UNIVERSITÄT OSNABRÜCK

LV Internetpolitik
Fachbereich 1
49069 Osnabrück

Cyberwar

Grundlagen-Methoden-Beispiele

Version 12.0 vom 07.09.2016

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, Chinas, Russlands und die Cyberpolitik der Europäischen und Afrikanischen Union besprochen.

Inhalt

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[1]. Die folgende Arbeit unternimmt eine aktuelle Bestandsaufnahme und geht auf die theoretischen und praktischen Probleme des Cyberwars (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, Chinas, Russlands und die Cyberpolitik der Europäischen und Afrikanischen 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 (Internet der Dinge)**, 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[2]. Eine erhebliche geplante Erweiterung ist auch die Vernetzung von Kraftfahrzeugen zur car-to-car-communication[3].

[1] vgl. USAF 2010a, DoD 2011

[2] 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. In einer schwedischen Firma haben sich die Mitarbeiter Identifikationschips einpflanzen lassen, um so automatisch Türen öffnen und Geräte nutzen zu können. Die Information kann jedoch beim Händeschütteln durch einen kleinen Sender gestohlen werden, vgl. Astheimer/Balzter 2015, S.C1. RFIDs sind eine Untergruppe der **smart cards**.

[3] vgl. Quirin 2010, S.2f.

- Die Fernwartung und –steuerung von Industriemaschinen über speicherprogrammierbare Steuerungen, auch als Industrial Control Systems ICS bzw. **Supervisory Control and Data Acquisition SCADA** bezeichnet. SCADA-Systeme ermöglichen die Kommunikation mit Maschinen über das Internet.
- Die Kombination aus machine-to-machine communication, Internet of Things und SCADA-Systemen ist ein zentrales Element **cyber-physischer Systeme CPS**, in denen Produktionsprozesse zunehmend durch Netzwerke von Maschinen, Produkten und Materialien gemanagt und ggf. auch modifiziert werden[4].
- Andere Erweiterungen des Netzes sind intelligente Haushaltsgeräte und Stromzähler (**smart grid**[5]) und die Nutzung externer Rechenzentren über das Internet anstelle der Vorhaltung eigener Kapazitäten (**cloud computing**[6])
- Die Einführung internetfähiger Mobiltelefone (**smartphones**[7]), die nun auch die Funktionen von Navigationsgeräten (Global Positioning System GPS-Standortangaben) integrieren und nun im Rahmen des **'bring your own device (BYOD)'–Konzepts** als Schlüsselgerät für die kabellose Koordination multipler Geräte und Maschinen, z.B. in **smart homes**.
- Der Trend entwickelt sich von **smarter cities** mit erweiterter IT-Infrastruktur zu **smart cities**, wo die gesamte Stadt mit einer vorgeplanten umfassenden IT-Infrastruktur für alle relevanten städtischen Funktionen ausgestattet ist.[8]
- 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[9]

---

[4] Synonyme sind Smart factory, Integrated Industry oder **Industrie 4.0** (nach Mechanisierung, Elektrifizierung und standardisierter Massenproduktion).

[5] Anfang 2013 legte der europäische Dachverband der Energieversorger Entso-e Pläne für die ferngesteuerte Kontrolle von großen Haushaltsgeräten wie Kühlschränken für alle EU-Bürger vor, so dass Energieversorger im Falle von Engpässen Geräte herunterregeln oder ganz abschalten können. Dieses Konzept könnte aus der Cybersicherheitsperspektive eine neue erhebliche Gefahrenquelle darstellen; Schelf 2013, S.1. Die deutsche Bundesregierung unterstützt dieses Vorhaben, vgl. Neubacher 2013, S.82

[6] 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. Außerdem können Cloud-Anbieter ggf. die Daten einsehen, um sie zu scannen und zu analysieren, ggf. können sie unter bestimmten Umständen den Zugang sperren, vgl. Postinett 2013b, S.12

[7] Für Android-Smartphones sind mehr als eine Million Virusvarianten, die von anpassungsfähigen Viren stammen, bekannt, FAZ 2013b, S.21.

[8] Im Moment werden Masdar City in Abu Dhabi und New Songdo in Südkorea errichtet, die IT von New Songdo wird von Cisco bereitgestellt, vgl. Frei 2015, S.27

[9] vgl. Grant 2010

Aus all dem resultiert eine deutlich gestiegene Verwundbarkeit und informationstechnische Abhängigkeit kritischer Infrastrukturen (KRITIS)[10]. Auf der anderen Seite ist die Durchführung eines Angriffs erheblich vereinfacht[11].

- 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.

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 war, cyber warfare, Cyber-Krieg, Krieg der Computer, Computerkrieg) 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[12].

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[13].

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

[10] 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.

[11] vgl. Megill 2005, DoD 2011

[12] vgl. Wilson 2008, S.3ff.

[13] vgl. auch CSS 2010, Libicki 2009, S. XIV

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[14].
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[15]. Großangelegte Spionageangriffe können jedoch auch zu Computer- und Netzwerkstörungen führen und werden dann mitunter in der Literatur ebenfalls dem Cyberwar zugerechnet.

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

1.4.1 Grundlagen

Die Vernetzung von Computern in einer besonders geschützten Internetumgebung bildet zusammen mit der Verbesserung von Verschlüsslungen 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[16].

Dazu gehört neben bereits etablierten Anwendungen

- wie dem Radarflugzeugsystem **Airborne Early Warning and Control System (AWACS)**, das der großräumigen Radarüberwachung aus der Luft dient,

[14] vgl. auch Mehan 2008, CSS 2010
[15] vgl. Libicki 2009, S.23
[16] vgl. Neuneck/Alwardt 2008

- 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[17])
- und die **integrierte Kriegführung**.

Die **Drohnen** dienen nicht mehr nur der Aufklärung, sondern können auch zur Terroristenbekämpfung eingesetzt werden, wie z.B. schon in Afghanistan und Pakistan erfolgreich geschehen[18]. Drohnen eignen sich generell für alle Arten von Operationen, die „dull, dirty, dangerous or difficult" sind[19]. Der operative Erfolg der Drohnen hat die Nachfrage entsprechend steigen lassen[2021].

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. 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.[22] Ziel der IO ist die Erlangung und Optimierung von 5 Kernfähigkeiten (core capabilites), 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[23]

[17] vgl. Hürther 2010, S.33-34
[18] vgl. Rüb 2010, S.5
[19] vgl. Jahn 2011, S.26: also alles, was „langweilig, schmutzig, gefährlich, schwierig oder anders" ist
[20] vgl. FAZ 2010b, S.6
[21] Zunehmend geht der Trend zur Miniaturisierung, wie z.B. beim Modell Rabe, das nur noch Spielzeuggröße hat, vgl. Singer 2010; auch an Reichweite, Bewaffnung und Lautstärke wird geforscht, vgl. Jahn 2011, S.26. Inzwischen sind auch private Drohnen wie die französische AR-2.0 verfügbar, die per Smartphone kontrolliert werden und ca. 50 Meter hoch fliegen kann, vgl. Fuest 2012, S.37.
[22] vgl. Wilson 2007
[23] vgl. USAF 2010b, S.5

- der Irreführung des Gegners (**military deception MILDEC**), z.B. der gegnerischen Luftabwehr wie während des Irakkrieges[24]
- 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[25], die Entwendung von Informationen als **computer network exploitation (CNE)** und die Schutzmaßnahmen gegen beides als **computer network defence (CND)**[26]
- die klassische elektronische Kampfführung (**electronic warfare EW**) mit Hilfe der Schädigung des Gegners durch Störsignale und ähnliche Maßnahmen.

1.4.2 Definition des Cyberwar

Abgesehen von den praktischen Schwierigkeiten einer Definition des Cyberwar hat es auch politische und rechtliche Bedenken gegen eine offizielle Definition gegeben, denn eine Handlung, die die Kriterien einer solchen Definition erfüllt, könnte einen erheblichen politischen und militärischen Handlungsdruck auslösen[27].

Ein Vergleich der Cyberwar-Konzepte mehrerer NATO-Staaten mit Russland und China zeigt auch unterschiedliche Auffassungen zu der Frage, ob der Cyberwar nur die militärische, oder auch die zivile und wirtschaftliche Seite mit einbeziehen soll[28]. Die USA haben dennoch eine genauere und pragmatische Cyberwar-Definition erarbeitet.

2007 hatte das strategische Kommando USSTRATCOM den *network warfare* (Krieg im Netz) noch als „den Einsatz von Computernetzwerken mit der Absicht, dem Gegner die effektive Nutzung seiner Computer, Informationssysteme und Netzwerke zu verwehren“ definiert[29].

Damals diskutierte der ehemalige Chef des Cyber Command CYBERCOM, General Keith Alexander, die Notwendigkeit einer erweiterten Definition, die

[24] vgl. USAF 2010b, S.32
[25] vgl. Wilson 2008
[26] vgl. CSS 2010
[27] vgl. Beidleman 2009, S.9ff. and S.24
[28] vgl. IT Law Wiki 2012a, S.1-4
[29] vgl. Alexander 2007, S.61: “The command defines *network warfare* as “the employment of computer network operations with the intent of denying adversaries the effective use of their own computers, information systems and networks”.

klarstellt, dass es auch um den Schutz der eigenen Systeme und der Handlungsfreiheit (**freedom of action**) geht[30]. Dabei wurde deutlich, dass der Cyberwar nicht als eigenständige Maßnahme, sondern als integraler und *unterstützender* Bestandteil allgemeiner militärischer Operationen angesehen wird und dass dieser nicht nur wie oben beschrieben offensive, sondern auch defensive Komponenten enthält[31].
Das bedeutet aber auch, dass der Cyberwar ein Zusammenspiel von Mensch und Maschine ist, also die Computer dies nicht alleine durchführen können und dass es sich in Anpassung an die jeweilige Lage um ein ganzes Bündel von Maßnahmen handelt, also in der Regel nicht nur um einen einzigen Schlag geht, auch wenn ein solcher am Anfang stehen mag.

Diese Überlegungen spiegeln sich in der aktuellen **Cyberwar-Definition** der US Army wieder[32]:

„Cyberwar ist jener Teil der Operationen im Cyberspace, durch die die Wirkungen der verfügbaren Cyberkapazitäten über die defensiven Grenzen des eigenen Netzwerkes hinaus ausgedehnt werden, um den Gegner aufzuspüren, ihn abzuschrecken, ihn zu blockieren und um ihn zu schlagen. Der Cyberwar zielt auf Computer, Telekommunikationsnetzwerke und eingebaute Prozessoren in technischen Geräten, den Systemen und der Infrastruktur."

Diese Definition stellt klar, dass der Cyberwar nicht auf das Internet beschränkt ist, sondern die gesamte Digitaltechnologie umfasst[33]. Weiterhin wird geklärt, dass der Cyberwar nur ein Teilaspekt militärischer Cyberaktivitäten ist.

2014 wurde das Kommando über die NSA und Cybercom von Vice Admiral **Michael Rogers** übernommen, einem Kryptologie-Spezialisten der zehnten Flotte. Rogers betonte die wachsende Bedeutung und Häufigkeit von Cyberattacken und berichtete in diesem Zusammenhang über ein Eindringen von Hackern in ungesicherte Marine-Netzwerke im Jahre 2013 zu Spionagezwecken[34].

[30] vgl. Alexander 2007, S.61: "We are developing concepts to address war fighting in cyberspace in order to assure freedom of action in cyberspace for the United States and our allies while denying adversaries and providing cyberspace enabled effects to support operations in other domains."
[31] vgl. Alexander 2007, S.60
[32] vgl. IT Law Wiki 2012, S.2. Übersetzte Fassung, der englische Originaltext lautet: „Cyberwar is the component of CyberOps that extends cyber power beyond the defensive boundaries of the GIG to detect, deter, deny, and defeat adversaries. Cyberwar capabilities target computer and telecommunication networks and embedded processors and controllers in equipment, systems and infrastructure."
CyberOps = Cyber Operations, GIG = Global Information Grid, d.h. das militärische Netzwerk.
[33] vgl. auch Beidleman 2009, S.10
[34] vgl. Winkler 2014b, S.3

1.4.3 Cyberwar und Völkerrecht

Der Begriff des Gegners (‘adversary’) in der o.g. Definition wird in der Literatur sowohl auf staatliche als auch auf nicht-staatliche Akteure bezogen. Ein nicht-staatlicher Akteur bzw. dessen Attacken können durchaus auch eine militärische Antwort erfordern, wenn polizeiliche oder nachrichtendienstliche Mittel allein nicht ausreichen. Selbst wenn Krieg völkerrechtlich ein Konflikt zwischen Staaten ist, muss sich ein Cyberwar-Konzept auch mit Angriffen nicht-staatlicher Akteure auseinandersetzen.

Dies führt zu der entscheidenden Frage, ab wann man von einem Krieg sprechen kann. Letztenendes ist die Entscheidung zum Krieg ähnlich wie in konventionellen Auseinandersetzungen eine strategische und politische Entscheidung, die nicht schon vorab definiert werden kann. Dies gilt auch für die Art der Gegenmaßnahme, denn man kann einen Cyberangriff im Prinzip auch mit politischen Sanktionen oder konventionell vergelten, Automatismen sind wegen des Eskalationspotentials nicht unproblematisch[35].

Man darf auch das **Attributionsproblem**, d.h. die korrekte Zuordnung eines Angriffs zu einem bestimmten Angreifer, nicht außer Acht lassen, denn man kann nicht auf einen bloßen Verdacht hin in eine bestimmte Richtung vergelten.

Um die resultierenden Unsicherheiten und um eine unkontrollierte Eskalation von Cyberkonflikten zu vermeiden, hat die US-Regierung im Frühjahr 2012 eine Initiative zur Errichtung von **Cyber-Hotlines** (in Analogie zu den ‘roten Telefonen’ des kalten Krieges) mit Russland[36] und China[37] gestartet.

Die UN-Organisation International Telecommunications Union (ITU) wurde bei den World Summits on the Information Society 2003 und 2005 beauftragt, ihren Mitgliedern als neutrale Organisation der Cybersicherheit zu dienen. So leitete die ITU die Untersuchung der 2012 entdeckten Computerinfektionen mit der Spionagesoftware Flame[38].

Seit Jahren wird eine globale **Cyber-Konvention** diskutiert, aber da der Cyberspace die einzige vom Menschen künstlich erzeugte Domäne ist, würde eine Konvention nicht nur die Aktivitäten innerhalb einer natürlich gegebenen Domäne regulieren, sondern könnte sich auch *auf die Struktur der Domäne selbst* auswirken oder diese gar bestimmen[39].

---

[35] Gleichwohl gibt es Überlegungen zu voll automatisierten Gegenantworten bei Cyberattacken, Nakashima 2012b
[36] vgl. Nakashima 2012a
[37] vgl. Spiegel online 2012
[38] vgl. ITU 2012
[39] vgl. auch Fayutkin 2012, S.2

Jedoch wurde von den Vereinten Nationen im Juli 2015 eine Art **Cyber-Konvention** angenommen, der *Report of the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications (ICT)*. Der Report enthält Empfehlungen zur Guten Cyberpraxis, aber auch einige Verbote[40]. Die Staaten sollten zusammenarbeiten, um die Sicherheit und Stabilität der Nutzung der Informations- und Kommunikationstechnologie zu gewährleisten und schädlichen Handlungen vorbeugen und zu diesem Zwecke einen Informationsaustausch mit allen relevanten Informationen betreiben. Auf der anderen Seite sollten die Staaten schädliche Aktivitäten weder unterstützen noch durchführen, die Verbreitung schädlicher Anwendungen verhindern und die Privatsphäre und die Menschenrechte im Internet respektieren.

Diese Dokument wurde von der amerikanischen Cyberdiplomatie unterstützt, weil aus amerikanischer Sicht die meisten Cybervorfälle unter der völkerrechtlichen Schwelle einer Gewaltanwendung liegen, so dass kein Gegenschlag zur Selbstverteidigung zulässig ist; aus diesem Grunde sollten sich Staaten in Friedenszeiten gewissen grundlegenden Selbstbeschränkungen unterwerfen[41].

Das NATO Cyber Defense Centre of Excellence (CCD CoE) hat 2013 das **Tallinn Manual** on the International Law applicable to Cyber Warfare vorgelegt, das von einer internationalen Expertengruppe erstellt wurde und sowohl das Völkerrecht des *jus ad bellum* (Recht zur Anwendung von Gewalt) wie das *ius in bello* (Völkerrecht im Rahmen bewaffneter Auseinandersetzungen) behandelt [42].

Insgesamt befinden sich die vorgeschlagenen Regeln für den Cyberkrieg im Einklang mit den Regeln zur konventionellen Kriegsführung und der Cyberwar wird wie jede andere militärische Auseinandersetzung behandelt (use of force, rule 11). Gemäß Regel (rule) 41, "*means of cyber warfare are cyber weapons and their associated cyber system, and methods of cyber warfare are the cyber tactic, techniques, and procedures by which hostilities are conducted (Übersetzung: Mittel des Cyberwars sind Cyberwaffen und das zugehörige Cybersystem und Methoden des Cyberwars sind die Cybertaktik, -techniken und –prozeduren, mit denen die Feindseligkeiten ausgetragen werden)*". Das Schlüsselelement ist jedoch die **Cyberattacke**, die definiert wird als "*a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction of objects (Übersetzung: eine defensive oder offensive Cyberoperation, bei der mit einem Personenschaden oder Toten oder der Beschädigung oder Zerstörung von Objekten gerechnet werden muss*") (rule 30). Cyberwar-Aktivitäten können auch mit anderen militärischen Mitteln beantwortet

[40] UN 2015
[41] vgl. Rõigas/Minárik 2015
[42] vgl. CCD CoE 2013, Schmitt 2013

werden (verhältnismäßige Gegenantwort, rule 5.13). Die Regeln gelten jedoch nicht für die reine Cyberspionage (rule 6.4) und Angriffe müssen einem Staat eindeutig zugeordnet werden können (rule 6.6). Nicht-staatliche Akteure können jedoch unter diese Regeln fallen, falls der Staat über sie effektive Weisungsbefugnis und Kontrolle hat (rules 6.10, 6.11) [43]. Laut einer Mitteilung des CCD CoE im Februar 2016 sind die Arbeiten zu einem Update als Tallinn Manual 2.0 bereits im Gange. Die NATO betrachtet den Cyberspace nun auch formell als Ort militärischer Handlungen[44].

1.4.4 Cyberwar und Drohnen

Ein spezielles Cyberwar-Problem stellt der Fortschritt der Drohnen-Technologie dar. Drohnen können der Beobachtung, aber auch der gezielten Tötung von Gegnern dienen[45]. Der technische Fortschritt ermöglicht immer umfangreichere **Assistenzfunktionen**, d.h. die menschliche Entscheidung immer weitgehender von Computern unterstützt und beeinflusst[46]. In diesem Zusammenhang kam bereits die Frage einer **Haftbarkeit von Maschinen** auf[47]. Jeder Schritt in Richtung vollautomatisierter Drohnen würde jedenfalls deutlich verstärkte Anstrengungen im Bereich der Cyber-Sicherheit erfordern, um zu verhindern, dass die Maschinen von gegnerischen Hackern übernommen werden (Kapitel 3.2.9) [48].
Autonome Drohnen können ihre Entdeckung durch Halten von Funkstille vermeiden, so dass die Autonomie Teil eines Tarnkappendrohnenkonzepts ist wie bei der 2013 von China getesteten **Lijan-**Drohne[49].
Das Funktionieren autonomer Maschinen ist von der zugrunde liegenden Programmierung abhängig, was jedoch zu ethischen und praktischen Dilemmata führen kann[50]. Falls das programmierte Verhalten bekannt ist, könnten Drohnen

[43] Gemäß des Manuals ist die Nutzung von scheinbar harmlosen, aber schädigenden Cyberfallen (**cyber bobby**) nicht akzeptabel. Jedoch wären evtl. nicht-schädigende Fallen vorstellbar, z.B. eine harmlose Datei, die man mit Wissen der Nutzer in sensitiven Ordnern ablegt. Jedwede Nutzung durch Öffnen, Ändern, Kopieren und Exportieren wäre für die Administratoren ein Indiz für Eindringlinge.
[44] vgl. Gebauer 2016
[45] vgl. Thiel 2012, S.Z2
[46] Eine mögliche Zukunft mit vollautomatisierten Tötungen bleibt jedoch Spekulation. Die Erforschung von autonomen Kampfrobotern (**lethal autonomous robots LARs**) macht Fortschritte, vgl. Klüver 2013, S.2. Wissenschaftler erwarten, dass die praktischen Fortschritte in der **Künstlichen Intelligenz (KI)** schon bald den Einsatz von Kampfrobotern erlauben werden, die autonom über Kampf und Töten entscheiden können. Deshalb befürworten Forscher der KI und der Robotik in einem offenen Brief vom 27.07.2015 den Bann für autonome Waffen dieses Typs, vgl. Future of Life Institute 2015
[47] Im zivilen Sektor wird dies in den USA für selbstfahrende Autos (also Autos mit Autopilot-Funktionen) diskutiert, Kalifornien plant entsprechende Reglungen für das Jahr 2015, vgl. Burianski 2012, S.21
[48] Die größten Drohnen sind mittlerweile in der Lage, konventionelle Flugzeuge zu ersetzen, so dass ein gegnerisches Eindringen ein erhebliches Sicherheitsrisiko darstellt. Das europäische Drohnenprojekt **Neuron** ist ein unbemanntes Kampfflugzeug (unmanned aerial combat vehicle UACV) mit Tarnkappen (Stealth)-Technologie, welches zu größeren Schlägen aus der Luft als bisherige Drohnen fähig sein soll (vgl. Bittner/Ladurner 2012, S.3; Hanke 2012, S.14).
[49] vgl. TAZ online 2013
[50] vgl. Hevelke/Nida-Rümelin 2015, S.82

(oder Autos) durch Vortäuschung von bestimmten Situationen oder Objekten absichtlich irregeführt, abgefangen oder zerstört werden.

Die Drohnentechnologie leidet unter bestimmten Schwachstellen, die sich im Verlust einer relevanten Zahl von Drohnen widerspiegelt. Für die USA wurde der Verlust von 5 Global Hawks, 73 Predator- und 9 Reaper-Drohnen berichtet, für Deutschland in der letzten Dekade der Verlust von 52 meist kleinen Drohnen[51]. Meistens wurden diese Verluste durch Bedienungsfehler und konventionelle technische Probleme verursacht. Zudem kann ein Verlust der Verbindung zur Bodenstation ggf. eine Landung erzwingen und dann die nachfolgende Zerstörung, falls die Drohnen sonst in gegnerische Hände fallen könnten.
Eine systematische Untersuchung der *Washington Pos*t fand 418 Drohnenabstürze im Zeitraum von 2001 bis 2014, wesentliche Ursachen waren beschränkte Möglichkeiten von Kameras und Sensoren zur Kollisionsvermeidung, Pilotenfehler, mechanische Defekte und unzuverlässige Kommunikations-verbindungen[52].

Tests in New Mexico im Jahre 2012 haben die Anfälligkeit von Drohnen für falsche GPS-Signale (**GPS spoofing**) nachgewiesen. Dies galt auch für die neue Flugüberwachung durch Automatic Dependent Surveillance Broadcast systems (ADS-B). Auch hat man festgestellt, dass Drohnen unbeabsichtigt durch Signale, die an andere Drohnen gerichtet sind, abgelenkt werden können.[53]

Das Luftfahrtunternehmen *Airbus* entwickelt ein System zur Drohnenabwehr mit Radar und Infrarotkameras mit einem Erfassungsradius von 10 Kilometern[54]. Die angreifende Drohne kann dann durch elektromagnetische Störsignale, die die Funkverbindung zwischen dem Drohnenpiloten und der Drohne unterbrechen, deaktiviert werden.

Die Drohnenabwehrforschung in Deutschland untersucht nun die Verwendung von Laserstrahlen. Im Mai 2015 konnte eine kleine Quadrokopter-Drohne durch Energien von 20 Kilowatt über 3,4 Sekunden zerstört werden[55]. Für größere Objekte werden jedoch höhere Energieniveaus von bis zu 200 Kilowatt benötigt, die Entwicklung ist bereits im Gange.

Die Entwicklung geht hin zu komplexen Drohnenverteidigungssystemen, den **Anti-UAV defense systems (AUDS)**. Computer können sich nähernde Drohnen durch Geräuschmuster, durch optischen Bewegungsmustervergleich (zur

[51] vgl. Gutscher 2013, S.4, Spiegel 2013a, S.11
52 vgl. Whitlock 2014
[53] vgl. Humphreys/Wesson 2014, S.82
[54] vgl. Lindner 2016, S.24, Heller 2016, S.68
[55] vgl. Marsiske 2016

Abgrenzung von Vögeln), Signalerkennung und Infrarotkameras erkennen. Fortgeschrittene AUDS-Systeme kombinieren diese Methoden[56]. Das **Geofencing**, d.h. die elektromagnetische Abriegelung von Flugverbotszonen wird zur Zeit entwickelt. Die niederländische Polizei versucht, Drohnen mit Hilfe abgerichteter Adler zu fangen und zu Boden zu bringen.

Jedoch gibt es auch das Risiko von Cyberattacken, das auf lange Sicht das größte technische Risiko darstellen könnte (Kapitel 3.2.9).

Der Verkauf eines bestimmten Drohnenmodells an mehr als einen Staat führt zu einer Verbreitung des Wissens um Fähigkeiten und Schwachstellen[57]. Um sensitives Wissen zu schützen, benutzen die USA das **Black box-Prinzip**, bei dem z.B. Technologiemodule für den EuroFighter, aber auch die EuroHawk-Drohnen als geschlossene Einheiten geliefert werden ohne Zugang für Ausländer[58]. Dasselbe Prinzip wird für die indischen und australischen U-Boote der französischen Firma DNCS angewendet, was zusammen mit einer Vielzahl anderer Daten im August 2016 durchsickerte. Aber DNCS erklärte, dass die Daten für die australischen U-Boote vom Typ *Barracuda* nicht geleakt worden waren, sondern nur für die indischen U-Boote des Typs *Scorpene*[59].
DNCS vermutet, dass das Datenleck Teil einer ökonomischen Kriegführung der Mitbewerber aus Japan und Deutschland gewesen sein könnte, aber die Mitbewerber verneinten dies bzw. kommentierten dies nicht[60].

Die mittlerweile suspendierte[61] EuroHawk-Drohne kombinierte die Drohnentechnologie der Global Hawk-Drohne von Northrop Grumann mit dem neuartigen hochentwickelten Aufklärungssystem **ISIS** der EADS-Tochter Cassidian. Während eines Überführungsfluges nach Europa riss der Kontakt für einige wenige Minuten ab. Da solche Zeitfenster potentielle Gelegenheiten für (Cyber-)Angriffe sein können, ist die Cybersicherheit für zukünftige Entwicklungen besonders wichtig.

---

[56] vgl. Brumbacher 2016, S.5

[57] Und herkömmliche Spionage ist nach wie vor ein Problem. In Norddeutschland wurde 2013 ein Mann verhaftet, der Schwachstellen von Drohnen in einer Drohnenforschungseinrichtung auszukundschaften versuchte und bei dem der Verdacht einer Arbeit für Pakistan bestand, vgl. Focus 2013, S.16. Die Sicherheitsfirma FireEye berichtete über eine großangelegte Spionagekampagne namens **Operation Beebus** gegen Anbieter von Drohnentechnologie, bei der ein Zusammenhang mit einer chinesischen Hackergruppe vermutet wurde, Wong 2013, S.1/4. Irans neue Überwachungsdrohne **Jassir** wies Ähnlichkeiten zu der zuvor abgefangenen ScanEagle-Drohne auf, Welt online 2013

[58] vgl. Löwenstein 2013, S.5, Hickmann 2013, S.6

[59] vgl. Hein/Schubert 2016, S.22

[60] vgl. FAZ 2016a, S.29

[61] vgl. Buchter/Dausend 2013, S.4, Vitzum 2013, S.6. Eines der Probleme war ein fehlendes Kollisionswarnsystem (sense-and-avoid system), wobei die genauen Hintergründe zwischen den beteiligten Akteuren umstritten sind. Die Vermeidung von Kollisionen und die Integration in den zivilen Luftverkehr sind jedoch generell wichtige Herausforderungen für die Drohnentechnologie.

In der Europäischen Union sind verschiedene Forschungsprojekte im Gange, bei denen die Steuerung von Drohnen im Alltagsbetrieb nicht mehr von Menschen, sondern von Computern übernommen werden soll. Relevante Projekte sind das zur inneren Sicherheit zählende INDECT-Projekt seit 2009[62] und verschiedene weitere als Teil der Sicherung der europäischen Außengrenzen als **European Border Surveillance System (EUROSUR)** von 2008 bis 2012.

Zu den Eurosur-Projekten gehörten hier[63]:

- OPARUS (Open Architecture for UAV-based Surveillance Systems) zur Grenzüberwachung aus der Luft, bei dem es auch um die Eingliederung der Drohnen in den zivilen Luftraum ging
- TALOS (Transportable autonomous patrol for land border surveillance) mit Patrouillenmaschinen
- WIMAAS (Wide Maritime area airborne surveillance) zur Nutzung von Drohnen zur Seeüberwachung

Die Idee, die Alltagsüberwachung von einem Computer steuern zu lassen, dem **Unmanned Units Command Center UUCC**, war ein Teil dieser Projekte, aber aus einer Cyberwar-Perspektive wäre das die entscheidende Schwachstelle, so dass höchste Anforderungen für die Cybersicherheit und –stabilität gestellt werden müssten. Die EU hat ihre Aktivitäten zur Cybersicherheit weiter verstärkt, siehe Kapitel 4.5.

Das beschriebene Grenzsicherungskonzept ist auch als **virtual border** (virtuelle Grenze) oder **virtual wall** (virtueller Wall) bekannt und verbindet physische Barrieren mit computergestützten Überwachungsmaßnahmen für lange, schwer zu kontrollierende Grenzen. Solche Ansätze werden auch für Saudi-Arabien (durch EADS[64]) und in einigen Abschnitten der US-Grenze entwickelt[65].

Die geplante Öffnung des zivilen Luftraums für private Drohnen in den USA wird zu einem Drohnenboom führen, durch den die Cybersicherheit für Drohnen noch relevanter sein wird als bisher[66].

---

[62] vgl. Welchering 2013a, S.T6. Die Forschung zur automatischen Erkennung von Bedrohungssituationen richtet sich auf Szenarien wie das folgende: Falls eine Kamera ein verdächtiges Verhalten feststellt, soll die Kombination aus automatisch aktivierten Beobachtungsdrohnen, Richtmikrofonen und automatisierter Gesichtserkennung die Identifikation der Zielperson und ggf. ihrer Absichten ermöglichen. Falls nötig, sollen auch Daten aus Facebook, Twitter, Google plus, Kreditkartendaten usw. genutzt werden, um gefährliche Handlungen zu erkennen.
[63] vgl. Oparus 2010, SEC 2011, S.7, Talos Cooperation 2012.
[64] vgl. Hildebrand 2010, S.6
[65] vgl. Miller 2013, S.12-13
[66] vgl. Wysling 2014, S.5

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).[67]

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, kann aber auch Folge eines heftigen Sonnensturms sein[68]. 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

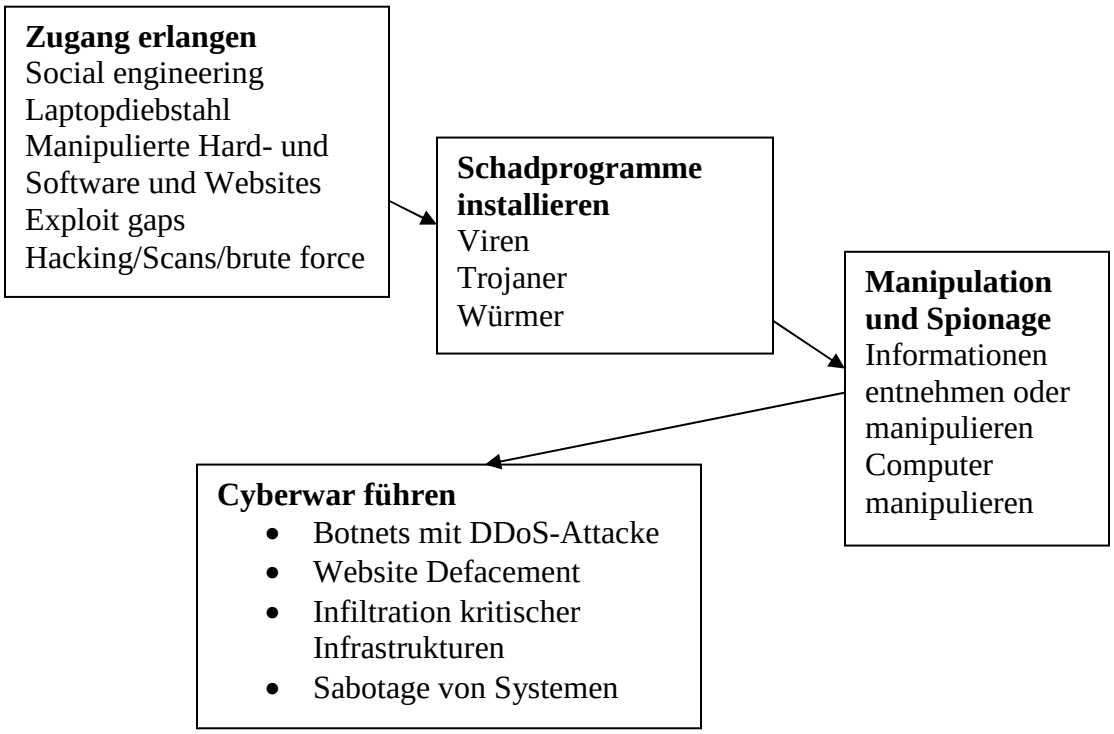
Computer und Netzwerke können auf verschiedene Weise angegriffen werden, wobei dies technisch durch heimliche Platzierung von Programmen (Computerbefehlen) auf dem angegriffenen Computer oder durch Störung der Kommunikation zwischen den Computern geschieht. Angriffe im Cyberwar werden in aller Regel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

[67] vgl. Wilson 2008, S.11
[68] vgl. Morschhäuser 2014, S.1-2

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.
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[69].



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[70] erfolgen kann. Die übliche IT-Architektur besteht aus vielen verschiedenen

[69] vgl. Northrop Grumman TASC 2004
[70] Ein Portscanner überprüft, welche Dienste ein System über das Internetprotokoll anbietet, und welches Antwortverhalten es zeigt.

Hardware- und Softwarekomponenten von mehreren Anbietern, was es schwierig macht, alles stets auf dem neuesten Stand zu halten. Spezielle Programme können den Update-Status eines Computers überprüfen und dann ggf. auch schon bekannte Schwachstellen zum Angriff nutzen[71].

