angesiedelte **NATO Communication and Information Systems Services Agency NCSA** betreut umfassend die Informations- und Kommunikationssysteme der NATO<sup>126</sup> und bildet im Rahmen des 2002 verabschiedeten NATO Cyber Defense Programms die vorderste Verteidigungslinie der NATO zum Schutz ihrer eigenen IT-Infrastruktur<sup>127</sup>.

Innerhalb des NCSA ist das für Kommunikations- und Computersicherheit zuständige NATO Information Security Technical Centre (NITC) angesiedelt, das sich wiederum in das Nato Computer Incident Response Capability Technical Centre (NCIRC) für die Behandlung von sicherheitsrelevanten Vorfällen (incidents) und das Nato Information Security Operations Centre für die zentrale Betreuung und das Management des NATO-Computernetzwerks gliedert.

Seit dem Angriff auf Estland 2007 widmet die NATO auch dem Schutz der Mitgliedsstaaten vor Cyber-Angriffen vermehrte Aufmerksamkeit.

Im Mai 2008 wurde das der NATO im Bereich Cyberwar zuarbeitende **Cooperative Cyber Defence Centre of Excellence (CCD CoE, estnisch: K5 oder Küberkaitse Kompetentsikeskus)** in Tallinn, Estland, ins Leben gerufen<sup>128</sup>, das bisher von Estland, Litauen, Lettland, Italien, Spanien, der Slowakei und Deutschland unterstützt wird und 30 Mitarbeiter umfasst. Das CCD CoE wird also bisher nur von wenigen NATO-Mitgliedern unterstützt<sup>129</sup>, wobei Polen 2011 beitreten will. Bisher fanden als NATO Cyber Defence Übungen **Digital Storm** und **Cyber Coalition** 2008, 2009 und 2010 statt, wobei das CCD CoE diese Übungen gemeinsam mit dem NCIRC und anderen NATO-Einrichtungen organisierte<sup>130</sup>. Mit Schweden hat das CCDCoE im Mai 2010 die Übung **Baltic Cyber Shield** durchgeführt.

Im November 2010 wurde auf dem Gipfel in Lissabon eine neue NATO-Strategie beschlossen mit dem Ziel, die Aktivitäten im Cyberwarbereich zu intensivieren und zu koordinieren („*bringing all NATO bodies under centralized cyber protection*“)<sup>131</sup>.

---

<sup>126</sup> vgl. Schuller 2010, S.6

<sup>127</sup> vgl. NCSA 2009a-c

<sup>128</sup> Faktisch hat das CCD CoE nach einer 2004 von Estland ausgehenden Initiative schon seit 2006 existiert, vgl. CCDCoE 2010a

<sup>129</sup> Die NATO will sich im Falle eines Cyberangriffes im ersten Schritt lediglich auf Konsultationen stützen, vgl. von Kittlitz 2010, S.33

<sup>130</sup> vgl. Wildstacke 2009, S.28/29, CCDCoE 2010b

<sup>131</sup> vgl. NATO 2010. Die NATO sieht nicht nur den Cyberwar, sondern alle Arten von Cyberattacken als relevant an, die von Hunker 2010 auch als cyber power bezeichnet werden.

