

# **Angriff aus den Tiefen des Cyberspace**

Kriminelle, militärische und strategische  
Anwendungen von Cyber-Waffen

Ein Positionspapier der  
**JANUS** Consulting  
in Kooperation mit der Sicherheits-Fachzeitschrift  
**SECURITY *insight***

## **Inhaltsverzeichnis**

Für die Sicherung des unternehmerischen Erfolges!.....	3
Wider die IT-Ignoranz!.....	4
Executive Summary.....	5
Die Anfänge.....	6
Die Fauna des Netzes: die kriminelle Ebene.....	7
Entwicklung der Cyber-Kriegsführung.....	9
Militärische Anwendung des Cyber Warfare: die operative Ebene.....	11
DDoS-Angriffe und kritische Infrastruktur: die strategische Ebene.....	13
Der (Cyber)-Krieg: ein wahres Chamäleon.....	15
Fazit.....	19
Unter Mitwirkung von.....	20

## **Für die Sicherung des unternehmerischen Erfolges!**

Die globalisierte Wirtschaft, das Machtstreben einzelner Staaten und der verständliche Wunsch von Mitbewerbern nach „Vorsprung durch Informationen“ stellen unsere Unternehmen heute vor ganz neue Herausforderungen.

Der Konkurrenzkampf, also der Kampf um Marktanteile, Zukunftstechnologien und -produkte wird durch die Wirtschaftskrise noch verschärft. Fakt ist, dass in Zeiten der Rezession oder der Stagnation der weltweiten Nachfrage nach Produkten oder Dienstleistungen immer mehr Unternehmen bewusst wird, dass sie ihr künftiges Wachstum nicht mehr durch wachsende Absatzmärkte, sondern nur noch auf Kosten der direkten Konkurrenz und deren Marktanteile erreichen können. Dies wird als weitere Konsequenz haben, dass Unternehmen sich verstärkt dazu entschließen werden, neue Märkte und Regionen, die sicherheitskritisch sind, zu entwickeln.

Der Verdrängungswettbewerb, der Kampf um Marktanteile und Kunden wird härter, das Bewahren angestammter Positionen eine noch größere Herausforderung. Bisher gut abgeschottete Traditionsmärkte, Stamm- und Zukunftsprodukte werden nun verstärkt ins Visier der (inter-)nationalen Konkurrenz genommen.

Unternehmen, die in ihrer bisherigen Struktur von Dauer schienen, verschwinden, werden übernommen oder übernehmen andere. Die zur Verfügung stehende Zeit, Entscheidungen zu treffen, schwindet. Die Bedeutung von Informationen als „Ressource“ und als Wettbewerbsfaktor sowie der Drang nach Erkenntnis über die weitere Entwicklung steigen weiter an.

Sicherheitsrisiken und -gefahren sind mehr denn je Risiken ökonomischer Natur geworden. Unternehmenssicherheit und Informationsschutz können gar nicht anders, als Tendenzen frühzeitig zu erkennen und bereits im Vorfeld Strategien zur Krisenprävention und -bekämpfung im Rahmen eines Intelligence-orientierten, betriebswirtschaftlich fundierten Selbstverständnisses zu entwickeln. Agieren statt reagieren, verhindern statt ertragen! Unternehmenssicherheit und Informationsschutz als Garanten des unternehmerischen Erfolges. Weg vom Kostenfaktor hin zum unabdingbaren Erfolgsfaktor.

Denn kein Unternehmen erzielt langfristige Erfolge, wenn seine materiellen und immateriellen Werte ungeschützt sind.



**Karl Stefan Schotzko**, GF  
VSW Verband für Sicherheit in der  
Wirtschaft Baden-Württemberg e.V.

## Wider die IT-Ignoranz!

Es ist keine Schande, beim Dreisatz zu zögern, bei den drei Newton'schen Gesetzen zu passen oder die Grundlagen chemischer Gleichungen nicht zu beherrschen. Aber wehe, es hapert an Heine und Dürrenmatt, von Goethe ganz zu schweigen! In der gesellschaftlichen Akzeptanz von mangelndem Allgemeinwissen herrscht zwischen den Mathematik- und Naturwissenschaften auf der einen und den Geisteswissenschaften auf der anderen Seite ein seltsames Missverhältnis. Der Mathe-Ignorant darf mit gönnerhafter Nachsicht rechnen, der Unbelesene dagegen trifft auf Unverständnis, ja Verachtung.

Kurioserweise ist das in Gesellschaft, Wirtschaft und Politik mit Blick auf die moderne Informationstechnologie (IT) nicht anders. Seinen Machiavelli sollte der Machtpolitiker ebenso wie der CEO intus haben. Letzterer lässt zudem auch gerne durchblicken, dass er die Märkte versteht, die Finanzen im Griff hat und strategisch-marketingtechnisch-kommunikations-theoretisch auf der Höhe der Zeit ist. Sein Sicherheitschef hebt gern hervor, wie gut er die Ermittlungsarbeit beherrscht. Aber bei beiden hapert es meist am Verständnis für die IT-Zusammenhänge; man ist schließlich nur „Anwender“. Gewiss, Viren, Würmer und Trojaner sind gefährlich. Und Hacker auch. Die zu bekämpfen delegiert jeder Konzernlenker an seinen Sicherheitschef und der wiederum an seine Spezialisten aus der IT-Abteilung. Der Außenminister twittert gern, der Innenminister surft regelmäßig. Aber was wirklich in der digitalen Welt passiert, wissen auch sie nicht aus erster Hand, sondern lassen es sich ebenfalls von ihren Spezialisten erklären.

Die Diskrepanz zwischen den segensreichen Möglichkeiten des Cyberspace und den gleichzeitig daraus erwachsenden immensen Gefahren für die Funktionsfähigkeit dieser Welt ist erschreckend. Gewiss, Militär- und Sicherheitsbehörden sowie Konzerne unternehmen große Anstrengungen, Bedrohungs- und Verteidigungsszenarien aufzustellen sowie technische und auch mentale Maßnahmen zu ergreifen, um die digitalen Infrastrukturen sicher(er) zu machen. Doch nach nun fast 20 Jahren der dominanten Präsenz von Internet und Netzwerken geht die Entwicklung nur schleppend voran, vor allem was das konzertierte Zusammenwirken aller Kräfte angeht. Die Leistungsfähigkeit der Datenübertragung für die ganze Welt ist schneller gesteigert als das IT-Sicherheitskonzept für ein mittelständisches Hightech-Unternehmen erarbeitet – denn der schnelle Bildaufbau beim Surfen liegt einem näher als die schwarze Seele eines anonymen Wirtschaftsspions in Fernost.

Hinzukommt, dass die Einstellung gegenüber IT und IT-Sicherheit eine Generationenfrage ist. Die vor 1970 Geborenen sind erst im Erwachsenenalter an die Digitalwelt herangeführt worden – diese Generation bildet einen Großteil der heutigen Entscheidungsträger. Die „cyberspace-ferne“ Sozialisation bestimmt die Prioritäten nicht nur bei der Gefahrenwahrnehmung, sondern – mehr noch – bei der Gefahrenbekämpfung. Das mag als Erklärung dienen, genügt aber nicht als Ausrede! Die Bedrohung aus dem Cyberspace wächst mit jedem Tag. Wenn ihre Bekämpfung nicht Schritt hält, ist es nur eine Frage der Zeit, bis aus dem derzeit herrschenden „Kalten Cyber-Krieg“ ein realer „Cyber-Krieg“ hervorgeht. Den Dreisatz nicht zu beherrschen ist ebenso peinlich wie den „Faust“ nicht Goethe zuordnen zu können. Akzeptieren wir nicht länger die mit einem entschuldigenden Lächeln verbundene IT-Ignoranz jener, die über unsere Sicherheit entscheiden.



**Marcus Heide**  
Chefredakteur **SECURITY insight**

## Executive Summary

Kriminelle, militärische und strategische Einsätze von Cyber-Waffen sind Realität. Privatpersonen, Firmen und sogar Länder stehen im Visier der Angreifer und nur selten werden die Angreifer aus dem Cyberspace sichtbar. Die informationsintensivsten Gesellschaften sind am anfälligsten für Angriffe und Störungen durch Cyber-Attacken. Wettbewerber suchen nach Bauplänen, Kalkulationen und Blaupausen, die Unternehmen digital gespeichert haben. Mit dem Ende des Wirtschaftsbooms und einer drohenden Absatzkrise ringen Marktteilnehmer und ihre Berater mit allen Mitteln um Aufträge und ihre Zukunft. Gezielt werden Nachrichten über Privatpersonen und Firmen in Umlauf gebracht, um ihre Reputation negativ zu beeinflussen.