- durch Ausprobieren **(Hacken**) von Passwörtern, wobei dies inzwischen auch automatisiert unter Einsatz großer Rechnerkapazitäten **(brute force**) erfolgt
- durch Irreführung von Computernutzern durch **social engineering**, bei denen man den Nutzern unter einem Vorwand Zugangsdaten wie das Passwort entlockt. Aber auch Insider, insbesondere solche mit IT-Kenntnissen, können die Sicherheitsmaßnahmen einer Organisation überwinden, was z.B. bei Wiper-Malwareattacken diskutiert wurde, siehe Kapitel 3.3.
- Eine zunehmend verwendete Technik besteht im Angriff auf einfache Angestellte, um von da aus an Administratorenrechte zu gelangen (**lateral movement**)[72]. Infolgedessen sammeln Cyberangreifer inzwischen immer systematischer Personaldaten, um relevante und/oder verwundbare und/oder mit Sicherheitsfragen befasste Zielpersonen zu identifizieren.[73]
- 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 oder Anhänge mit Schadsoftware zu öffnen (individuell maßgeschneiderte e-mails werden auch als **spear-phishing** bezeichnet), 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

[71] vgl. Kurz 2013, S.31

72 Eine der größten bekannten Aktivitäten der Cyberkriminalität, der Diebstahl von 1 Milliarde Dollar von insgesamt 100 Finanzinstituten durch die **Carbanak**-Gruppe wurde auf diese Weise durchgeführt, vgl. Bilanz 2015, S.50-57. Zudem übernahmen sie die Kontrolle über die Überwachungskameras und konnten so in Ruhe vorab die Abläufe in den Instituten studieren, vgl. Kaspersky Lab 2015c, S.1

73 Aktuelle Attacken betrafen die US-Personalbehörde **Office of Personnel Management (OPM)**, wo in zwei Angriffswellen ca. 22 Millionen Personendatensätze abgegriffen wurden, dies betraf Sicherheitsüberprüfungen, Gesundheitsdaten, Lebensläufe, Einstellungsgespräche und 1,1 Millionen digitalisierte Fingerabdrücke. Am 23.09.2015 aktualisierte das OPM die Zahl der entwendeten Fingerabdrücke auf 5,6 Millionen. In 19,7 Millionen Fällen wurden jeweils ca. 100 Seiten starke Dossiers kopiert, vgl. Winkler 2015, S.3; zudem wurden US Datingportale angegriffen, ein aktueller Angriff erbeutete Registrierungen von Regierungsangestellten und Armeeangehörigen, vgl. Mayer 2015, S.13. Im März 2016 fand ein ethischer Hacker eine Sicherheitslücke, die ihm Zugang zu allen 1,59 Milliarden *Facebook*-Nutzerkonten gegeben hätte. Facebook wurde informiert und schloß die Lücke, SZ online 2016.

- Die Platzierung von Schadprogrammen kann aber auch durch das Einlegen **infizierter Datenträger** (früher Disketten, heute insbesondere infizierte USB-Sticks) geschehen.
- Auch die **IT-Umgebung** kann für Eindringversuche genutzt werden, wie z.B. Router[74], kabellose Mäuse und Drucker. Zunehmend werden Netzwerkdrucker und Multifunktionsdrucker angegriffen, was das Abfangen der Daten oder das erneute Ausdrucken von Dokumenten ermöglicht[75].
- Eine weitere Methode ist die **interdiction**, d.h. der Austausch von verschickten CD-ROMs und anderen physischen Medien durch infizierte Datenträger.
- Es gibt immer wieder Debatten wegen schon vorher eingebauter Hintertüren ('**backdoors**'[76]), 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[77]. 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[78]. 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[79]. Nicht nur Hersteller, sondern auch die globalen Lieferketten bilden mögliche Angriffspunkte[80]: eine Studie des US-Senats von 2012 berichtete, dass in US-Waffen mehr als eine Million gefälschter Chips installiert

[74] vgl. Handelsblatt 2014 b, S. 23
[75] vgl. Dörfler 2015, S.P4
[76] Eine spezielle Variante sind sogenannte **bugdoors**, d.h. Programmierfehler (bugs), die als Backdoors dienen können und die manchmal absichtlich eingebaut werden; vgl. Kurz 2012, S.33
[77] Die Welt 10 Januar 2007
[78] 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. Die US-Behörden wiesen Huawei wegen Sicherheitsbedenken an, ihre Anteile an der Cloud computing Firma 3Leaf zu verkaufen; Wanner 2011, S.8
[79] Auch hier kann es Sicherheitsprobleme geben, wie die auf ca. 130 Millionen Smartphones vorinstallierte Software **Carrier IQ**, die unter anderem Tastatur- und Standortdaten protokolliert; vgl. Postinett 2011, S.32
[80] vgl. USAF 2010a, S.5

wurden, 70% der Chips kamen aus China, aber relevante Mengen stammten auch aus Großbritannien und Kanada[81]. Da jeder Chip minimale Konstruktionsunterschiede aufweist, können diese Unterschiede gemessen und als einzigartiger Fingerabruck genutzt werden, als sogenannte **Physically Unclonable Function (PUF)** [82].

- **Staatstrojaner** werden von Staaten geschaffen und/oder genutzt, um Zielcomputer zu überwachen. Aber wie jede andere Backdoor-Technologie können Staatstrojaner Sicherheitslücken schaffen, die dann von Dritten genutzt werden könnten.
- 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-Überwachungs-verordnung (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[83]. Die nationalen Zugriffsrechte haben aber zur Folge, dass man sich mit einer ausländischen oder internationalen IT-Plattform auch die anderen Nachrichtendienste ins Haus holt[84].
- Mittlerweile ist bekannt, dass viele Firmen einschließlich von IT-Sicherheitsanbietern Informationen über Sicherheitslücken an die Geheimdienste weitergeben, bevor diese veröffentlicht bzw. geschlossen werden, um so die Geheimdienstarbeit zu unterstützen[85]. Nutzer von Geräten, Software und IT-Sicherheitsanwendungen müssen also davon ausgehen, dass der Geheimdienst des jeweiligen Herstellungslandes *eventuell* einen Zugang hat und nutzt, dass dies über Geheimdienstkooperationen[86] *eventuell* auch indirekt für die Dienste anderer Staaten gilt und ein zero day-exploit eventuell keineswegs ‘zero’

[81] vgl. Fahrion 2012, S.1
[82] vgl. Betschon 2016, S.39
[83] vgl. Scheidges 2010, S.12-13. Welchering 2013c, S.T2 berichtete über eine potentielle Schwachstelle der **Quantenkryptographie**: Die Blendung von Photonenempfängern mit einem Lichtpuls durch einen zwischengeschalteten Angreifer erlaubt unter Umständen das Abfangen, Entschlüsseln und Ersetzen von Photonen.
[84] vgl. Scheidges 2010, S.12-13
[85] vgl. FAZ 2013a, S.1
[86] Es gibt z.B. das sogenannte **five eyes-agreement** der geheimdienstlichen Zusammenarbeit zwischen den USA, Großbritannien, Kanada, Australien und Neuseeland basierend auf dem **UKUSA agreement** von 1946, dessen Geheimhaltung im Juni 2010 aufgehoben wurde. Außerdem gibt es z.B. eine Zusammenarbeit der amerikanischen und deutschen Dienste im Rahmen der Überwachung und Vorbeugung terroristischer Aktivitäten, vgl. Gujer 2013, S.5. Siehe Kapitel 2.2.11 für weitergehende Informationen.

ist. Zusammen mit der Überwachung des Informationsflusses[87] und dem oben beschriebenen Zugang zu Verschlüsselungssystemen, kann auch die Cybersicherheit *zwischen* Computern ein Problem sein. Mittlerweile hat die US-Regierung die Nutzung von Exploits offiziell bestätigt, wobei die Entscheidung hierzu nach einer sorgfältigen Risiko-Nutzen-Abwägung erfolgt, d.h. wer könnte noch davon wissen, wie groß ist das Risiko der Entdeckung, welchen Schaden könnten die eigenen User und Firmen nehmen[88].

- Ein weiteres Problem ist der **Zugriff vor der Verschlüsselung**, da manche Provider verschlüsselte Nutzerdaten für die interne Verarbeitung entschlüsseln und anschließend wieder verschlüsseln. Durch den Zugriff auf solche Zentralrechner können Angreifer die Verschlüsselung also umgehen. Aus diesem Grunde waren schon 2010 mehrere Staaten an den Blackberry-Provider Research in Motion (RIM) herangetreten, Server in ihren Ländern zu installieren[89].
- Die Vergabe von sensiblen Aufträgen an externe IT-Anbieter birgt Risiken durch Bildung zusätzlicher Schnittstellen, die von Angreifern ausgenutzt werden können[90]. Zudem droht der Verlust interner IT-Kompetenz.
- Ein neues Gebiet des Cyberwars sind **offline-Attacken** auf Computer, die nicht mit dem Internet verbunden, also offline sind. Solche Computer können natürlich durch infizierte USB-Sticks befallen werden, aber man nahm an, dass die Wahrung räumlicher Distanz (**air gaps**) doch eine hohe Sicherheit bieten würde.
- Nach Berichten über ein Schadprogramm namens **BadBios** Ende 2013, bei dem eine Datenübertragung durch die Luft vermutet wurde[91], berichtete die New York Times über die Möglichkeit eine Übertragung von Informationen aus Computern über Radiofrequenzen, die von der NSA im Rahmen der aktiven Verteidigung eingesetzt wird (Projekt **Quantum**). Dazu reicht ein heimlich eingebauter winziger Sender in einem USB-Stick oder im Computer aus, wobei die Information einige Kilometer weit gesendet werden kann[92]. Auch wenn die technischen Details unbekannt

[87] Dies schließt die konventionelle Überwachung papierbasierter und analoger Kommunikation wie auch das Abhören von Daten aus Glasfaserkabeln mit ein, vgl. Gutschker 2013b, S.7, Welchering 2013b, S.6. In Überstimmung mit den jeweils gültigen nationalen Gesetzen, wie z.B. dem 1994 **Communications Assistance for Law Enforcement Act (CALEA)** und dem **Foreign Intelligence Surveillance Act (FISA)** in den USA, geben Provider ggf. Zugang zu Daten oder Systemen.
[88] Daniel zitiert von Abendzeitung 2014
[89] vgl. Schlüter/Laube 2010, S.8
[90] Einige Beispiele für externe Auftragsvergabe: Die Schweiz plant eine umfangreiche Auftragsvergabe ihrer öffentlichen IT-Infrastruktur, die Bundeswehr hat Verschlüsselungssysteme von US-Anbietern genutzt, vgl. Scheidges 2011, S.17, Baumgartner 2013, S.25. Die US-Firma CSC unterstützte Deutschland bei der Entwicklung des elektronischen Passes und des öffentlichen De-Mail-Systems, vgl. Fuchs et al. 2013a, S.1 and 2013b, S.8-9
[91] vgl. Betschon 2013b, S.34
[92] vgl. Winker 2014a, S.3

sind, haben Forscher gezeigt, wie ein akustisches, auf hochfrequenten Audiosignalen beruhendes verdecktes Computernetzwerk errichtet werden kann, das sogar keylogging über mehrere Stationen erlaubt[93]. Die Verwundbarkeit nimmt zu, denn die Computer kommunizieren zunehmend mit Smartphones oder sind in Smart Home oder Smart Entertainment-Umgebungen einbezogen. So kann auch das Auto oder der Fernseher [94] als Einfallstor genutzt werden.

2.2.3 Schadprogramme installieren

Während es bei der Computerspionage, die private, kommerzielle, kriminelle, politische oder militärische Grunde haben kann, um Versuche geht, in Computer 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. Mittlerweile ist es gängig, zuerst ein kleines Backdoor-Programm zu installieren und weitere Programme nachzuinstallieren und ggf. auch die Zugriffsrechte auf den infizierten Computer zu erweitern.
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[95] und **Rootkits** (Programme, die dem Angreifer das heimliche Einloggen und Steuern des Computers ermöglichen).

Cyberwaffen sind demnach Softwareprogramme, mit deren Hilfe man andere Computer angreifen, infiltrieren, ausspionieren und manipulieren kann und die ihre Ausbreitung selbsttätig steuern können. Derartige Programme nehmen an Häufigkeit zu, so dass die bisherige Einteilung in Viren, Würmer und Trojanern langsam an Bedeutung verliert. Der Ausdruck ‚Cyberwaffe' soll nicht suggerieren, dass es sich um ein militärisches Instrument handelt, denn auch hier gibt es keinen

[93] vgl. Hanspach/Goertz 2013, S.758 ff.
[94] Durch manipulierte Videodateien, vgl. Schmundt 2014, S.128
[95] vgl. Stark 2009, Schmitt 2009, S.83

substantiellen technischen Unterschied zu der Software, die im Bereich der Cyberkriminalität eingesetzt wird.

Die höchstentwickelten Cyberwaffen werden typsicherweise für das Ausspionieren von besonders wichtigen Zielen eingesetzt und mit Ausnahme von Stuxnet nicht für die Zerstörung. Die höchstentwickelten Programme weisen technische Gemeinsamkeiten auf (siehe auch Kapitel 3.3), die eine moderne Cyberwaffe charakterisieren: Anfangs wird nur ein kleines Programm geladen, um das Eindringen zu erleichtern. Um einer Entdeckung vorzubeugen, führt das Schadprogramm Schritte zur **Selbstverschlüsselung** durch und bereitet eine Option zur **Selbstlöschung** vor, die nach Abschluss der Cyberspionage-Operation genutzt werden kann. Zum letzteren gehört ggf. auch die Fähigkeit, **sich selbst abschalten** (stilllegen) zu können. Danach wird weitere Malware geladen in Abhängigkeit von der vorgefundenen Information. Anstatt große Schadprogramme zu kreieren, werden mittlerweile variable Module nachgeladen, die passgenau an die Zielperson und die Computerumgebung angepasst sind. Die fortgeschrittensten Programme erlauben eine mehr oder minder totale Kontrolle des Computers und einen Zugriff auf alle Daten. Die Speicherung der Malware und ggf. der Information findet an ungewöhnlichen Orten wie der Registry oder sogar der in der Hardware befindlichen Firmware statt, um so eine Entdeckung, aber auch eine Entfernung vom Computer zu blockieren. Ein typischer Schritt besteht darin, sich über User ohne besondere Rechte zu Administratorenrechten hochzuarbeiten (**lateral movement**). Dies resultiert in einem **Advanced Persistent Threat (APT)**, d.h. dem dauerhaften Zugang nicht-autorisierter Personen zu einem Netzwerk. Die Analyse der Malware wird durch falsche Spuren (**false flags**) erschwert, bei denen irreführende Zeitstempel und Spracheinstellungen in dem zur Programmierung genutzten Computer verwendet werden, zudem werden Code-Bruchstücke, die auf andere Hackergruppen hinweisen, eingebaut.
Mittlerweile entwickelt sich eine neue Terminologie zu Cyberwaffen, man spricht nun auch von **digitalen Waffen (D-Waffen), elektronischen Waffen (E-Waffen)** oder auch von **virtuellen Waffen**[96].

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)

96 vgl. Schmundt 2015, S.120-121, Langer 2014b, S.1

von mehreren Rechnern koordiniert angegriffen, was selbst leistungsfähige oder gut gesicherte Computersysteme funktionsunfähig machen kann[97].
Das Werkzeug, um mit einer DDoS-Attacke anzugreifen, ist das **Botnetz**.
Man kann Computer mit Hilfe eingeschleuster Programme[98] 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[99].

Die Dominanz der Botnetze hat mit folgendem zu tun:

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[100].
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[101].

---

[97] 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.

[98] 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.

[99] 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.

[100] Zudem können Staaten auch auf informelle Hackergruppen, d.h. nicht in offiziellen staatlichen Positionen arbeitende Spezialisten zurückgreifen, die im Falle einer erfolgreichen Rückverfolgung (Attribution) auch als Puffer dienen können, d.h. der Staat kann die Verantwortung dann ggf. zurückweisen. Hacker, die ihr Know-How in den Dienst des Staates stellen, um diesen zu schützen, werden zuweilen auch als **white hat** oder **ethische Hacker** im Unterschied zu destruktiv agierenden **black hat**-Hackern bezeichnet.

[101] WhiteWolfSecurity 2007

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[102]. Gleichwohl ist zumindest vorläufig davon auszugehen, dass der Einsatz von Botnetzen vorerst ein Kernelement massiver Angriffe bleiben wird.

Eine Unterart einer Cyberwaffe ist die **logische Bombe**, d.h. eine Schadsoftware, die erst zu einem definierten Zeitpunkt oder nach einer vorgegebenen Zahl an Computeraktivitäten aktiv wird. Ein aktuelles Beispiel einer logischen Bombe ist die datenlöschende Wiper-Malware Schadsoftware **DarkSeoul**, die im März 2013 in allen infizierten Computern gleichzeitig aktiv wurde[103]. Mittlerweile wurden verschiedene destruktive Attacken mit Wiper-Malware berichtet, siehe Kapitel 3.3.

Eine neue Variante der DDoS-Attacken ist sogenannter **fake traffic**. In einem Test konnte eine fake traffic software von einem Computer aus 100,000 Klicks auf eine einzige Website ausführen, aber es so aussehen lassen, als wenn jeder Klick von einem anderen Computer gekommen wäre, d.h. man kann auf ein Botnetz verzichten. Man kann auf Twitter ebenso große Mengen an fake tweets erzeugen und menschliche Kommunikation vortäuschen (**socialbots, internet of thingies**)[104].

2.2.5 Attribution

Die Attribution, d.h. die Lokalisation und Identifikation eines Angreifers, um Gegenmaßnahmen einleiten zu können, ist ein notwendiges, aber bislang nur schwer zu realisierendes Ziel.

---

[102] vgl Gaycken 2009

[103] vgl. Darnstaedt/Rosenbach/Schmitz 2013, S.76-80

[104] vgl. Graff 2014, S.13. Ein neuer Trend der Bot-Kommunikation ist der **Bot-Journalismus**, bei denen ohne menschliches Zutun Wetter- und Sportnachrichten erstellt werden. Anbieter dieses neuen Service sind z.B. die Firmen Narrative Science und Automated Insights, vgl. Dörner/Renner 2014, S.18-19

Dennoch macht die **Attributionsforschung** Fortschritte. Zum einen kann man, statt einen infizierten Rechner sofort abzuschalten, diesen nutzen, um die Art der Informationen und den/die Computer, an den diese Informationen geschickt werden, zu ermitteln, wenngleich die Informationen evtl. erst über Zwischenserver („springboard computers“) geleitet werden.

Zudem hinterlassen Hacker auch **digitale Fingerabdrücke**, womit man charakteristische Zugriffsmuster oder Programmcodes bezeichnet. Diese erlauben eine Differenzierung zwischen Angreifergruppen[105].
Diese Zugriffsmuster können sich ggf. auf **malware families** (verwandte Arten von Schadsoftware), die Nutzung von bestimmten Werkzeugen oder Werkzeugkombinationen, Zielrichtung des Datendiebstahls, Nutzung bestimmter Verschlüsslungen, Nutzung verdeckter Kommunikation zu Kontrollrechnern des Angreifers (z.B. durch Vortäuschung legitimen Datenaustauschs) und der benutzten Sprache (inkl. Schreibfehlern, -stil, bevorzugten Begriffen etc.) beziehen [106].

Inzwischen werden die **Programmierstile** von Programmieren gesammelt und ausgewertet, so dass neue Softwareprogramme mit älteren abgeglichen werden können (‘Stilometrie’). Die NSA untersucht z.B. die Art und Weise, wie Klammern gesetzt, Variablennamen benutzt und Leerstellen gesetzt werden und die Struktur des Programmiertexts. Programmtexte werden z.B. während Hackercamps gesammelt oder auch Arbeiten von Informatikstudenten. Jedoch nimmt die Nutzung von Verschleierungssoftware (**obfuscation software**) zur Ersetzung von Namen und Veränderung von Klammern zu[107].

Wichtig ist jedoch, dass selbst eine erfolgreiche Abgrenzung einer bestimmten Gruppe von Angreifern noch keine Auskunft darüber gibt, ob diese im Dienste eines Staates stehen.

Die Praxis der Attribution hat sich mittlerweile gewandelt. Eine wachsende Zahl privater Sicherheitsfirmen sammelt Daten und führt Langzeitanalysen zur Identifikation von Angreifern durch, siehe auch Kapitel 3.3. In schwierigen Fällen tendieren die Firmen auch zur Kooperation und zur Kombination ihrer Analysen. Da die ausgefeiltesten Attacken typischerweise von Gruppen ausgeführt werden, die über mehrere Jahre operieren und nicht etwa als isolierte ‘Hit and run’-Angriffe, werden die Anstrengungen zur Attribution immer effektiver, siehe auch Kapitel 3.3.

[105] vgl. Mayer-Kuckuck/Koenen/Metzger 2012, S.20-21
[106] vgl. Mandiant 2013
[107] Welchering 2016, S.T4

Laut Angaben von Yomiuri Shimbun hatte das japanische Verteidigungsministerium im Jahr 2008 an die Firma Fujitsu Ltd. den Auftrag erteilt, in drei Jahren eine Cyberwaffe zu entwickeln, die nicht nur Cyberattacken zurückverfolgen, sondern auch die Quellecomputer unschädlich machen soll. Diese Waffe soll in der Lage sein, auch zwischengeschaltete Computer zu überwinden. Die Entwicklung, für die ein Budget von 178,5 Millionen Yen bereitgestellt wurde, wurde bereits in Testnetzwerken erfolgreich erprobt[108].

Die dem US-Verteidigungsministerium zugehörige **Defense Advanced Research Projects Agency DARPA** hat im Rahmen des ‚**Plan X**', zu dem auch eine teilweise geheime Tagung am 27.09.2012 gehörte, ein Projekt gestartet, das den gesamten Cyberspace (Computer und andere Digitalgeräte) erfassen und optisch als aktuelle digitale Landkarte darstellen soll[109]. Das Budget der Plan X-Forschung beträgt 110 Millionen US-Dollar.

2.2.6 Abwehr von Cyberattacken

2.2.6.1 Erkennung und Vorbeugung von Attacken

Zusätzlich zu den üblichen Empfehlungen zur Cyberabwehr wie der Nutzung starker (schwer zu erratender) Passwörter, aktualisierten Systemen, vorsichtigem Verhalten im Internet, Vermeidung verdächtiger e-mails und Anhänge usw. wird die automatisierte Erkennung von Angriffen immer mehr verstärkt.

Die US-Regierung baut im Moment hochentwickelte Sensorsysteme aus[110]: Das **Continuous Diagnostics and Mitigation (CDM)**-Programm kann abnormes Verhalten in Echtzeit erkennen und entsprechende Übersichtsberichte an Administratoren erstellen.
Einstein 3A arbeitet mit Sensoren an Webzugangspunkten, um Bedrohungen aus dem zu schützenden System herauszuhalten, während das CDM Bedrohungen identifizieren soll, wenn sie schon im System sind.

US-Forscher haben Mustererkennungsalgorithmen zur Cyberabwehr entwickelt, die im Falle eines erkannten Angriffes die Löschung von Datenpaketen des Angreifers erlauben. Zur Vermeidung von Eskalationen ist jedoch keine automatisierte Vergeltung vorgesehen. China erforscht Simulationen von Cyberattacken[111].

[108] vgl. Daily Yomiuri online 03 Jan 2012
[109] vgl. DARPA 2012, Nakashima 2012b
[110] vgl. Gerstein 2015, S.4-5
[111] vgl. Welchering 2014b, S.T4

Zu diesem Zweck hat die Deutsche Telekom 200 **Honeypot** ('Honigtopf')-Computer in ihrem Netz installiert, die durchschnittliche Mobiltelefone und Computer simulieren. Diese Computer erfassen jede Aktivität des Angreifers[112], das Analysesystem wird auch als Sandkasten (**sandbox**) bezeichnet. Da fortschrittliche Malware in virtuellen Maschinen (Testumgebungen) ruhig bleibt, versuchen fortschrittliche sandboxes echten Computern so gut wie möglich zu ähneln. Jedoch ist Malware ggf. durch das sogenannte **code morphing** geschützt, das ist eine Verschleierungsmethode, um Software gegen Nachbau durch reverse engineering, Analysen, Modifikationen und Codeknacken (cracking) zu schützen.

Rob Joyce, Leiter der **NSA Tailored Access Operations (TAO)**-Gruppe, gab auf einer öffentlichen Präsentation bei einer Konferenz im Januar 2016 Sicherheitsempfehlungen. Zum Eindringen werden auch die winzigsten Lücken genutzt, auch vorübergehende Lücken während der (Fern-)Wartung. Andere interessante Ziele sind Lüftungs- und Heizungssysteme, wenn die Gebäudeinfrastruktur entsprechend vernetzt ist, Cloud Service-Verbindungen, hartkodierte Passwörter, Logdateien von Systemadministratoren, sowie Smartphones und andere Geräte, während Zero day-Lücken in der Praxis nicht so bedeutsam seien[113]. Deshalb enthielten die Sicherheitsempfehlungen das **Whitelisting** (nur gelistete Software kann genutzt werden), die Nutzung aktualisierter Software, segmentierter Netzwerke (mit Abtrennung wichtiger Bereiche), **Reputationsmanagement** zur Wahrnehmung abnormen Nutzerverhaltens und eine genaue Überwachung des Netzwerkverkehrs.

2.2.6.2 Analyse von Sicherheitslecks

Das gesicherte **Secret Internet Protocol Router Network SIPRNET** der USA ist inzwischen zu groß geworden und hat zu viele Zugangsberechtigte[114], wie die Debatten nach den aus dem SIPRNET stammenden WikiLeaks-Enthüllungen vom 28.11.2010 gezeigt haben[115].
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

[112] vgl. Dohmen 2015, S.75
[113] vgl. Beuth 2016a, S.1-3
[114] Es handelte sich um 2,5 Millionen Zugangsberechtigte und 280.000 Personen für die höhere Geheimhaltungsstufe; vgl. Schneider 2011, S.9
[115] vgl. Schaaf 2010, S.9

bekommt nur die Informationen, die für die Aufgabe notwendig sind) Rechnung[116]. In einem ersten Schritt haben die USA die Zahl der Zugangsberechtigten verkleinert[117].

Im Jahr 2012 hatte ein IT-Administrator innerhalb des Schweizer Geheimdienstes, des **Nachrichtendienstes des Bundes NDB**, eine nicht autorisierte Datensammlung begonnen, die jedoch rechtzeitig entdeckt worden konnte. Gegenmaßnahmen bestanden hier in der Trennung von und Zugangsbeschränkung für sensitive Datenbanken und dem **Vier Augen-Prinzip** für Eingriffe in die IT[118].

Die öffentliche Enthüllung der Überwachungsprogramme PRISM der NSA und Tempora der britischen GCHQ mit der Einbeziehung großer Internetfirmen wie auch von Telekommunikationsanbietern[119] durch den früheren Mitarbeiter der Sicherheitsfirma Booz Allen Hamilton, Edward Snowden, und die nachfolgende Berichterstattung in der Zeitung *The Guardian* führten zu einer breit angelegten Sicherheitsdebatte[120].
Tatsächlich haben in den USA 1,5 Million Personen eine Sicherheitsstufe für Cyberangelegenheiten, davon arbeiten 480.000 in privaten Firmen[121]. Vom ODNI (office of the Director of National Intelligence, das die Geheimdienste der USA, die Intelligence Community, koordiniert) wurde berichtet, dass 70% des Geheimdienstbudgets in private Firmen fließen[122]. Es wurde auf der anderen Seite darauf verwiesen, dass die Zusammenarbeit mit Privatfirmen schon lange besteht[123] und es notwendig ist, Expertenwissen für den rapide wachsenden Cybersektor nutzen zu können.

2.2.6.3 Abwehr von DDoS-Angriffen

Die deutsche Sicherheitsbehörde BSI hat generelle Empfehlungen zur Abwehr von DDoS-Attacken herausgegeben[124]. Der attackierte Server kann die Antwortzeit zum angreifenden Computer verlängern, so dass letzterer sehr lang auf die

[116] vgl. Sattar et al. 2010, S.3
[117] vgl. Schneider 2011, S.9
[118] Vgl. Gujer 2012a, S.30, Gujer 2012b, S.24, Häfliger 2012a, S.29. Die wichtigste Einrichtung der Schweizer Cybersicherheit ist die **Melde- und Analysestelle Informationssicherung Melani**, bei der das Verteidigungs- und das Finanzministerium sowie der NDB mitwirken, Gujer 2012a, S.30.
[119] vgl. Tomik 2013b, S.2.
[120] Jedoch wurden einige dieser Sachverhalte bereits während der europäischen "Echelon-Debatte" in den 1990er Jahren erörtert, zum Beispiel die vermuteten globalen Überwachungskapazitäten der Telekommunikation, des Internets und der emails durch die NSA. Die Debatte mündete in der Erstellung eines zusammenfassenden Berichtes durch die EU 2001, vgl. Ulfkotte 1998, S.8, FAZ 2000, S.1, Schröm 1999a/b, Schmid 2001, Schöne 1999, S.32, Schöne 2000, S.39
[121] vgl. Gartmann/Jahn 2013, S.24
[122] vgl. Huber 2013, S.18-19
[123] BAH knackte die Codes deutscher U-Boote im zweiten Weltkrieg, vgl. Gartmann/Jahn 2013, S.24. Andere Sicherheitsfirmen sind z.B. Xe und USIS.
[124] vgl. BSI 2012

Antworten warten muss. Diese Methode ist auch als **Teerfalle** oder Teergrube bekannt (**tar pitting**).
Zudem kann die Zahl der Verbindungen pro IP-Adresse beschränkt werden. Wenn bestimmte Quelladressen blockiert werden, nennt man dies **sinkholing**. Durch Blockade von vermuteten Herkunftsregionen der Attacke (Geoblocking) kann die Wirksamkeit der Abwehr weiter erhöht werden, aber mit dem Risiko, auch legitime Anfragen zu blockieren. **Blackholing** ist die Abschaltung der attackierten IP-Adresse, was sinnvoll sein kann, wenn dadurch Kollateralschäden an anderen Computersystemen des Attackierten verhindert werden können.
Als vorbeugende Maßnahme kann der eingehende Internetverkehr ggf. auf die sichereren **Transport Layer Security (TLS)/Secure Sockets Layer (SSL)**-Ports beschränkt werden. Zu guter Letzt können ggf. auch **DDoS mitigation services** eingesetzt werden, d.h. der Internetprovider wird einbezogen, um eingehenden Internetdatenverkehr zu reduzieren oder zu blockieren.

2.2.6.4 Automatisierte Cyberabwehr

Die Forschungsagentur des US-Verteidigungsministeriums **Defense Advanced Research Projects Agency DARPA** führte am 04.08.2016 die **Cyber Grand Challenge** in Las Vegas durch, wobei 7 Computer Cyberattacken wahrnahmen und vollautomatisch, d.h. ohne jeden menschlichen Eingriff, darauf reagierten. Dieser Wettbewerb ging über 12 Stunden und 30 Runden. Die Computer und ihre Programmierteams wurden aus hundert Bewerbern ausgewählt[125].
Eine Maschine namens *Mayhem* gewann den Wettbewerb, indem sie die meiste Zeit über passiv blieb, während die anderen sich gegenseitig bekämpften. Eine andere Maschine nahm eine Sicherheitslücke wahr, der von ihr hergestellte Patch verlangsamte jedoch die Maschine, so dass die Maschine entschied, den Patch besser wieder zu entfernen [126]

Die DARPA war mit dem Ergebnis zufrieden, da es ein erster Schritt in Richtung vollautomatischer Abwehr- und Reaktionssysteme war.[127]. Da die Zahl der Sicherheitslücken inzwischen immens ist128, könnten automatisierte Systeme unbekannte Lücken wahrnehmen und stoppen.

Während es möglich sein mag, die Routineüberwachung an Maschinen zu übertragen, wird die menschliche Aufsicht unverzichtbar bleiben. Andernfalls könnte eine irregeführte (gespoofte) Maschine sich entschliessen, das eigene Netzwerk anzugreifen. Oder ein Angreifer könnte die Maschine davon

[125] vgl. DARPA 2016
[126] vgl. Atherton 2016
[127] vgl. DARPA 2016
[128] Eine US-Datenbank hat 75.000 Sicherheitslücken in 2015 gesammelt, vgl. Betschon 2016; in einem Test fand das Pentagon 138 Sicherheitslücken in seinen Systemen, vgl. Die Welt online 2016

überzeugen, in den inaktiven Zusatnd überzugehehn oder einen Patch zu konstruieren, der das Verteidigungssystem lahmlegt.

2.2.7 Sicherheit von Smartphones

Das Abhören von Regierungshandys[129] ist nur ein Teil der Sicherheitsprobleme, die sich aus der Nutzung von Smartphones, Personal digital assistants (PDAs) and Tablet PCs ergeben. Das Smartphone ersetzt zunehmend den Computer in Alltagsroutinen wie dem Internetzugang und der Arbeit mit emails und der Trend geht in Richtung Nutzung als digitaler Generalschlüssel (**virtual master key**) für das Onlinebanking, Kontrolle intelligenter Haustechnik (**smart homes**)[130], der Energieversorgung über intelligente Stromnetze (**smart grid**) und zukünftig auch für die Autosteuerung im Rahmen von **e-mobility**-Projekten[131]. Das Smartphone wird zunehmend als erster Internetzugang insbesondere in Afrika genutzt, wo deshalb die Internetnutzung rapide zunimmt.[132]
Das **bring your own device–(BYOD)-Konzept** beschreibt die Möglichkeit, kabellos zahlreiche Geräte mit Hilfe eines zentralen Gerätes zu steuern. Momentan wird die Unterhaltungselektronik zunehmend zentral von Festplattenrekordern oder z.B. der X-Box gesteuert, aber auch hier geht die Entwicklung in Richtung Smartphone oder Tablet. Die BYOD-Philosophie produziert eine Art **Schatten-IT** in Unternehmen, die sehr schwierig zu kontrollieren und zu sichern ist[133].

Im Ergebnis könnten erfolgreiche Angreifer nicht nur Kenntnis über alle privaten Dateien und das Onlinebanking erhalten und die Nutzer über die Mobilfunkzellen verfolgen, sondern auch die Kontrolle über den Haushalt und das Auto übernehmen.
Relevante Angriffswege (*zusätzlich* zu allen Risiken, die aus emails und Internetzugang resultieren) [134] sind das einfache Abfangen von Funkwellen durch Antennen (der GSM Standard ist nicht sicher[135]), Vortäuschen von Funkmasten durch **IMSI-Catchers**, Zugang zu Knotenrechnern oder deren Kabel[136], Einbringen von Trojanern oder Viren durch infizierte Apps, unzulässiger Datenfluss durch versteckte App-Funktionen[137], oder durch Zusendung unsichtbarer und stummer SMS (**stealth SMS**), um Spionagesoftware wie

[129] vgl. Graw 2013,S.4-5. Derartige Vorkommnisse wurden u.a. für Indonesien, Deutschland und Brasilien berichtet.
[130] vgl. RWE 2013
[131] vgl. Heinemann 2013, S.3
132 vgl. Langer 2014a, S.7
[133] vgl. Müller 2014, S.16
[134] vgl. Ruggiero/Foote 2011
[135] vgl. FAZ 2013c, S.14
[136] vgl. Wysling 2013, S.5
[137] vgl. Focus online 2013

Flexispy [138] aufzuspielen. Im Juli 2015 wurde über eine neue Sicherheitslücke in Android-Smartphones berichtet, bei der **MMS** Schadcode übertragen können, wobei die MMS danach gelöscht wird, d.h. die Nachricht muss zur Aktivierung nicht geöffnet werden. Die **StageFright**-Malware erlaubt den Angreifern dann die Nutzung der Audio- und Videofunktionen[139]. Die später entdeckte Variante Stagefright 2.0 nutzte MP3.Musikdateien anstelle von MMS.
Krpto-Handys mit End-zu-End-Verschlüsselung sind eine empfohlene Sicherheitslösung, aber sie haben auch Nachteile, weil sie oft umständlich zu handhaben sind und überdies auch nur funktionieren, wenn die Gegenseite dasselbe Verfahren benutzt, andernfalls wird die Verschlüsselung abgeschaltet[140].