## 5 Literaturquellen

- ArcSight (2009): Cyberwar: Sabotaging the System. Managing Network-Centric Risks and Regulations. ArcSight White Paper Research 021-111609-03
- Bardt, H. (2010): Rohstoffe für die Industrie. Frankfurter Allgemeine Zeitung Nr. 275/2010, S.12
- BBC News (2009): Major cyber spy network uncovered. 29. März 2009
- Bierach, B. (2010): Australien will Seltenerdmetalle fördern. Neue Zürcher Zeitung 18.12.2010, S.11
- Bischoff, M. (2009): Kommando Strategische Aufklärung (Kdo StratAufkl) -Stand Juli 2009, <http://www.manfred-bischoff.de/KSA.htm>
- Büschemann, K.-H., Uhlmann, S. (2010): Deutschland braucht eine Rohstoffstrategie. Süddeutsche Zeitung vom 15.10.2010, S.19
- Busse, N. (2007): Krieg im Cyberspace. Frankfurter Allgemeine Zeitung 22.11.07, S.10.
- CCD CoE (2010a): History and way ahead. Website des Cooperative Cyber Defence Centre of Excellence. <http://www.ccdcoe.org/12.html>
- CCD CoE (2010b): CCD COE Supports NATO's "Cyber Coalition 2010". <http://www.ccdcoe.org/212.html>
- Die Welt (2007): US-Geheimdienst kontrolliert Windows Vista. [http://www.welt.de/wirtschaft/webwelt/article707809/US\\_Geheimdienst\\_kontrolliert\\_Windows\\_Vista.html](http://www.welt.de/wirtschaft/webwelt/article707809/US_Geheimdienst_kontrolliert_Windows_Vista.html)
- DHS (2008): The Cyber-Terror Threat. New Jersey Office of Homeland Security and Preparedness 7 pages
- Eberbach, H.E. (2002): Neuorientierung des Militärischen Nachrichtenwesens der Bundeswehr <http://www.europaeische-sicherheit.de/alt/ausgaben/10oktober2002/1002,04.html>
- ENISA (2009): Analysis of Member States' Policies and Regulations. Policy Recommendations, 112 pages
- ENISA (2010a): Interim findings of CYBER EUROPE 2010, the First Pan-European Cyber Security Exercise; a successful 'cyber stress test' for Europe. Press release 10 Nov 2010
- ENISA (2010b): Q&As on the first, pan-European Cyber Security Exercise 'CYBER EUROPE 2010'.
- EU (2007): Mitteilung der Kommission an das Europäische Parlament über die Bewertung der Europäischen Agentur für Netzwerk- und Informationssicherheit (ENISA). (Europäische Kommission, KOM(2007) 285 endg.

EU (2009a): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Internet of Things — An action plan for Europe COM(2009) 278 final

EU (2009b): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" COM(2009) 149 final

EU (2010): Bürgerinfo EU-Vorschlag – Schutz kritischer digitaler Systeme

EU-ISS (2007): Chaillot Paper No. 76 des Europäischen Institutes für Sicherheitsstudien EU-ISS

Falliere, N. (2010): Stuxnet Introduces the First Known Rootkit for Industrial Control Systems. Meldung von Symantec 06.08.2010, <http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices>

FAZ (2010a): Rätselhaftes Schadprogramm Stuxnet. Frankfurter Allgemeine Zeitung Nr. 224/2010, S.17

FAZ (2010b): Amerika gehen die Drohnen aus. Frankfurter Allgemeine Zeitung Nr. 230/2010, S.6

FAZ (2010c): Iran erfolgreich sabotiert? Frankfurter Allgemeine Zeitung Nr. 275/2010, S.6

FAZ (2010d): Australien sichert Japan seltene Erden zu. Frankfurter Allgemeine Zeitung Nr. 275/2010, S.12

FAZ (2010e): Getöteter Iraner mit Stuxnet befasst. Frankfurter Allgemeine Zeitung Nr. 280/2010, S.5

FAZ (2010f): Amazons Wikileaks-Rauswurf nährt die Zweifel an der Cloud. Frankfurter Allgemeine Zeitung Nr. 283/2010, S.17

FAZ (2010g): Bundesregierung plant „Cyber-Abwehr-Zentrum“. Frankfurter Allgemeine Zeitung Nr. 302/2010, S.14

Fischermann, T. (2010): Attacke im Sicherungskasten. Die Zeit Nr.38/2010, S.26

Fritz, J. (2008): "How China will use cyber warfare to leapfrog in military competitiveness," Culture Mandala: The Bulletin of the Centre for East-West Culture and Economic Studies, Bond University, Vol. 8, No. 1, October 2008, pp.28-80

Gaycken, S. (2009): Die Zukunft des Krieges –Strategische Konzepte und strukturelle Konzepte des Cyberwarfare. Paper. Universität Stuttgart, 18 S.