Angreifer können Regierungen, NGOs<sup>1</sup>, aber auch frustrierte Einzeltäter sein. Dabei haben diese Angriffe auf die Reputation von Unternehmen nicht nur große finanzielle Schäden zur Folge, sondern eben auch die nachhaltige Schwächung der Wettbewerbsposition. Dabei verstoßen diese Operationen nicht unbedingt gegen das Gesetz, sondern werden häufig innovativ unter Ausnutzung sämtlicher Kommunikationsmöglichkeiten mit dem Ziel geführt, die Glaubwürdigkeit des Gegners zu untergraben. Die Einbeziehung des „Web 2.0“ ist unumgänglich in dieser Art der wirtschaftlichen Kriegsführung.

Schon die Konflikte der Gegenwart werden auf dem Boden, in der Luft, zur See, im Weltraum und eben im Cyberspace geführt. So ist es im vergangenen Jahr den Taliban in Afghanistan kurzfristig gelungen, mit einer handelsüblichen Software den Datenstrom einer „Predator“-Drohne anzuzapfen. Der nächste Schritt wäre ein „Angriff per Mann in der Mitte“<sup>2</sup> auf diese Datenströme. In einem solchen Fall würde der Feind die Datenströme manipulieren und ein falsches Lagebild vortäuschen. So könnte ein geplanter Angriff auf feindliche Stellungen ein Krankenhaus oder sogar die eigenen Stellungen treffen. US-Präsident Barak Obama hat die Gefahr von Cyber-Angriffen auf das Militär und die amerikanische Wirtschaft erkannt und diese als die größte Herausforderung und Bedrohung für die Vereinigten Staaten genannt. Am 20. Mai 2010 benannte er den Vier-Sterne-General Keith Alexander als obersten Befehlshaber des neuen „Cyber Command“, eine Einheit, die den Kampf gegen Cyber-Angriffe führen soll. Seine Einheit umfasst 30.000 Soldaten, weitere 90.000 Mitarbeiter aus dem Verteidigungsministerium stehen ihm ebenfalls zur Verfügung.

Im Vergleich dazu stehen die Bemühungen in Europa, sich vor dieser neuen Form der Kriegsführung zu schützen, nicht einmal am Anfang. Es besteht kein permanenter Dialog auf nationaler oder europäischer Ebene zwischen Regierungen, Wirtschaft und Militär. Unternehmen verfügen nur selten über Schutzmaßnahmen. Schlimmer noch: Viele Unternehmen haben gar keine Schutzmaßnahmen gegen Cyber-Attacken eingeführt.

Auch haben Unternehmen ihre kommunikativen Verteidigungsmaßnahmen nicht dieser neuen Bedrohung angepasst. Was zur Folge hat, dass diese bei Attacken meist „kalt erwischt“ werden. Dabei können Unternehmen gezielt entgegenwirken, indem sie möglichst frühzeitig Themen identifizieren, die positiv besetzt werden können, und diese dann gezielt im Fall eines Angriffs kommunizieren. Gleichzeitig sollten in einer Phase des direkten Angriffes durch aggressive Mitbewerber oder „pressure groups“<sup>3</sup> die Schwachstellen des Gegners aufgeklärt werden, um hier mit kommunikativen Mitteln Reputation und Glaubwürdigkeit des Gegners gezielt zu schwächen. Hier zeigen sich bei vielen Unternehmen Fähigkeitslücken, die nur durch Ausbildung und Training geschlossen werden können.

Cyber-Krieg mag in erster Linie ein militärisches Thema sein, skrupellose und kriminelle Gegner in der Welt der Wirtschaft bedienen sich aber schon heute derselben Mittel wie die Militärs. Für Firmen ist es deshalb zunehmend wichtig, sich dem Thema Cyber-Security zuzuwenden und durch geeignete Maßnahmen ihr Unternehmen vor diesen Angriffen zu schützen. Die Zeit damit zu beginnen war gestern.

---

1 Non-Governmental Organization (Nichtregierungsorganisation)

2 Beim Angriff „per man in the middle“ (Angriff per Mann in der Mitte) belauscht der Hacker eine Kommunikation zwischen zwei Gesprächsparteien und verfälscht den Austausch, indem er sich als eine der beiden ausgibt.

3 Interessenverbände, Lobby- oder Aktionsgruppen

## Die Anfänge

Es dauerte fast 20 Jahre, bis aus einem Kuckucksei ein Quantensprung wurde. Im August 1986 war der Astronom Clifford Stoll, als er nach einem winzigen Abrechnungsfehler<sup>4</sup> im Computersystem des Lawrence Berkeley National Laboratory (LBNL) suchte, auf Spuren eines Eindringlings gestoßen, der sich über das Telefonnetz unbefugt Zugang zu geheimen LBNL-Dateien verschafft hatte. Mit Hilfe der Deutschen Bundespost gelang es Stoll, diese zu einem Hacker aus Hannover zurückzuverfolgen, der im Auftrag des sowjetischen Geheimdienstes KGB<sup>5</sup> in Datenbanken für die amerikanische Strategische Verteidigungsinitiative (SDI) eingedrungen war. Schon damals konnte der deutsche Hacker verschiedene Rechner so manipulieren, dass er Zugriffsrechte auf die dortigen Benutzerkonten erlangen konnte. Dies beschrieb Stoll später in seinem Buch<sup>6</sup> als das „Ausbrüten eines Kuckuckseis“.

Zwischenzeitlich ist die Nutzung von Computernetzwerken und des Internets zur Selbstverständlichkeit geworden. Nicht nur unser Alltagsleben ist ohne sie für die Informationsgewinnung, die Kommunikation, das Online-Banking und die Kreditkartennutzung, die „Just-in-Time“-Produktion sowie den Online-Handel und Ähnliches nicht mehr vorstellbar. Auch sind die postindustrialisierten Länder vom Informationsmanagement und den **Steuerungsprozessen** (SCADA<sup>7</sup>) in ihrer **kritischen Infrastruktur** extrem abhängig geworden.

Stromversorgungsnetze und Kraftwerke, Flugsicherungssysteme sowie der elektronische Geldverkehr- und Börsenhandel sind nur wenige Beispiele für Netzwerke, die unsere Zivilisation aufrechterhalten. Störung oder Unterbrechung derselben hätte gravierende Folgen für Sicherheit und Wohlstand der postindustriellen Gesellschaften der Nordhalbkugel. Die Angriffe aus dem Internet, denen schon ganze Staatswesen ausgesetzt waren<sup>8</sup> lassen erahnen, wie in Zukunft nicht-kinetische Angriffe auf ganze Staaten aussehen könnten.

Auch auf rein militärischem Gebiet ist die Vernetzung von Rechnern mit Sensoren und Effektoren unabdingbar für die Kommunikation, Kontrolle, Steuerung, Nachrichtengewinnung, Aufklärung und Überwachung (C4ISR) von Streitkräften – und somit für den militärischen Erfolg geworden.

Fast 20 Jahre nach dem ersten Angriff aus dem Netz auf Daten der US Air Force vollzog diese mit ihrem Mission Statement vom Dezember 2005 (To fly and fight in Air, Space and Cyberspace) einen programmatischen Quantensprung, der der atemberaubenden technischen Entwicklung auf dem Gebiet der Elektronik Rechnung trug. Neben Land, Meer, Luft, Weltraum, dem elektromagnetischen Spektrum und der menschlichen Psyche ist der Cyberspace eine eigenständige Dimension menschlicher Existenz geworden. Ein Aufenthalts-, Bewegungs- und Aktivitätsraum, der große Chancen und Möglichkeiten bietet, aber auch große Gefahren birgt.

---

4 Ein Unbekannter hatte neun Sekunden Computerrechenzeit in Anspruch genommen, ohne dafür zu zahlen.

5 „Komitee für Staatssicherheit“

6 „Kuckucksei. Die Jagd auf die deutschen Hacker, die das Pentagon knackten“ - Verlag: Krueger W. - Dezember 1993 - ISBN-10: 381051862X

7 Supervisory Control and Data Acquisition

8 Estland im April/Mai 2007 und Georgien im August 2008

## Die Fauna des Netzes: die kriminelle Ebene

Im Juli 2001 löste das Auftreten des Web-Wurms „Code Red“, der die Internet Information Server Software von Microsoft (IIS, ein Teil des Betriebssystems „Windows“, der es erlaubt, den eigenen PC als Webserver einzurichten) infiziert hatte, erstmals die Besorgnis aus, dass das Internet als Ganzes lahmgelegt werden könnte.