Forscher der Deutschen Telekom haben gezeigt, dass das Eindringen in ein Smartphone einschließlich des Diebstahls aller Daten, Änderung der Einstellungen und der Installation eines Tools zum Fernzugriff in der Praxis nur rund 5 Minuten braucht[141]. Inzwischen wird deutschen Ministern die Nutzung von **Einweg-Handys** empfohlen, die einmalig während einer Reise gebraucht werden und dann zerstört werden.[142]

Forscher fanden Schwächen im Verschlüsselungsalgorithmus A5/1 des **Global System for Mobile Communications (GSM)**, der durch den stärkeren Schlüssel A5/3 abgelöst wurde. Das Roaming-Protokoll–SS7 weist Schwachstellen auf, die zur Umleitung von Anrufen oder Zugriff auf Orts- und Kommunikationen durch Angreifer genutzt werden konnten.[143] Dies kann durch Anfragen oder das Vortäuschen der SS7-Datenbank, des **Home-Location-Registers (HLR)** geschehen. Eine weitere Methode ist das Entwenden von SIM-Kartenschlüsseln. Mittlerweile ist geplant, konventionelle SIM-Karten durch eingebettete umprogrammierbare (eingebettete) SIM-Karten zu ersetzen (**embedded SIM**). Das Konzept stammt aus dem ursprünglich für Maschine-zu-Maschine-Kommunikation entwickelten GSMA-Standard, der einen Operatorwechsel aus der Distanz “over the air” erlaubt[144].

Im Rahmen einer Untersuchung von Smartphones durch die französische Sicherheitsfirma *Eurecom* wurden 2000 Applications (Apps) für Android-

---

[138] vgl. Welt 2013, S.3, Opfer 2010
[139] vgl. Steler 2015
[140] vgl. Drissner 2008, S.4, Opfer 2010
141 Zu diesem Zweck hat die Deutsche Telekom 200 Honeypot (‘Honigtopf’)-Computer installiert, die durchschnittliche Mobiltelefone und Computer simulieren. Diese Computer erfassen jede Aktivität des Angreifers; vgl. Dohmen 2015, S.75
[142] vgl. Der Spiegel 2015, S.18
143 vgl. Der Spiegel online 2014, S.1, vgl. Zeit online 2014a
144 Zeit online 2015b, GSMA 2015. Da eingebettete Programme ebenfalls infiziert werden können, kann dies eine zukünftige wesentliche Schwachstelle von Smartphones und der smart industry werden, siehe Kapitel 3.2.12

Mobiltelefone auf ein Samsung-Smartphone geladen. Dann wurde die **Hintergrundkommunikation**, d.h. Internetverbindungen, die nicht auf dem Schirm angezeigt werden, untersucht. Die untersuchten Apps sendeten im Hintergrund Daten an ca. 250.000 Webseiten, die aktivste App allein an 2.000 Server. Typischerweise handelt es sich um Webseiten von Analyse- und Marketingdiensten.[145]
Ein weitere Problem sind **gefälschte Apps**, die legitime Inhalte zu haben scheinen, aber Malware enthalten, die Smartphones dazu zwingen kann, im Hintergrund andere Webseiten zu laden. Die **XCode Ghost** Malware infizierte iO-Apps von Apple im September 2015 über ein infiziertes Softwareentwicklungs-Toolkit für die Programmierung von Apps. Mehr als 250 infizierte Apps wurden deshalb aus App Stores entfernt[146].

QR codes (Quick Response Codes), d.h. matrix-förmige oder zweidimensionale Barcodes können die Smartphones beim Scannen zu bösartigen Webseiten umleiten[147]. Die **Near Field Communication (NFC)** ist eine berührungslose smart card-Technologie, die z.B. zum Bezahlen per Handy über Kurzstreckensignale benutzt wird. In 2 Hackerwettbewerben für mobile Endgeräte 2012 und 2014 wurden Sicherheitslücken gefunden, die dann geschlossen wurden[148].

Anfang 2016 versuchte das FBI, ein iPhone eines Verdächtigen zu entschlüsseln, was dann mit Hilfe der israelischen Firma *Cellebrite* gelang[149].
Im August 2016 wurde die hochentwickelte iPhone-Malware **Pegasus** von der Sicherheitsfirma *Lookout* und dem kanadischen *Citizen Lab* berichtet, die zunächst in drei iPhones in Mexiko, den VAE und Kenia gefunden wurde[150]. Nach dem Anklicken eines bösartigen Links wurde die modular aufgebaute Malware mittels eines drive-by downloads auf das iPhone geladen und war dann in der Lage, Passwörter, Photos, emails, Kontaktlisten und GPS-Daten zu sammeln[151].
Lookout vermutete, dass diese Malware vom privaten Cyberwaffenanbieter *NSO Group* aus Israel stammte. Die NSO group erklärte jedoch, ihre Produkte nur an Regierungen, Nachrichtendienste und Militärs im Rahmen der jeweiligen gesetzlichen Reglungen zu verkaufen[152].

[145] vgl. Spehr 2015, S.T4
[146] vgl. T-online 2015
[147] vgl. Beuth 2016a, S.1-3
[148] vgl. Lemos 2015
[149] vgl. FAZ online 2016
[150] vgl. Die Welt online 2016
[151] vgl. Die Welt online 2016, FAZ online 2016
[152] vgl. Jansen/Lindner 2016, S.28

2.2.8 Cybersicherheit von komplexen Maschinen

2.2.8.1 Smart Industry (Industrie 4.0)

Komplexe Industriemaschinen, die durch SCADA- und ICS-Systeme gesteuert werden, stellen neben Autos und Flugzeugen das wichtigste Sicherheitsproblem dar, wobei diese Maschinen zu gezielten Angriffen auf die Infrastrukturen oder Individuen genutzt werden können.
Industriemaschinen bzw. cyber-physische Systeme kommunizieren nicht in geschlossenen Systemen, sondern können in der Regel über das mit dem Internet verbundene Betriebsnetzwerk erreicht werden, was Angriffe von außen ermöglicht[153]. Die Hackergruppe **Dragonfly** (**Energetic Bear/Crouching Yeti**) drang bei den Anbietern von ICS-Programmen ein, so dass alle Nutzerunternehmen die Malware automatisch mit dem nächsten Update in ihre Programme luden[154]. Die Gruppe nutzt die **Havex/Backdoor Oldrea**-Malware zur Infiltration und Modifikation von ICS- und SCADA-Systemen und installiert eine Backdoor. Zusätzlich zur Infektion von Anbietern von ICS-Programmen boten die Hacker ‚Wasserlöcher' (**watering holes**) an, d.h. sie infizierten häufig besuchte Webseiten der Zielgruppe, um die Besucher dann zu anderen bösartigen Webseiten umleiten zu können und zudem wurden e-Mails mit infizierten PDF-Dateien eingesetzt[155]. Als weiteres Werkzeug diente **Trojan.Karagany**, der aber auch auf dem Schwarzmarkt verfügbar ist. Die Arbeitszeiten lassen die Gruppe in Osteuropa (GMT plus 4 Stunden) vermuten [156].

Aber wie die japanische Softwarefirma *Trend Micro* gezeigt hat, werden ICS- und SCADA-Systeme inzwischen regelmäßig von Angreifern auf Schwachstellen geprüft. Eine simulierte Wasserversorgung wurde als "Honigtopf" zum Anlocken von Hackern installiert. Über 28 Tage wurden 39 Cyberattacken aus 14 Ländern mit Manipulationen und Einspielung von Schadsoftware beobachtet. Das US-amerikanische ICS Emergency Response Team berichtete über 172 Sicherheitslücken bei 55 verschiedenen Anbietern[157]. SCADA-Systeme haben oft keine automatischen Sicherheitsupdates bzw. Virusscans und Firewalls können oft nicht implementiert werden, ohne die Haftung des Maschinenherstellers entfallen zu lassen[158].

153 Für die Kontrolle von Maschinen aus der Distanz wird auch Satellitenkommunikation genutzt, die nötigen **Very Small Aperture Terminals VSATs** sind jedoch ebenfalls anfällig, vgl. Reder/van Baal 2014, S.V2
154 vgl. Metzler 2015, S.34
155 vgl. Campbell 2015, S.11
156 vgl. Symantec 2014b
157 vgl. Betschon 2013a, S.38
158 vgl. Striebeck 2014

In einem Eindringtest war ein ethischer Hacker in der Lage, die Wasserversorgung in Ettlingen in weniger als 2 Tagen zu infiltrieren und die Kontrolle zu übernehmen[159].
Am 18.12.2014 berichtete das Bundesamt für Sicherheit in der Informationstechnik BSI, dass Hacker in das normale Büronetzwerk eines Stahlunternehmens vorgedrungen waren und von dort aus in die Produktions-IT gelangten und einen Hochofen beschädigten[160].

Das US Industrial Control Systems Cyber Emergency Response Team (**ICS-CERT**) empfiehlt[161] die Minimierung aller Netzwerkkontakte der Kontrollsystemgeräte mit Schutz durch Firewalls und Vermeidung von Internetzugängen. Falls ein Zugang über das Netz nicht vermieden werden kann, kann der Zugang mit Virtual Private Networks (VPNs) abgesichert werden. Voreingestellte Systemzugänge sollten nach Möglichkeit entfernt, umbenannt oder deaktiviert werden.
Shodan ist die erste Suchmaschine, die nach mit dem Internet verbundenen Dingen, Webcams und ICS/SCADA-Systemen sucht und von Hackern genutzt werden kann, aber eben auch von Netzwerkadministratoren, die so die eigene Arbeitsumgebung nach Schnittstellen zum Internet abchecken können. Natürlich gelten auch hier die allgemeinen Empfehlungen zur Cyberabwehr (starke Passwörter, Whitelisting von Anwendungen (**Application Whitelisting** AWL etc.).

Smarte Gegenstände, die mit IP-Adressen versehen sind, erlauben eine präzise Steuerung von Produktionsabläufen, aber können als **Thingbots** missbraucht werden. Die Sicherheitsfirma Proofpoint berichtete von der missbräuchlichen Versendung von e-mails zwischen Dezember 2013 und Januar 2014, wobei mehr als ein Viertel von Thingbots verschickt wurde, d.h. infizierten Geräten wie Routern, Fernsehern und mindestens einem Kühlschrank. Dies wurde durch Probleme mit der Konfiguration, veralteter Firmware und Verwendung von Standardpasswörtern möglich.[162]

Ein Hauptproblem von **Smart Home**-Funktionen und ihrer Sicherheit sind die mangelnde Kompatibilität der Geräte mit häufigen Modifikationen durch Updates und konkurrierenden bzw. überlappenden Standards wie z.B. *ZigBee* mit weiteren nachgeordneten Standards, *Thread, Home Matic, Qivicon* etc. was zu Störungen der Konnektivität und einer hohen Zahl an potentiell verwundbaren Schnitttellen beiträgt[163].

159 vgl. Reder/van Baal 2014, S.V2
160 vgl. Krohn 2014, S.24
161 vgl. ICS-CERT 2016a
162 vgl. Market Wired 2014, S.1-2
163 vgl. Weber 2016, S.T1

2.2.8.2 Die Cybersicherheit von Autos und Flugzeugen

Die Digitalisierung von Autos macht schnelle Fortschritte, z.B. für Fahrassistenzsysteme, Motordiagnostik, Informations-, Navigations- und Unterhaltungssysteme, Sicherheits- und Kamerasysteme[164]. Das wichtigste Angriffsziel ist das **controlled area network (CAN)**, ein serielles Bussystem zur Vernetzung von Steuergeräten[165].
2016 werden 80 Prozent aller neu zugelassenen Autos in Deutschland einen Internetanschluss haben[166]. Ab 2018 müssen neu zugelassene Fahrzeuge in der EU das **E-call-**System haben, bei dem das Auto dann automatisch Notrufe bei Unfällen tätigen kann. Das System kann jedoch auch das Fahrverhalten durch Datensammlungen verfolgen[167].
Daneben gibt es auch den Trend, die IT-Infrastruktur fest in das Auto zu integrieren, wie momentan geplant bei Audi mit dem System Google Android. Forscher haben vier Gruppen von Sicherheitsproblemen ausgemacht, nämlich die Verbindung des Autos zu auswärtigen Servern (**Car to X connection**), die Sicherheit der Unterhaltungselektronik im Auto, die Wegfahrsperre und die internen Schnittstellen der Komponenten im Auto.[168].

Es gibt zunehmend Berichte über Autohacks, Nach einem erfolgreichen Eindringversuch von chinesischen Studenten (**Tesla**-Vorfall) wurde betont, dass solche Hacks eine direkte physische Verbindung zu den Systemen des Autos erfordern und nicht aus der Distanz erfolgen können[169]. Bis heute fanden alle Hacks in Forschungsumgebungen statt, typischerweise durch ethische Hacker, die die betroffenen Unternehmen informierten, so dass alle Sicherheitslücken rechtzeitig geschlossen werden konnten[170]. Jedoch gelang Mitte 2015 der erste Autohack aus der Distanz, wobei ein Cherokee Jeep-Modell aus 15 Kilometern Entfernung angegriffen werden konnte[171].

Smartphone Apps werden zunehmend physische Autoschlüssel ersetzen und werden es z.B. ermöglichen, das Auto mit anderen zu teilen. Das **keyless**-System erlaubt es, mit dem Smartphone über Bluetooth die Autotüren zu öffnen und den

164vgl. Hawranek/Rosenbach 2015, S.65
165 vgl. Fuest 2015, S.34-35
166 vgl. Schneider 2014
167 vgl. Fromme 2015, S.17
168 vgl. Karabasz 2014, S.14-15
169 vgl. Lewicki 2014, S.62
170 Mittlerweile engagieren Autohersteller Hacker, um die Sicherheit der Fahrzeuge zu prüfen, z.B. von der britischen Telekommunikationsfirma BT, vgl. FAZ 2015b, S.18
171 vgl. Der Standard 2015, S.1. Bisher gab es nur eine ‚echten' Autohack außerhalb von Forschungsumgebungen, dabei hat ein Mitarbeiter aus Ärger über seine Entlassung im Jahre 2010 hundert Fahrzeuge blockiert.

Motor zu starten[172], aber solche Signale können von Angreifern mit Hilfe eines **Repeater**-Gerätes leicht abgefangen und reproduziert werden[173].

Das Automodell Tesla S wurde Ende 2015 mit Autopiloten-Funktionen für partiell autonomes Fahren ausgestattet, darüberhinaus können ab jetzt kabellose Updates via WLAN als **firmware over the air (FOTA)** erfolgen, was die Anfälligkeit für Hackerangriffe erhöht[174], aber auch rasche Sicherheitsupdates ermöglicht[175]. Ein Tesla-Modell kollidierte am 07.05.2016 mit einem weißen LKW-Anhänger, der von der Sensoren des Autopiloten nicht erkannt worden war, der Fahrer hatte aber auch nicht reagiert[176].

Ähnliche Probleme tauchen in Zivilflugzeugen auf, in denen interne Netzwerke von der Unterhaltungssystemen für Passagiere manchmal nur durch eine Firewall getrennt sind. Zudem nimmt die interne Vernetzung der Bordsysteme ständig zu, so dass das Risiko für eine komplette Übernahme durch Hacker steigt. Kürzlich wurde berichtet, dass ein US-Experte in der Lage war, in das Unterhaltungssystem für Passagiere einzudringen und in einem Fall in der Lage war, auch in die Kontrollsysteme des Flugzeugs zu gelangen[177]. Auf einer höheren Ebene weist auch das US-Luftverkehrskontrollsystem Schwächen auf, insbesondere bei der Abgrenzung der Systeme, insbesondere auch der Schlüsselsysteme gegenüber weniger sicheren Systemen. Das US Government Accountability Office hat Empfehlungen zur Behebung dieser Probleme herausgegeben.[178]

2.2.8.3 Die Black Energy Attacken

Das US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) hat eine Malwarekampagne entdeckt, die mindestens seit 2011 läuft, verschiedene ICS-Systeme betraf und bei denen eine Variante der **Crimeware BlackEnergy** bei vernetzten Benutzerschnittstellen (auch Mensch-Maschine-Schnittstellen bzw. human-machine interfaces HMIs) eingesetzt wurde[179]. Unter anderem waren die Systeme *GE Cimplicity, Advantech/Broadwin WebAccess*, und *Siemens WinCC* betroffen.

---

[172] vgl. Rees 2016, S.2
[173] vgl. Heute 2016
[174] Das FBI und die US-Verkehrsbehörde National Highway Traffic Safety Administration NHTSA haben 2016 in einer Mitteilung ihre zunehmende Besorgnis über Hackerangriffe auf Autos geäußert und die Updates über Fernwartung als wichtige Schwachstelle beschrieben, vgl. BBC 2016
[175] vgl.Becker 2016, S.78
[176] vgl. Fromm/Hulverschmidt 2016, S.25
177 vgl. Rosenbach/Traufetter 2015, S.72f.
178 vgl. GAO 2015, S.1
[179] vgl. ICS-CERT 2016a

Crimeware ist Malware zur Unterstützung krimineller Aktivitäten. Weit verbreitete Crimeware besteht aus Spionagesoftware, um an Onlinebankingdaten zu gelangen, oder Trojanern, um Botnetze für DDoS-Attacken einzurichten. Eine zunehmend genutzte Crimeware-Art ist **Ransomware** (wörtlich 'Erpressungssoftware'), die Dateien oder Festplatten des Zielcomputers verschlüsselt, um dann Geld für die Entschlüsselungscodes zu fordern, z.B. als Überweisung von virtuellem Geld (Bitcoins) auf Auslandskonten. Moderne Ransomware kann auch externe Festplatten und Cloudspeicher verschlüsseln, aktuelle Beispiele für Ransomware sind **Locky** und **Cryptowall**[180].

The **Sandworm** or **Quedagh**-Gruppe group (die Namen beziehen sich auf gefundene Referenzen zur Science Fiction Welt *Dune* – der Wüstenplanet) nutzt die weit verbreitete Crimeware BlackEnergy gegen relevante Zielcomputer.
BlackEnergy ist seit 2007 verfügbar und mittlerweile existiert die Variante **BlackEnergy3**. BlackEnergy wurde ursprünglich erschaffen, um Botnetze für DDoS-Attacken zu errichten. Die Sandworm/Quedagh-Gruppe hat Modifikationen der herkömmlichen BlackEnergy-Malware vorgenommen und sie um vielfältige Funktionen ergänzt wie das Kapern inaktiver Laufwerke und die Fähigkeit zum umfangreichen Informationsdiebstahl[181]. Im Sommer 2014 fand die IT-Sicherheitsfirma *F-Secure Labs* diese Variante bei einem Angriff gegen ein ukrainisches Ziel, davor wurde bereits die NATO im Dezember 2013 angegriffen[182]. Jedoch bestätigte die NATO, dass die geheimen operativen Netzwerkbereiche nicht betroffen waren, da diese vom Internet abgetrennt sind[183].

Am 23.12.2015 kam es zu Stromausfällen in der Ukraine durch Cyberattacken bei drei regionalen Stromanbietern, die insgesamt ca. 225.000 Kunden betrafen[184]. Drei weitere Anbieter waren betroffen, hatten aber keine Stromausfälle. Die Eindringlinge[185] waren in der Lage, Stromverbindungen aus der Distanz zu öffnen, was zum Stromausfall führte, was in koordinierter Form in einem kleinen Zeitfenster geschah[186]. **Telephone denial of service-Attacken (TDoS attacks)**

[180] Anfang 2016 waren eine Reihe deutscher Kliniken erheblich von Ransomwareattacken betroffen, für weitere Details zur Ransomware vgl. Jüngling 2015, S.67. Mittlerweile wird Entschlüsselungs-´und Verschlüsselungs-Detektor-Software entwickelt, um der Ransomware entgegenzuwirken, vgl. Steier 2016a, S.36. Es gibt noch zahlreiche weitere kriminelle Aktivitäten im Internet, z.B. im DarkNet, welches typischerweise mit TOR-Browsern zugänglich ist, Überlappungen zum Cyberwar finden sich z.B. in der Anwendung von DDoS-Attacken.
[181] vgl. F-Secure Labs 2014, S.2, 10-11
[182] vgl. BBC 2014, S.1, F-Secure Labs 2014, S.2
[183] vgl. BBC 2014, S.2
[184] vgl. ICS-CERT 2016b
[185] Die Nutzung von BlackEnergy läßt die Urheberschaft der Sandworm/Quedagh-Gruppe zwar plausibel erscheinen, einen eindeutigen Beweis hierfür gibt es aber nicht.
[186] vgl. ICS-CERT 2016b

wurden genutzt, um die Anbieter–Hotlines mit Anrufen zu fluten, so dass die Kunden die Stromausfälle nicht telefonisch weitermelden konnten[187].
Am Schluss wurde die Wiper-Malware **KillDisk** benutzt, um die Systeme zu beschädigen.
Für diesen Vorfall in der Ukraine konnte das US ICS-CERT jedoch *nicht* bestätigen, dass die BlackEnergy3-Variante die Stromausfälle verursacht hatte, die Stromverbindungen konnten von den Angreifern auch ohne diese Schadsoftware geöffnet werden[188].

2.2.9 Die Professionalisierung des Cyberwars

Ursprünglich waren Cyberattacken das Ergebnis spontanen Hackens, aber inzwischen herrscht ein Trend zur Professionalisierung von Strukturen und Prozessen.
Auf der militärischen Ebene umfasst dies ein systematisches Training. Die US Navy trainiert zur Zeit 24.000 Personen im Jahr in ihrem **Information Dominance Center** und die US Air Force hat einen Kurs in der Nellis Air Force Base in Nevada eingerichtet (erste Absolventen im Juni 2012), in dem trainiert wird, wie man elektronische Eindringlinge erkennt, Netzwerke verteidigt und Cyberattacken ausführt[189].
Die Entwicklung geht nun in Richtung formalisierter Offizierslaufbahnen wie seit April 2010 die des ‚US Air Force 17 deltas officer' (**17D officer**), die eine Spezialisierung für Kommunikationsoffiziere darstellt[190]. Ebenfalls wurde ein undergraduate cyber training (UCT) eingerichtet, in dem Grundlagenwissen vermittelt wird und die Fähigkeit, gleichzeitig sein Netzwerk zu verteidigen und dennoch handlungsfähig zu bleiben[191].
Das **US Department of Homeland Security DHS** hat inzwischen einen eigenen Wettbewerb zur Rekrutierung talentierter junger Hacker durchgeführt, die Virginia Governors Cup Cyber Challenge[192].
Die **Central Intelligence Agency (CIA)** hat die geplante Errichtung eines neuen Direktorats "Digitale Innovation" bekannt gegeben. Weitere Reformen zielen auf die Schaffung von 10 integrierten Zentren, in denen analytische und operative Fähigkeiten zusammengeführt werden sollen[193]. Zur Verbesserung der Effizienz verknüpft die NSA 2016 die defensiv und offensiv ausgerichteten Abteilungen

[187] vgl. Zetter 2016
[188] vgl. ICS-CERT 2016a
[189] vgl. Barnes 2012
[190] vgl. Schanz 2010, S.50ff., Franz 2011, S.87. Für den gängigen Begriff **cyber warrior** (Cyberkrieger) wurde der förmlichere Begriff **cyber warfare operator** eingeführt.
[191] vgl. Black zitiert bei Schanz 2010, S.52
[192] vgl. Perlroth 2013, S.1. Die Nachrichtenagentur Reuters meldete am 19. April 2013, dass die NSA und die US Air Force Academy gegeneinander in einer dreitägigen Cyberwarübung antraten. Die NSA unterhält eine eigene Comic-Serie für Kinder **CryptoKids**, vgl. Pofalla 2013, S.44.
193 vgl. Die Welt 2015 online, S.1, Tagesschau 07.03.2015

IAD/SID. Das **Information Assurance Directorate (IAD)** versucht, Sicherheitslücken zu finden und zu schließen, während das **Signal Intelligence Directorate (SID)** Sicherheitslücken für Cyberoperationen einsetzt[194].

China berichtete im Jahr 2011, eine militärische Gruppe von 30 Cyberexperten zu haben, die auch als **Blaue Armee** bezeichnet wird und ein Cyber-Trainingszentrum in Guangdong[195].

Das russische Verteidigungsministerium startete 2012 ein IT-Forschungsprojekt, das auch Mittel und Wege zur Umgehung von Anti-Viren-Software, Firewalls sowie auch von Sicherheitsmaßnahmen in laufenden Systemen erforscht[196]. Zudem wurde ein allrussischer Hackerwettbewerb ins Leben gerufen, um begabte junge Cyberspezialisten rekrutieren zu können[197].

Israelischen Medien zufolge hat die Armee des Landes eine neue militärische Kategorie geschaffen, den 'attacker' (Angreifer), der den Gegner über große Distanzen bekämpft, z.B. durch Drohnen oder Cyberoperationen, während sich die Kategorie des 'fighter' (Kämpfers) auf Soldaten bezieht, die physisch im Kampfgeschehen zugegen sind. Außerdem wurde die Ausbildung von Cyber-Verteidigern (**cyber defenders**) begonnen und der erste Kurs wurde 2012 abgeschlossen. Zur Vorbereitung wird eine intensivierte Cyberausbildung an Schulen angeboten, zudem werden sogenannte 'cyber days' zur Einführung in das ethische (white hat) Hacken durch die Armee angeboten und Hacker-Wettbewerbe[198].
Israel hat die **National Authority for Cyber Defense** für den Schutz von Zivilisten gegen Cyberangriffe eingerichtet, während sich eine Spezialeinheit um die nachrichtendienstlichen Belange kümmert[199].
In Beersheba in der Negevwüste entsteht eine '**Cyberhauptstadt**', in der sowohl Privatfirmen wie auch militärische Einheiten angesiedelt sein werden, einschließlich 35.000 Soldaten. Dies schließt auch den militärischen Nachrichtendienst und die **Cyber-Eliteeinheit 8200** mit ein[200].

Großbritannien plant die Aufstellung einer **Joint Cyber Reserve** genannten Cyberarmee zur Verteidigung und Gegenschlägen in Cyberkonflikten. Die Regierung plant Investitionen in Höhe von 600 Millionen Euro[201].

---

[194] vgl. Gierow 2016, S.1-2
[195] vgl. Kremp 2011
[196] Zitiert in Prawda 2012, der original englische Text lautete: "methods and means of bypassing anti-virus software, firewalls, as well as in security tools of operating systems"
[197] vgl. Prawda 2012
[198] vgl. Croitoru 2012, S.30
[199] vgl. EPRS 2014, S.5/6
[200] vgl. Rößler 2016, S.6
[201] vgl. Spiegel online 2013

Die Schaffung oder Anpassung von Cyberwaffen, -systemen und –werkzeugen wie auch die Cyberabwehr erfordert Teams, die u.a. Spezialisten für bestimmte Systeme, Software, Hardware, SCADA-Anwendungen usw. umfassen [202] Außerdem ist eine klare Abgrenzung und Zuweisung defensiver und offensiver Rollen erforderlich.
Zudem fußen Cyberattacken zunehmend auf systematischen Analysen, Probeläufen in Simulationen und Testumgebungen, bevor das echte Zielsystem angegriffen wird. Dies dient der Verminderung des Entdeckungsrisikos und der Rückverfolgung (Attribution) sowie der Verbesserung der Dauer und des Umfangs des Angriffs[203].

Auch die Rekrutierungsmethoden seitens der Nachrichtendienste und des Militärs haben sich deutlich weiterentwickelt. Studien zeigen, dass Hacker trotz der ursprünglichen Distanz unter Umständen für den Staat zu arbeiten bereit sein können[204]. Im Ergebnis konnten die Rekrutierungsmethoden in der Cybersicherheit inzwischen einfacher gestaltet werden[205].

2.2.10 Ist die Cyberwar-Thematik overhyped?

Intensiv wird über die Frage diskutiert, ob die Cyberwardebatte nicht übertrieben oder nur ein Mythos sei, den militärische Einrichtungen dazu nutzen, um ihre Expansion in den Cybersektor zu rechtfertigen. Eines der Kernargumente ist, dass ein Cyberwar gerade beim meistzitierten Beispiel, dem Angriff auf Estland 2007, nicht wahrscheinlich sei. Einige Autoren sehen die Schläge als zu unkoordiniert und unausgereift an, um auf staatliche Angreifer aus Russland hinzudeuten, vielmehr sprächen die Angriffsmuster für die Aktivitäten patriotischer **script kiddies**, d.h. Angreifern, die mit im Internet erhältlichen Standardwerkzeugen operiert hätten[206].

---

[202] vgl. Zepelin 2012, S.27, Chiesa 2012, Folie 64, Franz 2011, S.88. Bencsath vermutete, dass die Entwicklung der 2012 entdeckten Spionagesoftware Flame bis zu 40 Computer-, Software- und Netzwerkspezialisten erforderte, FAZ2012a, S.16

[203] vgl. Zepelin 2012, S.27. Nach Chiesa 2012 werden unbekannte Sicherheitslücken (zero day-exploits) auch gehandelt, siehe Folien 77 bis 79 Außerdem gibt es standardisierte Software zur Generierung von Schadprogrammen zu kaufen, vgl. Isselhorst 2011, Folie 9.

[204] vgl. Zepelin 2012, S.27. Krasznay 2010 zitiert bei Chiesa 2012, Folie 69.

[205] vgl. Zepelin 2012, S.27. Der offene Ansatz kann wie folgt illustriert werden: Wenn man seit 2012 in den USA Suchbegriffe zum Thema cyberwar auf der Seite startpage.com eingab (ein Service, der anonyme Suche bei Google erlaubt), konnte es passieren, dass auch eine gesponserte Anzeige der National Security Agency NSA erschien (ebenso bei *ixquick* und *metacrawler*). Diese bot Cyberkarrieren unter dem Link www.nsa.gov/careers an mit der Zeile “National Security Agency has cyber jobs you won’t find anywhere else!”. Im Jahr 2016 ist die Anzeige verfügbar unter intelligencecareers.gov/nsa. Die CIA hat ebenfalls eine eigene Suchmaschinenanzeige kreiert “CIA Cyber careers – The work of a Nation – cia.gov The Center of Intelligence –Apply today” und hat seit Juni 2014 einen eigenen offiziellen Twitter-Account.

[206] vgl. Luschka 2007, S.1-3

Ein anderes Argument ist, das in den meisten Fällen, wo von Cyberwar gesprochen wird, letztlich nur Cyberspionage betrieben worden sei, die konventionelle Spionage aber üblicherweise nicht als kriegerischer Akt angesehen wird.
Dennoch gibt es erhebliche Unterschiede zischen konventioneller (physischer) Spionage und der Cyberspionage: Ein herkömmlicher Spion benötigt eine lange Vorbereitung, bis eine Position erreicht wird, von der dieser sensitive Informationen erlangen kann, wobei dies stets mit einem hohen persönlichen Risiko der Entdeckung und Bestrafung verbunden ist[207]. Im kalten Krieg dauerte es oft Jahre, um tausende Seiten geheimer Informationen auszuschleusen.
Cyberspionage kann hingegen von zu Hause und mit geringem Bestrafungsrisiko im Falle der Entdeckung betrieben werden. Es dauert nur noch Sekunden, tausende von Seiten aus einem infizierten System auszuschleusen. Demzufolge findet Cyberspionage weitaus häufiger und aggressiver statt als herkömmliche Spionage. Aber entscheidend ist folgendes: durch die Installation von Backdoor-Programmen kann der Spion sich auch später noch zur Beschädigung oder Zerstörung der befallenen Systeme, z.B. einer kritischen Infrastruktur entschließen. Die Grenze zwischen passiver Spionage und aktiver Zerstörung und Sabotage schwindet also.

Schließlich sind auch konventionelle Waffen zunehmend von Computern abhängig, so dass Cyberaktivitäten auch konventionelle Fähigkeiten betreffen. Infolgedessen wächst das militärische IT-Personal; der Cyberspace Operations and Support Staff der US Air Force umfasste zum Beispiel im Mai 2012 63828 Personen, davon 4095 Offiziere[208].

Zusammenfassend stellt nicht jede größere Cyberattacke einen Cyberwar dar und der Begriff sollte vorsichtig verwendet werden, aber dennoch sollte die Cyberwarproblematik ernst genommen werden[209].

2.2.11 Nachrichtendienstliche Kooperation

Die Berichterstattung des Jahres 2013 vermittelte den Eindruck, dass sich die nachrichtendienstliche Kooperation auf Computer und die Erfassung und Auswertung von allen Form von Telekommunikation (Signals Intelligence SigInt) konzentriert. Die Zusammenarbeit wurde jedoch während des zweiten Weltkrieges begonnen und dann im Zuge des kalten Krieges und der Terrorbekämpfung, die

[207] Eine kurze und einfache Einführung bietet Melton 2009, S.200ff.
[208] vgl. Matthews 2013, S.8
[209] Die zunehmende Bedeutung der Drohnen und des Cyberwars spiegelte sich auch in dem US-Plan wieder, eine neue Kriegsmedaille für herausragende Kriegsführung für Drohnen- und Cyberkrieger in 2013 zu schaffen, immerhin die erste seit 1944. Dieser Plan wurde aufgegeben, nachdem Veteranen und andere gesagt hatten, dass diese Soldaten sicherlich unter hohem Stress stehen, jedoch nicht direkt feindlichem Feuer ausgesetzt seien, NTV 2013.

schon Jahrzehnte vor den Anschlägen des 11.Septemeber 2001 (9/11) begann, erweitert. Deshalb umfasst die Zusammenarbeit auch die Bearbeitung von Informationen, die von und durch Menschen gewonnen wurden (human intelligence HumInt), der Auswertung von Bildern (imaging intelligence ImInt) und von frei zugänglichen Informationen (open source intelligence OsInt)[210].

Das System der nachrichtendienstlichen Zusammenarbeit besteht aus drei Ebenen, der Zusammenarbeit der Dienste innerhalb eines Landes (**intelligence community**), der weitverbreiteten bilateralen Zusammenarbeit und der multinationalen Zusammenarbeit. Viele Staaten haben mehrere Dienste, die äußere und innere sowie zivile und militärische Angelegenheiten abdecken. Es gibt nicht endende Diskussionen über die optimale Zahl und Größe von Diensten: ein einheitlicher Dienst mag zu schwer zu kontrollieren sein, außerdem wäre der Schaden im Falle einer Infiltration enorm, und schließlich kann auch die interne Kommunikation zu kompliziert sein, so dass ggf. auch zu späte Reaktionen und blinde Flecken in der Bedrohungsanalyse entstehen können. Kleinere Organisationen können Spezialisierungsvorteile aufweisen, sind aber mit dem Risiko überlappender Aktivitäten und Verantwortlichkeiten behaftet, zudem kann es zu Konkurrenzdenken und Kommunikationsdefiziten zwischen den Einrichtungen kommen. Die Standardlösung sind mehrere Dienste mit einer koordinierenden Ebene[211]. Die größte Intelligence Community befindet sich in den USA (1981 formal etabliert), die seit 2004 (als Reaktion auf 9/11) vom **Director of National Intelligence DNI** koordiniert wird, davon sind die 8 militärischen Dienste in der Dachorganisation **Defense Intelligence Agency DIA**[212] zusammengefasst.