Gaycken, S. (2010): Wer war's ? Und wozu? In: Die Zeit Nr.48/2010, S.31

Georgien (2008): Russian Invasion of Georgia – Russian Cyberwar on Georgia. Stellungnahme der georgischen Regierung vom 10 November 2008. <http://georgiaupdate.gov.ge>

Glenny, M. (2010): Die neuen Cyberkrieger. Financial Times Deutschland, 12.10.2010, S.23/26

Goetz, J, Rosenbach, M., Szandar, A. (2009): Krieg der Zukunft. In: Der Spiegel 7/2009, S.34-36

Grant, R. (2010): Battling the Phantom Menace. Air Force Magazine April 2010, S.38-42

Handelsblatt (2010): Update macht Programme von Microsoft sicherer. Handelsblatt vom 14.10.2010, S.27

Hegmann, G. (2010): Rüstungsindustrie verteidigt Internet. Financial Times Deutschland, 02.06.2010, S.5

Herwig, M. (2010): Die @-Bombe. Welt Am Sonntag Nr.39, 29.06.2010. S.60-61

Hiltbrand, R.K. (1999): Cyberwar: Strategic Information Warfare. Presentation Originally published Spring 1999, 6 pages

Hürther, T. (2010): Das automatisierte Töten. Die Zeit Nr. 29, S.21

Hunker, J. (2010): Cyber war and cyber power. Issues for NATO doctrine. Research Paper No. 62 - November 2010 of the NATO Research College, Rome

Iran Daily (2010): Stuxnet hits Computers. 26 July 2010, S.2

ISIS (2010): Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security Report by David Albright, Paul Brannan, and Christina Walrond, 22 Dec 2010, 10 S.

Kanwal, G. (2009): Emerging Cyber War Doctrine. Journal of Defence Studies Vol 3. No 3. July 2009, page 14-22

Kaspersky (2010): Stuxnet-Trojaner öffnet Zero-Day-Lücke in Windows. Meldung des Kaspersky Lab ZAO vom 19.07.2010

Kittlitz, A. von (2010): Stuxnet und der Krieg, der kommt. Frankfurter Allgemeine Zeitung Nr.283/2010, S.33

Knop, C. (2010): Jetzt kommt die Cloud. Frankfurter Allgemeine Zeitung Nr.229/2010, S.14

Knop, C., Schmidt, H. (2010): Unternehmen und Staaten im Cyberkrieg. Frankfurter Allgemeine Zeitung Nr.237/2010, S.20

Könen, J., Hottelet, U. (2007): Tagesgeschäft Spionage. Handelsblatt Nr. 171/2007, S.2

Krekel, B. (2009): Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network. Exploitation Prepared for The US-China Economic and Security Review Commission. Northrop Grumman Corporation. October 9, 2009

Krüger, P.A., Martin-Jung, H., Richter, N. (2010): Der Wurm und der Luftballon. Süddeutsche Zeitung vom 02./03.10.2010, S.9

Ladurner, U., Pham, K. (2010): Iran im Krieg 2.0. Die Zeit Nr.40, S.12

Leppegrad, L. (2009): Ihr Rechner ist besetzt! Die Zeit Nr.10/2009, S.34

Libicki, M. C. (2010): Cyberdeterrence and cyberwar. Prepared for the United States Air Force. Project Air Force of the Rand Corporation.