Im Gegensatz zu **Viren**, die sich immer in ein Wirtsprogramm einnisten müssen, um sich zu vermehren, sind **Würmer** eigenständige, sich selbst replizierende Programme und meist viel „ansteckender“.

Hierbei lief der Angriff, der auf die Web-Seiten des Weißen Hauses gerichtet war, in mehreren Phasen ab: In der Vorbereitungs- bzw. Rekrutierungsphase identifizierte „Code Red“ verwundbare (ungepatchte) IIS-Programme auf Computern, um sie zu infizieren. Damit wurden die infizierten Computer/Server in einen so genannten Zombie (Computer, der ohne Wissen des Betreibers zu Internet-Angriffen genutzt werden kann) verwandelt. Ab dem 12. Juli 2001 rekrutierte „Code Red“ zunächst nur ca. 20.000 Zombies. Die intensive Rekrutierungsphase begann am 19. Juli 2001, als innerhalb von 14 Stunden 359.000 Rechner/Server in Zombies verwandelt wurden. Durch die intensive Rekrutierung und Kommunikation mehrerer Generationen von Zombies untereinander wurde die Datenübertragungsfähigkeit des Internets stark in Anspruch genommen. Das Internet hatte seine Belastungsgrenzen erreicht, sodass das Internet Storm Center bei incidents.org die Alarmstufe „Orange“ auslöste; eine Stufe unter „Rot“, was den Zusammenbruch des Internets bedeutet.

Am nächsten Tag überschwemmte dieses Zombie-Netzwerk die Server, auf denen die Webseiten des Weißen Hauses abgelegt waren, mit einer Flut von Anfragen und drohten diese lahm zu legen. Die schnelle Reaktion der Administratoren dieser Server, die deren IP-Adressen änderten, ließ diese Attacken aber weitgehend ins Leere laufen. Am 29. Juli forderte das Weiße Haus in einer Pressekonferenz alle Nutzer der IIS-Software von Microsoft auf, ihre Rechner gegen die Übernahme durch den „Code Red“-Wurm zu schützen. Bei der zweiten Angriffswelle konnten die Betreiber dieses illegalen **Bot-Netzes** nur auf die bislang noch nicht geschützten 175.000 Rechner zurückgreifen, sodass sich die Störung des Internets in Grenzen hielt.

Angriffe aus dem Internet, die der Verweigerung von Dienstleistungen von Servern und Programmen dienen, werden als Denial of Service (**DoS**) oder, wenn sie von Zombies aus koordinierten Bot-Netzen erfolgen, als Distributed Denial of Service (**DDoS**) bezeichnet.

Die Liste der erkannten DDoS-Angriffe im wirtschaftlichen und politischen Bereich weist schon eine beträchtliche Länge auf. Angefangen von der Lahmlegung der Internetdienste von Yahoo und CNN im Februar 2000 bis zur Blockierung der Server von InternetX im Januar 2010, wodurch der Zugriff auf die dort „gehosteten“ Internetseiten kaum oder gar nicht möglich war. Diese Attacken können beträchtliche Schäden verursachen. So wird geschätzt, dass die mehrtägigen DoS-Angriffe auf Microsoft einen Schaden in Höhe von 500 Millionen US-Dollar verursacht haben.

Die „Dienstleistungen“ von Bot-Netzen, mit deren Hilfe auch Spam-E-Mails verschickt werden können, werden von kriminellen Betreibern zu Preisen von 10 bis 40 \$ pro Stunde angeboten, damit missgünstige Zeitgenossen ihren Konkurrenten Schaden zufügen können.<sup>9</sup>

---

<sup>9</sup> Zurzeit werden ca. 43 % der Spam-Mails durch das Bot-Net „Rustock“ mit einem Bestand von 150.000 Zombies verschickt.

Angriffe aus Bot-Netzen werden auch zur Erpressung von Firmen genutzt, deren Internet-Dienstleistungen blockiert werden. Für die Unterlassung dieser Angriffe muss dann die Firma „Schutzgeld“ zahlen. So wurde zum Beispiel im August 2005 versucht, von der FLUXX AG ein Lösegeld von 40.000 Euro zu erpressen.

Ebenso wurden Würmer – wie der „W32/Leaves“ – speziell für die Fernsteuerung privater PCs entwickelt: das Computer Emergency Response Team der Carnegie Mellon University zählte über 23.000 Zombies in dem von diesem Wurm angelegten Bot-Netz: Das größte dieser Bot-Netze, mit Namen „Conficker“, das erstmals am 21. November 2008 entdeckt wurde, wird auf die sagenhafte Zahl von 10 Millionen Zombies geschätzt.

Auch politische Konfrontationen können Auslöser für Cyber-Schlachten sein: Nachdem im April 2001 ein chinesisches Jagdflugzeug und ein amerikanisches Aufklärungsflugzeug vor der Küste Chinas zusammenstießen<sup>10</sup>, tobte ein regelrechter Internetkrieg zwischen amerikanischen und chinesischen Hackern. In dessen Folge wurden ca. 600 chinesische und 1.000 amerikanische Webseiten zerstört. Selbst DDoS-Angriffe sind in diesem Zusammenhang erfolgt.

Ebenso griffen nach den Terroranschlägen des 11. September 2001 amerikanische Hacker Webseiten des iranischen Innenministeriums, der palästinensischen Autonomiebehörde und der Taliban-Partei in Afghanistan an.

Eine weitere Angriffsmöglichkeit im Internet besteht im Einsatz so genannter **Trojanischer Pferde** oder kurz **Trojaner**<sup>11</sup> genannt. Hiermit werden Computerprogramme bezeichnet, die als nützliche Anwendung getarnt sind und ohne das Wissen des Nutzers mehr oder weniger schädliche Anwendungen im Computer ausführen. Sie zählen ebenfalls zu den unerwünschten beziehungsweise schädlichen Programmen, der so genannten **Malware**<sup>12</sup>.

Trojaner werden oft gezielt in Computer eingeschleust, können aber auch durch Zufall über externe Medien (Internet, CD/DVD, Sticks) in den Computer gelangen. Sie werden hauptsächlich zur Ausspähung des Datenverkehrs oder der Benutzeraktivitäten – bis hin zur Anfertigung eines Protokolls der Tastatureingaben und dessen Weiterleitung – verwendet. Auch sensible Daten wie Passwörter, Bankverbindungen oder Kreditkartennummern werden von ihnen an Unbefugte übermittelt. Ebenso können sie illegale Dialer-Programme<sup>13</sup> oder unerwünschte Werbung aus dem Internet einblenden. Schließlich kann sogar der ganze Rechner durch einen Trojaner fremdbestimmt werden.

Im März 2010 wurde in Boston der Hacker Albert Gonzales zu 20 Jahren Gefängnis verurteilt. Er hatte im bisher größten Fall von Kreditkartenbetrug in den USA mit zwei russischen Komplizen mehr als 130 Millionen Kredit- und Lastschriftkartennummern ausspioniert. Ab Oktober 2006 hatte Gonzales Hackerangriffe auf die Computerdienstleister großer Einzelhandelsunternehmen und Finanzinstitute gestartet. Mehr als 250 Unternehmen waren von diesem „Datenklau“ betroffen, den Gonzales anschließend für Finanztransaktionen missbrauchte.

---

<sup>10</sup> Die amerikanische EP-3 E musste in China notlanden und die Besatzung wurde zunächst in Gewahrsam genommen.

<sup>11</sup> Benannt nach der in der Ilias überlieferten List des Odysseus im Trojanischen Krieg, griechische Kämpfer im Bauche eines hölzernen Pferdes hinter die Stadtmauer von Troja zu schmuggeln – insofern ist die Kurzform „Trojaner“ irreführend.

<sup>12</sup> Schadprogramme

<sup>13</sup> Einwahlprogramme

## Entwicklung der Cyber-Kriegsführung

Der Begriff „Cyber-Krieg“ wurde erstmals von John Arquilla und David Rohnfeldt in ihrem Artikel „Cyberwar is coming“ in der Zeitschrift „Comparative Strategy“ (April 1993) verwendet.