Die zweite Ebene wird durch ein Geflecht von **bilateralen Kooperationen** gebildet, z.B. Deutschland verfügt über Kontakte zu mehr als 100 Staaten[213]. Je nach Intensität und Qualität der politischen Beziehungen kann es sogar offizielle Repräsentanten (Legalresidenturen) geben, daneben ist es durchaus üblich, als (mehr oder weniger geduldete) Alternative Nachrichtendienstmitarbeiter als diplomatisches Personal in Botschaften bzw. Konsulate zu entsenden. Dies ist

[210] vgl. Best 2009
[211] vgl. Carmody 2005
[212] Air Force Intelligence, Surveillance and Reconnaissance Agency (ISR), United States Army Intelligence Corps (G2), Office of Naval Intelligence (ONI), Marine Corps Intelligence Activity (MCIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO) for satellites, National Security Agency (NSA) for SigInt. Nicht-militärische Organisationen sind die Central Intelligence Agency (CIA), Office of Intelligence and Counterintelligence (Energieministerium), Bureau of Intelligence and Research (INR) (Außenministerium), Office of Intelligence and Analysis (OIA) (Finanzministerium), Office of National Security Intelligence (NN) (Antidrogenbehörde Drug Enforcement Administration DEA), Homeland Security DHS (Heimatschutzministerium) und das Federal Bureau of Investigation (FBI). DNI Handbook 2006
[213] vgl. Daun 2009, S.72

notwendig, um beide Länder betreffende nachrichtendienstliche Vorgänge und Belange zu erkennen, zu besprechen und ggf. auch zu bereinigen.

Die höchste Ebene der Zusammenarbeit ist die **multilaterale Kooperation**, denn selbst der größte Dienst verfügt nicht über die personellen, technischen oder finanziellen Ressourcen, um den Globus vollständig abzudecken. Der Informationsaustauch verläuft typischerweise wie folgt[214]:

- **Do ut des** – Geben und nehmen, geschenkt wird nichts
- **Need to know** – nur das, was man wissen muss, bekommt man gesagt, auch um die Folgen durch undichte Stellen zu reduzieren
- **Third party rule** – Eine erhaltene Information darf nicht ohne Genehmigung an Dritte weitergegeben werden
- **Assessed intelligence** – es werden keine Rohdaten von Originalquellen weitergegeben, sondern nur bearbeitete Berichte, dies dient dem Schutz von Quellen und Ermittlungsmethoden[215].

Aufgrund dieser Austauschregeln können kleinere Gruppen einfacher zu einer vertieften Zusammenarbeit gelangen als größere. Die USA hatten bereits nach dem 2. Weltkrieg die inzwischen offiziell bestätigte **5-eyes** Kooperation mit Großbritannien, Kanada, Australien und Neuseeland eingerichtet und als Reaktion auf 9/11 die (offiziell nicht bestätigte, sondern im November 2013 von der Zeitung *The Guardian* und anderen[216] berichteten) erweiterten Kooperationen **9-eyes** mit Dänemark, Frankreich, den Niederlanden und Norwegen und **14-eyes** mit Belgien, Italien, Spanien, Schweden und Deutschland.

In der Europäischen Union begann die Zusammenarbeit mit der Bildung kleiner Arbeitsgruppen zur Terrorismusbekämpfung in den Siebziger Jahren und wurde danach schrittweise ausgebaut. Das Situation Center **SitCen** (welches seit 2010 dem **Standing Committee on operational cooperation on internal security COSI** untersteht)[217] wertet die Informationen aus, die von Organisationen der Mitgliedsstaaten, Arbeitsgruppen zur Terrorbekämpfung usw. geliefert werden. [218] Afrika hat inzwischen die multinationale Kooperation **Committee of Intelligence and Security Services of Africa CISSA** als Teil der Afrikanischen Union eingerichtet (siehe auch Kapitel 4.7).

[214] vgl. Jäger/Daun 2009, S.223
[215] vgl. Wetzling 2007
[216] wie z.B. Shane 2013, S.4
[217] Note of 22 October 2009 which was followed by a Draft Council Decision: Council Decision on setting up the Standing Committee on operational cooperation on internal security (EU doc no: 16515-09 and EU doc no: 5949-10).
[218] vgl. Scheren 2009

3. Cyberwar in der Praxis

3.1 Einführung

In der allgemeinen 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 (Kapitel 3.2.6). 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, durch das 1982 der Druck in der Tscheljabinsk-Pipeline über den zulässigen Höchstwert gebracht wurde[219]. Es folgte eine Explosion von ca. 3 Kilotonnen Stärke, immerhin einem Fünftel der Hiroshima-Bombe[220]. 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[221].

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[222]. 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[223].

---

[219] vgl. Kloiber/Welchering 2011, S.T6
[220] vgl. Falliere 2010, Herwig 2010
[221] vgl. Vistica 1999
[222] vgl. Hegmann 2010
[223] vgl. Hunker 2010, S.3

3.2.3 Der Hainan- oder EP3-Zwischenfall von 2001

Im zeitlichen Zusammenhang mit dem Zusammenstoß eines 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[224].

3.2.4 Großangriffe auf westliche Regierungs- und Industrie-Computer 2000-2011

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[225], 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[226]. 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[227].
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[228].

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, 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

[224] vgl. Fritz 2008 und Nazario 2009, der in seinem Papier einen Überblick über politisch motivierte DoS-Attacken gibt.
[225] 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
[226] vgl. Fischermann/Hamann 2010
[227] vgl. Fritz 2008, S.55 und auch Stokes 2005
[228] vgl. ArcSight 2008, S.2

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[229]. Operation Aurora wird inzwischen der **Axiom/Deep Panda Group** zugeschrieben, siehe Kapitel 3.3.5. Zwei weitere groß angelegte Cyberattacken richteten sich 2009 gegen Firmen der Öl-, Gas- und petrochemischen Industrie (**Operation Night Dragon**) und über 5 Jahre ab Juli 2006 gegen insgesamt 72 globale Organisationen (**Operation Shady RAT**), wobei China eine Beteiligung energisch bestreitet[230][231]. 2011 wurden weitere Angriffe dieser Art, u.a. auf die Rüstungsfirma Lockheed Martin und Googles Mailservice Gmail berichtet[232].

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[233]. Estlands Netz wurde daraufhin von Russland aus mit gewaltigen Datenmengen bombardiert, wobei dies nicht vom russischen Staat ausging, sondern 'nur' von nationalistisch gesinnten Kreisen[234][235]. 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[236].

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

[229] vgl. Markoff/Barbosa, 18.02.2010
[230] Alperovitch 2011, McAfee 2011. RAT steht für remote administration tool.
[231] vgl. FAZ 2011b, S.7.
[232] vgl. Koch 2011, S.20. Der Angriff auf Lockheed Martin im Mai 2011 steht möglicherweise im Zusammenhang mit einem vorangegangenen Angriff auf die US-Sicherheitsfirma RSA im März 2011, bei dem u.a. Informationen zu dem weit verbreiteten Sicherungssystem **SecurID** entwendet wurden, vgl. FAZ 2011a, S.11. RSA hatte für Lockheed Martin das Konzept einer sicheren Cloud (Secure Cloud) entwickelt, vgl. Fuest 2011
[233] vgl. Busse 2007
[234] Später bekannte sich die russische patriotische Jugendorganisation **Naschi** (die Unsrigen) zu dem Angriff, vgl. Frankfurter Allgemeine Zeitung 11.03.09
[235] vgl. Koenen/Hottelet 2007, S.2
[236] vgl. Wilson 2008, S.7ff.

einfliegen und angreifen konnten. Dies ist ein klassisches Beispiel für die Idee des Cyberwars als operativer Ergänzung zu konventionellen Maßnahmen[237].

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[238]. Schon Wochen vorher wurde die Internetseite des georgischen Staatspräsidenten am 20. Juli 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[239].
Schon im August 2003 konnte der Internetwurm *Slammer* für einige Stunden in das zum Glück abgeschaltete Atomkraftwerk in David-Besse in Ohio eindringen[240]. Seit 2006 mussten zweimal Atomkraftwerke nach Cyberangriffen abgeschaltet werden[241]. Im April 2009 gelang es Hackern, in die Stromnetzkontrolle der USA vorzudringen[242] 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 2009/2011

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[243]. 2011 wurde berichtet, dass die Computer der Creech Air Force Base in Nevada, die als Steuerzentrale für Predator- und Reaper-Drohnen dient, von einem Computervirus befallen wurden; laut US Air Force

[237] vgl. Herwig 2010, S.60
[238] vgl. die Stellungnahme der georgischen Regierung von 2008
[239] vgl. Gaycken 2009 mit Abbildung des großen Stromausfalls in Northeast USA 2003
[240] vgl. Wilson 2008, S.22
[241] vgl. ArcSight 2009
[242] vgl. Goetz/Rosenbach 2009, Fischermann 2010, S.26
[243] vgl. Ladurner/Pham 2010, S.12

hatte dies jedoch keinen Einfluss auf die Einsatzfähigkeit der Drohnen[244]. Der Iran brachte 2011 eine US-Drohne vom Typ RQ-170 in seinen Besitz[245].
Die US Navy hat 2012 entschieden, die Kontrollsysteme der Drohnenbasen auf Linux umzurüsten, was von der Rüstungsfirma Raytheon mit einem Budget von 28 Million US-Dollar durchgeführt werden soll[246]. Die Verwundbarkeit von Drohnen ist aber auch typabhängig, da diese mit unterschiedlichen Kontrollmethoden und verschieden großer Systemautonomie gesteuert werden[247].

3.2.10 Lokale Cyberkonflikte

Eine wachsende Zahl lokaler politischer und/oder militärischer Konflikte wird von mehr oder weniger koordinierten Cyberattacken begleitet, die sich ggf. über einen längeren Zeitraum hinziehen können. Diese Attacken betreffen auch sicherheitsrelevante Systeme des Gegners, und werden eventuell auch von gleichzeitigen Medienkampagnen begleitet[248]. Wichtige Beispiele unter vielen sind die Konflikte von Indien und Israel mit Akteuren aus den Nachbarstaaten[249].
Während der Krimkrise im März 2014 wurden Cyberattacken zwischen der Ukraine und Russland berichtet, außerdem berichtete die russische Rüstungsfirma **Rostec**, eine US-Drohne MQ-5B über der Krimhalbinsel mittels elektromagnetischer Störmanöver zur Landung gezwungen zu haben[250].

3.3 Hochentwickelte Hackereinheiten und Malware-Programme

Mittlerweile wurden mehrere hochentwickelte Hackergruppen und Malwarefamilien entdeckt und berichtet, die in den folgenden Abschnitten dargestellt werden. Typischerweise geht man davon aus, dass diese Gruppen zu Staaten (Regierungen/Nachrichtendienste/Militär) gehören bzw. von diesen unterhalten werden. Gründe für diese Annahme sind der betriebene Aufwand und die Komplexität der verwendeten Instrumente, der Bedarf an Spezialisten, die diese Operationen über Jahre durchführen und zugleich verbergen müssen, die Auswahl von politisch und strategisch besonders wichtigen Zielen, der Bedarf an systematischer Sammlung von Informationen usw. Außerdem sind diese Attacken typischerweise nicht sofort profitabel, im Unterschied zu Cyberkriminellen, die Geld mit Bankingtrojanern, Ransomware und ähnlichem verdienen können.
Zudem hat jede dieser Gruppen ein charakteristisches Muster von Zugangswegen, ausgenutzten Schwachstellen und Werkzeugen, was diese Gruppen unterscheidbar

[244] vgl. Los Angeles Times 13 October 2011
[245] vgl. Bittner/Ladurner 2012, S.3. Als Eindringmethode wurde die Verwendung eines manipulierten GPS-Signals (GPS spoofing) diskutiert, aber das konnte nicht belegt werden.
[246] vgl. Knoke 2012
[247] vgl. Heider 2006, S.9
[248] vgl. Saad/Bazan/Varin 2010
[249] vgl. Saad/Bazan/Varin 2010, Valeriano/Maness 2011, Even/Siman-Tov 2012, S.37
[250] vgl. FAZ online 2014

macht.251. Ein weithin genutzter Begriff für diese Muster ist **Tactics, Techniques, and Procedures (TTPs)**. Da jede Gruppe auch zu bestimmten Zielen tendiert, spricht man auch von einer Opferlogik, engl. **victimology**.
Jedoch müssen Zuordnungen zu Staaten mit großer Vorsicht gehandhabt werden. Manchmal werden falsche Fährten (false flags) gesetzt, um andere für einen Angriff beschuldigen zu können, oder es wird Malware verwendet, die bereits auf dem Schwarzmarkt erhältlich ist. Manchmal sind Cyberwaffen wenn auch unter Auflagen sogar kommerziell erhältlich.
Zudem hat noch keine Regierung oder Behörde eine Verbindung zu einer Hackereinheit offiziell bestätigt. Eine 'Verbindung' zu einem Staat ist zudem ein unscharfer Begriff, man kann daraus nicht erkennen, ob eine Einheit Teil einer staatlichen Organization ist oder lediglich mit diesem auf Vertragsbasis arbeitet oder anderweitig kooperiert.
Die nun vorgestellten Gruppen sind die meistberichteten in den Medien, jedoch wird die Nummer größerer aktiver Hackereinheiten so auf rund hundert Gruppen geschätzt.

Aus amerikanischer Sicherheitsperspektive hat Russland innerhalb der letzten zehn Jahre erhebliche Fortschritte mit der Errichtung hochspezialisierter Einheiten gemacht. Während die Gruppen **APT28, APT29** und **The Waterbug group** inzwischen von vielen Analysten Russland zugeschrieben werden, ist die Debatte über mögliche Verbindungen zu Russland offen für Gruppen mit dem Fokus auf Industrie und ICS-Systeme wie **Energetic Bear/Dragonfly** und **Sandworm/Quedagh**[252].
Die **Comment Crew/APT1** und die **Axiom/DeepPanda Group** werden im Zusammenhang mit China diskutiert, während für die **Lazarus Group** ein Zusammenhang mit Nordkorea vermutet wird. Die **Equation Group** wird typischerweise mit den USA in Verbindung gebracht, wobei Bezug zu den sogennnten *Snowden leaks* genommen wird. Aber es gilt unbedingt zu beachten, dass alle angesprochenen Regierungen solche Verbindungen verneint bzw. nicht kommentiert haben.

3.3.1 Die Equation Group

Das esrte Unterkapitel beschreibt die Entdeckungsgeschichte der Stuxnet, Duqu und Flame-Malware, die mit der Entdeckung von Stuxnet in 2010 begann, gefolgt von Flame und Duqu. Später wurde jedoch gezeigt, dass Stuxnet schon mindestens seit 2005 existiert hat.

[251] Siehe auch Jennifer 2014
[252] Siehe z.B. Jennifer 2014

Forscher von *Kaspersky Labs* entdeckten die Equation Group 2015, die schon seit vielen Jahren aktiv war, mit ersten Spuren bis zurück in das Jahr 1996. Dies wird im zweiten Unterkapitel beschrieben. Stuxnet, Duqu und Flame konnten mit anderen Malwarefamilien der Equation Group zugeschrieben werden. Jedoch waren die ersten Stuxnetversionen anders, auch mit einem anderen Angriffsziel (Klappen statt Zentrifugen), so dass womöglich eine weitere Programmiergruppe an der Entwicklung von Stuxnet beteiligt war.

Das dritte Unterkapitel beschreibt den **Shadow Brokers**–Vorfall vom August 2016. Die Malware wurde von den Shadow Brokers als von der Equation Group stammend präsentiert und wurde wegen Ähnlichkeiten zu von Edward Snowden präsentierten Malwarelisten von den Medien mit der NSA in Verbindung gebracht. Nachforschungen konnten jedoch nicht zeigen, dass die NSA gehackt wurde, die Malware war zudem von 2013 oder noch älteren Datums.

3.3.1.1 Entdeckungsgeschichte - Der ‚digitale Erstschlag'

Eine Serie von hochentwickelten Spionageprogrammen und Trojanern wurde seit Ende 2006 vor allem auf iranischen Computern installiert und ausgeführt.
Ein sehr großes Program namens **Flame** diente dabei als Technologieplattform für die Entwicklung weiterer Programme wie **DuQu** und später **Stuxnet,** das die Funktion von Uranzentrifugen in iranischen Nukleareinrichtungen störte.
In den Jahren 2011 und 2012 haben US-Medien berichtet, dass diese Aktivitäten Teil einer amerikanisch-israelischen Kooperation namens '**Olympic Games**' waren, um die iranischen Nuklearfabriken lahmzulegen, aber die offizielle Bestätigung hierfür steht nach wie vor aus. Der folgende Abschnitt berichtet die Ereignisse in Reihenfolge der Entdeckung.

Fernwartungs- und -Steuerungsfunktionen (**Industrial Control Systems ICS**) wie die Supervisory Control and Data Acquistion SCADA[253]) 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[254].
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[255].
Stuxnet wurde mit Hilfe von infizierten USB-Sticks in Computer eingebracht. In Windows existierte eine Schwachstelle in LNK-Dateien, die als Eintrittspforte

[253] vgl. Shea 2003
[254] vgl. Welt online 2010b. Siemens baut daher seine Cyberwarforschung aus, vgl. Werner 2010, S.7
[255] Da Stuxnet sehr viele (Dutzende) Funktionen hat, wird es in der Literatur auch als Trojaner oder als Virus bezeichnet, vgl. auch FAZ2010a.

genutzt wurde[256]. 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[257].
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[258]. 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 bestimme Netzwerkkarte des Typs CP 342/5 daran angeschlossen ist[259]. 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[260].
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[261]. Es kamen Vermutungen auf, dass dadurch möglicherweise zum Atombombenbau benötigte Urangaszentrifugen im Iran geschädigt wurden, da ihre Zahl 2009 aus unerfindlichen Gründen rückläufig war und die Internationale Atomenergiebehörde IAEO auch 2010 über Stillstände berichtete[262], die daraufhin vom Iran auch bestätigt wurden[263][264].
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[265] ergab sich in den Medien das Bild einer gezielten Superwaffe, die möglicherweise von

[256] Am 13.10.2010 gab Microsoft deshalb 16 Updates heraus, die insgesamt 49 Sicherheitslücken schlossen, vgl. Handelsblatt 2010, S.27.
[257] vgl. Rieger 2010, S.33, der auch den Begriff des digitalen Erstschlags prägte.
[258] vgl. Krüger/Martin-Jung/Richter 2010, S.9
[259] vgl. Schultz 2010, S.2
[260] vgl. Kaspersky 2010
[261] vgl. Falliere 2010
[262] vgl. FAZ2010c, S.6
[263] 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.
[264] Das Institute for Science and International Security (ISIS) vermutete aufgrund entsprechender Befehle im Stuxnet-Code und der phasenweise rückläufigen Zentrifugenzahl, dass möglicherweise ca. 1000 Urangaszentrifugen 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. Stuxnet zeichnete auch normale Funktionsabläufe auf und konnte diese während der Aktionen auf den Kontrollgeräten simulieren, Broad/Markoff/Sanger 2011, S.3.
[265] vgl. Schultz 2010, S.2

Geheimdiensten konstruiert wurde, um das iranische Atomprogramm zu sabotieren[266].

Die oben beschriebenen Eigenschaften von Stuxnet treffen auf die Stuxnet Versionen 1.0 und höher zu. Symantec berichtete 2013 über die Existenz früherer Versionen, die u.a. durch die Nutzung anderer Schwachstellen (exploit) für das Eindringen charakterisiert sind. Stuxnet Version 0.5 wurde ab November 2005 entwickelt und ab November 2007 eingesetzt. Die Infektion erfolgte nur über Step 7-Systeme und führte zu einem zufälligen Klappenschluß, der die Urangaszentrifugen schädigen konnte. Die Infektionen mit Version 0.5 endeten im April 2009[267].

Die *New York Times* berichtete am 15.01.2011, dass das Heimatschutzministerium Department of Homeland Security und die dem Energieministerium zugehörigen Idaho National Laboratories Siemens-Systeme 2008 auf Schwachstellen untersuchten, und dass möglicherweise Befunde aus diesen Tests zur Entwicklung von Stuxnet genutzt wurden, nachdem sie in der Lage waren, die iranischen Urangaszentrifugen zu Testzwecken nachzubauen[268].

Am 01.06.2012 berichtete die New York Times, dass Stuxnet Teil eines **Olympic Games** genannten Cyberattackenprogramms war, das 2006 vom ehemaligen US-Präsidenten George W. Bush initiiert worden war[269]. Die Berichte der New York Times wurden offiziell *nicht* bestätigt, aber Aussagen des New York Times-Artikels von 2012 wurden von offizieller Seite als unautorisierte Preisgabe vertraulicher Information gewertet, wobei wiederum nicht gesagt wurde, *welche* Textpassagen damit gemeint waren[270].

Durch einen technischen Fehler hatte Stuxnet den Computer eines Ingenieurs infiziert und sich dadurch im Internet in andere Länder ausgebreitet[271]. Dies würde auch erklären, warum auch andere Staaten betroffen waren, insbesondere Indonesien, Indien, Aserbeidschan und Pakistan, und neben einem Dutzend weiterer Staaten auch die USA und Großbritannien[272]. Zudem 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 Ablaufen von Lizenzen zu verhindern, ließ sich die geplante Befristung nicht

[266] vgl. Ladurner/Pham 2010, S.12
[267] vgl. McDonald et al. 2013, S.1-2
[268] vgl. Broad/Markoff/Sanger 2011, S.4
[269] vgl. Sanger 2012, S.3
[270] vgl. NZZ 2012, S.1, FAZ 2012b, S.7
[271] vgl. Sanger 2012, S.6
[272] vgl. Handelsblatt 2010, S.27, Symantec 2010, S.5-7

aufrechterhalten, d.h. der Angriff wurde im Bezug auf die Software sehr präzise ausgeführt, nicht jedoch im Bezug auf Zeitpunkt und Ort[273].

Es muss aber auch der Schaden betrachtet werden, den Stuxnet für die Zukunft anrichtet, denn mit Stuxnet wurde auch das Know-How allgemein preisgegeben[274]. 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[275]. 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[276].

Die Stuxnet-Attacke wurde von anderen Aktivitäten begleitet. Relevante Teile des Quellcodes der Spionagesoftware **W32.DuQu**, die im September 2011 entdeckt wurde, waren identisch zu Stuxnet[277]. DuQu benutzte ein gestohlenes Sicherheitszertifikat eines taiwanesischen Unternehmens zum Eindringen und konnte z.B. screenshots machen, Tastatureingaben protokollieren (keylogging) und Informationen aus den befallenen Computern verschicken und wie Stuxnet verfügte es auch über ein Verfallsdatum mit Selbstzerstörung[278]. Es wurde vermutet, dass DuQu evtl. dazu dienen sollte, Informationen aus den Zielsystemen zu gewinnen, die für die Schaffung von Stuxnet genutzt wurden[279].

Nachdem im April 2012 iranische Ölterminals von einer datenvernichtenden Schadsoftware namens **Wiper** getroffen wurden, entdeckte die Sicherheitsfirma Kaspersky Labs im Mai 2012 ein anderes multifunktionales ‚Virus'[280] namens

[273] 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
[274] vgl. Rosenbach/Schmitz/Schmundt 2010, S.163, Rieger 2011, S.27
[275] Iran Daily 26 July 2010
[276] vgl. Knop/Schmidt 2010, S.20
[277] vgl. Goebbels 2011, S.8. Der Name stammte von dem im Programmiercode verwendeten Präfix DQ.
[278] vgl. Goebbels 2011, S.8
[279] vgl. Welchering 2012, S.T1
[280] Flame war mit 20 MB sehr viel größer als Stuxnet und konnte unter anderem keylogging und screenshots durchführen, Kontrolle über das Mikrofon und den Datenfluss erlangen und es hatte auch Zugang zu den Bluetooth-Anwendungen, vgl. Spiegel 2012, S.123. Wie Stuxnet kann es sich auch selber löschen. Der Name stammte von dem im Programmiercode verwendeten Wort flame. Flame ist ein Beispiel dafür, warum die Differenzierung in Viren, Würmer und Trojaner zunehmend an Bedeutung verliert.

Flame, das sehr detaillierte Informationen über die infizierten Systeme weitergibt und das wiederum eine technische Verwandtschaft zu Stuxnet aufwies[281].

Die Washington Post berichtete, dass Flame bereits im Jahre 2007 entwickelt wurde und Teil der Cyberaktivitäten gegen den Iran war[282]. Der Programmteil, der die Infektion durch USB-Sticks ermöglichte, wurde zuerst in Flame und dann in Stuxnet verwendet[283].
Im weiteren Verlauf des Jahres 2012 wurde über weitere technisch mit Flame verwandte Schadsoftware berichtet: der Trojaner **Gauss** sammelte Informationen über finanzielle Transaktionen, z.B. von libanesischen Banken und eine kleine Variante von Flame namens **Mini-Flame**[284].

3.3.1.2 Die Tools der Equation Group

Anfang 2015 berichtete die Sicherheitsfirma *Kaspersky Labs* über eine neue Malware-Familie, die sich **Equation group** nennt. Die Malware kann bis 2001 zurückverfolgt werden, eventuell sogar bis 1996. Aufgrund technischer Überlappungen könnte es sein, dass Stuxnet Teil einer größeren Malware-Familie ist.[285]

Zunächst wurden zwei Arten von Schadprogrammen auf der gemeinsamen **EquationGroup**-Plattform entwickelt, das eine ist das um 2001-2004 genutzte **EquationLaser**-Programm, das später von den weiter entwickelten Programmen **EquationDrug** und **Grayfish** abgelöst wurde (vermutlich zwischen 2008 und 2013), das andere war **Fanny** aus dem Jahr 2008, welches zwei unbekannte Lücken (zero-day exploits) nutzte, die später auch bei Stuxnet genutzt wurden. Computer, die mit Fanny infiziert wurden, wurden zum Teil auch mit den Nachfolgern **DoubleFantasy** und **TripleFantasy** infiziert. Beide Arten von Schadprogrammen wurden typischerweise gemeinsam benutzt, wobei nach der Ausnutzung einer Internet-Schwachstelle DoubleFantasy geladen wurde, um zu prüfen, ob der Computer ein interessantes Ziel ist; und falls dies der Fall war, wurden EquationDrug oder Grayfish nachgeladen[286].

Grayfish infiziert den boot record des Betriebssystems und übernimmt die totale Kontrolle, d.h. betreibt den gesamten Computer[287]. Es sammelt Daten und legt sie verschlüsselt als **encrypted Virtual File System** in der Registry des Computers

[281] vgl. Welchering 2012, S.T1, Graf 2012, S.8, Gostev 2012, S.1
[282] vgl. Graf 2012, S.9, was aber offiziell ebenfalls nicht bestätigt wurde.
[283] Nakashima/Miller/Tate 2012, S.1-4
[284] vgl. Focus 2012, Symantec 2012, Mertins 2012, S.10
285 vgl. Kaspersky Lab 2015, S.3
286 vgl. Kaspersky Lab 2015, S.5, 8
287 vgl. Kaspersky Lab 2015, S.10. Schon EquationDrug war in der Lage, die volle Kontrolle zu erlangen, siehe S.8

ab, wo es für Antivirus-Produkte unsichtbar ist[288]. Fanny ist ein Wurm, der nicht mit dem Internet verbundene Computer über USB-Sticks befällt und dann bei der nächsten Gelegenheit alle Informationen versendet, wenn der Stick in einen mit dem Internet verbundenen Computer gesteckt wird.[289]

Die EquationGroup-Malware wird durch interdiction verbreitet, bei der versandte CD-ROMs und andere physische Medien während des Transportes entnommen und durch infizierte ersetzt werden. EquationDrug und Grayfish können auch noch die Firmware infizieren, d.h. die in die Hardware eingebetteten essentiellen Programme eines Computers[290]. Dadurch übersteht die Schadsoftware auch eine Neuinstallation des Betriebssystems und erlaubt eine tief verborgene Datenspeicherung. Diese anspruchsvollen Angriffsmethoden wurden jedoch nur gegen bedeutende Ziele, insgesamt einige hundert Computer eingesetzt.

Wichtige Verbindungen zwischen der EquationGroup Malware-Familie und der Stuxnet-Familie sind die folgenden[291]: Grayfish nutzt in einem Infektionsschritt eine Hash-Code Verschlüsselung, die Ähnlichkeiten zum Gauss-Programm aufweist. Fanny, Stuxnet, Flame und Gauss nutzen einen gemeinsamen LNK-exploit, während Fanny, Stuxnet, DoubleFantasy und Flame eine bestimmte Methode zur Eskalation von Nutzerprivilegien verwenden. Zudem nutzen DoubleFantasy, Gauss und Flame noch eine spezifische Methode der USB-Infektion.

Mitte 2015 berichtete *Kaspersky Labs* über einen sie auch selbst betreffenden Befall mit **DuQu 2.0**, einem Schadprogramm mit Ähnlichkeiten zu DuQu[292]. Auch andere wichtige Ziele wurden angegriffen, insbesondere Computer von Teilnehmern der P5+1-Treffen, d.h. der Gespräche über das iranische Atomprogramm. Die Schadsoftware nutzte eine Schwachstelle zum ‚**lateral movement**', also der Hochstufung eines nicht-privilegierten Nutzers zu Administratorenrechten[293]. Die Programmieren setzten ‚**false flags**', d.h. nutzten Codeelemente, die auf andere Hackergruppen verweisen sollten[294]. Auch Zeitstempel wurden manipuliert.

Regin ist ein mehrstufiges, modular aufgebautes Programm, d.h. es kann maßgeschneiderte Module auf den infizierten Computer nachladen und wurde Ende 2014 entdeckt, könnte aber schon 2008 oder früher kreiert worden sein. Während bisher keine Evidenz für eine Verwandtschaft mit Stuxnet berichtet

[288] vgl. Kaspersky Lab 2015, S.10-12
[289] vgl. Kaspersky Lab 2015, S.13
[290] vgl. Kaspersky Lab 2015, S.15-16
[291] vgl. Kaspersky Lab 2015, S.5
[292] vgl. Kaspersky Lab 2015b, S. 3
[293] vgl. Kaspersky Lab 2015b, S.4
[294] vgl. Kaspersky Lab 2015b, S.43

wurde, fand die Sicherheitsfirma *Symantec* ein ähnlich hohes Entwicklungsniveau und einem modularen Ansatz, wie er auch schon bei Flame und **Weevil (Careto/The Mask)** gefunden wurde, während der Aufbau mit dem schrittweisen Laden ähnlich in der Duqu/Stuxnet-Familie gesehen wurde[295]. Ähnlich wie bei der Equation Group wurden encrypted virtual file system containers und eine RC5-Verschlüsselung benutzt[296]. Regin hat viele Eigenschaften wie die Überwachung des Datenflusses, die Entnahme von Informationen und das Sammeln von Daten[297]. Wie bei den anderen beschriebenen Schadprogrammen wurden wieder nur wenige ausgewählte Ziele attackiert[298].

Im Februar 2014 wurde eine weitere spezielle Cyberattacke von *Kaspersky Labs*[299] berichtet. Die Schadsoftware **Weevil (Careto/The Mask)** war neben vielen anderen Funktionen unter anderem in der Lage, Skype-Gespräche mitzuschneiden. Wie bei anderen ausgefeilten Attacken, wurden nur wenige Computer infiziert, aber das Profil der Ziele ist stets ähnlich: Forschungseinrichtungen, Anbieter kritischer Infrastrukturen, Diplomaten, Botschaften und politische Aktivisten. Ungeachtet des hochentwickelten modularen Designs konnte bisher keine klare Verbindung zur Equation Group gezeigt werden, der Ursprung ist nach wie vor unklar.

3.3.1.3 Der Shadow Brokers-Vorfall

Im August 2016 gab eine bis dahin unbekannte Gruppe namens **Shadow Brokers** an, Cyberwaffen der Equation Group in ihrem Besitz zu haben. Zum Beweis veröffentlichten sie eine frei zugängliche Datei und boten eine weitere Datei zur Versteigerung an mit einem Schätzpreis von 1 Million Bitcoins (500 Millionen Euro zu der Zeit)[300]. Die Auktion wurde jedoch ganz schnell abgeschaltet, das letzte Gebot lag bei 0,12 Bitcoins (60 Euro). [301] Die Medien spekulierten, dass dies eine symbolische Warnung Russlands gewesen sei wegen der Verdächtigungen im sogenannten **DNC hack** (siehe nächstes Kapitel) in den Medien, d.h. sie wollten zeigen, dass auch sie in der Lage sind, Spionageaktivitäten der anderen zu verfolgen und ggf. bei Bedarf zu zeigen[302].

Die Analyse der öffentlichen Datei zeigte Software von 2013; die Experten vermuteten, dass das Material von einem von der Equation Group genutzten Command and Control-Server kopiert wurde, also kein ‘NSA hack’ oder ähnliches stattgefunden hat.

---

[295] vgl. Symantec 2014a, S.3
[296] vgl. Symantec 2014a, S.3
[297] vgl. Symantec 2014a, S.11
[298] vgl. Martin-Jung 2014, S.17
[299] vgl. Kaspersky 2014
[300] vgl. Jones 2016
[301] vgl. Beuth 2016b, Spiegel online 2016
[302] vgl. Jones 2016

In einem späteren Statement auf *Pastebin* und *Tumblr* – das laut eigener Angabe von den Hackern selbst stammte- erklärten diese, dass das Material von einem Vertragsmitarbeiter der Firma *RedSeal* nach einer Sicherheitsübung kopiert worden war. *RedSeal* ist eine Firma, die zum Portfolio von In-Q-Tel gehört[303]. In-Q-Tel wurde 1999 von der CIA als Venture Capital-Firma für strategische Investments in Startups etc. gegründet. Das Statement ist vielleicht korrekt, aber es ist ungewöhnlich, dass Hacker ihre Eindringstrategie einfach veröffentlichen, so ist es theoretisch denkbar, dass diese Mitteilung auch zur Verschleierung anderer Sicherheitslücken gedient hat oder ein Versuch war, die CIA in die Affäre hineinzuziehen.

Das Material schien jedenfalls echt zu sein und einige Dateinamen waren identisch zu denen, die Edward Snowden als NSATools bezeichnet hatte, wie z.B. *Epicbanana, Buzzdirection, Egregiousblunder, Bananaglee, Jetplow* und *Extrabacon*[304]. Die IT-Firmen Cisco und Fortinet bestätigten die Existenz von Sicherheitslücken; eine der Cisco-Lücken war zum Zeitpunkt der Veröffentlichungen noch nicht geschlossen, während die Fortinetlücken nur ältere Versionen betrafen[305].

3.3.2 APT28 und APT29

3.3.2.1 APT28 (alias Sofacy, Pawn Strom, Csar Team, Sednit, Fancy Bear)

APT 28 (**alias Sofacy, Pawn Strom, Csar Team, Sednit, Fancy Bear**) ist eine Gruppe, die sich auf Ziele mit politischer Relevanz für Russland richtet. Die Zeitzonen für die Kompilierung der Malware decken sich mit der Moskauer Standardzeit, die russische Sprache wird verwendet und typischerweise werden Tools für langfristige Einsätze angewendet. Die eingebauten Hintertüren nutzen das http-Protokoll und den Mailserver des Zielcomputers.[306] APT 28 nutzt eine Vielfalt an Malware (**Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer and DownRange**) und verfügt auch über Malware für Smartphones[307].

In einem Hackerangriff im Jahre 2015 auf den französischen Sender **TV5Monde** wurde dieser zeitweise von augenscheinlich dschihadistischen Angreifern offline genommen, später ergaben sich jedoch Hinweise auf APT28[308]. Der Server für die Satellitensignale wurde angegriffen und da dieser von einem Drittanbieter gewartet wurde, konnte ein längerer Ausfall des Signals erreicht werden[309].