Markoff, J., Barboza, D. (2010): 2 China Schools Said to Be Tied to Online Attacks. Published: February 18, 2010 New York Times

Mayer-Kuckuck, F. (2010): China verknappt exotische Rohstoffe. Handelsblatt 10/11.09.2010, S.34-35

Mayer-Kuckuck, F., Hauschild, H. (2010): Chinesischer Huawei-Konzern wehrt sich gegen Generalverdacht. Handelsblatt 26.08.2010, S.28

Megill, T.A. (2005): The Dark Fruit of Globalization: the hostile use of the internet. An USAWC Strategy Research Project. 18 March 2005

Mehan, J.E. (2008): CyberWar, CyberTerror, Cybercrime. Role of Process in a Changing and Dangerous Cyber Environment. Presentation 20 pages, IT Governance Ltd 2008

Menn, A. (2010): Schutz vor dem Wolkenbruch. Handelsblatt Topic Cloud Computing vom 02.12.2010, S.H12-H13

Mertins, S. (2010): Manöver gegen Web War II. Financial Times Deutschland 11.11.2010

Mildner, S., Perthes, V. (2010): Der Kampf um Rohstoffe. Handelsblatt Nr.235/2010, S.12-13

NATO (2010): "Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation", 11 S. Adopted by Heads of State and Government in Lisbon

Nazario, J. (2009): Politically Motivated Denial of Service Attacks. The proceedings of the Conference on Cyber Warfare 2009, IOS press.  
[http://www.ccdcoe.org/publications/virtualbattlefield/12\\_NAZARIO%20Politically%20Motivated%20DDoS.pdf](http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf)

NCSA (2009a): The Mission Priority 1: Support to NATO operations: Combating Cyber attacks. [http://www.ncsa.nato.int/topics/combating\\_cyber\\_terrorism.htm](http://www.ncsa.nato.int/topics/combating_cyber_terrorism.htm)

- NCSA (2009b): Where does NCSA fit in the NATO structure?  
[http://www.ncsa.nato.int/ncsa\\_in\\_nato\\_struc.html](http://www.ncsa.nato.int/ncsa_in_nato_struc.html)
- NCSA (2009c): NATO Communication and Information Systems Services Agency (NCSA), Sector Mons (Formerly Regional Signal Group SHAPE – RSGS) Unit History (As of: March 2005)
- Neuneck, G., Alwardt, C. (2008): The Revolution in Military Affairs, its Driving Forces, Elements and Complexity. Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg/Working Paper 13/2008
- Northrop Grumman TASC (2004): Cyber Warrior Hacker Methodology. Presentation, 44 S.
- Porteous, H. (2010): Cyber security and Intelligence: the US approach. The Parliamentary Information and Research Service of the Library of Parliament of Canada, International Affairs, Trade and Finance Division 8 February 2010, 14 pages
- Postinett, A. (2008): Wolken-Reich. Handelsblatt Nr.245/2008, S.12
- Quirin, I. (2010): Vorfahrt fürs Netz. FTD Dossier Intelligente Netze 15.10.2010, S.2-7.
- Rieger, F. (2010): Du kannst Dich nicht mehr verstecken. Frankfurter Allgemeine Zeitung Nr.43/2010, S.5
- Rogers, J. (2009): From Suez to Shanghai: the European Union and Eurasian maritime security. Occasional Paper - n°77, March 2009
- Rosenbach, M., Schmitz, G.P., Schmundt, H. (2010): Mord ohne Leiche. Spiegel 39/2010, S.163.
- Rüb, M. (2010): Jenseits der Partnerschaftsrhetorik. Frankfurter Allgemeine Zeitung Nr. 129/2010, S.5
- Sattar, M., Löwenstein, M., Carstens, P. (2010): Vertrauliches, Geheimes und streng Geheimes. Frankfurter Allgemeine Zeitung Nr.279/2010, S.3
- Schaaf, S. (2010): Wikileaks verstreut massenhaft schmutzige Wäsche. Financial Times Deutschland 29.11.2010, S.9
- Schäder, B., Fend, R. (2010): Peking macht seltene Erden noch rarer. Financial Times Deutschland 30.12.2010, S.3
- Scheidges, R. (2010a): „Herkules“ versagt im Praxistest. Handelsblatt April 2010, S.2-3
- Scheidges, R. (2010b): Bundesamt misstraut US-Firmen. Handelsblatt 02.12.2010, S.12-13
- Schmitt, J. (2009): Virtuelle Spürhunde. Der Spiegel 10/2009, S.83