In seiner **engeren militärischen Bedeutung** werden darunter hochtechnisierte Unterstützungsmaßnahmen im Zusammenhang mit militärischen Operationen verstanden, die auf der Computerisierung, der Elektronisierung und der Vernetzung fast aller militärischen Bereiche basiert. Hierbei ist er Teil der „Information Operations“ (IO)<sup>14</sup> und wird in der militärischen Fachsprache als „Computer Network Operations“ bezeichnet.

In seiner **allgemeinen Bedeutung** wird unter „Cyberwar“ eine kriegerische Auseinandersetzung in und um den virtuellen Raum mit den Mitteln der Informationstechnik verstanden.

Die hauptsächlichlichen Methoden des Cyber-Krieges bestehen aus den folgenden Techniken:

1. **Spionage:** Das illegale Eindringen in fremde Computernetze zum Zweck der Erlangung geheimer Informationen.
2. **Defacement:** Die Veränderung von Website-Inhalten, um Propaganda zu verbreiten oder den Betreiber zu diskreditieren.
3. **Social Engineering:** Das Erschleichen des Vertrauens von Benutzern durch falsche E-Mails oder gefälschte Webseiten zur Erlangung sensibler Daten, z. B. Kreditkartennummern, Passwörter etc.
4. **Datenmanipulation:** Die Zerstörung oder Veränderung fremder Daten, ohne dass dies der Benutzer bemerkt, sodass dadurch Computeroperationen fehlschlagen oder falsche Ergebnisse liefern.
5. **DDoS-Angriffe:** Distributed Denial of Service: mit Hilfe von – in Bot-Netzen zusammengefassten – Zombie-Computern ausgeführten Angriffe zur Blockierung von Internet-Diensten oder der Manipulation/Zerstörung sensibler Infrastruktureinrichtungen.
6. **Kontrollverlust:** Übernahme der Kontrolle in Computern/Netzwerken oder die Lahmlegung derselben durch das Einschleusen von Trojanern oder durch schon beim Bau installierte Hardware- oder Softwarekomponenten.

Im „**Virtual Criminology Report**“<sup>15</sup> der Internet-Sicherheitsfirma McAfee aus dem Jahr 2007 wurde festgestellt, dass es in 120 Staaten Entwicklungen an Cyber-Waffen gäbe. John Green, der Vizepräsident des McAfee Avert Laboratory, kommt in diesem Bericht zu dem Schluss, dass sich Cyber-Kriminalität zu einem signifikanten Problem entwickelt habe und eine globale Herausforderung darstelle. Sie sei heute nicht nur eine Bedrohung für Individuen und der Industrie, sondern zunehmend auch eine Bedrohung für die nationale Sicherheit.<sup>16</sup>

---

<sup>14</sup> Der Begriff „Information War“ wurde ab 1976 geprägt. Heute umfassen die Information Operations neben den „Computer Network Operations“ die PSYOPS (psychologische Kriegsführung), Military Deception (Täuschmaßnahmen), Operations Security (Schutz der eigenen Informationen) und elektronische Kampfführung.

<sup>15</sup> McAfee Virtual Criminology Report 2007, Santa Clara, November 2007, S. 12

<sup>16</sup> Demgegenüber wird im McAfee Virtual Criminology Report 2009 festgestellt, dass bereits fünf Staaten (USA, Russland, China, Frankreich und Israel) über fortschrittliche Cyber-Waffen verfügen. McAfee Virtual Criminology Report 2009, Santa Clara, November 2009, S. 13

Laut dieses Berichts steht die Volksrepublik China an der Spitze der Entwicklungen für den Cyber-Krieg. Sie wird beschuldigt, wiederholt Cyber-Angriffe auf Computernetzwerke in Indien, Taiwan, Deutschland und in den USA unternommen zu haben. Im Juni 2007 erreichten die Anschuldigungen gegen China einen Höhepunkt, als die „Financial Times“ meldete, dass chinesische Hacker in die Computernetze des Pentagons eingedrungen seien und diese zeitweise sogar blockiert hätten.

Die USA sind aber ihrerseits an dieser Entwicklung nicht unbeteiligt: Im Jahr 1999 übernahm das Space Command der US-Luftwaffe die Federführung beim Aufbau des „Info War Team“, das beauftragt wurde, offensive Waffen für den Cyber-Krieg zu entwickeln. Im März 2004 schließlich gab das US-Verteidigungsministerium die Errichtung eines Information Operations Team mit dem Namen „Network Attack Support Staff“ bekannt.

Auch Israel zählt zu den fünf führenden Mächten in der Cyber-Kriegsführung. Das Land verfügt mit seiner geheimen „Einheit 8200“ auch über einen Eliteverband für den Kampf in der virtuellen Welt.<sup>17</sup>

Auf jeden Fall zählt in der Cyber-Welt Einfallsreichtum und Flexibilität mehr als materielle Überlegenheit, sodass auch kleine Staaten auf der gleichen Ebene Konflikte austragen können wie die Supermächte. Sogar Individuen sind nun in der Lage, ganzen Staaten erhebliche Schäden an ihrer kritischen Infrastruktur zu verursachen.

---

<sup>17</sup> Dafür musste sich Israel aber auch der bisher heftigsten DDoS-Angriffe erwehren. Während der 23-tägigen Militäroperationen gegen die palästinensische Terrororganisation Hamas vom 27. Dezember 2008 bis 18. Januar 2009 wurden israelische Regierungsw Webseiten von arabischen Hackern mit bis zu 15 Millionen E-Mails pro Sekunde bombardiert; es gelang ihnen aber nicht – dank geschickter israelische Abwehrmaßnahmen –, diese lahmzulegen.

## Militärische Anwendung des Cyber Warfare: die operative Ebene

Während der Luftkriegsoperationen der NATO gegen Serbien vom 24. März bis 10. Juni 1999 wurden erste nicht-kinetische Mittel der Informationskriegsführung zur Unterdrückung der integrierten Luftverteidigung Serbiens getestet. Nach dem Abschluss der Luftoperationen bemerkte der Chef der US Air Force Europe, General John Jumper, dass man statt über Störsender, die die gegnerischen Radaranlagen mit Elektronen bombardieren, lieber über Mikrochips reden sollte, die Elektronen so manipulieren, dass sie in das Herz und das Gehirn der gegnerischen SAM-10- oder SAM-12-Raketensysteme vordringen und Geräten „einreden“ können, dass sie nicht mehr länger Radargeräte, sondern Kühlschränke sind.

Einen weiteren Hinweis auf die Existenz solcher nicht-kinetischer Waffen erhielt die Weltöffentlichkeit durch den mysteriösen Luftangriff der israelischen Luftwaffe auf eine syrische Nuklearanlage an den Ufern des Euphrats am 6. September 2007.<sup>18</sup> Meldungen zufolge sollen anschließend russische Experten nach Syrien gereist sein, um zu untersuchen, warum die syrischen Luftabwehrsysteme – russischer Provenienz – die angreifenden israelischen Flugzeuge nicht bemerkt hatten.

Vertreter der US-Luft- und Raumfahrtindustrie und der US-Luftwaffe deuteten an, dass die Israelis eine Version des amerikanischen „Suter“-Airborne-Network-Attack-Systems verwendet hätten. Dieses System kann man als Revolution im gesamten Bereich der Kriegsführung bezeichnen.

Bisher bestanden nicht-kinetische Waffen zur Störung und Lahmlegung gegnerischer Sensoren und Kommunikationssysteme aus:

- HPM Hochenergie-Mikrowellen<sup>19</sup> (in Entwicklung)
- EMP Elektromagnetischem Puls<sup>20</sup>: elektromagnetische Störfelder, die von nuklearen Explosionen ausgelöst werden
- EMC Elektronische Gegenmaßnahmen<sup>21</sup>: Stör- und Täuschsender sowie Radar-täuschung (Düppel/Window/Chaff)
- Laser-Blend-Einrichtungen.

Das „Suter“-System sendet demgegenüber keine Energie oder Geräusche, sondern einen gezielten Strom aus Datenpaketen mit „Malware“ in die Empfangsantennen des Gegners. Dadurch ist es in der Lage, das ganze System zu korrumpieren, oftmals auch ohne dass der Gegner dies bemerkt. Hierdurch kann das System lahmgelegt, verwirrt oder gar die Kontrolle darüber übernommen werden – unabhängig davon, ob seine Verbindungen auf Kabel basieren oder drahtlos betrieben werden.