---

[303] vgl. Ragan 2016
[304] vgl. Steier 2016b, Spiegel online 2016, Solon 2016
[305] vgl. Steier 2016b
[306] vgl. Weedon 2015, S.71-72
[307] vgl. Alperovitch 2016
[308] vgl. FAZ online 2015, S.1
[309] vgl. Wehner 2016, S.6

Der Verfassungsschutz BfV bekam einen Hinweis aus dem Ausland, dass ein Cyberangriff mit Datenaustausch zwischen zwei Bundestagscomputern mit einem osteuropäischen Server im Gange sei[310]. Untersuchungen bestätigten das Eindringen in mehrere Computer durch infizierte emails[311], einschließlich der Übernahme von Administratorenrechten[312]. Da das komplette Ausmaß der Infektion nicht ermittelt werden konnte, empfahl das BSI den Austausch des gesamten Netzwerkes. Die Bundestags-IT war nicht an das sichere IVBB-Netzwerk angeschlossen[313]. Der Angriff wies Ähnlichkeiten zum Angriff auf den französischen TV-Sender TV5Monde auf[314].

Einer der für die Attacke auf den Bundestag genutzten Server war identisch zu denen der DNC-Attacke von 2016 und ebenso ein gefälschtes Sicherheitszertifikat[315].

3.3.2.2 APT29 (alias Cozy Duke/Cozy Bear)

Im Februar 2013 hat *Kaspersky Lab* mit **MiniDuke** eine neue Schadsoftware entdeckt, die aus 20 KB Assembler-Code bestand und in PDF-Dateien eingebettet wurde, die als spear-fishing mail versendet wurden. Auf diese Weise wurden insgesamt 59 Computer in 23 Staaten infiziert. Die Schadsoftware fungierte als Brückenkopf zur Installation weiterer Schadprogramme. MiniDuke prüfte, ob es sich auf einem echten Computer oder nur einer **virtuellen Maschine** (einem simulierten Computer) befand und benutzte Twitter zur Kommunikation mit dem Angriffsserver. Informationen wurden in kleinen Bildern verborgen, einer als **Steganographie** bekannten Methode. Solche virtuellen Maschinen können Teil von Cloudsystemen sein, aber auch als Prüfumgebungen für Schadprogramme dienen, das Programm blieb dann inaktiv, um die Analyse zu verhindern[316].

The Dukes sind eine Malwarefamilie mit einer stetig wachsenden Zahl an Werkzeugen wie **MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke** und **GeminiDuke**, die von einer Gruppe benutzt werden, die als **The Dukes** oder auch als **APT29** bezeichnet wird[317]. Die Attacken zeigen ein zweistufiges Vorgehen mit einem initialen

310 vgl. Baumgärtner/Röbel/Schindler 2015, S.28. Aufgrund der initialen Analyse wurde der russische Auslandsnachrichtendienst SWR hinter dem Angriff vermutet, Baumgärtner/Müller/Röbel/Schindler 2015, S.34.
311 vgl. Mertins 2015, S.4
312 vgl. Hoppe/Osman 2015, S.1
313 vgl. Erk et al. 2015, S.2
314 vgl. FAZ online 2015, siehe auch Wehner 2015, S.1
315 vgl. Baumgärtner/Neef/Stark 2016, S.90-91
316 vgl. Raiu/Baumgartner/Kamluk 2013
317 vgl. Weedon 2015, S.70-71

Einbruch in das attackierte System, dem, falls es sich um ein relevantes Ziel handelt, der Übergang zu einer Langzeitüberwachung folgt[318]. Für dieses Vorgehen sind mehrstufige Ladevorgänge und Backdoors verfügbar. Zugangswerkzeuge (Remote Access Tools RATs) waren u.a. **AdobeARM, ATI-Agent** und **MiniDionis**[319]. Um eine Entdeckung zu verhindern, prüft die Malware die Sicherheitseinstellungen des Computers sehr gründlich. Das Profil der infizierten Computer (aus sicherheitspolitischer Perspektive relevant für die russische Föderation), die Zeitzonen der Programmierung, die sich mit der Moskauer Zeit decken, die Nutzung hochspezifischer Spear-Phishing e-Mails und eine Fehlermeldung in russischer Sprache in PinchDuke sind Gründe für die Vermutung, dass es sich um eine hochentwickelte russische Cyberspionage-Gruppe handeln könnte.

3.3.2.3 Der DNC hack

Das Democratic National Committee (DNC), das formelle Leitungsgremium der Demokratischen Partei, alarmierte die Sicherheitsfirma *Crowd Strike* wegen eines Angriffs auf ihre Systeme[320].
Das Eindringen von APT29 lässt sich in den Sommer 2015 zurückverfolgen, während APT28 unabhängig davon im April 2016 in das Netzwerk eindrang. Das zweite Eindringen interferierte mit dem ersten und führte zur Entdeckung. APT29 nutzte das **SeaDaddy**-Programm, welches bei Bedarf das automatische Nachladen von Malwarecode erlaubte, während APT28 mit der **X-Agent**-Malware agierte, um so Anweisungen aus der Entfernung geben zu können, Dateien übertragen zu können und Tastendrücke prtokollieren zu können[321]. Die US-Ermittler sind überzeugt, dass Russland hinter den Angriffen steckt, was jedoch von der russischen Regierung verneint wurde[322]. Einer der für die DNC-Attacke genutzten Server war identisch zu dem der Attacke auf den Bundestag und ebenso ein gefälschtes Sicherheitszertifikat [323].
Später bekannte sich ein rumänischer Hacker mit dem Namen **Guccifer 2.0** zu den Angriffen, aber bei Anfragen war nicht in der Lage, auf rumänisch adäquat zu antworten und er benutzte einen russischen Kommunikationskanal[324]. Infolgedessen verdächtigen die US-Ermittler Guccifer 2.0, wenn existent, ein Mitarbeiter der russichen Nachrichtendienste zu sein, der später auch noch Kontaktdatenlisten von führenden Mitgliedern der demokratischen Partei veröffentlichte[325].

---

[318] vgl. F-Secure Labs 2015
[319] vgl. Alperovitch 2016
[320] vgl. Alperovitch 2016, Nakashima 2016a
[321] vgl. Alperovitch 2016
[322] vgl. Nakashima 2016a
323 vgl. FAZ online 2015, siehe auch Wehner 2015, S.1
[324] vgl. Baumgärtner/Neef/Stark 2016, S.90-91
[325] vgl. Lichtblau/Weiland 2016

Ende August 2016 wurde ein erfolgreiches Eindringen in Onlinewahlsysteme von Illinois und Arizona berichtet, in Illinois wurden Daten von 200.000 Wählern kopiert[326]. Die Medien spekulierten darüber, dass dies Teil einer russischen Kampagne sei, definitive Beweise wurden bisher aber nicht gefunden.[327]

3.3.3 Die Waterbug Group (Turla Malware-Familie)

Waterbug ist der Name für die Gruppe, die die Malware **Wipbot/Tavdig/Epic Turla, Uroburos/Turla/Snake/Carbon** und **agent.btz/Minit** einsetzt.

Nach einem erfolgreichen Eindringen in das Email-System des Verteidigungsministers im Jahr 2008 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[328]. Die Infektion mit einem Wurm namens **agent.btz/Trojan Minit** führte zu einem Paket von Sicherheitsmaßnahmen mit dem Namen **Operation Buckshot Yankee**, das auch die Schaffung des US Cyber Command einschloss[329].

Die Multifunktionsmalware namens **Uroburos/Turla/Snake/Carbon**, die als rootkit arbeitet, ist in der Lage, innerhalb eines Intranets ein eigenes Peer-to-Peer Netzwerk aufzubauen und weist viele technische Überlappungen zu **agent.btz/Trojan Minit**[330] auf. In diesem Netzwerk sucht Uroburos dann einen Computer, der doch mit dem Internet verbunden ist, um dann den Datenaustausch zu beginnen. Uroburos wird nicht aktiv, wenn der Computer bereits mit der Malware agent.btz befallen ist, was auf einen gemeinsamen Ursprung hindeutet[331]. Angreifer setzten die Snake/Uroburos/Turla-Malware gegen ukrainische Computer in 2013/2014 ein. Zusammen mit der Malware agent.btz aus dem Jahre 2008 scheint es sich um eine Malwarefamilie zu handeln, die bis in das Jahr 2005 zurückreicht. Die Angreifergruppe nutzt satellitengestützte Internetlinks für ihre Aktionen[332].

Wipbot/Tavdig/Epic Turla wurde nach ersten Hinweisen im September 2014 in den Systemen der schweizerischen Rüstungsfirma RUAG gefunden, die Waterbug Group zog sich aber im Mai 2016 zurück, nachdem sie aus Medienberichten erfahren hatte, dass sie von der RUAG entdeckt worden war[333].

---

[326] vgl. Nakashima 2016b, Winkler 2016, S.4
[327] vgl. Winkler 2016, S.4
[328] vgl. Glenny 2010, S.23
[329] vgl. Brown/Poellet 2012, S.131
[330] vgl. Symantec 2016, S.10-11
[331] vgl. Fuest 2014a, S.1-3
[332] vgl. Weedon 2015, S.72-73
[333] vgl. Jürgensen 2016, S.28

3.3.4 APT1 (Comment Crew)

Chinas Volksbefreiungsarmee PLA wird verdächtigt, große Cybereinheiten an mindestens einem halben Dutzend Standorten zu unterhalten[334].
Die NSA verfolgte im Jahr 2014 20 Gruppen aus China, von denen sie über die Hälfte der PLA zuschrieb[335].

Die dritte Abteilung der PLA ist für die Signal Intelligence SigInt zuständig und ist in zwölf Büros gegliedert. Das zweite Büro ist auch als **Unit 61398** bekannt und es wird vermutet, dass es auf englischsprachige Organisationen spezialisiert ist, während das zwölfte Büro, die **Unit 61486** eine vermutete Spezialisierung auf Satelliten- und Luftfahrtunternehmen hat. Diese Einheit wurde von Sicherheitsfirmen auch **Putten Panda** genannt und ihre Cyberaktivität konnte mit der Unit 61398 wegen der Nutzung gemeinsamer Infrastruktur verknüpft werden[336].

2013 hat die IT-Sicherheitsfirma **Mandiant** eine tiefgreifende Analyse chinesischer Cyberaktivitäten vorgelegt[337]. Demnach hat die staatlich gestützte cyber war unit 61398 in der Datong Road in Pudong bei Schanghai in den vergangenen Jahren 141 große Cyberattacken auf Regierungseinrichtungen, Unternehmen und Energieversorger durchgeführt und Mandiant vermutet, dass diese Einheit identisch mit der Hackergruppe APT1 sei, China dementierte dies energisch. Die übliche Cybertaktik besteht in gezielten spear-phishing mails, die Schadsoftware zur Installation kleiner Backdoor-Programme enthält, womit die Möglichkeit zu erweiterten Zugriffen gegeben ist.

Später wurden 5 höhergestellte chinesische Militärs offiziell von den USA angeklagt, auch eine Person, die unter dem Decknamen **'UglyGorilla'** agierte. China wies die Beschuldigungen zurück, aber US-Medien spekulierten, dass dieser Vorgang zu dem deutlichen Rückgang mutmaßlicher chinesischer Aktivitäten in den letzten beiden Jahren beigetragen hat[338].

3.3.5 Axiom Group (Deep Panda)

Die Axiom Group ist auch unter vielen anderen Namen bekannt, wie **DeepPanda, Shell_Crew, Group 72, Black Vine, HiddenLynx, KungFu Kittens** etc.

[334] vgl. Finsterbusch 2013, S.15
[335] vgl. Perlroth 2014
[336] vgl. Novetta 2015, S.15, Perlroth 2014
[337] vgl. Mandiant 2013
[338] vgl. Mandiant 2013, Jones 2016, S.5, Nakashima 2016b

Die Gruppe führt hochentwickelte Phishingattacken durch Aufsatteln auf laufende reale Konversationen (**piggybacking**) durch, um das Opfer zum Anklicken von infizierten Links zu motivieren[339].
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[340]. Andere Operationen waren Angriffe auf die Elderwood-Plattform von 2011-2014, die VOHO-Kampagne, bei der 2012 rund 1.000 Organisationen mit waterholing attackiert wurden, ein Angriff auf japanische Ziele in 2013 und Angriffe auf US think tanks in 2014. Verschiedene Zero-day exploits und spezielle Malwarefamilien wurden genutzt, so etwa **Zox, Hikit, Gh0st RAT, PoisonIvy, Hydraq** und **Derusbi**[341]. Zox und Hikit wurden nur bei Axiom beobachtet, während die andere Malware auch von anderen Organisationen genutzt wird.[342] Angriffsziele waren eine große Bandbreite an Regierungseinrichtungen, Unternehmen der Technologiebranche und akademischen Institutionen.

3.3.6 Die Lazarus Group

Über mehrere Jahre wurden Eindringversuche und Wiperattacken vor allem in Südkorea (insbesondere Operation Troy 2009, Darkseoul/Destover 2013) und den USA beobachtet, aber auch in anderen Ländern.
Ende 2014 wurde eine Cyberattacke auf **Sony Pictures Entertainment (SPE)** diskutiert, die die Veröffentlichung eines von Nordkorea handelnden Films „*The Interview*“ betraf. Ein wesentlicher Aspekt war der Einsatz vom Wiper-Malware, die Daten und Dateien von Computern löschte, Die Attacke schien jedoch nur eine Überlappung von verschiedenen Angriffsserien zu sein, denn Sony wurde schon häufiger attackiert, und Südkorea ist schon lange das Ziel ausgedehnter Cyberspionage. Zudem ist das der dritte große Vorfall mit Wiper-Malware in den letzten Jahren, Deshalb muss jeder Aspekt gesondert betrachtet werden, zudem zeigt der Vorgang die enormen praktischen Hürden der Attribution und der digitalen Forensik.

In 2016 unternahmen IT-Sicherheitsfirmen mit Firmen wie *Symantec*, *Kaspersky*, *Alien Vault* etc. unter Führung von *Novetta* die **Operation Blockbuster**[343]. Die gemeinsame Analyse ergab starke Hinweise, dass zumindest zwei der drei großen

[339] vgl. Alperovitch 2014. Die IT-Sicherheitsfirma Crowd Strike nutzt den auf Windows und Mac-Servern, Desktops und Laptops eingesetzten Kernelsensor *Falcon host* zum Erkennen von Angriffen und dem Abgleich mit einer Datenbank (threat intelligence repository) für die Attribution.
[340] vgl. Markoff/Barbosa, 18.02.2010
[341] vgl. Novetta 2015, S.12-13
[342] vgl. Novetta 2015, S.20
[343] vgl. Novetta 2016

Wiperattacken und der Sony/SPE-Hack von derselben Gruppe durchgeführt wurden, die nun Lazarus Group[344] genannt wird. Während viele Spuren darauf hinweisen, dass die Lazarus Group in Verbindung mit Nordkorea steht, fehlen immer noch eindeutige Beweise. Die Gruppe erweitert ihre Malware ständig, wie zum Beispiel die Trojaner **Hangman/Volgmer** in 2014 und **Wild Positron/Duuzer**[345] in 2015.
Im Sommer 2016 wurde diskutiert, ob die Lazarus Group hinter den Angriffen auf das Interbankensystem SWIFT steht, siehe Kapitel 3.3.6.4.

Novetta identifizierte 45 Malwarefamilien mit vielen Beispielen von wiederwendetem Code und überlappender Programmierung. Das schloss auch recht spezielle Anwendungen wie ähnliche **Suicide Scripts** ein, mit denen man Malwareprogramme nach erfolgreicher Ausführung wieder entfernen kann und ein typisches **space-dot-encoding**, bei dem Begriffe, die von Sicherheitssoftware erkannt werden können, durch unnötige Leerstellen und Symbole gespreizt werden[346]. Die Programme enthielten auch besondere Rechtschreibfehler wie 'Mozillar' statt ‚Mozilla' in mehreren Malwarefamilien, eine Nutzung von BAT-Dateien über viele Hangman/Volgmer-Varianten, um Malwarebestandteile nach der Infektion wieder löschen zu können und außerdem wurde für verschiedene Malware-Dropper dasselbe Passwort verwendet[347]. Die Zeitstempel der Programme deuten auf eine Gruppe in der Zeitzone GMT+8 oder GMT+9 hin, was auf Korea passen würde[348].

3.3.6.1 Wiper Malware-Attacken

Am 15.08.2012 wurde die saudische Ölfirma ARAMCO mit der **Shamoon/Disttrack**-Malware angegriffen; am 20.03.2013 wurden südkoreanische Banken und Sender von der Malware namens **DarkSeoul/Jokra** während Sony von der **Destover**-Malware am 24.11.2014 betroffen war. Es gab gewisse Ähnlichkeiten:

Nach dem Eindringen wurde die Malware auf den Computern platziert[349]. Die kommerziell verfügbare Software **EldoS RawDisk**[350] wurde benutzt, um die

[344] vgl. Novetta 2016
[345] vgl. Guerrero-Saade/Raiu 2016, S.2
[346] vgl. Novetta 2016
[347] vgl. Guerrero-Saade/Raiu 2016
[348] vgl. Guerrero-Saade/Raiu 2016, S.6
[349] Dies erfolgte schrittweise. Bei Darkseoul wurde ein Trojaner für den Fernzugriff am 26.Januar 2013 kompiliert, der Wiper schon am 31.Januar 2013 während dann ein Trojaner für den Start der Attacke am 20.März 2013 kompiliert wurde, vgl. McAfee 2013, S.4
350 vgl. Baumgartner 2014, S.2, 4

Windows-Laufwerke zu erreichen. In allen Fällen fungierte die Malware als **logische Bombe**, d.h. sie wurde erst zu einem vordefinierten Zeitpunkt aktiv[351].

In allen drei Fällen wurden Daten von Computern und File-Servern gelöscht und Re-Booting wurde blockiert. Im Aramco-Fall wurde die Ölversorgung vorübergehend beeinträchtigt[352] (32.000 Computer beschädigt), in Seoul wurde die Geschäftstätigkeit der betroffenen Firmen ebenfalls vorübergehend beeinträchtigt (30.000 Computer beeinträchtigt), für Sony Pictures kam es neben Schäden und Datenlecks zur zunächst gestoppten und später nur begrenzten Publikation des Films *The Interview*.

Zudem bekannten sich in allen drei Fällen ‚**Hacktivisten**' (Hacker und Aktivisten)-Gruppen zur Urheberschaft, aber verschiedentlich wurde vermutet, dass diese Gruppen vielleicht nur Tarnung von staatlichen Aktivtäten sind bzw. diese im Dienste von Staaten stehen könnten[353], diese waren *Cutting Sword of Justice* (Aramco), *Whois/NewRomanic Cyber Army Team* (im Darkseoul hack[354]) und die *Guardians of Peace* (Sony Pictures). Durch die Operation Blockbuster scheint nun klar zu sein, dass *Whois/NewRomanic Cyber Army Team* und die *Guardians of Peace* Aliasnamen der Lazarus Group waren[355]
Alle Attacken wurden von Warnungen begleitet, die auch graphisch illustriert waren (wie z.B. mit Skeletten und Totenköpfen) und/oder vage formulierten Statements, die keine eindeutige politische Einordnung erlaubten[356]. Das in den Warnungen verwendete Englisch sprach für nicht-native Autoren.

Operation Blockbuster brachte zahlreiche Befunde, die eine Verbindung zwischen der Darkseoulattacke und dem Sony/SPE-Hack nahelegen. Jedoch fand sich keine klare Verbindung zu dem Angriff auf Aramco und der Shamoon-Malware. Novetta vermutet einen Kontakt zwischen den Aramco-Hackern und der Lazarus Gruppe über ein Technologieaustauschabkommen zwischen Nordkorea und dem Iran[357]. Jedoch müsste dann weiter geklärt werden, wieso die Lazarus Group, die schon seit Jahren aktiv war und ihre Fähigkeiten gezeigt hatte, Hilfe von einer anderen Gruppe brauchte, zudem litt der Iran im selben Jahr wie Aramco unter einer Wiperattacke.

351 vgl. Darnstaedt/Rosenbach/Schmitz 2013, S.76-80
352 Zuvor wurden wie bereits erwähnt im April 2012 iranische Ölterminals von einer datenvernichtenden Wiper-Schadsoftware getroffen
353 vgl. McAfee 2013
354 vgl. Sherstobitoff/Liba/Walter 2013, S.3. Die IT-Sicherheitsfirma Crowd Strike vermutet, dass die Angreifer mit der Gruppe identisch sind, die sie Silent Chollima nennen und die seit 2006 aktiv ist, vgl. Robertson/Lawrence/Strohm 2014.
355 vgl. Novetta 2016
356 vgl. auch Baumgartner 2014, S.4-6
357 vgl. Novetta 2016, S.15

3.3.6.2 Cyberspionage in Südkorea

Die IT-Sicherheitsfirma McAfee identifizierte eine lange Serie von Cyberspionageaktivitäten von mindestens 2009 bis 2013, wo die "**Troy**"-Familie von Trojanern (benannt nach dem Trojaner **HTTP Troy**) mit vielen Gemeinsamkeiten benutzt wurde, um militärische Ziele wie auch andere Unternehmen anzugreifen. So wurde z.B. für die Angriffe auf militärische Ziele ein gemeinsames Verchlüsselungspasswort benutzt, das auch für die **TDrop**-Malware aus der Darkseoulattacke verwendet wurde[358]. Weitere Gemeinsamkeiten betrafen den benutzten Code und die Nutzung bestimmter dll.files. Das zeigt an, dass diese Attacken mehr als **Cybervandalismus** gewesen sind, also nicht nur der Schädigung der befallenen Systems dienen sollten.

Die IT-Sicherheitsfirma Symantec war zudem in der Lage, verschiedene Attacken gegen nicht-militärische Ziele gegen Banken und Rundfunkunternehmen mit den Angreifern von Darkseoul (Symantec verwendet die Bezeichnung **Trojan.Jokra**) in Verbindung zu bringen, die zusätzlich zum Angriff am 20.03.2014 die Trojaner **Dozer** und **Koredos** in DDoS- und Wiper-Malwareattacken in 2009 and 2011 zum Einsatz brachten[359]. Am 63. Jahrestag des Beginns des Koreakriegs wurden die Trojaner **Castov** und **Castdos** eingesetzt, um DDoS-Attacken gegen die südkoreanische Regierung zu starten.
Ende 2014 und somit im ähnlichen Zeitraum wie der Sony Hack wurde der einzige südkoreanische Betreiber von Atomkraftwerken **Korea Hydro and Nuclear Power Co (KHNP)** wiederholt angegriffen und eine Reihe von Personal- und technischen Daten geleakt[360].

3.3.6.3 Der 'Sony Hack´ (alias SPE hack)

In den Medien wurde der Begriff Sony-Hack für den Angriff der Hackergruppe **Guardians of Peace (GoP)** verwendet. Sony als Medienanbieter war aber auch von anderen Attacken betroffen, z.B. im April 2011 von einem massiven Angriff von Unbekannten, die unter anderem die Daten von 77 Millionen Playstationnutzerkonten entwendeten.[361] und im Dezember 2014 wurde Sony auch von der Hackergruppe **Lizard Squad** angegriffen[362][363].

---

[358] vgl. McAfee 2013, S.28
359 vgl. Symantec 2013, S.1-2
360 vgl. Leyden 2014, S.1-3. KHNP bestätigte, dass keine kritischen Daten abgeflossen sind und ließ Cyberübungen zur Erhöhung der Sicherheit durchführen.
361 vgl. Lambrecht/Radszuhn 2011, S.25, Betschon 2014, S.34
362 2015 wurde die Hackerplattform **Darkode** durch Europol und das FBI durch erfolgreichen Einsatz von verdeckt operierenden Ermittlern geschlossen, vgl. Finsterbusch 2015, S.26. Lizard Squad nutzte diese Plattform.
363 vgl. Handelszeitung online 2014, S.1

Am 21.11.2014 wurde Sony von einer Gruppe, die sich the Guardians of Peace (GoP; Hüter des Friedens) nannte, informiert, dass diese 100 Terabytes an Daten in ihrem Besitz hätte und sie forderten Geld, um eine Veröffentlichung zu vermeiden[364]. Am 24.11.2014 begann die Veröffentlichung von Daten wie von den GoP angekündigt. Am 01.12.2014 wurden große Mengen von internen Sony-Daten, vom St. Regis-Hotel in Bangkok/Thailand und anderen Orten geleakt. In den folgenden Tagen wurden weitere Daten publiziert.[365]
Am 16.12.2014 erwähnten die GoP erstmals ausdrücklich den Film *The Interview* und drohten mit Terror mit Verweis auf die Ereignisse von 9/11; die geplante Veröffentlichung für den 25.12.2104 wurde zunächst abgesagt[366].

Der US-Präsident Obama betrachtete dies als einen Akt des Cybervandalismus und bat China um Unterstützung gegen nordkoreanische Attacken, da der einzige Internetprovider in Nordkorea die chinesische Firma China Unicom[367] ist. Ein nachfolgender Zusammenbruch des nordkoreanischen Internets am 22.12.2014 löste Spekulationen über einen Vergeltungsakt aus, jedoch hatte das nordkoreanische Netz schon vorher manchmal technische Probleme.[368] An Weihnachten 2014 wurde der Film *Das Interview* in einer begrenzten Anzahl von Kinos publiziert. Zudem wurden Sanktionen gegen einige nordkoreanische Personen Anfang 2015 verhängt, diese standen aber mit militärtechnologischen Angelegenheiten, nicht mit dem Sony-Hack in Verbindung[369].

Die Herkunft des Angriffs wurde intensiv diskutiert. Die zentralen Argumente für Nordkorea als Ursprung waren die folgenden:
Das FBI fand heraus, das einige der von den Hackern für den Sony-Hack genutzten IP-Adressen ausschließlich von Nordkorea genutzt werden und die Hacker wohl aus Versehen ihre Facebook-Accounts über diese Adressen nutzten[370]. Hinzu kommen die Ähnlichkeiten in den Wiper-Malwareattacken. Die Systemeinstellungen des zur Programmierung der Malware genutzten Computers waren koreanisch, außerdem benutzten die Hacker einige koreanische Begriffe[371].Der Sony-Hack und die anderen Angriffe auf Südkorea verwendeten einen gemeinsamen Command and Control-Server, der sich in Bolivien befand[372]

364 vgl. Fuest 2014b, S.31
365 vgl. Betschon 2014, S.34
366 vgl. Steinitz 2014, S.11
367 vgl. FAZ 2014a, S.21. FAZ 2014b, S.1. Das nordkoreanische Internet umfasst ein paar Tausend IP-Adressen, da es noch ein nationales Netz mit dem Namen Kwangmyong (Helligkeit) mit einigen tausend Webseiten gibt, SZ2014a, S.1
368 vgl. SZ2014b, NZZ 2014
369 vgl. Zoll 2015, S.1
370 FBI Direktor James Comey zitiert bei Schmidt/Perlroth/Goldstein 2015, S.1f.; die exklusive Nutzung durch die Nordkoreaner wurde in einem Tweet von KajaWhitehouse erwähnt, die ebenfalls Comey zitierte.
371 vgl. Fuest 2014b, S.31
372 vgl. Robertson/Lawrence/Strohm 2014, S.1

Außerdem wurde über Nordkoreas wichtigsten Nachrichtendienst, das **Reconnaissance General Bureau**, berichtet, dass dieser über Cyberfähigkeiten verfügt, insbesondere zwei Einheiten mit den Namen **Unit 121 (Einheit 121)** und and **No. 91 office (Büro Nr.91)**. Es gibt einige wenige Berichte, nach denen einige dieser Personen aufgrund der begrenzten Internetkapzitäten des Landes vom Ausland aus operieren sollen[373]. Es wurde außerdem argumentiert, dass Nordkorea ein klares politisches Motiv gehabt hat[374], jedoch hat Nordkorea jede Beteiligung an dem Angriff auf das Schärfste zurückgewiesen[375].

Alternative Theorien wurden diskutiert, denn die Angreifer haben anfangs nach Geld gefragt[376] und erst später, als die Medien einen möglichen Zusammenhang mit dem Film *The Interview* erörterten, erfolgte ein Wechsel zu der politischen Forderung, den Film nicht zu veröffentlichen. Die norwegische IT-Sicherheitsfirma Norse vermutete 6 Personen aus den USA, Kanada, Singapur und Thailand hinter den Guardians of Peace, einer von diesen war ein ehemaliger Sony-Mitarbeiter mit IT-Kenntnissen des Unternehmensnetzwerkes[377]. Insbesondere fand man Kommunikationen dieses Mitarbeiters mit einer Person, die direkt mit dem Server in Verbindung gebracht werden konnte, wo die erste Version der Malware im Juli 2014 kompiliert wurde[378]. Die genutzten IP-Adressen wären auch von anderen Hackergruppen genutzt worden und die Schadsoftware wäre auf dem Schwarzmarkt verfügbar gewesen[379][380].

Die US-Behörden bestätigen jedoch ihre Einschätzung und argumentierten, dass sie nicht alle Beweise offenlegen könnten, um Hackern keine zu große Einsicht in ihre Ermittlungsmethoden zu geben[381]. Deshalb hielt das FBI an seinen Schlussfolgerungen zur Angriffsquelle fest[382]. Zudem berichtete die *New York Times*, dass die NSA in der Lage gewesen sei, in nordkoreanische Netzwerke über Malaysia und Südkorea vorzudringen, so dass sie in der Lage gewesen sei,

373 vgl. Robertson/Lawrence/Strohm 2014, S.2
374 vgl. Fuest 2014b, S.31
375 vgl. NZZ 2014
376 vgl. Fuest 2014b, S.31
377 vgl. SZ 2014c, Bernau 2014, S.1
378 vgl. The Security Ledger online 2014, S.1
379 Siehe z.B. Bernau 2014, S.1
380 vgl. Fuest 2014b, S.31. Theoretisch könnten die initialen Leaks und die späteren Drohungen von zwei verschiedenen Akteuren stammen, da es unter der von den GoP genutzten mail-Adresse inkonsistente Botschaften gab (vgl. auch also Fuest 2014b, S.31 der von einer North Korean Hacking Army berichtet, die aber die koreanische Sprache fehlerhaft benutzte).
381 vgl. Zoll 2015, S.1
382 vgl. SZ 2014c

nordkoreanische Hackeraktivitäten zu beobachten und nachzuverfolgen, aber eine offizielle Bestätigung dieser Darstellung wurde nicht gegeben[383].

3.3.6.4 Die SWIFT-Attacken

Im Sommer 2016 vermuteten Sicherheitsexperten von *BAE Systems* die Lazarus Group hinter dem Eindringen in das globale Finanznetzwerk **SWIFT** (Society for Worldwide Interbank Financial Telecommunication), wodurch am 04.02.2016 der Transfer von 81 Millionen Dollar von der Zentralbank in Bangladesh zu anderen Konten möglich war[384]. Ursprünglich sollten 951 Millionen Dollar transferiert werden, aber ein Schreibfehler im Wort 'foundation' alarmierte die Banker und weitere Transfers konnten gestoppt werden. Die Sicherheitsprobleme entstanden womöglich durch veraltete Computer, die Überweisungszeiten lagen außerdem außerhalb der Arbeitszeiten in Bangladesch, um Rückfragen und Informationen der Bank vor dem Transfer zu verhindern[385]. Mittlerweile wurden weitere Attacken auf das SWIFT System für Banken in Ecuador, der Ukraine und Vietnam berichtet[386]. Der WiperCode, der zur Spurenverwischung genutzt wurde, war derselbe wie beim Sony/SPE-Hack[387].

3.3.7 Weitere Gruppen

In Kapitel 2.2.8 wurden zwei spezialisierte Hackergruppen mit einem Fokus auf die Industrie berichtet, die Gruppe **Dragonfly (Energetic Bear/Crouching Yeti/Koala)** und die **Sandworm/Quedagh** Gruppe, die die **BlackEnergy** Malware benutzt.

Eine weitere zielgerichtete Infektion diplomatischer und Regierungseinrichtungen war **Red October** von 2007-2013. Durch spear-phishing wurde ein Trojaner auf den infizierten Computern platziert, um unter anderem auch Dateien, die mit der klassifizierten Software *acid cryptofiler* [388] bearbeitet wurden, zu extrahieren. Im Dezember 2014 tauchte eine ähnliche Malware für Smartphones unter dem Namen **Cloud Atlas/Inception**[389] wieder auf.

383 vgl. FAZ 2015a, S.5. Die Frage kam auf, wieso der Hack nicht früher bemerkt wurde. In der Shamoon-Wiperattacke fanden sich jedoch Hinweise, dass ein Insider mit hohen Zugangsrechten beim Eindringen in die System half, Aramco wollte dies jedoch nicht kommentieren, Finkle 2012, S.1
384 vgl. Brächer 2016, S. 26-27
385 vgl. Storn 2016, S. 29
386 vgl. FAZ 2016b, S.23, Storm 2016
387 vgl. Storm 2016
388 vgl. Kaspersky Labs 2013
389 vgl. Dilger 2014

3.4 Cyberwar gegen den Islamischen Staat ('IS')

Der **Islamische Staat IS** (synonym auch **ISIS, ISIL** und **Daesh**) ist ein wichtiger dschihadistischer Akteur in den andauernden Konflikten in Syrien und Irak und kontrolliert relevante Gebiete beider Länder seit der Übernahme vom Rakka in Syrien und Mosul im Irak in 2014.
Die USA gaben 2016 offiziell bekannt, dass das US Cyber Command aktiv gegen den IS vorgeht, um die Kommunikation durch Beeinträchtigung der Netzwerke zu unterbrechen, insbesondere sie durch Überlastung außer Funktion zu setzen, um die Rekrutierung, die Planung und den Resourceneinsatz zu treffen[390]. Die Aktivitäten sind in die allgemeinen militärischen Maßnahmen eingebettet. Während der IS formal kein Staat ist (da er vom Ausland nicht als solcher anerkannt wird),[391] kommt er aus militärischer Sicht einem Staat gleich (Größe, Macht, Bevölkerung, Gebiete, Kontrolle).

Nach den Terroranschlägen in Paris vom November 2015 erklärte die Gruppe **Anonymous** (zuweilen als 'hacktivists' = hacking activists bezeichnet) dem IS den Cyberkrieg, der dann intensiv in den Medien diskutiert wurde. Diese Erklärung kam jedoch unerwartet, da Anonymous schon im August 2014 den „full-scale cyberwar" (umfassenden Cyberkrieg) gegen den IS erklärt hatte[392], die zweite Erklärung kann man evtl. als Erneuerung bzw. Bekräftigung interpretieren. In der Woche nach den Paris-Attentaten war Anonymous in der Lage, 5.500 ISIS-Twitter-Accounts lahmzulegen[393]. Im Jahre 2015 wurden noch weitere Cyberwar-Érklärungen gegen Israel und die Türkei abgegeben. Mittlerweile hat Twitter die eigenen Aktivitäten verstärkt und in einem Jahr ab Mitte 2015 360.000 Accounts geschlossen, die Terroraktivitäten guthießen[394].