- Schneider, W. (2011): Das Unheimliche am Internet. Neue Zürcher Zeitung NZZ Folio Januar 2011, S.9
- Schröder, T. (2008): Was Du siehst, sehe ich auch. Frankfurter Allgemeine Sonntagszeitung Nr.3, S.58
- Schuller, K. (2010): Der Spion, der aus dem Cyberspace kam. In: Frankfurter Allgemeine Sonntagszeitung Nr.51 vom 26.12.2010, S.6.
- Schultz, S. (2010): Virenjäger sezieren Sabotage-Software. Spiegel online 01.10.2010, <http://www.spiegel.de/netzwelt/netzpolitik/0,1518,720681-2,00.html>
- Singer, P.W. (2010): Der ferngesteuerte Krieg. Spektrum der Wissenschaft Dezember 2010, S.70-79
- Stark, H. (2009): Digitale Spionage. Der Spiegel 11/2009, S.33
- Steinmann, T. (2010): Deutschland im Visier der Cyberkrieger. Financial Times Deutschland 29.12.2010, S.10
- Stokes, G. (2005): Cyber Security Fundamentals: What You Should Know About Protecting Data & Systems Orus Group LLC, Orus Group Cyberwar Institute
- Symantec (2010): W32.Stuxnet Dossier by Nicolas Falliere, Liam O Murchu, and Eric Chien. Version 1.3. November 2010, 64 S.
- Thibaut, M., Alich, H. (2010): Paris und London besiegeln Militärkooperation. Handelsblatt Nr.213/2010, S.15
- Tinnel, L.S., Saydjari O.S., Farrell D. (2002): Cyberwar Strategy and Tactics. An Analysis of Cyber Goals, Strategies, Tactics, and Techniques. Proceedings of the 2002 IEEE Workshop on Information Assurance. United States Military Academy, West Point, NY June 2002, p.228-233
- Uhlmann, P. (2010): Informationsprofis arbeiten enger zusammen. Truppe für Operative Information - Übergabe InfoOp. Stand vom: 01.07.2010 [http://www.opinfo.bundeswehr.de/portal/a/opinfo/unsere\\_l/zopinfo/infoop/uebergabe](http://www.opinfo.bundeswehr.de/portal/a/opinfo/unsere_l/zopinfo/infoop/uebergabe)
- USAF (2010a): US Air Force Doctrine Document (AFDD) 3-12, Cyberspace Operations 15 July 2010, 55 S.
- USAF (2010b): US Air Force Doctrine Document (AFDD) 3-13, Information Operations 17 September 2010, 54 S.
- Vistica, G. (1999): We're in the Middle of a Cyberwar. Newsweek 13.09.1999
- Werner, K. (2010): Siemens zieht in den Cyberkrieg. Financial Times Deutschland 21.12.2010, S.7
- White Wolf Security (2007): Estonia and Cyberwar – Lessons Learned and Preparing for the Future By White Wolf Security, 3 pages, 6 April 2007

Wildstacke, N. (2009): Cyber Defence –Schutzlos in einer vernetzten Welt? Das CERT Bundeswehr Bonn 16.02.2009 Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr. Präsentation 31 S.

Wilson, C. (2007): Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues. CRS Report for Congress Order Code RL31787. Updated June 5, 2007

Wilson, C. (2008): CRS Report for Congress: Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress Updated January 29, 2008 Clay Wilson, Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division Order Code RL32114

## **6 Literaturhinweis**

Möchten Sie mehr über die Sicherheitspolitik und ihre Grundlagen erfahren?  
Das **Kompendium der Sicherheitspolitik** bietet Ihnen kompaktes und hochaktuelles Grundlagenwissen.

**Kompendium der Sicherheitspolitik**

**440 Seiten**

**EUR 29,80**

**Verlag Dirk Koentopp, Osnabrück**

**2., erweiterte Auflage 2011**

**ISBN: 978-3-938342-26-8**

**[www.dirk-koentopp.com](http://www.dirk-koentopp.com)**