Es können auch irreführende Daten oder „Phantomziele“ eingespeist oder aber sichtbar gemacht werden, was der Gegner momentan auf seinem Radarschirm sieht. Auf diese Weise kann die US-Luftwaffe kontrollieren, ob ihre „Stealth“-Flugzeuge auf dem Radarschirm des Gegners erscheinen – die beim Einsatz von „Suter“ allerdings nicht mehr nötig wären.

---

18 Operation „Orchard“

19 High Power Microwave

20 Electromagnetic Pulse

21 Electronic Countermeasures

Im April 2008 testete die US Air Force in ihrer Übung JEFEX 08-3 die Version „Suter V“, die in der Lage ist, kinetische und nicht-kinetische Waffen sowie Aufklärungs- und Überwachungssensoren zu integrieren.<sup>22</sup>

Die US Air Force implementiert ihre Netzangriffsfähigkeiten sowohl auf globaler als auch auf lokaler Ebene durch Spezialisten, die in so genannten **Cyber-Cells** zusammengefasst und den jeweiligen Regionalkommandos zugeordnet sind. Jedes Team besteht aus offensiven Hackern, defensiven Netzwerk-Sicherheitsspezialisten und Spezialisten für elektronische Aufklärung, die die Schwachstellen der gegnerischen Systeme erkunden sollen.

Auch die US Army und das Marine Corps arbeiten mit „Viper“ und „Corporal“ an Systemen, um gegnerische Kommunikationssysteme auf nicht-kinetische Weise lahmzulegen.

„Cyber-Dominanz“ – die Überlegenheit im und die Kontrolle des Cyberspace – ist zum offiziellen Bestandteil der US-Militärstrategie geworden. Der Cyberspace wird einerseits als eigenständiger Kampfraum, andererseits auch als „Ermöglicher“ und „Unterstützer“ eigener militärischer Operationen gesehen.

Cyber-Operationen umfassen nach General Robert Elder<sup>23</sup>

1. den Schutz der eigenen Computer-Netzwerke und des eigenen elektromagnetischen Spektrums sowie die Abwehr gegnerischer Angriffe darauf
2. den Betrieb der eigenen Infrastruktur für die Aufrechterhaltung der Befehlskette, für Kontrolle, Kommunikation sowie den Betrieb der verschiedensten Aufklärungssensoren und die Erstellung eines sich daraus ergebenden Lagebildes
3. offensive Cyberspace-Operationen
4. Unterstützung eigener militärischer Operationen.

Für den Kampf im Cyberspace haben die US-Streitkräfte im Oktober 2009 das United States Cyber Command geschaffen, das die Cyber-Kommandos der drei Teilstreitkräfte und des Marinekorps vereinigt. Dieses Kommando koordiniert die Computer-Netzwerk-Verteidigung und die Cyber-Angriffsoperationen der US-Streitkräfte. Eigenen Angaben zufolge wurde es als Reaktion auf Einbrüche in Teile des US-Stromnetzes und das Eindringen in Datenbanken für das neue Kampfflugzeug F-35 gegründet.

Die US-Luftwaffe ihrerseits hat ihre Cyber-Angriffswaffen im 67. Network Warfare Wing (Geschwader) zusammengefasst, das der 24. United States Air Force unterstellt ist. Dieses, aus 8.000 Soldaten bestehende Geschwader, hat ca. 100 Standorte auf fünf Kontinenten; es ist verantwortlich für die Organisation, die Ausrüstung sowie für das Training der Cyber-Kampfkkräfte der US Air Force.

---

<sup>22</sup> Die US Air Force benutzte für die Lokalisierung der Ziele RC-135 Rivet Joint und für die Neutralisierung der Radar- und Kommunikationssysteme die EC-130 Compass Call. Bei der israelischen Luftwaffe sollen für diese Aufgaben die Flugzeuge Gulfstream 550 CAEW und SEMA benutzt werden.

<sup>23</sup> Kommandeur des kurzzeitig bestehenden US Air Force Cyberspace Command (8. Air Force)

## DDoS-Angriffe und kritische Infrastruktur: die strategische Ebene

Estland ist eines der am stärksten vernetzten Länder der Erde. Dank des Neuaufbaus der Infrastruktur nach der Unabhängigkeit von der Sowjetunion besitzt es eine weit fortgeschrittene Informations- und Kommunikationstechnik-Infrastruktur (IKT). Beim Ranking für E-Government<sup>24</sup> innerhalb der EU lag Estland auf dem dritten Platz. Hierbei werden 97 % aller Bankgeschäfte elektronisch abgewickelt. Die Abdeckung mit Handys erreicht 107 %; alle Schulen sind ans Internet angeschlossen und die Stimmabgabe per Internet bei öffentlichen Abstimmungen ist gelebte Realität („eStonia“).

Im April 2007 ließ die estnische Regierung ein russisches Kriegerdenkmal aus der Innenstadt Tallins auf einen Soldatenfriedhof verbringen. Dies löste nicht nur innerhalb der starken russischen Minderheit Estlands, sondern auch bei der russischen Regierung und innerhalb des russischen Volkes große Empörung aus. Danach wurde Estland nicht nur Ziel eines russischen Propagandafeldzugs sowie russischer Wirtschaftssanktionen, sondern auch Ziel heftiger Cyber-Angriffe. Diese Aktionen können als erste Cyber-Angriffe auf ein Staatswesen als Ganzes – und somit als strategisch – gewertet werden.

Diese Angriffe liefen in mehreren Phasen ab:

- 1) In der ersten Phase vom 27. bis 30. April 2007 waren spontane DoS- und DDoS-Angriffe zu beobachten, die auf kleinen Bot-Netzen basierten und die Webseiten der Regierung sowie estnischer Parteien und Nachrichtenagenturen zum Ziel hatten. Ebenfalls wurden durch Spam-Angriffe die E-Mail-Adressen estnischer Regierungsvertreter lahmgelegt.
- 2) In der zweiten Phase vom 30. April bis 18. Mai 2007 fanden koordinierte Angriffe statt, die auf größere Bot-Netze (rund eine Million Zombies) abgestützt waren. Sie beeinträchtigten zeitweise die kritische Informationsinfrastruktur Estlands. Server von Internet Service Providern waren ebenso das primäre Ziel – sodass zeitweilig die Netzwerke und damit auch die Kommunikationswege der Regierung unterbrochen waren. Weitere Angriffsziele waren die Webseiten des Parlaments, von Ministerien, Zeitungen und Radio- und Fernsehsendern. Auch wurden sämtliche Notrufnummern, Handynetze und der Kreditkartengeldverkehr zeitweise blockiert. Am 10. und 15. Mai befanden sich die beiden größten Banken Estlands (mit 85 % Marktanteil) im Visier der Hacker. Ebenfalls angegriffen wurden die Computer der Telefonvermittlung.
- 3) Nach dem 19. Mai 2007 kam es zu weiteren sporadischen DDoS-Angriffen.

Nach der im **McAfee „Virtual Criminology Report 2009 – The Age of Cyberwar“**<sup>25</sup> vorgestellten Skala für die Bewertung von Cyber-Angriffen hat es sich dabei um den in seinen Konsequenzen schwersten Cyber-Angriff auf einen Staat gehandelt<sup>26</sup>. Auf der bis „10“ reichenden Skala wurden die Estland-Angriffe mit „4“ bewertet, während die Angriffe auf Georgien im August 2008 mit „3“ und die Angriffe am 4. Juli 2009 auf das Weiße Haus und viele US-Ministerien, die New Yorker Börse und Yahoo – möglicherweise nordkoreanischen Ursprungs – mit „1“ bewertet wurden. Überrascht waren NATO-Experten auch von der raschen Reaktion der Hacker auf die estnischen Abwehrmaßnahmen – dies ließ auf sehr qualifizierte Angreifer schließen.<sup>27</sup>

---

24 Unter E- Government versteht man die Vereinfachung und Durchführung von Information und Kommunikation sowie Transaktionen zwischen staatlichen Behörden bzw. zwischen diesen Institutionen und Bürgern oder Unternehmen. durch den Einsatz digitaler Informations- und Kommunikationstechniken.

25 <http://resources.mcafee.com/content/NACriminologyReport2009NF>

26 Die Skala reicht von 1 bis 10; wobei 1-3 geringe Auswirkungen/kurze Dauer; 4-8 mittlere Auswirkungen/mittlere Dauer und 8-10 schwere Auswirkungen/lange Dauer bezeichnet.