Um die Überwachung von e-Mails zu umgehen, werden zunehmend Messengerdienste mit Verschlüsselung benutzt[395]. Ein dem Islamischen Staat (IS) zugeschriebenes Dokument aus dem Januar 2015 listet insgesamt 33 Messengerdienste auf und unterteilt sie in 5 Sicherheitskategorien. In der Praxis wurde der sichere Messengerdienst *Telegram* von IS-Aktivisten genutzt, da dieser die Kommunikation und Versendung von Dateien ohne digitale Spuren erlaubt. Telegram schloss mehr als 660 IS-Konten seit November 2015[396].
Ursprünglich wurde vermutet, dass die Attentäter von Paris im November 2015 Kommunikationskanäle in der *Playstation 4 (PS 4)* genutzt hätten, aber Beweise hierfür konnten nicht vorgelegt werden.

---

[390] vgl. Paletta/Schwartz 2016, S.1-2
[391] vgl. Kurz 2016, S.14
[392] vgl. Anonhq 2014
[393] vgl. Chip.de 2015
[394] vgl. DW online 2016
[395] vgl. Langer 2015b, S.5
[396] vgl. Dörner/Nagel 2016, S.37

In Januar 2016 gab der IS ein Cyberwar-Magazin namens *Kybernetiq* heraus mit Cyberwar-Informationen[397]. Am 08.03.2016 erhielt der Fernsehsender *Sky News* die Personaldateien von 22.000 IS-Kämpfern zugespielt, die Personen- und Kontaktdaten insbesondere von ausländischen Kämpfern enthielten[398]. Dazu hieß es, die Dateien stammten aus einem internen Leck in der IS-Sicherheitsabteilung.

Im April 2016 gaben die USA offiziell den Abwurf von **Cyberbomben** auf die IS-Systeme bekannt, wobei Details dieser Maßnahmen geheim blieben[399]. Jedoch wurde berichtet, dass die USA in der Lage waren, die Systeme zu infiltrieren, um so falsche Befehle einzuspeisen, Finanztransaktionen zu behindern und die Kommunikation in sozialen Netzwerken einzudämmen[400].
Jedoch wollte das Pentagon seine Aktivitäten verstärken, da der IS weiter operierte, z.B. mittels der Nachrichtenagentur *Amaq* oder der weiteren Herausgabe des regelmäßig erscheinenden Magazins *Dabiq*. Deshalb ließ der Chef des Cybercom, Rogers, die 100 Mann starke Einheit "**Joint Task Forces Ares**" errichten[401].
Im Mai 2016 wurde Generalleutnant Cardon durch Cybercom angewiesen, die Zusammenarbeit von **Ares** mit dem Zentralkommando für den Mittleren Osten und Asien zu sichern und digitale Waffen zu entwickeln oder zu beschaffen[402].
Der IS hat gezeigt, dass er alle Arten von Kommunikationswegen zu nützen weiß und dass er möglicherweise nicht so sehr auf eine zentralisierte Serverarchitektur angewiesen ist wie die großen Staaten, d.h. er ist schwer greifbar. [403] Zum Beispiel half die NSA den deutschen Behörden bei der Entschlüsselung der Anweisungen der IS-Anleiter für die Terrorangriffe in Würzburg und Ansbach im Juli 2016. Die Kommunikation schien aus Saudi-Arabien zu kommen, aber die saudi-arabische Botschaft erklärte, dass für die Instruktion des einen Attentäters zwar eine saudische Telefonnummer benutzt wurde, sich die Person aber in den vom IS kontrollierten Gebieten aufhielt[404].
Um die Cyberwarfähigkeiten der USA weiter zu stärken, plant Präsident Obama nun die Aufwertung von Cybercom zu einem eigenständigen militärischen Kommando mit einem Fokus auf die militärischen Aspekte des Cyberspace. Die Verbindung zur NSA würde aufgehoben und die NSA soll in Zukunft von einem Zivilisten geführt werden[405].

[397] vgl. Cyberwarzone 2016
[398] vgl. DW 2016
[399] vgl. Strobel 2016, S.2
[400] vgl. Lange 2016, S.5
[401] vgl. Strobel 2016, S.2
[402] vgl. Strobel 2016, S.2, Rötzer 2016, S.2
[403] vgl. Rötzer 2016, S.2
[404] vgl. FOCUS Online 2016
[405] vgl. Strobel 2016

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 Cyberwars 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[406].

Die Aufgaben der Behörde sind unter anderem[407]:

- Mitarbeit im Arbeitskreis KRITIS zum Schutz **Kritischer Infrastrukturen** vor Angriffen[408]
- Schutz der Regierungskommunikation, u.a. durch Kryptohandys für die Regierung, aber auch im **Informationsverbund Bonn-Berlin IVBB** und

[406] 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

[407] vgl. BSI Jahresberichte 2005, 2006-2007 und 2008-2009 und 2010

[408] 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“ (KRITIS) auszuarbeiten (Umsetzungsplan UP KRITIS)

dem **Informationsverbund Bundesverwaltung IVBV,** der vom BSI seit 2009 regelmäßig auf Schadsoftware gescannt wird[409]

- 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 Internetzwerk-Architektur) –Technologie
- Arbeit auf dem Gebiet der Kommunikationssicherheit (**Comsec**), zu der auch die Gebäudeabschirmung gehört[410]
- Arbeit an stabilen und resistenten Computertechniken wie der Hochverfügbarkeit[411] oder der **Mikrokerntechnologie**, bei der Rechnerbereiche intern noch mal gegeneinander abgeschottet werden usw.
- Als Teil der am 23.02.2011 publizierten **Nationalen Cyber-Sicherheitsstrategie für Deutschland** hat ein **Nationales Cyber Abwehrzentrum** mit 10 Beamten im BSI seine Arbeit aufgenommen[412]. Die Arbeit des neuen Cyber-Abwehrzentrums wurde bislang jedoch durch Abstimmungsprobleme zwischen den Mitgliedsbehörden (Regierung, Nachrichtendienste, Polizei usw.) beeinträchtigt [413].
- Zudem wurde ein **Nationaler Cyber-Sicherheitsrat** ins Leben gerufen, dem u.a. die Staatssekretäre der großen Bundesministerien angehören[414].

Im Jahr 2016 ist eine neue Entschlüsselungsbehörde, anfangs mit 60, später mit 400 Mitarbeitern unter dem Namen **Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITIS)** geplant. Diese wird die Bundespolizei, das BKA und den Verfassungsschutz mit Codeknacken unterstützen. Der BND wird nicht beteiligt sein[415].
Die neue Nationale Cyber-Sicherheitsstrategie für Deutschland von 2016 sieht zudem die Schaffung eines **nationalen CERT** mit sog. **Quick Reaction Forces** vor, die beim BKA, dem BSI und dem BfV angesidelt sein werden[416].

---

[409] vgl. Steinmann 2010, S.10
[410] um Probleme wie das Abfangen von vom Computer abgestrahlten Informationen zu bewältigen, vgl. SchrÖder 2008
[411] 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.
[412] vgl. FAZ 2010g, S.4, Tiesenhausen 2011, S.11, BMI 2011
[413] vgl. Goetz/Leyendecker 2014, S.5
[414] Im Wirtschaftssektor wurde als Kooperation das **International Security Forum ISF** mit momentan 326 Mitgliedsfirmen geschaffen. 2012 gründeten der deutsche IT-Verband BITKOM und der BSI die **Allianz für Cybersicherheit** mit 68 Mitgliedsfirmen und 22 Mitgliedsorganisationen, die in der Cyberabwehr auf Grundlage von Vertraulichkeitsvereinbarungen kooperieren, vgl. Karabasz 2013, S.14-15
[415] vgl. Heil/Mascolo 2016, Mascolo/Richter 2016, S.2
[416] vgl. Biermann/Beuth/Steiner 2016

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 einschließlich des Schutzes der Computer und Abwehr von Cyberangriffen[417] 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[418]. Das KSA, das seit 2008 den Kern des Militärischen Nachrichtenwesens der Bundeswehr (MilNWBw) bildet, hatte 2010 eine Stärke von ca. 6.000 Mann[419] und ist zuständig für die

- für die Elektronische Kampfführung (EloKa), d.h. die Störung feindlicher Kommunikation und
- seit 2007 gehört dem KSA auch die Einheit **Computer- und Netzwerkoperationen CNO**[420] an, die auch für den Cyberwar zuständig ist, d.h. den Kampf im Internet gegen mögliche Angreifer[421] und seit 2012 einsatzbereit ist[422]
- und für die Aufklärungssatelliten des Typus Synthetic Aperture Radar (SAR-Lupe) [423] 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. Das Herkules-Projekt hat die IT-Infrastruktur deutlich vereinfacht, indem die Zahl der Softwareprogramme

[417] vgl. Rühl 2012, S.10
[418] vgl. Eberbach 2002
[419] vgl. Bischoff 2012
[420] vgl. Bischoff 2012
[421] Goetz 2009, S.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.
[422] vgl. Steinmann/Borowski 2012, S.1
[423] vgl. Bischoff 2012. 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. Für 2017 ist für SAR-Lupe das Nachfolgesystem SARah geplant.

von 6000 auf weniger als 300 reduziert werden konnte; dennoch bleibt die Struktur immer noch komplex[424].

Im Ergebnis sieht die aktuelle Cyberstruktur der Bundeswehr nun wie folgt aus:

Die 60 Spezialisten des **Computer Emergency Response Team der Bundeswehr (CERTBw)** sind für die Überwachung der IT-Infrastruktur zuständig, die 2015 200.000 Computer umfasste. Die Empfehlungen werden dann von 50 Spezialisten des **Betriebszentrums IT -Systeme der Bundeswehr (BITS)** geprüft und ggf. umgesetzt[425]. Die militärgeheimdienstlichen Fragen werden vom MAD betreut; die Offensivkapazitäten sind im KSA als CNO angesiedelt (siehe oben)[426].

Das Bundesverteidigungsministerium BMVg teilte im September 2015 mit, die Aktivtäten im Cyber- und Informationsraum bündeln zu wollen[427], Ziel ist die Errichtung eines **'Cyberinformationsraumkommandos'**[428]. Momentan sind 320 Personen im Cybersektor aktiv.
Das neue Kommando wird 2017 errichtet und in Zukunft das **Kommando Strategische Aufklärung KSA** mit den bereits oben genannten Untereinheiten für die elektronische Kampfführung EloKa, die Netzwerkoperationen (CNO) und die Satelliten (mit dem gesamten Geoinformationswesen GeoBw) führen. Dieser Transfer wird dem CIR mehr als 13.700 Soldaten zuführen[429]. Die CNO-Kapazitäten werden ausgebaut, um Cyberangriffsübungen ausführen zu können, als sog. **Red teaming**[430].

Im Jahr 2015 berichtete die Bundeswehr[431] über 71 Millionen unautorisierte oder bösartige Zugriffsversuche, davon hatten 8,5 Millionen die Gefahrenstufe hoch. Während Auslandseinsätzen wurden 150.000 Attacken, davon 98.000 mit hoher Gefahrenstufe beobachtet. Insgesamt konnten 7.200 Malwareprogramme entdeckt und entfernt werden. Durchschnittlich werden in der Truppe 1,1 Millionen e-Mails pro Tag verschickt.

Zur Überprüfung der Abwehrkapazitäten fand vom 30.11.-01.12.11 die länderübergreifende Übung **Lükex 2011** statt, bei der ein vom Bundesamt für

[424] vgl. Handelsblatt 2014, S.16
[425] vgl. BmVg 2015a
[426] vgl. BmVg 2015a
[427] vgl. Leithäuser 2015b, S.4
[428] vgl. Köpke/Demmer 2016, S.2
[429] vgl. BmVg 2016
[430] vgl. BmVg 2016, S.28
[431] vgl. Köpke/Demmer 2016, S.2

Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem BSI entwickeltes umfassendes Angriffsszenario auf kritische Infrastrukturen getestet wurde[432].

Der Bundesnachrichtendienst BND hat 2013 eine Cyberabteilung eingerichtet[433][434]. Aus Sicht des BND stellen China und Russland diesbezüglich besonders wichtige Staaten dar, wobei die Russen anders als die Chinesen die staatlichen Hacker von privaten Firmen aus agieren lassen. Der BND plant auch die Entwicklung von Cyberkapazitäten, um die Server von Cyberangreifern abschalten zu können. Der BND hat die **Strategische Initiative Technik (SIT)** initiiert, um die Fähigkeit zur Echtzeitüberwachung von Metadaten zu verstärken und weitere Maßnahmen[435]. Zudem ist die aktive Unterstützung der Cyberabwehr geplant, indem die vom Dienst gewonnenen Informationen der Vorbereitung auf Attacken helfen soll. Jedoch wurden die benötigten Mittel von 300 Millionen Euro bis 2020 noch nicht bewilligt[436].

Der deutsche Bundestag ist seit Jahren ein primäres Angriffsziel[437].

4.3 Die Cyberwarstrategien der USA und Chinas

Medienberichten zufolge wird die Zahl der Staaten, die versuchen, Cyberwarkapazitäten aufbauen, auf mehr als 100 geschätzt. Nach US-Schätzungen versuchen ca. 140 ausländische Nachrichtendienste in Computer der Regierung oder von US-Firmen einzudringen[438].
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[439].

4.3.1 Strategische Ziele

Das Primärziel aller Akteure ist die Erringung der **elektromagnetischen Dominanz** und insbesondere der **Überlegenheit im Cyberspace**[440], d.h. der Beherrschung des Cyberspace im Konfliktfall. Da die gegnerischen Systeme

[432] vgl. Spiegel online 2011
[433] vgl. Flade/Nagel 2015, S.4
[434] vgl. Spiegel 2013b, S.22, auch Spiegel 2013c, S.15
[435] vgl. SZ 2014a, S.1
[436] vgl. Spiegel 2014, S.18
437 Jedoch stehen auch Regierungsbehörden im Fokus wie das Außenministerium und die Botschaften, vgl. Lohse/Sattar/Wehner 2015, S.3
[438] vgl. Wilson 2008, S.12
[439] vgl. Kanwal 2009. Ende 2010 wurde Frankreichs Wirtschaftsministerium Opfer einer großen Spionageaktion, die vermutlich auf die Erforschung der politischen Strategie für das G20-Gremium zielte, vgl. Meier 2011, S.9
[440] vgl. USAF 2010a, S.2

jedoch wiederhergestellt werden können, beschränkt sich die Zielsetzung in der Praxis auf die Sicherstellung der eigenen Handlungsfreiheit (**freedom of action**) und die Beschränkung der Handlungsfreiheit des Feindes, wobei beides im Verbund mit konventionellen Operationen steht.

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[441]. 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.[442]

Im April 2015 publizierte das US-Verteidigungsministerium (Department of Defence DoD) die neue **DOD Cyber Strategy**[443]. Das DoD hat fünf strategische Zieiele definiert, nämlich den Aufbau von Kapazitäten, die Verteidigung und Risikominimierung für die eigenen Systeme, den Fokus auf die USA und ihre vitalen Interessen, die Verfügbarkeit von Optionen im Cyberspace, um Konflikte zu kontrollieren und angemessen behandeln zu können und die Schaffung internationaler Allianzen und Partnerschaften[444].

4.3.2 Cyberwarkapazitäten

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. 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.

---

[441] vgl. Krekel et al. 2009
[442] vgl. Tinner et al. 2002
443 vgl. DoD 2015
444 vgl. DoD 2015, S.8

Die USA haben ihre Cyberwarkapazitäten über zwei Jahrzehnte systematisch aufgebaut und koordiniert[445].
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[446].
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[447], 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[448], und ist räumlich bei der NSA angesiedelt[449]. Das US CYBERCOM ist dem strategischen Kommando US STRATCOM unterstellt, das übergeordnet für die Planung und Ausführung von Operationen im Cyberspace zuständig ist[450].
Das US CYBERCOM schützt jedoch nur die Websites mit der vom US-Militär genutzten Domain ‚.mil', während das Heimatschutzministerium Department of Homeland Security DHS weiterhin für die zivile Regierungsdomain ‚.gov' zuständig ist[451].

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. 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 Cyber Storm I-IV in den Jahren 2006, 2008, 2010 und 2012 unter der Leitung des Department of Homeland Security (DHS) stattfanden, bei denen ebenfalls Großangriffe auf die

[445] vgl. Hiltbrand 1999
[446] vgl. Porteuos 2010, S.3
[447] USAF: 24th Air Force, Army Forces Cyber Command (ARFORCYBER), Fleet Cyber Command (10th fleet/FLTCYBERCOM) und das Marine Forces Cyber Command (MARFORCYBER), vgl. auch Dorsett 2010
[448] vgl. Hegmann 2010, S.5, The Economist 2010, S.9/22-24, Glenny 2010, S.23
[449] vgl. DoD 2011, S.5
[450] vgl. USAF 2010a, S.21-22
[451] vgl. Porteuos 2010, S.7

IT-Infrastruktur der USA getestet wurden. Für die DHS-Übung von 2010 wurden Codes für das Border Gateway Protocol BGP entwickelt, die den Datenverkehr im Internet unterbrechen können. Dies geschieht, indem man die Routen- und Transportinformation entfernt, die man für die Weiterleitung von Daten zwischen zwei Providern braucht.[452] Die Codes sollten in der Übung in Kalifornien getestet werden, man nahm aber aus Furcht vor ungeplanten Ausfällen davon Abstand[453]. Solche Werkzeuge zur Internet-Abschaltungen werden auch als "**kill switches**" bezeichnet [454].
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.

Die Frage, inwieweit eine offensivere Ausrichtung notwendig ist, wurde im Umfeld der 2011 publizierten Strategiepapiere diskutiert, die insgesamt weiter defensiv ausgerichtet waren.
Das Weiße Haus hatte in seiner *International Cyberspace Strategy* im Mai 2011 betont, dass es sich für die Einhaltung internationaler Normen und Standards im Internet einsetzen will, um die Funktion und Informationsfreiheit im Internet zu sichern[455]. Das US-Verteidigungsministerium hatte dann in Juli 2011 die neue Cybersicherheitsstrategie veröffentlicht, die die Notwendigkeit der Kooperation zwischen den Behörden wie auch der verstärkten Zusammenarbeit mit der Rüstungsindustrie betont.[456]

Angesichts der wachsenden Probleme z.B. durch zunehmende Infiltration von kritischen Infrastrukturen, hat Präsident Obama am 12.02.2013 eine Executive Order erlassen, um einen Rahmen für die Zusammenarbeit der für den Schutz kritischer Infrastrukturen zuständigen Behörden und Einrichtungen zu schaffen, mit dem die Identifikation, Kontrolle, Eindämmung und Kommunikation von Cyberrisiken erreicht werden soll.[457].

Ab 2012 begann US-Verteidigungsministerium mit der Einrichtung der **Cyber Mission Force (CMF)**, die insgesamt 6200 Militärs, Zivilisten und Vertragsmitarbeiter umfassen sollen[458]. Diese sind dann in 133 Teams organisiert,

[452] vgl. Welchering 2011, S.T2
[453] vgl. Welchering 2011, S.T2, der auch berichtete, dass Ägypten diese Codes dann nutzte, um das Internet am 27.01.2011 weitestgehend zu kappen, und so die Protestbewegung gegen die Regierung zu hemmen. Dieselbe Methode wurde bei einem Internetkollaps in Syrien Ende November 2012 berichtet, Spiegel online 2012b.
[454] von Tiesenhausen 2011, S.11
[455] White House 2011, insbesondere S.5 und 9
[456] DoD 2011, S.8-9
[457] White House 2013
458 vgl. DOD 2015, S.6

die ihrerseits in drei Gruppen geordnet sind. **Cyber Protection Forces** werden für die Abwehr im Allgemeinen und **National Mission Forces** für die Abwehr massiver Cyberattacken auf die Vereinigten Staaten zuständig sein, während **Combat Mission Forces** Kampfhandlungen (Combatant Command operations) mit Cyberoperationen unterstützen werden Cyber Protection Forces und Combat Mission Forces werden den Combatant Commands zugeordnet, während die National Mission Forces dem zentralen Cyberkommando US CYBERCOM unterstellt sind.
Das US-Verteidigungsministerium hat konstatiert, dass ihr eigenes Netzwerk immer noch aus tausenden von Netzwerken weltweit bestehen würde[459]

Eine Analyse der dem US-Verteidigungsministerium zugehörigen **Defense Advanced Research Projects Agency DARPA** hat gezeigt, dass aktuelle Computerprogramme für Sicherheitssoftware inzwischen bis zu 10 Millionen Programmzeilen umfassen, also immer komplexer und teurer werden, während Schadsoftware seit vielen Jahren im Schnitt nur 125 Programmzeilen lang ist[460]. Daraus ergibt sich jedoch, dass sich die zukünftige Forschung nicht mehr nur auf Defensivmaßnahmen konzentrieren kann[461]. Die NSA rüstete sich auch zum offensiveren Umgang mit China[462].
Es wurde berichtet, dass die Presidential Policy Directive PPD 20 von Oktober 2012 nun die Bedingungen definiert, unter denen Angriffe auf ausländische Server erlaubt sind.[463] Die Arbeiten im defensiven Sektor gehen jedoch unvermindert weiter[464].

Auch die chinesische Führung hat sich intensiv mit der Materie auseinandergesetzt und baut wie viele andere Staaten Cyberwarkapazitäten auf und aus.
Der Cyberwar ist eine relativ kostengünstige Waffe und ermöglicht, zu anderen Staaten weitaus rascher aufzuschließen als durch massive Ausgaben zur

459 vgl. DoD 2015, S.7
460 vgl. Dugan 2011, S.16/17: "Over the last 20 years, using lines of code as a proxy and relative measure, the effort and cost of information security software has grown exponentially—from software packages with thousands of lines of code to packages with nearly 10 million lines of code. By contrast, over that same period, and across roughly 9,000 examples of malware—viruses, worms, exploits and bots—our analysis revealed a nearly constant, average 125 lines of code for malware. This is a striking illustration of why it is easier to play offense than defense in cyber, but importantly, it also causes us to rethink our approach."
461 Ein Teilgebiet des Plan X genannten Forschungsprogramms der DARPA, "focuses on building hardened "battle units" that can perform cyberwarfare functions such as battle damage monitoring, communication relay, weapon deployment, and adaptive defense." vgl. DARPA 2012, S.2
462 vgl. Barnford 2010
463 vgl. Biermann 2012, S.1. Jedoch wird auch in anderen Ländern wie z.B. der Schweiz über die rechtlichen Grundlagen für Maßnahmen gegen ausländische Computer diskutiert, vgl. Häfliger 2012b, S.23
464 Nach Clauss 2012 errichtet die NSA das Utah Data Center, das digitale Kommunikationen von 2013 an dauerhaft speichern und analysieren soll, die computerisierte Analyse soll im Jahr 2018 verfügbar sein; Clauss 2012, S.60. Die defensive Entschlüsselung und Wiederverschlüsselung von verschlüsselten Botschaften z.B. durch secure socket layer (SSL)-Interzeption ist jedoch ohnehin schon jetzt kommerziell verfügbar, Creditreform 2012, S.48.

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[465].

Außenpolitisch hat China das Problem, von Staaten umgeben zu sein, die China nicht unbedingt positiv gegenüberstehen bzw. mit den USA verbündet sind[466], wie z.B. Japan, Taiwan und Südkorea, so dass China (noch) nicht ernsthaft in der Lage ist, den USA im Falle eines ernsten 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[467]. 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 (SIPRNET) und als dritten Bereich das militärische Hochsicherheitsnetz[468]. Beim Cyberwar könnte auch ein Schlag gegen den zweiten Bereich die Handlungsfähigkeit der vernetzten Kriegsführung schon erheblich beeinträchtigen[469].

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[470] an seltenen Erden (speziellen Industriemetallen), die für die IT- und Elektronik-Industrie unersetzlich sind und die bisher nicht hinreichend wirtschaftlich recycelt können, und China schränkte vor dem Hintergrund eines wachsenden Eigenbedarfs bei gleichzeitig schwindenden bekannten Vorräten

[465] vgl. Kanwal 2009, S.14
[466] vgl. Rogers 2009
[467] vgl. Krekel et al. 2009
[468] 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.
[469] 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 Kampfjets mussten zwei Tage auf dem Boden bleiben, vgl. Leppegrad 2009.
[470] vgl. Büschemann/Uhlmann 2010, S.19

zunehmend das Exportvolumen ein[471]. Der hohe Marktanteil kam durch die zunächst konkurrenzlos billigen Lieferungen aus China zustande, weshalb andere Marktteilnehmer aufgaben; die Exploration außerhalb Chinas wurde unter Hochdruck wieder aufgenommen und hat zu deutlich sinkenden Preisen geführt[472].

4.3.3 Die Zentralisierungsproblematik

In der Sicherheitsarchitektur herrscht ein Trend zur Zentralisierung vor, um die Koordination zu verbessern, aber auch, um Angriffspunkte durch zu kleinteilige oder zu komplexe Netzwerkarchitekturen und um Schnittstellen zu verringern.

Eine vereinfachte Netzwerkstruktur und Zentralisierung wäre durch den Einsatz des cloud computings denkbar, bei dem sich die Daten und Programme nicht mehr auf den Festplatten der Computer befinden, sondern die Arbeit nach dem Login auf Computern von großen Rechenzentren erledigt wird[473]. Dadurch würde nicht nur die Komplexität der Netzwerke, sondern auch die Zahl möglicher Angriffspunkte erheblich reduziert. Dabei muss man jedoch bedenken, dass diese zentralen Rechenzentren selbst Angriffspunkte von Cyberattacken[474], aber auch Gegenstand klassischer Spionage und konventioneller physischer Angriffe sein können[475].

Generell ist hier eine Trendwende zu beobachten, denn das Internet bzw. der Vorgänger ARPANET wurden installiert, um die Erfolgswahrscheinlichkeit eines physischen Angriffs durch Dezentralisierung zu reduzieren. Insgesamt liegt also ein strategisches Optimierungsproblem vor, bei dem die Vorteile der Dezentralisierung (Schutz vor physischen Angriffen) gegen die der Zentralisierung (Schutz vor virtuellen Angriffen) abgewogen werden müssen.

Während die Frage der technischen Zentralisierung ein Optimierungsproblem darstellt, besteht doch weitgehende Einigkeit über die Notwendigkeit einer administrativen Zentralisierung und Koordinierung der nationalen Cyberaktivitäten. Ein aktuelles Beispiel ist die Errichtung des **Hohen Cyberrats** (Shoray-e Aali-e Fazaye Majazi) im Iran, der nun die Aktivitäten aller im

---

[471] 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

[472] vgl. FAZ 2010d, S.12, Bierach 2010, S.11, FAZ 2013d, S.24

[473] ENISA 2009, S.2; vgl. auch Dugan 2011, S.8

[474]Cloud computing ist ebenfalls anfällig. Während Angriffen auf US-Banken im Jahr 2012 wurden Computer in cloud computing-Zentren von den Angreifern für ihren Datenverkehr missbraucht, vgl. The Economist 2013, S.59. Dem cloud computing-Service Evernote wurden alle Passwörter gestohlen, vgl. FAZ 2013b, S.21.

[475] Zudem können Probleme mit der Stromversorgung Großrechner schwer beschädigen wie kürzlich im Oktober 2013 im Utah Data Center, vgl. Spiegel online 2013b

Cyberspace tätigen Einrichtungen koordiniert[476]. Zuvor wurde 2010 als Reaktion auf die Stuxnet-Attacke das Cyber Defense Command zum Schutz kritischer Infrastrukturen errichtet.
Die Zentralisierungsdebatte wird auch in Indien geführt. Hier sind die Ministerien Cybersicherheitsfragen durch Gründung von Cyberagenturen gelöst, was jedoch in ca. 30 Agenturen mit überlappenden oder unzureichend definierten Verantwortlichkeiten endete. Aus diesem Grunde wurde in einer aktuellen Analyse der indischen Marine eine Restrukturierung mit verbesserter Kommunikation unter der Führung neu zu errichtender zentraler Cyberbehörden empfohlen[477].

Große Serverfarmen können auch zur Analyse sehr großer Datenvolumina genutzt werden, man spricht auch von **big data**. Wie in Kapitel 2.2.2 dargelegt, ist das Hauptproblem nicht die Informationsgewinnung, sondern die Speicherung und zielgerichtete Analyse[478].
Die Speicherung von Metadaten (wer hatte wann mit wem wie lange Kontakt?) wird auch zur Identifikation von Netzwerken verdächtiger Personen genutzt. Zum Beispiel konnten die Beteiligten des Anschlags in Madrid 2004 anhand der Verbindungsdaten als Netzwerk dargestellt werden[479].
Um das Datenvolumen zu reduzieren, benutzt z.B. der britische GCHQ (Government Communication Headquarters) die **massive volume reduction (MVR)-Prozedur**, bei der große Dateien wie Musikdateien von vornherein aussortiert werden[480].
Dann helfen Suchbegriffe (Selektoren) bei der Erkennung relevanter Daten. Zum Beispiel hat der deutsche BND im Jahre 2011 e-mails, SMS und Verbindungen mit mehr als 15000 Suchbegriffen geprüft, aber nur 290 von 2,9 Millionen initialen Checks in 2011 führte zu relevanten Befunden[481]. Mehr als 90% dieser BND-Suchbegriffe sind formale Begriffe wie Telefonnummern, email- oder IP-Adressen von verdächtigen Usern oder Unternehmen[482].

Ein gezieltere Ansatz ist die Erstellung von **User-Profilen**. Im März 2012 hat Google bekanntgegeben, dass Profile durch Verknüpfungen von Suchmaschinenutzungen, YouTube, Google plus und gmail erstellt werden[483]. Ähnliche Prozeduren sind auch von Betreiberfirmen sozialer Netzwerke bekannt, aber Google und andere Firmen wurden 2013 von einem mutmaßlich chinesischen

[476] vgl. Nligf 2012, wo auch die Existenz einer informellen ‘cyber army’ erwähnt wird.
[477] vgl. Chhabra 2014, S.66-67
[478] Das diskutierte Speichervolumen für das NSA data center bewegt sich im Bereich von Yottabytes, also 10^{24} bytes, Juengling 2013, S.52
[479] vgl. Hayes 2007. Die Identifikation von Netzwerken nennt man auch **community detection.**
[480] vgl. Tomik 2013a, S.6
[481] vgl. Amann 2013, S.17
[482] vgl. Schulz 2013, S.6
[483] vgl. Spiegel 2013d, S.111

Hackerangriff betroffen bei dem Profile chinesischer Nutzer geprüft und exportiert wurden[484].

4.4 Das Cyberwarkonzept Russlands

4.4.1 Definitionen und Hintergrund

Definitionen

2012 wurde ein Artikel veröffentlicht, der die offizielle russische Position darlegt und an eine Präsentation bei einer Sicherheitskonferenz in Berlin im November 2011 anknüpft[485].

Die Cyberwar-Definition beruht auf den Vereinbarungen der Shanghaier Organisation für Zusammenarbeit (SOZ)/**Shanghai Cooperation Organization (SCO)** von 2008, die eine weitgefasste Definition enthält: *"Cyberspace warfare ist ein Wettstreit zwischen zwei oder mehreren Ländern im Informations- und anderen Sektoren, um die politischen, ökonomischen und sozialen Systeme des Gegners zu stören, sowie mit massenpsychologischen Mitteln die Bevölkerung so zu beeinflussen, dass die Gesellschaft destabilisiert wird und um den anderen Staat zu zwingen, Entscheidungen zu treffen, die dessen Gegner begünstigen."* [486]

Diese Definition passt zu der Doktrin zur Informationssicherheit, die Präsident Putin im Jahr 2000 erließ[487] und integriert Aspekte des Cyberwars im engeren Sinne, des Informationskrieges und der psychologischen Kriegsführung. Diese Definition ist also sehr viel breiter angelegt als zum Beispiel die US-Definition, die sich auf die militärischen Aspekte konzentriert. Konsequenterweise ist auch die Definition von Cyberwaffen breit angelegt: "*Cyberwaffen sind Informationstechnologien, -fähigkeiten und Methoden, die im Cyberspace warfare angewendet werden*." [488]

---

[484] vgl. Süddeutsche Online 2013

[485] vgl. Bazylev et al. 2012, S.10

[486] Annex I to the Agreement between the Governments of the Member Countries of the Shanghai Cooperation Organization on Cooperation in International Information Security in Yekaterinburg in 2008, zitiert in Bazylev et al. 2012, S.11. Deutscher Text eigene Übersetzung, die amtliche englische Fassung lautet "*Cyberspace warfare is a contest involving two or more countries in information and other environments to disrupt the opponent's political, economic, and social systems, mass-scale psychological efforts to influence the population in a way to destabilize society and the state, and to force the opposing state to make decisions favoring the other opponent*."

[487] Annex I to the Agreement between the Governments of the Member Countries of the Shanghai Cooperation Organization on Cooperation in International Information Security in Yekaterinburg in 2008, zitiert in Bazylev et al. 2012, S.11. Deutscher Text eigene Übersetzung, die amtliche englische Fassung lautet „*Cyber weapons are information technologies, capabilities, and methods used in cyberspace warfare operations*."

[488] Annex I, zitiert in Bazylev et al. 2012, S.11

Russland betont die defensive Ausrichtung der Doktrin, die Notwendigkeit einer Cyber-Konvention der UN sowie einer internationalen Zusammenarbeit, um die Proliferation von Cyberwaffen zu stoppen[489].

Hintergrund

Die Wahl der Definition ist sowohl von theoretischen Überlegungen als auch durch historische Erfahrungen beeinflusst.

Der oben definierte Cyberspace warfare ist ein Teil modernen geostrategischen Handels[490]. Die Kontrolle des Informationsflusses und die Beeinflussung seiner Inhalte zur Unterstützung der eigenen Position sind nun Instrumente der soft power in internationalen Beziehungen[491]. Fehlende Kontrolle kann auch zur Destabilisierung und Destruktion führen[492].

Auch die historische Erfahrung wird eine Rolle spielen. Verschiedene Autoren vertreten die Auffassung, dass das Eindringen von Informationen vom Westen zum Kollaps der Sowjetunion und der sozialistischen Staatenwelt beigetragen hat[493].

Strategische Implikationen

Nach dem obigen Konzept ist es entscheidend, den Informationsfluss im eigenen Territorium kontrollieren zu können. Dies erfordert einen gesetzlichen Rahmen mit den Nationalstaaten als zentrale Akteure und technische Maßnahmen zur Kontrolle des Informationsflusses[494].

In Übereinstimmung mit den o.g. Definitionen und Konzepten sandten die SOZ/SCO-Mitgliedsstaaten Russland, China, Tadschikistan und Usbekistan ein offizielles Schreiben an die Vereinten Nationen (12.09.2011) mit einem Entwurf für einen International Code of Conduct for Information security, in dem die Rolle und die Rechte des souveränen Nationalstaates betont werden (Präambel/Sektion d) und dessen Recht, den Umgang mit Informationen gesetzlich zu regeln (Sektion f)[495].

---

[489] vgl. Bazylev et al. 2012, S.11-15

[490] vgl. Maliukevicius 2006, S.121

[491] vgl. Maliukevicius 2006, S.125ff.

[492] vgl. Bazylev et al. 2012, S.12

[493] Zum Beispiel haben leitende Offiziere des ehemaligen Ministeriums für Staatssicherheit (MfS) der DDR den Zerfall des Sowjetsystems analysiert und kamen zu dem Schluss, dass der sog. Korb III der KSZE-Schlussakte von 1975 mit Themen wie Reisen, persönlichen Kontakten, Informations- und Meinungsaustausch zur Aushöhlung des sozialistischen Staatensystems beigetragen hat (vgl. Grimmer et al. 2003, S. I/101, auch S. I/189-I/190).