27 Im März 2009 gab Sergei Markow, ein Duma Abgeordneter der Kreml- Partei „Vereinigtes Russland“ auf einer Podiumsdiskussion in Washington bekannt, dass die DDoS- Angriffe auf Estland von seinem Assistenten organisiert worden waren.

Die Angriffe auf Georgien im August 2008 zielten hauptsächlich auf die Fähigkeit des Landes, während des Kriegs mit Russland seinen politischen Standpunkt der Weltöffentlichkeit via Internet mitzuteilen. Hier waren die Webseiten des Präsidenten, der Regierung und von Nachrichtenagenturen die hauptsächlich Zielobjekte. Auffällig war die gute Koordination mit den gleichzeitig ablaufenden Operationen der russischen Streitkräfte.

Experten sind sich einig, dass es bisher noch keinen heißen „Cyber-Krieg“ gegeben hat, da noch keine Kritische Infrastruktur eines Landes angegriffen wurde. Das „Europäische Programm für den Schutz Kritischer Infrastrukturen“ vom 17.11.2005 identifiziert neun Sektoren, die als kritisch für die Sicherheit und das Wohlergehen der Gesellschaften der EU-Staaten zu gelten haben:

- 1) Energieanlagen und -netze (Strom, Öl, Gas)
- 2) Kommunikations- und Informationstechnologie (Fernmeldewesen, Rundfunk, Fernsehen)
- 3) Finanzwesen (Banken, Versicherungen, Investment)
- 4) Gesundheitswesen (Krankenhäuser, Rettungswesen, Pharmaindustrie, Blutversorgung, Laboratorien)
- 5) Lebensmittel (Produktionsmittel, Industrie, Großhandel)
- 6) Wasser (Staudämme, Aufbereitung)
- 7) Verkehr (Flughäfen, Leitsysteme, Häfen, Eisenbahnen, ÖPNV)
- 8) Erzeugung, Lagerung, Transport gefährlicher Güter
- 9) Staatliche Einrichtungen (wichtige Dienste, Anlagen, Denkmäler und Gedenkstätten).

Viele Unternehmen sind aus Kosten- bzw. Effizienzgründen dazu übergegangen, Steuerungsprozesse für Kraftwerke, Verkehrsmittel, Gesundheitseinrichtungen, Generatoren, Pumpen oder Turbinen über Fernwartung durchzuführen, was die Gefahren durch Cyber-Angriffe dramatisch erhöhen kann.

Schon im Jahr 1996 hatte die Studie des US-Verteidigungsministeriums „Information Warfare- Defence“ festgestellt, dass eine starke Verwundbarkeit der nationalen Infrastruktur besteht und dass die Bedrohung schnell zunehme. Manche Experten schätzen, dass eine Lahmlegung des Elektrizitätsnetzes in bestimmten Regionen der USA für zehn Tage 70 % aller ökonomischen Aktivitäten zum Erliegen bringen würde. Dass solche Befürchtungen nicht aus der Luft gegriffen sind, bewies ein Experiment des Idaho National Laboratory des US-Energieministeriums im März 2007. Hierbei gelang es Hackern, allein mit Malware einen laufenden Dieselgenerator, wie er in Kraftwerken eingesetzt wird, zur Selbstentzündung und damit zur Zerstörung zu bringen.

In einem Bericht des US-Rechnungshofes (GAO) vom Mai 2008 wurde der Tennessee Valley Authority, dem größten Stromversorger der USA, bescheinigt, dass er die Sicherheitsstandards für den Betrieb kritischer Computernetze nicht erfüllt habe (z. B. dass seine Firewalls leicht zu umgehen seien) und er somit durch Hacker äußerst verwundbar sei. Ebenso wurde durch einen Bericht des US-Verkehrsministeriums die Verwundbarkeit des Nationalen Luftverkehrskontrollsystems der Federal Aviation Administration (FAA) offengelegt. Hackern war es gelungen, an die Personaldaten von 48.000 Beschäftigten zu gelangen. Der Bericht kommt zu dem Schluss, dass von dieser Einbruchsstelle auch ein Angriff auf die operativen Luftverkehrskontrollsysteme möglich gewesen wäre. Allein im Rechnungsjahr 2008 wurde bei der FAA 800mal Cyber-Angriffsalarm gegeben. Tests bei den Computernetzwerken der FAA hatten fast 4.000 Schwachstellen aufgedeckt, von denen 763 als gravierend eingestuft wurden.

## Der (Cyber)-Krieg: ein wahres Chamäleon

„Der Krieg ist also nicht nur ein wahres Chamäleon, weil er in jedem konkreten Fall seine Natur etwas ändert, sondern er ist auch seinen Gesamterscheinungen nach, in Beziehung auf die in ihm herrschenden Tendenzen eine wunderliche Dreifaltigkeit, zusammengesetzt aus der ursprünglichen Gewaltsamkeit seines Elements, dem Hass und der Feindschaft (...), aus dem Spiel der Wahrscheinlichkeiten und des Zufalls (...) und aus der untergeordneten Natur eines politischen Werkzeugs.“ So charakterisierte Carl von Clausewitz vor 180 Jahren in seinem philosophischen Werk „Vom Kriege“ sowohl die Triebkräfte als auch die Unwägbarkeiten, Friktionen und Zufälle in der Kriegsführung. Diese Charakterisierung gilt für den Cyber-Krieg des 21. Jahrhunderts in ganz besonderem Maße.

Die Mysterien des Cyber-Krieges sind von vielfältiger Natur. Zunächst werden keine Soldaten und Armeen mit Panzern und Flugzeugen bewegt. Es fallen keine Schüsse und keine Bomben. Alles spielt sich im elektronischen Raum der Festplatten, Prozessoren und Verbindungslinien ab. Kampfmittel sind keine Explosivstoffe, sondern schriftliche Befehle an Rechenmaschinen, die durch das Internet verschickt werden. Die Vorbereitungen eines Angriffs sind unsichtbar, sodass ein Angriff oftmals nicht bemerkt wird, solange er die Funktion des Rechners nicht beeinträchtigt oder keine physischen Auswirkungen hat. Dass er aber große physische Auswirkungen haben kann, zeigt die große Verwundbarkeit der Kritischen Infrastrukturen ganzer Nationalstaaten.

Neben diesen Spezifika des Cyberspace kommen aber noch politische Unsicherheiten hinzu:

- Die erste betrifft die Akteure und die Zurechenbarkeit. Angriffe aus dem Cyberspace lassen sich sehr schwer zurückverfolgen und meist nicht eindeutig einem Täter oder einer Tätergruppe zuordnen. Ob der Angreifer kriminelle Absichten hatte oder Terrorgruppen oder staatliche Akteure politische Ziele verfolgten, kann nur mit einem hohen Unsicherheitsgrad nachvollzogen werden. Oft werden auch Hacker als Söldner von Kriminellen, Terrorgruppen oder staatlichen Akteuren angeworben, sodass sich ein regelrechtes Cyber-Söldnerwesen entwickelt hat. Oftmals bieten diese ihre „Dienste“ – mitsamt dem dazugehörigen Bot-Net – wie ein Dienstleistungsunternehmen an.
- Bei der Motivation der Angreifer kann es sich um einen kriminellen, wirtschaftlichen, politischen oder ideologischen Hintergrund handeln. Oftmals sind diese verschiedenen Motivationen aber nicht genau auszumachen oder sie gehen fließend ineinander über.
- Die Grenzen zwischen Spionage und Sabotage verschwimmen. Wenn ein Hacker erst einmal Zugang zu einem Computernetzwerk gefunden hat, kann er es bei der bloßen Spionage belassen, die Funktionsfähigkeit des Netzwerkes stören oder aber auch „Malware-Hintertüren“ (in einer Art „Schläferzustand“) zurücklassen, um einen künftigen Angriff zu ermöglichen. Der Schritt von der Spionage zur Sabotage sind dann nur noch einige wenige „Klicks“.

Experten sind sich einig, dass glücklicherweise noch kein wirklicher Cyber-Krieg stattgefunden hat, dass aber ein „Kalter Cyber-Krieg“ im Gange ist. Viele Staaten betreiben eine – weitgehend im Verborgenen ablaufende – Aufrüstung bei Netzwerk-Angriffswaffen. Es gibt genügend Anzeichen, dass Staaten Cyber-Waffen entwickeln, testen oder schon anwenden bzw. zu ihrer Anwendung anstiften.

Ähnlich wie im Kalten Krieg laufen auch heute im Cyberspace Geheimdienstoperationen ab. Diese können als eine Art „bewaffnete Aufklärung“ oder auch als „low intensity conflict“ angesehen werden, um sensible Daten des Gegners auszuspionieren, Schwachstellen und Eintrittspunkte in Computernetzen oder der Kritischen Infrastruktur zu erkunden bzw. um „Backdoor“-Programme für „Weapons of Mass Disruption“ zu hinterlassen.

Die geschilderte „Dreifaltigkeit“ von krimineller Ebene, operativ-militärischer und strategischer Ebene ist bestenfalls in einem analytischen Sinn voneinander zu trennen. In der Realität bilden sie ein Kontinuum, das fließend ineinander übergeht, oder Bereiche, die sogar gleichzeitig auftreten können. Auch dies trägt zur Mehrdeutigkeit und dem Mysterium des Cyber-Krieges bei.

Gerade diese Merkmale des Cyber-Krieges und die weitreichenden Konsequenzen, die ein erfolgreicher Angriff auf moderne Volkswirtschaften haben kann, machen die intensive theoretische und praktische Durchdringung des Themas sowie eine enge Kooperation der Wirtschaft mit den staatlichen Stellen unabdingbar.

Um sich besser gegen Angriffe aus dem Cyber-Raum schützen zu können, hat die NATO seit Oktober 2008 das **Cooperative Cyber Defence Centre of Excellence (CCD COE)**<sup>28</sup> akkreditiert. Es wurde in Tallin, Estland, eingerichtet und wird zurzeit von den drei baltischen Staaten, Deutschland, Italien, Spanien, der Slowakischen Republik und den USA betrieben.

Die hauptsächlichen Forschungs- und Aufgabenfelder dieses Zentrums sind:

- 1) Entwicklung eines rechtlichen Rahmens zur Verfolgung illegaler Cyber-Aktivitäten
- 2) Konzepte und Strategien für die Cyber-Verteidigung
- 3) Taktiken und Techniken der Cyber-Verteidigung
- 4) Schutz Kritischer Infrastrukturen.

Durch die Arbeit des Centres of Excellence soll die Interoperabilität innerhalb der Netzwerke der NATO-Länder verbessert, Doktrinen und Konzepte der Verteidigung entwickelt, der Informationsaustausch intensiviert, realitätsnahe Trainingskonzepte und Szenarien ausgearbeitet sowie einheitliche Standards innerhalb der NATO für die Cyber-Verteidigung entwickelt werden. Eine weitere Aufgabe des CCD COE ist die Schulung und Ausbildung qualifizierten Personals für die Cyber-Verteidigung.

Während unter Experten die Verwundbarkeit der Infrastruktur gegen Cyber-Angriffe eingehend diskutiert wird und Schutzmaßnahmen eingeleitet werden, ist die Problematik in der Öffentlichkeit der postindustrialisierten Länder noch weitgehend unbemerkt geblieben. Um dies zu ändern und die Reaktionsfähigkeit der USA auf strategische Cyber-Angriffe zu testen, führte das Bipartisan Policy Center in Washington am 16. Februar 2010 das hochrangig besetzte Planspiel „**Cyber Shock Wave**“ durch. Während der zwölf Stunden dauernden Simulation in einem Washingtoner Hotel wurde das Szenario eines massiven strategischen Cyber-Angriffs – verbunden mit Bombenanschlägen und einem Hurrikan – vor den Kameras von CNN durchgespielt. Die zehn Spieler, unter ihnen der ehemalige Minister für Heimatschutz, ein ehemaliger stellvertretender Außenminister und ein ehemaliger CIA-Chef, bildeten den „Nationalen Sicherheitsrat“. Dieser sollte im Planspiel den amerikanischen Präsidenten bei seinen politischen Reaktionen auf die Angriffe gegen die Kritische Infrastruktur beraten.

Das Szenario begann mit dem Ausfall von 60 Millionen Mobiltelefonen und setzte sich mit dem Zusammenbruch der Handels- und Finanztransaktionen im Internet fort. Schließlich brach in dem Szenario auch noch die nationale Stromversorgung zusammen und der Flugverkehr musste eingestellt werden. Gleichzeitig wurden Bombenanschläge auf Kraftwerke sowie auf Erdöl- und Erdgaspipelines verübt. Im Planspiel konnten die Angriffe zu einem Server aus Russland und einer Einzelperson im Sudan zurückverfolgt werden.

---

28 [www.ccdcoe.org](http://www.ccdcoe.org)

Zunächst empfahl der „Nationale Sicherheitsrat“, die Nationalgarde dem Präsidenten zu unterstellen und sie mit dem Schutz der Energieverteilungsnetze zu beauftragen. Nach der Rationierung von Benzin wurden sogar Energieversorgungsunternehmen der staatlichen Kontrolle unterstellt und Terroristen im Ausland verfolgt. Als Optionen wurden auch aktive Cyber-Gegenangriffe diskutiert.

Unabhängig davon, ob dies ein realistisches Szenario ist, muss man dennoch der Tatsache ins Auge sehen, dass Cyber-Angriffe in den letzten Jahren stetig zugenommen haben. Im ganzen Jahr 2008 wurden 54.640 Angriffsversuche auf das US-Verteidigungsministerium registriert; im ersten Halbjahr 2009 waren es bereits 43.785 (+ 60 %).

Dennis Blair, der ehemalige Koordinator der US-Geheimdienste, kam in seiner Bedrohungsanalyse vor dem US-Senat zu folgendem Schluss: „Schädliche Cyber-Aktivitäten treten mit einer noch nie dagewesenen Häufigkeit und noch nie praktizierten Raffiniertheit auf.“

Sowohl die alltäglichen Bedrohungen von Unternehmen durch Cyber-Kriminalität als auch die Aussicht auf ein nationales „Worst-Case-Szenari “ erfordern daher robuste und effektive Abwehrmaßnahmen von Unternehmen und Regierungen.

Vormals getrennte Zuständigkeiten wie Sicherheitsbeauftragter und IT-Sicherheit sollten zum besseren Schutz des Unternehmens zusammengelegt werden; der **Chief Security Officer** sollte dadurch in die Lage versetzt werden, sich ein Gesamtbild von der Sicherheitslage des Unternehmens zu machen und dadurch effektive und verbindliche Gegenmaßnahmen zu entwickeln und umzusetzen. Dieser Ansatz bedarf dringend der Umsetzung! Einen solchen ganzheitlichen Ansatz empfiehlt auch **BKA-Präsident Jörg Zierke** in Anbetracht der ständig steigenden Risiken.

Auf Regierungsebene ist in Deutschland die Novellierung des Gesetzes über das **Bundesamt für Sicherheit in der Informationstechnik**<sup>29</sup> (BSI, „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ vom 20. August 2009) ein notwendiger, allerdings nicht hinreichender Schritt. Mit dieser Novelle erhielt das BSI erweiterte Aufgaben und Kompetenzen. Im Einzelnen waren dies:

- die Aufgabe, Informationen über Sicherheitslücken und neue Angriffsmuster auf die Sicherheit der Informationstechnik zu sammeln und auszuwerten
- die Befugnis, Protokolldaten sowie Daten, die an Schnittstellen der Kommunikationstechnik des Bundes anfallen, zu erheben, auszuwerten, zu speichern, zu verwenden und zu verarbeiten
- die Möglichkeit der Weitergabe von Informationen und Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten an die betreffenden Stellen oder an die Öffentlichkeit
- die Befugnis, strenge und einheitliche Sicherheitsstandards für die Bundesverwaltung zu definieren und bei Bedarf geeignete Produkte entwickeln zu lassen oder bereitzustellen.

---

<sup>29</sup> Das Bundesamt für Sicherheit in der Informationstechnik hat am 1.1.1991 seine Arbeit aufgenommen und gliedert sich in drei operative Abteilungen:

Abt.1: Sicherheit in Anwendungen, Kritischen Infrastrukturen und Netzen

Abt.2: Kryptographie und Abhörsicherheit

Abt.3: Zertifizierung, Zulassung und Konformitätsprüfungen, Neue Technologien

Natürlich verfügen auch das Bundesamt für Verfassungsschutz, das Bundesamt für Verteidigung, die Bundeswehr, der Bundesnachrichtendienst und die Sicherheitsbehörden der Bundesländer über auftragsspezifische Expertise und Kenntnisse zu diesem Thema.