[494] Russland nutzt das System SORM für die Überwachung von Datenströmen, vgl. FAZ 2010h. Ein neues Sicherheitsgesetz wurde 2016 verabschiedet. Ab Juli 2018 sollen alle Inhalte von Telefonaten, sozialen Netzwerken und Messengerdiensten für 6 Monate gespeichert werden mit einem legalen Zugang für den Inlandsgeheimdienst FSB zu den Providern, vgl. Wechlin 2016, S.6.

[495] UN letter 2011, S.1-5. Die Rolle des Nationalstaats wird mehrfach betont. In der Präambel heißt es "policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues." und in Sektion (d) "that the code of

Technisch gesehen ist es machbar, bestimmte Webseiten zu blocken und/oder die user zu nationalen Substituten für Suchmaschinen, Twitter und andere Dienste zu verweisen. Für große Staaten sind solche Insellösungen jedoch eine Herausforderung und ggf. schwierig zu kontrollieren[496].

4.4.2 Die WCIT 2012

Im Jahre 1988 wurden Internationale Telekommunikationsrichtlinien, die International Telecommunication Regulations (ITR) von der International Telecommunication Union (ITU) verabschiedet, die verschiedene getrennte Vorgängerrichtlinien für Telegraphie, Telefon und Radio zusammenfassten[497]. Mit Blick auf die erheblichen technischen Veränderungen seit 1988 wurde vom 03.-14.12.2012 die World Conference on International Telecommunications (WCIT) in Dubai abgehalten, um die Schaffung angepasster neuer ITRs zu erörtern.
Aufgrund des weitgefassten Telekommunikationsbegriffes der ITU-Konstitution *("jede Übertragung, Emission oder Empfang von Zeichen, Signalen, Schriften, Bildern, Musik oder jedweder Art von Information per Kabel, Radio, optischen oder elektromagnetischen Systemen"*)[498], der Auffassung, dass die verschiedenen Technologien in Wirklichkeit nicht voneinander getrennt werden können und der bereits bestehenden Rolle in Cyberangelegenheiten[499] (wie der Untersuchung von Flame), vertrat die ITU die Auffassung, dass sie durchaus die zuständige Organisation für die Regulation des Internets und der Informations- und

---

conduct should prevent other States from using their resources, critical infrastructures, core technologies to undermine the right of the countries that have accepted the code of conduct to gain independent control of information and communications technologies or to threaten the political, economic and social security of other countries". Sektion (f): "To fully respect rights and freedom information space, including rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulation".

[496] Kürzlich war eine andere Technologie Gegenstand von Diskussionen. Bei der World Telecommunication Standardization Assembly (WTSA-12) in Dubai vom 20-29.11.2012 wurde eine technische Leitlinie Y.2770 2012 für die Anforderungen an die Deep Packet Inspection (DPI) (Tiefenanalyse von Datenpaketen) in Next Generation Networks von einem chinesischen Fachmann vorgelegt. Diese Leitlinie Y.2770 beschreibt die Anwendung der DPI z.B. für die Erkennung verschlüsselter Daten und die Einordnung von Datenpaketen wie z.B. VoIP, Videodateien, MP3-Musikdateien, BitTorrent-Datenströme, Business cards (vCards) etc. Die Genehmigung des Entwurfs durch die ITU-Mitglieder am 20.11.2012 (durch die sogenannte Traditional Approval Procedure TAP, d.h. eine Einigung ohne Gegenstimme der bei dem Meeting anwesenden ITU-Mitgliedsstaaten) könnte einem Schritt in Richtung einer standardisierten und gezielten Inhaltsanalyse darstellen; die ITU betonte jedoch, dass diese technische Leitlinie keinen Zugang zu privater Nutzerinformation eröffnet.

[497] vgl. WCIT2012 Präsentation, introductory section

[498] vgl. WCIT2012 Präsentation, section myths and misinformation. Der amtliche englische Originaltext lautet: *("any transmission, emission or reception of signs, signals, writing, images or sound or intelligence of any nature by wire, radio, optical or other electromagnetic systems")*

[499] vgl. Touré 2012. Touré, Generalsekretär der ITU sagte *"The word Internet was repeated throughout the conference and I believe this is simply a recognition of the current reality the telecommunications and internet are inextricably linked*" Übersetzung: „Das Wort Internet wurde während der Konferenz durchgängig wiederholt und ich glaube, dass es sich nur um eine Anerkennung der gegenwärtigen Realität handelt. Telekommunikation und Internet sind untrennbar miteinander verknüpft."

Kommunikationstechnologie (IKT), d.h. für die gesamte digitale Technologie sein kann[500].
Eine Gruppe von Staaten unter Führung von Russland, China, einigen arabischen und anderen Staaten vertraten dann auch die Auffassung, dass in Zukunft die ITU die zuständige Organisation für die Regulation des Internets sein sollte[501]. Während die öffentliche Berichterstattung auf das Internet fixiert war, sollte laut Vertragstextentwurf dieser Staaten die gesamte IKT erfasst werden[502]. Außerdem wurde argumentiert, dass das Internet alle Menschen auf der Erde betrifft und daher auch von einer UN-Organisation, der ITU, reguliert werden sollte.
Die USA, die EU, Australien und andere Staaten argumentierten, dass das gegenwärtige multi-stakeholder-Modell der Internet Governance, also die Einbeziehung verschiedenster Akteure in sich selbst verwaltenden Organisationen wie der Internet Corporation for Assigned Names and Numbers (ICANN), der Internet Society (ISOC), der Internet Engineering Task Force (IETF) und anderen unbedingt beibehalten werden sollte, da es sich als fair, flexibel und innovativ erwiesen hat. Dieses Modell war auch in der Lage, die rapide Expansion des Internets über den Globus zu erfolgreich zu bewältigen[503]. Zudem wurde betont, dass abgesehen von der ICANN, die noch durch ein Memorandum of Understanding mit dem US Handelsministerium (US Department of Commerce) verbunden ist, die USA die Organisationen nicht kontrollieren. Dieselben Staaten äußerten auch Bedenken, dass eine alleinige Kontrolle des Internets durch Staaten (im Rahmen der ITU) sich negativ auf die Informationsfreiheit[504] und auf die Innovationskraft auswirken würde, weshalb sich diese Staaten jeder Formulierung, die der ITU Einfluss auf das Internet geben würde, widersetzten[505].
Schließlich wurde ein rechtlich unverbindlicher Annex durch eine umstrittene Abstimmung angenommen, die u.a. festhält, dass der "*Generalsekretär [der ITU] angewiesen wird, weitere Schritte zu unternehmen, dass die ITU eine aktive und konstruktive Rolle in der Entwicklung des Breitbandes und dem Multistakeholder Modell des Internets gemäß Paragraph 35 der Tunis Agenda spielen kann*"[506]. Außerdem wurden neue ITRs angenommen, aber ein Konsens konnte nicht erreicht werden[507]. Infolgedessen haben die Vereinigten Staaten, die EU-Staaten, Australien und viele weitere Staaten die neue ITRs nicht unterschrieben[508].

---

[500] IKT wird in der WCIT2012 Präsentation genannt, section myths and misinformation
[501] vgl. Touré 2012
[502] vgl. WCITleaks 2012. Es handelt sich aber nur um ein 'geleaktes' Dokument ohne offiziellen Status.
[503] vgl. EU 2012b (Position Paper of the EU)
[504] vgl. Kleinwächter 2012, S.31, Lakshmi 2012, S.1
[505] vgl. Touré 2012
[506] vgl. WCIT2012 Resolution Plen/3. Englischer Originaltext: "*Secretary General is instructed to continue the necessary steps for ITU to play an active and constructive role in the development of broadband and the multistakeholder model of the Internet as expressed in paragraph 35 of the Tunis Agenda*"
[507] vgl. WCIT2012 Final Acts
[508] vgl. Betschon 2012, S.4; Lakshmi 2012 schätzte, dass 113 der 193 ITU-Mitgliedsstaaten die neuen ITRs unterschreiben, 80 nicht.

Die Härte der Auseinandersetzung zwischen zwei großen Staatenblöcken hinterließ bei einigen Beobachtern den Eindruck eines **digitalen kalten Krieges**.

Neben den oben diskutierten Aspekten hat die Internet-Governance auch noch Bedeutung für die Cyberfähigkeiten. Kürzlich analysierte die US Air Force das Problem und schlußfolgerte: "*Fehlende Aufmerksamkeit für die Verwundbarkeit, die aus der Internet Governance und dem friedlichen Wettbewerb resultieren kann, könnte unseren Gegnern einen strategischen Vorteil in Cyber-Konflikten verschaffen. Unsere eigenen Cyberattacken werden auch komplizierter, wenn Netzwerke, die nicht mit den Protokollen und Standards von US-Organisationen entwickelt wurden, von unseren Konkurrenten zum Einsatz gebracht werden*". [...] *Die Vereinigten Staaten genießen zur Zeit eine technische Dominanz durch die Position als Entwickler und Kernanbieter von Internet-Services, die durch die ICANN und das top-level Domain Name System ermöglicht werden*". [509]

4.5 Die Cyberpolitik der Europäischen Union

Im Unterschied zu den USA und China besteht die Europäische Union EU aus 28 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. 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 12 Mitglieder (Finnland, Frankreich, Deutschland[510], Niederlande, Norwegen, Ungarn, Spanien, Schweden, England, Schweiz, Österreich, Dänemark, Großbritannien mit 2 CERTs)[511][512]. Ab 2012 wurde ein CERT-EU-Team für die Sicherheit der IT-Infrastruktur dauerhaft eingerichtet [513]

[509] Englisches Original: "*Failure to pay attention to our vulnerabilities from Internet governance and friendly contest may provide our adversaries with a strategic advantage in cyber conflict. Our own cyber-attacks will also become complicated as networks that are not based on protocols and standards developed by US-entities are deployed by our competitors [ ]. The United States currently enjoys technological dominance through its position of developer and core provider of Internet Services made possible by the ICANN and the top-level Domain Name System.*" Yannakogeorgos 2012, S.119-120

[510] Zur deutschen Gruppe CERT-Bund siehe Website des BSI

[511] vgl. IT Law Wiki 2012b, S.1

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.“[514]

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[515].
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[516]. Das Mandat der ENISA wurde 2008 unverändert bis 2012, 2011 dann vorzeitig bis 2013 verlängert und soll 2013 bis 2020 verlängert werden, wobei die Befugnisse der ENISA erweitert werden sollen.
Die ENISA, deren 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[517], 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

[512] 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).
[513] vgl. EU2013b, S.5
[514] 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. Wenn man diese Umstände in Betracht zieht, erscheint die 2011 diskutierte Entwicklung einer **Konvention gegen Cyberwar** doch eher unwahrscheinlich, vgl. auch Dunlap 2011, S.83
[515] EU-ISS 2007
[516] ENISA 2007
[517] EU 2007, EU 2009b

Empfehlungen für verbesserte Prozesse und zu einer verstärkten Kooperation unter Federführung der ENISA gegeben[518].

- Im Einklang mit den Plan zum Schutz kritischer Infrastrukturen von 2009[519] 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[520]. Jedoch zeigten sich auch bei dieser Übung die uneinheitlich geregelten Zuständigkeiten innerhalb der EU und die mangelnden Strukturen kleinerer Staaten[521]. Nach der Auswertung sollen in die nächste Übung auch privatwirtschaftliche Akteure miteinbezogen werden.
- Mittlerweile hat im November 2011 auch eine gemeinsame Übung der EU und der USA, **Cyber Atlantic 2011**, stattgefunden.

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[522].
Ein rechtlicher Rahmen zur Förderung der Netzwerk- und Informationssicherheit (NIS) wurde Anfang 2013 vorgestellt. Dabei wurde festgestellt, dass es auf EU-Ebene immer noch keinen effektiven Mechanismus für die Kooperation und den gemeinsamen Austausch vertraulicher Informationen für NIS-Zwischenfälle zwischen den Mitgliedstaaten geben würde. Deshalb sollte jeder Mitgliedstaat eine zuständige Stelle (competent authority CA) für NIS etablieren und ein Kommunikationsnetzwerk mit den CAs der anderen Mitgliedstaaten einrichten, um frühzeitige Warnungen und wichtige Information weitergeben zu können. Auch die Zusammenarbeit mit privaten Einrichtungen sollte verstärkt werden [523].
2013 sollen die CSIRTs in der EU evaluiert werden und eine Anti-Botnetz-Initiative ist ebenfalls geplant.[524] Das neu gegründete **European Cybercrime Centre E3C** wird mit der ENISA und der europäischen Verteidigungsagentur (**European Defense Agency EDA**) verstärkt in NIS-Fragen zusammenarbeiten[525].

[518] vgl. ENISA 2009a
[519] vgl. EU 2009b
[520] vgl. ENISA 2010a, ENISA2010b
[521] 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."
[522] vgl. EU2009b, auch EU 2010b
[523] vgl. EU2013a
[524] vgl. EU2013b
[525] vgl. EU2013b, S.18

Für 2014 planten die ENISA und EU-Kommission eine cyber security-Championship für Studenten.

Großbritannien und Frankreich haben im November 2010 eine umfassende Militärkooperation vereinbart, bei der auch die Kooperation im Bereich des Cyberwars angestrebt wird[526].
Die europäische Verteidigungsagentur hat in einer Studie 2013 die Notwendigkeit der Entwicklung einer militärischen Cyberverteidigung auf europäischer Ebene gezeigt. [527]
Am 03.09.2014 wurde offiziell die Errichtung einer neuen, bei Europol angesiedelten **Joint Cybercrime Task Force J-CAT** bekannt gegeben, in der Europol, die European Cybercrime Taskforce, das FBI und die British National Crime Agency NCA zusammenarbeiten.

Ein neues Sicherheitsproblem stellt die rasche Ausbreitung des Cloud Computings dar, bei dem Daten auf externen Computern gespeichert werden, die sich ggf. in einem ausländischen Rechtsraum befinden. Neben den verschiedenen Sicherheitsaspekten[528] gibt es auch Unsicherheiten über Rechte und Verantwortlichkeiten bei grenzüberschreitenden Problemstellungen[529], so dass eine Anpassung der europäischen Rechtslage an die Erfordernisse des Cloud Computing diskutiert wird.
In der neuen **Cloud Computing Strategie** hat die EU drei vorrangige Probleme zur weiteren Bearbeitung identifiziert, nämlich die Fragmentierung des Marktes, der Vertragsgestaltung und die nicht einheitlichen nationalen Standards[530].

4.6 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[531] und bildet im Rahmen des 2002 verabschiedeten NATO Cyber Defense Programms die vorderste Verteidigungslinie der NATO zum Schutz ihrer eigenen IT-Infrastruktur[532].
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 Vorfallen

[526] vgl. Thibaut/Alich 2010, S.15
[527] vgl. EPRS 2014, S.8
[528] vgl. ENISA 2009b
[529] vgl. EU2011
[530] vgl. EU 2012a, S.5
[531] vgl. Schuller 2010, S.6
[532] vgl. NCSA 2009a-c

(incidents) und das Nato Information Security Operations Centre für die zentrale Betreuung und das Management des NATO-Computernetzwerks gliedert.

Angelegenheiten der Cyberabwehr werden vom im April 2014 so benannten **Cyber Defense Committee** gehandhabt.
Die **Smart Defense Initiative**[533] enthält 3 Elemente der Cyberabwehr, dies sind

- Malware Information Sharing Platform MISP (Informationsaustausch)
- Multinational Cyber Defense Capability Development MNCD2 (Enwicklung von Defensivfähigkeiten) and
- Multinational Cyber Defense Education and Training MNCDET (Ausbildung und Training)

Die **NATO Communications and Information Systems School NCISS** wird nach Portugal verlegt. Die Cyberabwehraktivitäten werden auch von der NATO School in Oberammergau unterstützt, während sich das NATO Defense College in Rom mit strategischen Überlegungen befasst. Das Cyberabwehrtraining der NATO schließt auch die Sicherheit und Forensik von Smartphones mit ein.

Eine Dokumentensammlung von nationalen Cyberstrategien für viele NATO- und Nicht-NATO-Staaten mit weiterführenden Links ist verfügbar unter ccdcoe.org/strategies-policies.html

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 **K**über**k**aitse **K**ompetentsi**k**es**k**us) in Tallinn, Estland, ins Leben gerufen[534], das in den ersten Jahren von Estland, Litauen, Lettland, Italien, Spanien, der Slowakei und Deutschland unterstützt wurde und zunächst 30 Mitarbeiter umfasste.[535], Weitere Staaten kamen später hinzu: Ungarn 2010, Polen und die USA 2011, Tschechien, Großbritannien und Frankreich in 2014, die Türkei, Griechenland und Finnland in 2015. 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[536]. Die **Cyber Coalition (CC)**-Übung findet nun regelmäßig statt. Mit Schweden hat das CCDCoE im Mai 2010 die Übung **Baltic Cyber Shield** durchgeführt. **Locked Shields** ist eine jährliche Echtzeit-Cyberübung, die seit

[533] vgl. NATO 2015
[534] Faktisch hat das CCD CoE nach einer 2004 von Estland ausgehenden Initiative schon seit 2006 existiert, vgl. CCDCoE 2010a
[535] Die NATO will sich im Falle eines Cyberangriffs im ersten Schritt lediglich auf Konsultationen stützen, vgl. von Kittlitz 2010, S.33
[536] vgl. Wildstacke 2009, S.28/29, CCDCoE 2010b

2012 vom CCDCoE organisiert wird, als Nachfolge der Übung Baltic Cyber Shield 2010.

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“)*[537].

Die NATO und das deutsche Bundesministerium der Verteidigung diskutieren die **hybride Kriegsführung (hybrid warfare)** als neue Herausforderung. In dieser wird physische Gewalt durch Spezialkräfte und durch unter anderer Flagge operierende Kräfte in Verbindung mit umfassenden Cyberaktivitäten angewendet, d.h. Informationskrieg und psychologische Kriegsführung über das Internet und Social Media einerseits und Cyberattacken auf der anderen Seite[538]. Im Ergebnis muß die Sicherheitspolitik mit einem besonderen Augenmerk auf die Resilienz der eigenen Systeme intensiv durchdacht werden[539]. Im November 2014 führte die NATO eine sehr große Cyberübung in Tartu (Estland) durch, an der mehr als 670 Soldaten und Zivilisten von Einrichtungen aus 28 Ländern teilnahmen[540].

Analysten des BND gehen davon aus, dass Cyberaktivitäten in bewaffneten Konflikten vor allem am Anfang des Konfliktes eine wichtige Rolle spielen[541]. Während diese Schlussfolgerung durch die bisherigen Erfahrungen mit großen Cyberattacken gerechtfertigt erscheint, sollte jedoch bedacht werden, dass die potentiellen Schwachstellen wie auch die Schadprogramme rasch zunehmen. So muss man davon ausgehen, dass in längeren Konflikten Schwachstellen nicht nur einmalig als Überraschungseffekt genutzt werden, sondern die Angreifer nach Abnutzung der ersten Schwachstelle in einem System anschließend eine weitere nutzen werden usw. Im Zeitalter von USB-Sticks und im Hinterland operierenden Kräften werden Internetblockaden und Kill Switches keinen zuverlässigen Schutz mehr bieten.

Die Bundesregierung berichtete in der ersten Jahreshälfte 2015 über 4.500 Malwareinfektionen; im Durchschnitt vergingen bis zur Entdeckung sieben Monate und bis zur Entfernung ein weiterer Monat[542]. Die Vorbereitung des Schlachtfeldes (*Preparing the battlefield*) gilt als wesentlich für erfolgreiche Strategien, in der Praxis werden vorsorglich Sender (**beacons**) oder Implantate in

[537] 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.
[538] vgl. NATO 2014, BMVg 2015b
[539] vgl. BMVg 2015b
[540] vgl. Jones 2014, S.1
[541] vgl. Leithäuser 2015, S.8
[542] vgl. Leithäuser 2015b, S.4

ausländischen Computernetzwerken platziert, das ist Computercode, mit dessen Hilfe die Arbeitsweise des Netzwerks untersucht werden kann[543].

Ein NATO-Staat hat einen Kampfjet zerlegt, um sämtliche Komponenten gegen Cyberattacken zu härten und baute den Jet anschließend wieder zusammen, aber die Kosten der Maßnahme führten zu der Überlegung, dass die Komponentensicherheit stattdessen von den Lieferanten garantiert werden sollte[544]. Das würde jedoch bedeuten, sich auf die Sicherheitsanstrengungen zahlreicher Anbieter verlassen zu müssen, d.h. es ist schwierig, die Cybersicherheit zu delegieren. Ähnliche Prüfungen bei Autohacks zeigten, dass die Vorstellung des **walled garden-**Konzepts, dass man die vielen Komponenten von außen ganzheitlich schützen könnte, Eindringtesten nicht standhielt, d.h. jede Komponente muss einzeln gesichert werden[545]. Ein Eurofighter-Kampfjet hat mehr als 80 Computer und 100 Kilometer Verkabelung[546].

Mögliche Präventionsmaßnahmen könnten z.B. stichprobenartige Entnahmen von „normal“ funktionierenden Computern/smarten Geräten mit eingehender Untersuchung sein, aber auch worst-case Übungen, bei denen geprüft wird, inwieweit sich Kommunikation und Operationen im Falle eines umfassenden Computersystemausfalls aufrecht erhalten lassen (EMP-Szenario).

4.7 Die Cyberpolitik der Afrikanischen Union

Im Mai 1996 startete die Economic Commission for Africa (ECA) der Vereinten Nationen die African Information Society Initiative (AISI), in der die Entwicklung von Nationalen Informations- und Kommunikationstechnologieplänen (National Information Communication [NICI] policies and plans) angeregt wurde[547].
Seither wurde die IT-Infrastruktur Afrikas erheblich ausgebaut, u.a. durch neue Breitband-Unterseekabel wie auch durch einen intensiven Wettbewerb zwischen europäischen und chinesischen Telekommunikationsanbietern (insbesondere Huawei and ZTE)[548].

2009 vereinbarten die Mitgliedsstaaten der Afrikanischen Union (AU) die Entwicklung einer Konvention zur Cyber-Gesetzgebung im Rahmen der AISI-

[543] vgl. Sanger 2015, S.5
[544] vgl. Leithäuser 2016, S.8
[545] vgl. Mahaffey 2016, S.V6
[546] vgl. Köpke/Demmer 2016, S.2
[547] vgl. ECA 2012, S.1
[548] vgl. Martin-Jung 2008, EMB 2010, Schönbohm 2012 der berichtete, dass im Jahr 2010 8400 Kilometer Unterseekabel entlang Ostafrikas gelegt wurden, um High-Speed-Internet zu fördern. Auch an der Westküste wurden die Unterseekabel durch weitere Kabel verstärkt, was z.B. für Nigerias Internetnutzung bedeutsam war, vgl. Adelaja 2011, S.7

Initiative, von der ein erster Entwurf im Jahr 2011 vorgelegt wurde[549]. Die Konvention befasst sich mit dem elektronischen Handel, Datenschutz und –verarbeitung und Cyberkriminalität im Allgemeinen, enthält aber keine speziellen Regelungen zum Cyberwar[550].

Zudem werden auch Kooperationen der Cyber-Gesetzgebung im Rahmen der regionalen Wirtschaftsgemeinschaften wie der ostafrikanischen East African Community EAC, der südafrikanischen South African Development Community SADC und der westafrikanischen Economic Community of West African States ECOWAS[551] diskutiert.
Ein wichtiger Aspekt in vielen Dokumenten ist die Forderung nach verstärkter inner-afrikanischer Kooperation und einem verbesserten Sicherheits-bewusstsein[552].
Südafrika hat bereits mit der Entwicklung einer Nationalen Cybersicherheitspolitik begonnen, die Arbeiten am **National Cyber Security Policy Framework** begannen 2010 und wurden vom Kabinett im März 2012 verabschiedet[553]. Ein vorrangiges Ziel war die Koordination aller mit Cybersicherheit befassten Stellen[554].

In Afrika wächst die Bedeutung von Smartphones rapide, weil dies die Überbrückung von Lücken in der digitalen Infrastruktur ermöglicht, was Afrika für die im Kapitel 2.2.7 gezeigten Sicherheitslücken besonders anfällig macht[555].

[549] vgl. ECA 2012, S.3, AU 2011
[550] vgl. AU 2011
[551] vgl. ECA 2012, S.4
[552] Für die allgemeine Kooperation in Sicherheitsfragen haben afrikanische Geheimdienste und Sicherheitsbehörden im Jahre 2004 in Nigeria das **Committee of Intelligence and Security Services of Africa CISSA** gegründet, das u.a. regelmäßige Mitgliedertreffen organisiert, vgl. Africa 2010, S.72f.. Inzwischen haben bereits 50 Geheimdienste und Sicherheitsbehörden das CISSA Constitutive Memorandum of Understanding unterzeichnet, CISSA 2012.
[553] South Africa 2012
[554] South Africa 2010, S.6
[555] vgl. Puhl 2013, S.118f.

5 Cyberwar und biologische Systeme

5.1 Intelligente Implantante

Es gibt eine wachsende Zahl intelligenter Implantate (**implantable medical devices IMDs**) mit kabellosen Verbindungen wie Herzschrittmacher, implantierbare Defibrillatoren, Neurostimulatoren ("Hirnschrittmacher"/deep brain neurostimulators), Implantate für besseres Hören und Sehen (cochleär und okulär) usw.

Da die Ärzte gerade in Notfällen einen einfachen und ungehinderten Zugang benötigen, ist der Schutz kompliziert, so dass die kabellose Kommunikation anfällig für Angriffe ist. Es wurde unter anderem nachgewiesen, dass Insulinpumpen gehackt und dann ferngesteuert werden konnten[556]. Aus diesem Grunde ist die Forschung zum Signalschutz und anderen Strategien bereits im Gange[557].

Als Reaktion auf die Bedrohungen im digital health-Sektorhat die amerikanische Food and Drug Administration FDA eine ‚*safety communication on health-related cyber security*' herausgegeben[558]. In dieser werden auch Empfehlungen zum Schutz von Kliniknetzwerken gegeben, um zu verhindern, dass Eindringlinge potentielle Ziele identifizieren können, d.h. Patienten mit Medizingeräten und die dazugehörigen technischen Spezifikationen. Da Kliniken auch Datenverbindungen zur Fernüberwachung von Patienten aufrechterhalten, sind Kliniken ein potentielles Ziel für Cyberattacken. Zudem wurde ein Richtlinienentwurf zur Cybersicherheit von Medizinprodukten herausgegeben, die von den Herstellern zu gewährleisten ist, um Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu sichern.[559]. Die Herausforderung besteht darin, Sicherheit und Privatheit mit der medizinischen Sicherheit und Nutzbarkeit in Einklang zu bringen[560].

Die drei Grundprinzipien der FDA sind die Begrenzung des Zugangs auf autorisierte Nutzer, die Beschränkung auf autorisierte und sichere Inhalte und die Aufrechterhaltung und Wiederherstellung der Funktion bei Störungen. Es geht dabei um ein umfangreiches Massnahmenpaket mit der Authentifizierung der User, abgestuften Zugriffsrechten, Vermeidung von fixen („hardcoded") Passwörtern (z.B. ein Passwort für die ganze Serie, schwierige Wechsel, Gefahr der leichten öffentlichen Zugänglichkeit), Kontrollen vor Software oder Firmwareupdates, insbesondere bei systemrelevanten Applikationen und

[556]vgl. Gupta 2012, S.13
[557] vgl. Xu et al 2011, Gollakota et al. 2011
[558] vgl. FDA 2013a
[559] vgl. FDA 2013b, S.2
[560] vgl. Gupta 2012, S.26

Malwareschutz und Sicherheit des Datentransfers des Gerätes, wobei auch anerkannte Verschlüsselungsmethoden genutzt werden sollte[561].

Inzwischen wurden Neuroimplantate für das Gehirn entwickelt, die die Hirnaktivität messen, die Befunde aus dem Gehirn senden ('brain radio')und auch auf gesendete Instruktionen von außen reagieren können, um ihrerseits die Hirnaktivität elektrisch zu beeinflussen[562]. Die Untersuchung der emittierten Signale erlaubt also, die Art der Neurostimulation ggf. anzupassen, z.B. um neuromuskuläre oder schwere depressive Erkrankungen behandeln zu können.
Das brain radio analysiert sogenannte **Latente Feldpotentiale** (latent field potentials LFPs), welche als komplexe Kurven dargestellt werden können, die jeweils ein spezifisches Aktivitätsmuster des Gehirns darstellen[563]. Die Sammlung und Analyse der LFP (im Sinne einer Entschlüsselung der Gehirnsignale) wird aufwendig sein und voraussichtlich einige Jahre dauern, die gesamte Untersuchung wird wohl ein knappes Jahrzehnt bis Ende 2023 dauern[564].
Die jüngsten Fortschritte veranlassten die DARPA am 12.11.2013, die Entwicklung neuer Geräte zur Behandlung schwerer Hirnverletzungen anzuregen.
Eine aktuelle Beschränkung ist der Bedarf zum Wechsel oder Wiederaufladen von Batterien, die Forschung versucht nun, den menschlichen Körper als Energiequelle zu nutzen, zum Beispiel durch Nutzung des Blutzuckers[565]. Mittlerweile wurden Herzschrittmacher entwickelt, die die Bewegung der Organe als Energiequellen nutzen können[566]
Retinaimplantate werden bereits als subretinale Implantate eingesetzt, d.h. hinter der Zellschicht, die normalerweise das Augenlicht wahrnimmt. Der Chip besteht aus 1500 Mikrophotodioden, die das Licht empfangen und jeweils an einen Verstärker und eine Elektrode gekoppelt sind, die ein verstärktes elektrisches Signal an die Bipolarzellen zur Weiterverarbeitung des optischen Eindrucks weitergeleitet.[567]. Der Chip benötigt jedoch noch eine externe Energieversorgung.

Das Hacken solcher Implantate birgt nicht nur Manipulationsgefahren, sondern auch das Risiko schwerer körperlicher Schäden[568], so dass der Gesetzgeber sicherstellen muss, dass das Hacken von Implantaten nicht nur als virtuelle Straftat verfolgt werden kann.

[561] vgl. FDA 2013b
[562] vgl. Young 2013, S.1, Medtronic 2013
[563] LFP Signale kodieren dynamische Komponenten des Verhaltens, Hintergrundaktivitäten des Gehirns und evtl. noch andere Aspekte, vgl. Stamoulis/Richardson 2010, S.8
[564] vgl. ClinicalTrials.gov 2013
[565] vgl. Jürisch 2013, S.10
[566] vgl. Welt online 20.01.2014
[567] vgl. Stingl et al 2013
[568] Wie das Setzen von Elektroschocks, vgl. Gollakota et al 2011, S.1

Ein anderes Phänomen sind tragbare Technologien (**wearable technologies**) wie *Google Glass*, also Brillen mit eingebauten Computerfunktionen und anderen Konkurrenzprodukten, die für 2014 auf dem Markt erwartet werden[569]. Angreifer könnten mit Hilfe dieser Computerbrillen nicht nur den User, sondern auch andere beobachten[570]. Andere Konzepte sind smarte Perücken oder Helme (**smart wigs** oder **smart helmets**), mit den gelähmte oder blinde Menschen unterstützt werden können und intelligente Pflaster, die den Gesundheitszustand der Nutzer aufzeichnen[571].

Aus der Cyberwar-Perspektive bieten kabellose tragbare Technologien zusammen mit der Option, Waffen im Rahmen des Internet of Things mit IPv6-Adressen zu versehen, neue Möglichkeiten, definierte Gruppen von Individuen und Objekten gezielt anzugreifen. Nachdem der Cyberwar ursprünglich die große Auseinandersetzung zwischen Computern sein sollte und mittlerweile als integraler Teil militärischer Handlungen betrachtet wird, könnte der Trend in Richtung hochselektiver gezielter Attacken gehen.

5.2 Beziehungen zwischen Cyber- und biologischen Systemen

5.2.1 Viren

Der Code innerhalb von Zellen besteht aus Nukleinsäuren, und Gene sind definierte Abfolgen von Nukleinsäuren. Gene dienen der Herstellung eines jeweils bestimmten Proteins, welches entweder für die Bildung von Körperstrukturen (z.B. Muskeln) oder zur Steuerung des Stoffwechsels in Form von Enzymen genutzt werden kann. So gesehen, sind Gene die Äquivalente zu Computerprogrammen.
Ursprünglich wurde der Begriff des Computervirus von seinem biologischen Gegenstück abgeleitet. Viren sind kleine, umhüllte gentragende Partikel, also das Gegenstück zur Schadsoftware. Sie produzieren Kopien in infizierten Zellen (Replikation) und verlassen die Zellen, um andere Zellen zu infizieren.

Früher ging man davon aus, dass der Schaden, den Viren anrichten, allein durch die Infektion und Zerstörung von Zellen verursacht würde. Mittlerweile hat man aber auch bei vielen Viren ‘Trojaner-artiges’ Verhalten gefunden, da die Viren das Netzwerk der Immunzellen stören können; in diesem Netzwerk kommunizieren

[569] vgl. Postinett 2013a, S.30
[570] Dazu werden RFID-Chips mittlerweile als Diebstahlschutz in wertvolle Pferde und als Kidnappingschutz zuweilen auch Kindern eingepflanzt.
[571] Die Untersuchung des Befindens kann auch mit Kameras erfolgen wie bei der Microsoft X-Box, vgl. Mähler 2013, S.38.

verschiedene Arten von Zellen durch Freisetzung und Empfang von Botenstoffen, den **Zytokinen**, miteinander.

Viele Viren finden Wege, die Produktion des Zytokins Interferon-gamma zu bremsen, welches eine Schlüsselrolle bei Antivirusmaßnahmen spielt[572]. Manche Viren, z.B. solche aus der Influenzavirengruppe, können das Immunsystem sogar verwirren, was zu gestörter oder exzessiver Freisetzung von Zytokinen führen kann und zudem auch Folgeinfektionen mit Bakterien begünstigt[573]. Die exzessive Zytokinfreisetzung, auch als Zytokinsturm oder **cytokine release syndrome** bekannt, kann in potentiell tödlichen schockartigen Reaktionen (Kreislaufzusammenbruch, Organversagen, Blutgerinnungsstörungen usw.)[574] enden.

Ein unkonventioneller Bereich sind Viren, die andere Viren befallen und dann zur Vermehrung nutzen, die **Virophagen**. Aus der Cyber-Perspektive wäre es womöglich interessant, Programme zu entwickeln, die sich in existierende Malware einbauen und diese so verändern oder umsteuern zu können, also Malware, die andere Malware befällt, was bislang jedoch hypothetisch ist.

Vom biologischen Aspekt her wurden bis 2012 neun Virophagen beschrieben, die alle gegen eine Untergruppe von Viren, nämlich große Doppelstrang-DNA-Viren gerichtet sind[575]. Der Virophage Sputnik richtet sich gegen das Mimivirus, das auch menschliche Pneumonie verursachen kann[576]. Interessanterweise ist das klassische Pockenvirus (Variola) ebenfalls ein großes Doppelstrang-DNA-Virus, so dass modifizierte Virophagen hier vielleicht neue Behandlungschancen bieten könnten. Es gibt nämlich eine zunehmende Zahl an Berichten über pockenartige Infektionen mit Affenpocken[577], in Deutschland kam es 1990 zu einigen tödlichen Pockenfällen, als Kuhpockenviren, die die Artenbarriere zu Katzen überwunden hatten, vorwiegend immunsupprimierte Menschen befiel[578].