Woran es allerdings immer noch mangelt, ist ein konzertiertes Zusammenwirken aller Kräfte, um einen umfassenden Schutz vor Cyber-Angriffen zu gewährleisten. Insbesondere die enge Verzahnung von Unternehmen, Regierungs- und Sicherheitsbehörden sowie Sicherheitsdienstleistern und Regierungsinstitutionen müsste in dieser Hinsicht angestrebt werden.

Eine Institution, die dies leisten könnte, müsste durch die Erweiterung des bisherigen **Bundessicherheitsrats** durch die Ausstattung mit einem handlungsfähigen Stab zu einem **Nationalen Sicherheitsrat** geschaffen werden – ein, wie sich bislang erwiesen hat, politisch derzeit nicht durchzusetzendes Unterfangen.

In Bezug auf Cyber-Angriffe sollte dieses Gremium:

- eine umfassende, ressortübergreifende Analyse der inneren und äußeren Sicherheitslage ermöglichen
- Notfallplanungen und Abwehrmaßnahmen koordinieren.

Als im Mai 2008 das Thema erstmals von der Politik diskutiert wurde gab es sehr kontroverse Positionen. Im Sinne einer koordinierten Bekämpfung neuer Gefahren und der Minimierung der Risiken sollte die Realitäten und Notwendigkeiten eines solchen Vorschlages spätestens jetzt erkannt und umgesetzt werden.

## Fazit

Sicherheit wird in einer globalisierten Wirtschaft immer mehr zu einem Wettbewerbsfaktor für Staaten und für Unternehmen und auch zu einem Überlebensfaktor in einer von komplexen Informationssystemen abhängigen Lebenswelt.

Sicherheit ermöglicht die Schaffung von Werten und verhindert den Abfluss strategischer Informationen an Konkurrenten und Gegner. Sicherheitsinvestitionen dürfen daher nicht an mangelndem Risikobewusstsein von Politikern und der Geschäftsleitung von Unternehmen scheitern.

Diese neue und wachsende Bedrohung erfordert robuste und effektive Abwehrmaßnahmen von Regierungen und Unternehmen. Auf Regierungsebene ist in Deutschland aus diesem Grund zwingend die Schaffung eines **Nationalen Sicherheitsrates**, dessen Besetzung und Stellenwert die Gefahren des 21. Jahrhunderts widerspiegeln, erforderlich.

Aber mittel- und langfristig wird auch ein nationaler Sicherheitsrat, resultierend aus einem alten, überholten Souveränitätsverständnis, die Lösung europäischer und globaler Sicherheitsprobleme nicht optimal betreiben können. Die Schaffung eines **europäischen Sicherheitsrates** ist ebenfalls erforderlich.

Auch auf der Unternehmensebene sind Veränderungen notwendig. Um sich systematisch gegen Gefahren abzusichern, sollten Unternehmen ihre Sicherheitskompetenzen bündeln. Vormalig getrennte Bereiche wie Security und IT-Sicherheit sollten zum besseren Schutz des Unternehmens zusammengelegt werden. Der **Chief Security Officer** sollte dadurch bei Gefahren und Angriffen in die Lage versetzt werden, schnell, umfassend und effektiv Gegenmaßnahmen ergreifen zu können.

**Dieser Ansatz bedarf dringend der Umsetzung.  
Die Zeit, damit zu beginnen, war gestern.**

## **Unter Mitwirkung von**

### **Bernd Oliver BÜHLER**

Studium der Wirtschaftswissenschaften mit Schwerpunkt Betriebswirtschaft an der Universität Poitiers in Frankreich. Aufbaustudium „Intelligence Economique“ an der Managementenschule ESLSCA in Paris.

### **Michael SOBBEK**

Jahrgang 1958. Ausbildung zum Bankkaufmann. Über 30 Jahre lang Mitarbeiter der Dresdner Bank AG. Zuletzt verantwortlich für den Bereich Krisen- und Sicherheitsmanagement in direkter Berichtslinie zum Vorstand (COO). Davor langjährige Erfahrung in Projektmanagement und Projektleitung in diversen IT-Projekten. Mitglied des Vorstandes der "Vereinigung für die Sicherheit der Wirtschaft e.V. Hessen Rheinland-Pfalz Saarland".

### **Dr. Frank KOSTELNIK**

Studium der Politikwissenschaft und Neueren Geschichte an der Uni Mannheim mit Schwerpunkt Außen- und Sicherheitspolitik. 1991-93 Wissenschaftlicher Mitarbeiter am sicherheitspolitischen Elitenforschungsprojekt EURO SIPLA und 1993-99 am Lehrstuhl für Sicherheitspolitik der Universität der Bundeswehr München. Promotion über „Die politische Anwendung militärischer Macht im Kalten Krieg“. Mitarbeiter der Zeitschrift Clausewitz-Studien. Seit 2003 Internetredakteur zum Thema deutsch-amerikanische Beziehungen.

### **Wolfgang REINEKE**

Seit 1974 selbstständiger Unternehmensberater und Coach in den Bereichen Öffentlichkeitsarbeit, strategische Planung und Führungsentwicklung für Vorstände in Unternehmen und Persönlichkeiten des öffentlichen Lebens. Seine Spezialgebiete sind Medien- und Teletraining für Unternehmen, Verwaltungen und Verbände, Krisen- und Konfliktbewältigungskonzepte und -trainings. Als Publizist arbeitet er mit namhaften deutschen Medien zusammen. Er ist Gründungsmitglied des Europäischen Instituts für Sicherheit in Luxemburg (Eis) und Präsident der Gesellschaft für Europäische Außen- und Sicherheitspolitik (GEAS). Für seine jahrzehntelange Tätigkeit in der Europäischen Politik wurde er im Jahr 2002 mit der Silbermedaille der „Fondation pour le Mérite Européen“ in Luxemburg ausgezeichnet. Er ist Mitglied des Londoner Internationalen Instituts für Strategische Studien (IISS).

### **Walter JERTZ**

Ausbildung zum Offizier und Jet-Piloten bei der deutschen Luftwaffe, 1976-78 Führungsakademie der Bundeswehr, Generalstabsausbildung, 1995 erster nationaler Befehlshaber im Einsatzgebiet, 1999 militärischer Sprecher der NATO während des Kosovo-Krieges, 2002-06 Befehlshaber des Luftwaffenführungskommandos, zuständig für alle Einsatzverbände der Luftwaffe. Generalleutnant a. D. Ausgezeichnet u. a. mit dem Bundesverdienstkreuz. Vorträge an nationalen und internationalen Universitäten und Ausbildungseinrichtungen mit Schwerpunkt Kriegs- und Krisenkommunikation. Buchautor, eigener Verlag und Medienberatung.

### **Norbert WOLF**

Norbert Wolf trat 1960 in Eutin in die Landespolizei Schleswig-Holstein ein. Nach unterschiedlichen Positionen beim Landeskriminalamt Schleswig-Holstein absolvierte er ein Studium an der Polizei-Führungs-Akademie, wurde 1974 zum Polizeirat befördert und zum Stellvertretenden Leiter der Polizeidirektion Kiel ernannt. Von 1974-1980 war er in verschiedenen Führungspositionen und im Landespolizeiamt in Kiel tätig. Während der Jahre 1981-1987 bekleidete er das Amt des Polizeichefs der Hansestadt Lübeck. Von 1988 bis 2008 leitete Wolf als Senior Vice President Corporate Security die Unternehmenssicherheit der Siemens AG mit weltweiter Zuständigkeit.

### **Maxim WORCESTER**

Zuvor war Maxim Worcester Senior Manager bei KPMG innerhalb des Advisory-Bereiches sowie in leitenden Funktionen bei der Economist Intelligence Unit, der Frankfurter Allgemeinen Zeitung, der Deutschen Börse und der Control Risks Deutschland GmbH tätig.

### **Andreas BERG**

Studium der Politikwissenschaft und Geschichte an der Rupertus-Carolus-Universität Heidelberg. Schwerpunkte: Sicherheits- und Verteidigungspolitik, Autokratische Systeme, Militärgeschichte.



**JANUS** Consulting GmbH

Erhalt und Entwicklung des unternehmerischen Erfolges

Max-Planck-Str. 6  
D - 63128 Dietzenbach

Tel: 06074 - 72934510  
Fax: 06074 - 72934567

Web: [www.janusconsulting.de](http://www.janusconsulting.de)  
Email: [kontakt@janusconsulting.de](mailto:kontakt@janusconsulting.de)