[572] vgl. Haller 2009, S.57
[573] vgl. Kash et al 2011, Stegemann-Koniczewski 2012
[574] Bei solchen Viren könnten Korrekturen der Kommunikation des Immunsystems (wie die Bremsung der Zytokinexzesse) durch Kortison und andere Subtanzen eine neue Option zur Abmilderung von Infektionen sein, neben der bereits etablierten Strategien der Vorbeugung durch Impfung und antivirale Medikamente, vgl. auch Li et al. 2012/Li, C., Yang P., Zhang Y., Sun Y., Wang W. et al 2012
[575] vgl. Zhou et al 2012
[576] vgl. Zhanga et al. 2012
[577] vgl. Shah 2014, S.27
[578] vgl. Scheubeck 2014, S.7

5.2.2 Bakterien

Bakterien sind einzellige Organismen, die andere Organismen infizieren können, so auch den Menschen[579]. Einige Bakterien, die bedeutsame Infektionen beim Menschen auslösen, können flüssige Plattformen, die sogenannten **Biofilme**[580] bilden, wo sie über Pheromone Informationen austauschen und Materialien und Nährstoffe teilen können; dieser Zustand wird auch als **Quorum sensing** bezeichnet (das heißt, die Plattform wird gebildet, sobald eine kritische Masse an Bakterien vorhanden ist). Neuere Forschungen zielen auf die Zerstörung dieser Plattformen und die Abschaltung der interbakteriellen Kommunikation, so dass den Immunzellen der Angriff und die Vernichtung der Bakterien erleichtert wird[581].

Die Biotechnologie ermöglicht die Veränderung von Genen oder die Einführung neuer Gene in Organismen, so dass Bedenken bestehen, dass gefährliche Organismen absichtlich[582] oder versehentlich erschaffen werden. Im vergangenen Jahrzehnt wurde das neue Phänomen des **bio-hacking** beobachtet[583]. Der typische Biohacker arbeitet außerhalb etablierter Forschungseinrichtungen oder Firmen und versucht in einer Art ethischem Hacken etwas Nützliches zu kreieren; wegen der Sicherheitsbedenken wird die Szene jedoch aufmerksam von Regierungseinrichtungen verfolgt[584]. Wie dem auch sei, es existieren hohe strukturelle, funktionelle und energetische Hürden für die Erschaffung stabiler Veränderungen von Genen oder Organismen. Außerdem hinterlassen genetische Veränderungen an Bakterien auch typische mikroskopische Veränderungen der Glykoproteinoberflächen, die dann als eine Art Fingerdruck eine Zuordnung zu einer Produktionsstätte erlauben helfen[585].

---

[579] Nur der Vollständigkeit halber, biologische Würmer sind vielzellige Organismen, die sich aktiv bewegen und Organismen infizieren können, während Viren passiv verbreitet werden (z.B. durch Husten, Durchfall, Schupfen, Blut usw.).

[580] vgl. Bakaletz 2012, S.2

[581] vgl. Gebhardt 2013, S.38.

[582] Dies wird nicht nur von Terroristen, sondern manchmal auch von Forschern beabsichtigt. Kürzlich verstärkte der Forscher Fouchier die ansteckenden Eigenschaften von Vogelgrippeviren, um die Viren besser zu verstehen, vgl. Guterl 2013, p46f. Sowohl die US als auch China äußerten schwerwiegende Bedenken, vgl. Guterl 2013, Zeng Guang 2013. Praktische Hinweise zur Abwehr von biologischen Waffen gibt es von der European Medicines Agency EMA, siehe EMEA 2002 (updated 2007).

[583] vgl. Kunze 2013, S.19-20

[584] In den USA ist die zuständige Sicherheitsbehörde das **National Science Advisory Board for Biosecurity** NSABB, aber die Biohackerszene wird auch vom FBI beobachtet, die CIA hat auch Interesse an der Materie, vgl. Hofmann 2012, S.14.

[585] In der Vergangenheit gab es Diskussionen, ob genetisch modifizierte Bakterien Maschinen mit Degradierung und Zersetzung anstecken könnten, jedoch wurde noch nie eine derartige Infektion beobachtet und die Frage blieb am Ende theoretischer Natur. Jedoch wurde 2016 das neue Bakterium *Ideonella sakaiensis 201-F6* entdeckt, das den weithin genutzten Kunststoff Polyethylen-terephthalat (PET) als Energie- und wesentliche Kohlenstoffquelle nutzt, vgl. Yoshida et al. 2016. Zwei Pilzarten wurden bereits 2011 identifiziert, vgl. Russell. et al. 2011, S.6076ff.: Zwei Isolate von *Pestalotiopsis microspora* waren in der Lage, mit Polyurethan als einziger Kohlenstoffquelle zu wachsen, sowohl unter aeroben als auch aneroben Bedigungen.

Ein spezielles Thema sind **Bakteriophagen**, das sind Viren, die Bakterien befallen und diese für ihre Vermehrung benutzen. Aus der Cyber-Perspektive ist folgendes interessant: maßgeschneiderte genetisch veränderte Bakteriophagen sind in der Lage, eine große Zahl verschiedener Ionen zu binden und können dann durch selbsttätige Aggregation für die Herstellung hocheffektiver Lithiumbatterie-Elektroden, photovoltaischer Zellen und Nanomaterialien genutzt werden[586]. Da die Phagen jedoch von einem Bakterium als Träger abhängig sind, besteht keine Gefahr, dass Bakteriophagen Digitaltechnologie durch Ionenbindung beschädigen, sie sind also keine anti-material weapons, d.h. keine Biowaffen zur Beschädigung von Materialien.
Vom biologischen Aspekt her wachsen die Sorgen wegen zunehmender Antibiotikaresistenzen, die typischerweise durch unsachgemäße Anwendung gefördert werden. Bakteriophagen wurden bereits als antibakterielle Viren in der Sowjetunion und noch heute in Russland und Georgien gegen schwere Infektionen genutzt[587]. Trotz der Erwartung einer kommenden post-antibiotischen Ära wird im Westen nur wenig geforscht und es gibt auch keine hinreichenden rechtlichen Regelungen[588]. Bakteriophagenenzyme sind jedoch militärisch bedeutsam, denn eines davon ist gegen die Standardbiowaffe Bazillus *anthracis* wirksam, besser als Milzbrand bekannt[589].

5.2.3 Kontrolle durch Cyber-Implantate

Aufgrund der Fortschritte im Bereich der Biologie und der Implantate-Forschung kam die Frage auf, ob Cyber-Implantate (Biochips) genutzt werden könnten, um menschliches Verhalten und die Entscheidungsfindung zu kontrollieren[590]. Jedoch sind diesem Cyborg-Szenario[591] gewisse Grenzen gesetzt:

Bestimmte von Parasiten als Wirt genutzte Insekten können von den Parasiten gezwungen werden, bestimmte Aktionen zum Schutz der Parasiten auszuführen (sog. Bodyguard manipulation) und deren Vermehrung durch Vermeidung von

[586] vgl. Yang et al. 2013, S.46ff
[587] vgl. Mandal 2014
[588] vgl. WHO 2014, Verbeken et al. 2014
[589] vgl. Zucca/Savoia 2010, S.83
[590] vgl. Juengling 2014, S.63
[591] Es gibt Unklarheiten zur Definition von Cyborgs. Eine weitgefasste Form sieht jede Form von Mensch-Maschine-System als Cyborg an, was auch tragbare Technologien umfassen kann. Eine engere Definition spricht nur von Cyborgs, wenn biologische und maschinelle Bestandteile physisch integriert sind. Retina- und Cochleaimplantate erfüllen auch die strikte Definition. Aus Cyberwar-Perspektive stellt (basierend auf Analysen der Hirnimplantat-Technologie) neben der Anfälligkeit für elektromagnetische Störungen die Notwendigkeit der externen Programmierung und Modifikation die wesentliche Verwundbarkeit von potentiellen Cyborgs dar, z.B. die Handheld Computer, die zur Modifikation von Hirnimplantaten gebraucht werden oder das Smartphone zur Steuerung der Biobots.

Freßfeinden zu begünstigen[592]. Auf der anderen Seite handelt es sich nur um bestimmte Aktionen, d.h. die Parasiten zwingen das Insekt nicht, „alles“ zu machen, was sie wollen. Parasiten sind jedoch in der Lage, die Konzentrationen der Neurotransmitter Dopamin und Serotonin (5-HT) zu beeinflussen, welche u.a. im limbischen (emotionalen) System des Gehirns eine Rolle spielen, also ähnlich wie moderne Psychopharmaka[593].

Beim Menschen kann der Parasit *Toxoplasma gondii* durch Infektion des Gehirns das menschliche Verhalten signifikant beeinflussen (wie z.B. Affekte, Suche nach neuen Erlebnissen, Schizophrenierisiko, dominantes Verhalten infizierten Männer etc.)[594], was durch Ergebnisse von mehreren psychologischen Standardfragebögen belegt werden konnte. Der Einfluss auf das Verhalten geht mit veränderten Dopamin- und Testosteronwerten einher[595], bedeutet aber keine Kontrolle des Verstandes oder Entscheidungsfindung. Menschen sind kein geplanter Wirt für Toxoplasma und sind somit eine Art Sackgasse. Im natürlichen Nagetierwirt erleichtern die durch den Parasiten induzierten Verhaltensänderungen die Übertragung auf die Katze als Zielwirt[596]. Außerdem ist noch unklar, inwieweit die Veränderungen beim Menschen wirklich Manipulationen oder nur Nebenwirkungen der chronischen Infektion darstellen.[597].

Implantierbare Hirnsonden (Tiefe Hirnstimulation [deep brain stimulation DBS] und Vagusnervstimulation VNS) werden bereits in einer Vielzahl von neuropsychiatrischen Erkrankungen getestet oder eingesetzt, wie Depression, Angststörungen, Schizophrenie, Zwangsstörungen, Tourette Syndrom, Tics, Epilepsie, Parkinson-Krankheit usw.[598]. Die Wirkung erfolgt durch elektrische Stimulation von spezialisierten Nervenzellknoten, den Nuklei, an denen die Sonden platziert werden und die sich tief im Gehirn befinden[599]. Jedoch reichen die Elektroden nicht bis in die graue Substanz der Hirnrinde (Neocortex), die für die intellektuellen Funktionen zuständig ist, d.h. die Implantate kontrollieren nicht den Verstand, ihr Einfluss ist mehr indirekter Natur, da die Nuklei, an denen das

[592] Zum Beispiel baut die Spinne *Plesiometa argyt* unter dem Einfluss der Parasitenwespe *Hymenoepimecis sp*. ein einzigartiges Kokon-Netz als feste Unterstützung des Wespenlarvenkokons. Manipulierte Raupen der Gattung *Thyrinteina leucocerae* blieben stets nahe bei den Puppen der Parasitenwespe *Glyptapanteles sp* und schlagen Freßfeinde durch gewaltsame Kopfstöße k.o. was zu deutlich höheren Überlebensraten der Parasitenpuppen führt. Eberhard 2000/2001 und Grosman et al., 2008 zitiert bei Maure et al. 2013, S.38

[593] vgl. Perrot-Minnot und Cézilly 2013, S.136-137

[594] vgl. Adamo und Webster 2013, S.1, Flegr 2013, S.127f.

[595] Die gestiegene Dopaminsynthese findet im infizierten Gehirn in Gewebezysten von Toxoplasma statt. Gestörte Dopaminspiegel spielen bei schweren psychiatrischen Erkrankungen wie der Schizophrenie eine Rolle.

[596] vgl. Adamo und Webster 2013, S.2, Flegr 2013, S.128

[597] vgl. Flegr 2013, S.127

[598] vgl. ClinicalTrials.gov - A service of the U.S. National Institutes of Health Search of: deep brain stimulation - List Results Seitenbesuch Juni 2014

[599] VNS wirkt hingegen durch eine elektrische Stimulation des Nervus vagus, des zehnten Hirnnervs, die in Halshöhe erfolgt

Implantat ansetzt, in das emotional-hormonale System des Menschen mit einbezogen sind[600] sowie in bestimmte Aspekte der Motorik.

Die US-Agentur DARPA initiierte 2006 **HI-Mems**-Projekte (hybrid insect micro electromechanical systems), um biologische Roboter zu entwickeln (biorobots, biobots), d.h. cyber-biologische Systeme von Insekten mit integrierter Elektronik. Eines der Ziele war die Entwicklung von Insektendrohnen für Spionagezwecke und andere militärische Aufgaben[601]. Seit kurzem kann ein Chip käuflich erworben werden, der nach Herstellung einer Verbindung die Kontrolle von Schabenbewegungen durch Smartphones erlaubt, hier als *RoboRoach* der Firma Backyard Brains, bei den Schaben handelt es sich um die Gattung *Blaberus Discoidalis*[602]. Der Chip wird jedoch *nicht* in den Kopf oder das Gehirn der Schabe implantiert, sondern lediglich mit kleinen Kabeln an den Fühlern der Schabe befestigt[603]. Elektrische Signale an den Fühlern bewirken dann eine Richtungsänderung der Schabe, wobei die Signale über Smartphone und Bluetooth versendet werden[604]. Typischerweise lässt die Kontrollwirkung nach ein paar Tagen nach, wobei umstritten ist, ob es sich um Gewöhnungseffekte oder einfach nur um Schäden an der Fühlerverbindung handelt.
Parallel zur Cyborgforschung werden auch **Biohybride** entwickelt, bei denen biologische und synthetische Materialien miteinander verknüpft werden.
Im Jahr 2016 wurde ein Schwimmroboter gebaut, der einen Rochen nachahmt und der aus einem feinen Goldskelett und einem Gewebe aus 200.000 genetisch veränderten Rattenherzmuskelzellen bestand[605]. Die Zellen wurden genetisch verändert, so dass die Geschwindigkeit und die Richtung durch Veränderung von Licht gesteuert werden konnte. Der Biohybrid blieb jedoch von der Anwesenheit einer physiologischen Kochsalzlösung umgebungsabhängig.

5.3 Zusammenfassung und Implikationen für den Cyberwar

Wenngleich Kommunikation und Netzwerke eine wichtige Rolle auch in biologischen Systemen spielen, ist die Vergleichbarkeit zu Computersystem

[600] Zielgebiete der tiefen Hirnstimulation bei schweren neuropsychiatrischen Erkrankungen sind unter anderem: Thalamus , subthalamic nucleus; nucleus accumbens; Cg25, subgenual area of cingulum, Kuhn et al. 2010, S.106. Im militärischen Bereich wurde eine Studie zur posttraumatischen Belastungsstörungen bei Soldaten 2012 geplant, aber nicht durchgeführt, Department of Veterans Affairs 2013
[601] vgl. Hummel 2014b
[602] vgl. Hummel 2014a, S.1
[603] vgl. Hummel 2014a, S.2
[604] Der Chip wird benötigt, um die Befehle des Smartphone in elektrische Signale umzusetzen, die Kontrolle der Schaben beschränkt sich auf das Geben von einfachen elektrischen Signalen, die keine Codes oder Bits enthalten, an die Fühler. Das Insekt wird irritiert und wechselt dann die Richtung. Technische Details finden sich bei Latif/Bozkurt 2012. Es ist daher noch ein weiter Weg zu Tier-Roboter-Hybriden, vgl. auch Hummel 2014b
[605] vgl. Park et al. 2016

begrenzt und jeder Vergleich oder Analogieschluss zwischen beiden Systemen sollte nur mit größter Zurückhaltung vorgenommen werden.

Dennoch hat sich auch hier die Rolle des Kommunikationsflusses gezeigt und in der bisherigen Cybersicherheitsdebatte liegt der Schwerpunkt eindeutig auf der Vermeidung von Infektionen, also auf der *eintreffenden* Kommunikation.
Deutlich weniger Aufmerksamkeit wird auf die *hinausgehende* Kommunikation gerichtet (die auch benötigt wird, um zum Beispiel initiale Trojanerinfektionen auszubauen). Der durchschnittliche User am Privat- oder Firmen-PC hat keinerlei Übersicht oder Kontrolle über Umfang oder Art des im Hintergrund ablaufenden Datenflusses aus dem Computer (oder dem Smartphone), also weder warum, zu wem und wieviel[606]. Die Berichte von Kaspersky, Symantec, McAfee, Mandiant und anderen zeigen, dass typischerweise selbst die massive Entwendung von Daten erst auffällt, wenn die Infektion bemerkt wurde, also viel zu spät. Ein Grund hierfür ist der "was nicht verboten ist, ist erlaubt"-Ansatz, d.h. außer einer Liste verbotener bzw. unsicherer Websites sind die Standardeinstellungen so, dass Daten faktisch fast überall hin gesendet werden können. Es würde Sinn machen, zumindest für sensible Netzwerke strengere Regeln einzuführen (z.B. reverse Protokolle, in denen nur ausdrücklich genehmigte Server und IP-Adressen angesteuert werden können) und verbesserte Tools, die eine bessere Übersicht über exportierte Daten und die Zulässigkeit dieser Datenströme erlauben.

[606] Sogar der Fernseher kann unbemerkt Daten verschicken, wenn er als Internet-TV (IPTV) designed wurde, vgl. SZ online 2013

6 Literaturquellen

Abendzeitung (2014): USA halten einige Lücken in Computersystemen geheim. Abendzeitung online 29.04.2014

Adamo S.A. and Webster J.P. (2013): Editorial. Neural parasitology: how parasites manipulate host behavior. The Journal of Experimental Biology 216, 1-2 doi:10.1242/jeb.082511

Africa, S. (2010): Governing Intelligence in the South African Transition, and Possible Implications for Africa, S.57-76 in: African security governance: emerging issues / ed. by Gavin Cawthra. - Johannesburg: Wits Univ. Press, 2009 - XII, 227 S.

Adelaja, O. (2011): Catching up with the rest of the world: the legal framework of cyber crime on Africa, 19 S. Paper at the 2011 Conference of the African Students Association of Australasia and the Pacific AFSAAP

Alexander, K.B. (2007): Warfighting in Cyberspace. JFQ, issue 46, 3rd quarter 2007, S.58-61

Alperovitch, D. (2009): Revealed: Operation Shady RAT. McAfee White Paper 2011, 14 S.

Alperovitch, D. (2014): Deep in Thought: Chinese Targeting of National Security Think Tanks 07.07.2014, 8 S.

Alperovitch, D. (2016): Bears in the Midst: Intrusion into the Democratic National Committee. From The Front Line, update 15.06.2016, 3 S.

Amann, M. et al. (2013): Der Freund liest mit. Der Spiegel 25/2013, S.15-20.

Anonhq (2014): ‚Anonymous' Hacker Group goes after ISIS. Eine Seite.

ArcSight (2009): Cyberwar: Sabotaging the System. Managing Network-Centric Risks and Regulations. ArcSight White Paper Research 021-111609-03

Astheimer, S, Balzter, S. (2015): Arbeit geht unter die Haut. Frankfurter Allgemeine Zeitung 21/22.02.2015, S.C1

Atherton, K.D. (2016): DARPA's Cyber Grand Challenge Ends In Triumph. Popular Science 06.08.2016, 2 S.

AU (2011): African Union Commission. Draft African Union Convention on the establishment of a credible legal framework for cyber security in Africa, 59 S.

Bakaletz, L.O. (2013): Bacterial biofilms in the upper airway – evidence for role in pathology and implications for treatment of otitis media. Paediatr Respir Rev 2012 September; 13(3): 154-159. doi:10.1016/j.prrv.2012.03.001

Bardt, H. (2010): Rohstoffe für die Industrie. Frankfurter Allgemeine Zeitung Nr. 275/2010, S.12

Barnes, J.E. (2012): Pentagon Digs In on Cyberwar Front. Wall Street Journal online 06.07.2012

Baumgärtner, M., Röbel, S., Schindler, J (2015), Die Handschrift von Profis. Der Spiegel 23/2015, S. 28

Baumgärtner, M., Müller, P., Röbel, S., Schindler, J (2015): Die Hütte brennt. Der Spiegel 25/2015, S. 34-35

Baumgärtner, M., Neef, C. Stark, H. (2016): Angriff der Bären. Der Spiegel 31/2016, S.90-91

Baumgartner, F. (2013): Riskanter Poker um das Datennetz des Bundes. Neue Zürcher Zeitung, 14 Nov 2013, S.25

Baumgartner, K. (2014): Sony/Destover: Mystery North Korean Actor's Destructive and Past Network Activity. Released on 04 Dec 2014, 11 Seiten. Securelist.com/blog/research/67895/destover

Bazylev, S., Dylevsky, I., Komov, S., Petrunin, A. (2012): The Russian Armed Forces in the Information Environment: Rules, and Confidence-Building Measures, Military Thought Nr. 2, 2012, S.10-15

BBC News (2009): Major cyber spy network uncovered. 29.03.2009

BBC (2014): Russian hackers used Windows bug to target NATO. BBC news online 14.10.2014, 3 Seiten

BBC (2016): FBI warns on risks of car hacking. Artikel 35841571. 18.03. 2016

Becker, J. (2016): Die Flut kommt. Süddeutsche Zeitung Nr.42/2016, S.78

Beidleman, S.C. (2009): Defining and deterring Cyber War. Approved for Public Release. US Army War College (USAWC) Class Of 2009, 36 S.

Bernau, P. (2014): Kamen die Hacker doch nicht aus Nordkorea? Frankfurter Allgemeine Zeitung online 31.12.2014, S.1

Best, R.A. (2009): Intelligence Issues for Congress. CRS Report RL33539

Betschon, S. (2012): Konferenz in Dubai gescheitert. Neue Zürcher Zeitung, 17.12.2012, S.4

Betschon, S. (2013a): Hacker im Honigtopf. Neue Zürcher Zeitung Nr. 73, S.38

Betschon, S. (2013b): Wenn Viren Luftsprünge lernen. Neue Zürcher Zeitung 07.11.2013, S.34

Betschon, S. (2014): High Noon in Hollywood Neue Zürcher Zeitung 18.12.2014, S.34

Betschon, S. (2016): Die Crux mit gefälschten Chips. Neue Zürcher Zeitung 31.08.2016, S.39

Beuth, P. (2016a): Sechs Tipps vom NSA-Hackerchef. Die Zeit online 29.01.2016, 3 Seiten

Beuth, P. (2016b): Unbekannte versteigern angebliche Waffen von Elitehackern. Die Zeit online 16.08.2016, 1 S.

Bierach, B. (2010): Australien will Seltenerdmetalle fördern. Neue Zürcher Zeitung 18.12.2010, S.11

Biermann, K. (2012): Obama erlaubt Angriff auf fremde Netze. Die Zeit online 15.11.2012, 2 Seiten

Biermann, K, Beuth, P. Steiner, F. (2016): Innenministerium plant drei neue Internet-Eingreiftruppen. Die Zeit online, 07.07.2016, 6 S.

Bilanz (2015): Dies ist ein Überfall! Bilanz April 2015, S.50-57

Bischoff, M. (2012): Kommando Strategische Aufklärung (Kdo StratAufkl) -Stand Oktober 2012, http://www.manfred-bischoff.de/KSA.htm

Bittner, J., Ladurner, U. (2012): Die Waffe der Überflieger. Die Zeit Nr. 50/2012, S.2-3

BMI (2011): Bundesministerium des Innern: Cybersicherheitsstrategie für Deutschland. 23.02.2011

BMVg (2015a): Überblick: Cyber-Abwehr der Bundeswehr Onlineartikel Berlin, 11.05.2015

BMVg (2015b): Auf der Suche nach der Bundeswehr der Zukunft. Onlineartikel Berlin, 20.07.2015

BMVg (2016): Abschlussbericht Aufbaustab Cyber- und InformationsraumEmpfehlungen zur Neuorganisation von Verantwortlichkeiten, Kompetenzen und Aufgaben im Cyber- und Informationsraum sowie ergänzende Maßnahmen zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung. April 2016, Offen, 53 Seiten

Brächer, M. (2016): Das fragile Netzwerk. Handelsblatt Nr. 155/2016, S.26-27

Brumbacher, B. (2016): Drohnen vom Himmel holen. Neue Zürcher Zeitung 12.04.2016, S.5

Broad, W.J., Markoff, J., Sanger, D.E. (2011): Israel Tests on Worm Called Crucial in Iran Nuclear Delay. New York Times 15.01.2011, 9 S.

Brown, G., Poellet, K. (2012): The Customary International Law of Cyberspace. In: Strategic Studies Quarterly. Volume 6 Fall 2012 Number 3, S.126 ff.

BSI (2012): Abwehr von DDoS-Angriffen. Dokument BSI-E-CS-002 Version 1.0 03.02.2012, 2 Seiten

Buchter, H., Dausend P. (2013): In die Luft geflogen. Die Zeit vom 29.05.2013, S.4

Burianski, M. (2012): Maschinen können nicht haften. Frankfurter Allgemeine Zeitung Nr. 272/2012, S.21.

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.

Campbell, R. (2015): Cybersecurity Issues for the Bulk Power system. Congressional Research Service R43989, 35 Seiten

Carmody, N.F. (2005): National Intelligence Reform. USAWC Strategy Research Report. US Army War College.

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

CCD CoE (2013): The Tallinn Manual on the International Law applicable to Cyber Warfare

Chhabra, S. (2014): India’s national cyber security policy (NCP) and organization – A critical assessment. Naval War College Journal, S.55-70

Chiesa, R. (2012): Presentation Security Brokers @ CONFidence X 2012 in Krakow, Poland, Public Version, 103 Folien.

Chip.de (2015): Anonymous gegen ISIS: Hacker enttarnen Terroristen. 18.11. 2015, eine Seite

CISSA (2012): Homepage des Committee of Intelligence and Security Services of Africa CISSA www.cissaau.org

Clauss, U. (2012): Sie speichern alles. Welt am Sonntag 13.05.2012, S.60

ClinicalTrials.gov (2013): DBS for TRD Medtronic Activa PC+S entry in ClinicalTrials.gov

Creditreform (2012): IT-Sicherheit: Angriffe aus Facebook &Co. abblocken. Creditreform 5/2012, S. 48.

Croitoru, J. (2012): Schule der Hacker. Frankfurter Allgemeine Zeitung Nr. 248/2012, S.30

Cyberwarzone (2016): Daesh (ISIS) has released a cyberwar magazine titled Kybernetiq. 09.01.2016, eine Seite

Daily Yomuri online (2012): Govt working on defensive cyberweapon/Virus can trace, disable sources of cyber-attacks. Yomiuri Shimbun 03 Jan 2012 http://www.yomiuri.co.jp/dy/national/T120102002799.htm

Darnstaedt, T., Rosenbach, M. und Schmitz, G.P. (2013): Cyberwar - Ausweitung der Kampfzone, Der Spiegel 14/2013,S.76-80.

DARPA (2012): DARPA-SN-12-51 Foundational Cyberwarfare (Plan X) Proposers' Day Workshop, 27 September 2012, 3 S.

DARPA (2016): Cyber Grand Challenge https://www.cybergrandchallenge.com 05.08.2016

Daun, A. (2009): Die deutschen Nachrichtendienste. In: Geheimdienste in Europa. Transformation, Kooperation und Kontrolle VS Verlag für Sozialwissenschaften, S.56-77.

Department of Defense (2015): The DOD Cyber Strategy April 2015, 8 Seiten

Department of Veterans Affairs (2013): A Pilot Study of Deep Brain Stimulation of the Amygdala for Treatment-Refractory Combat Post-Traumatic Stress Disorder (ADIP) entry in ClinicalTrials.gov

Der Spiegel online (2014): Im Zweifel einfach das Telefon wegschmeißen 27.12.2014, 2 Seiten

Der Spiegel (2015): Minister reisen mit Wegwerf-Handys. Der Spiegel 30/2015, S.18

DHS (2008): The Cyber-Terror Threat. New Jersey Office of Homeland Security and Preparedness 7 Seiten

Die Welt (2007): US-Geheimdienst kontrolliert Windows Vista. http://www.welt.de/wirtschaft/webwelt/article707809/US_Geheimdienst_kontrolliert_Windows_Vista.html

Die Welt online (2015): CIA plant Großoffensive gegen Cyberangriffe. Artikel 1381616569, S.1

Die Welt online (2016a): Pentagon: Hacker finden bei Test 138 Sicherheitslücken. http://www.welt.de/newsticker/news1/article156330187, 1 S.

Die Welt online (2016b): Mächtige Spionage-Software für iPhones entdeckt. 26.08.2016, 1 S.

Dilger, D.E. (2014): Massive, sophisticated "Inception - Cloud Atlas" malware infects Windows and Android but can't exploit Apple's iOS without jailbreak. Appleinsider 11 Dec 2014, 4 pages

DNI Handbook (2006): An overview of the United States Intelligence Community 2007. Published 15 December 2006

DoD (2011): Department of Defense Strategy for Operating in Cyberspace. July 2011, 13 Seiten

Dörfler, M. (2015): Sicherheitsrisiko Drucker. Frankfurter Allgemeine Zeitung Verlagsspezial IT-Sicherheit, 06.10.2015, S.P4

Dörner, A., Renner, K.-H. (2014): Roboter mit spitzer Feder. –Handelsblatt vom 07.07.2014, S.18-19

Dörner, S., Nagel, L.M. (2016): Russlands Zuckerberg. Welt am Sonntag 14.02.2016, S. 37

Dohmen, F. (2015): Überfall in 5 Minuten, Der Spiegel 20/2015, S.74-75

Dorsett, J. (2010): Information Dominance and the U.S. Navy's Cyber Warfare Vision. Presentation of VADM Jack Dorsett, DCNO for Information Dominance 14.04.2010

Drissner, G. (2008): Hört nichts. Financial Times Deutschland 11.07.2008, S.4

Dugan, R. (2011): Statement by Dr. Regina E. Dugan Director Defense Advanced Research Projects Agency Submitted to the Subcommittee on Emerging Threats and Capabilities United States House of Representatives March 1, 2011, 32 Seiten

Dunlap Jr., C. (2011): Perspectives for Cyber Strategists on Law for Cyberwar. Strategic Studies Quarterly, Spring 2011, S.81-99

DW (2016): IS-Datenleck wird größer und größer. Deutsche Welle.com 10.03.2016, eine Seite

DW online (2016): Twitter sperrt 360.000 Konten mit Terror-Botschaften. 19.08.2016, eine Seite

Eberbach, H.E. (2002): Neuorientierung des Militärischen Nachrichtenwesens der Bundeswehr. http://www.europaeische-sicherheit.de/alt/ausgaben/10oktober2002/1002,04.html

ECA (2012): Regional consultation on Harmonization of cyber legislation for Eastern, Southern and Northern Africa regions. UN Conference Center, Addis Ababa 20 – 22 June 2012, 5 S.

EMEA (2002): EMEA/CPMP Guidance document on use of medicinal products for treatment and prophylaxis of biological agents that might be used as weapons of bioterrorism. London 25. July 2002, CPMP/4048/01. Last update: 1 June 2007

EMB (2010): Petition an das Europäische Parlament vom Europäischen Metallgewerkschaftsbund (EMB) und den Europäischen Betriebsräten der Anbieter von Telekommunikationsinfrastruktur, S.1-5

ENISA (2009a): Analysis of Member States' Policies and Regulations. Policy Recommendations, 112 Seiten

ENISA (2009b): Cloud computing Benefits, risks, and recommendations for Information Security, November 2009, 113 S.

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’.

EPRS (2014): EPRS Briefing Cyber Defence in the EU, 10 Seiten

Erk, D. et al. (2015): Außer Kontrolle. Die Zeit Nr. 25/2015, S.2

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 (2011): Cloud Computing: Public Consultation Report. Information Society and Media Directorate-General. Brussels 05.12.2011, 7 S.

EU (2012a): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the Potential of Cloud Computing in Europe. Brussels 27.09.2012, 16 S.

EU (2012b): Motion for a resolution to wind up the debate on statements by the Council and the Commission pursuant to Rule 110(2) of the Rules of Procedure on the forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunication Union, and the possible expansion of the scope of international telecommunication regulations (2012/2881(RSP))

EU (2013a): Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. Brussels, 07 Feb 2013 COM (2013) 48 final, 28 S.

EU (2013b): Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace. 07 Feb 2013. Joint Communication to the European

Parliament, the Council, The European Economic and Social Committee and the Committee of the Region, 20 S.

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

Even, S. and Siman-Tov, D. (2012): Cyber Warfare: Concepts and Strategic Trends. Memorandum Nr. 117 des Institute for National Security Studies INSS, May 2012, 95 S.

F-Secure Labs (2014): BlackEnergy and Quedagh. The convergence of crimeware and APT attacks. F-Secure Labs Malware Analysis Whitepaper,15 S.

F-Secure Labs (2015): The Dukes - 7 years of Russian cyberespionage. F-Secure Labs Threat Intelligence Whitepaper, 27 S.

Fahrion, G. (2012): Pfusch am Gewehr. Financial Times Deutschland, 23.05.2012, S.1

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

Fayutkin, D (2012): The American and Russian Approaches to Cyber Challenges. J Def Manag 2:110. doi:10.4172/2167-0374.1000110

FAZ (2000): Amerikaner hören angeblich Datenleitungen in Europa ab. FAZ 24.01.2000, S.1

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

FAZ (2010h): Unternehmen und Staaten im Cyberkrieg. Frankfurter Allgemeine Zeitung online 12.10.2010

FAZ (2011a): Hacker greifen Rüstungskonzern Lockheed an. Frankfurter Allgemeine Zeitung Nr. 125/2011, S.11

FAZ (2011b): Unverantwortliche Vorwürfe. Frankfurter Allgemeine Zeitung Nr. 181/2011, S.7

FAZ (2012a): Eine neue Waffe im Cyberkrieg. Frankfurter Allgemeine Zeitung 30.05.2012, S.16

FAZ (2012b): Unmut über „Lecks“. Frankfurter Allgemeine Zeitung 09.06.2012, S.7

FAZ (2013a): Tausende Unternehmen informieren Geheimdienste. FAZ Nr. 136, 15.06.2013, S.1

FAZ (2013b): Auf dem Handy lauern Gefahren. FAZ Nr. 53, 04.03.2013, S.21

FAZ (2013c): Das Smartphone ist gefährdeter als der Schlüsselbund. Frankfurter Allgemeine Zeitung Nr. 249, S.14

FAZ (2013d): Seltene Erden sind günstig wie lange nicht. Frankfurter Allgemeine Zeitung Nr. 249, S.24

FAZ (2014a): Wenn sinnlose Anfragen das Internet zusammenbrechen lassen. Frankfurter Allgemeine Zeitung, 24.12.2014, S.21

FAZ (2014b): Amerika bittet China um Hilfe gegen Hacker. Frankfurter Allgemeine Zeitung, 22.12.2014, S.1

FAZ online (2014): Flugkörper UAV MQ-5B abgefangen. Online report vom 14.03.2014

FAZ (2015a): “NSA hat Computer in Nord Korea schon vor 4 Jahren infiltriert”. Frankfurter Allgemeine Zeitung, 20.01.2015, S.5

FAZ (2015b): Ein Konzern als Hacker. Frankfurter Allgemeine Zeitung, 22.04.2015, S.18

FAZ online (2015): Cyber-Angriff auf TV5 Monde. Ermittler verfolgen Spur nach Russland. FAZ online 09.06.2015

FAZ (2016): Australien fordert mehr Datenschutz im U-Boot-Bau. Frankfurter Allgemeine Zeitung 27.08.2016, S.29

FAZ (2016b): Immer mehr Banken werden von Hackern bestohlen. Frankfurter Allgemeine Zeitung 01.09.2016, S.23

FAZ online (2016): So kam die Spionage-Software aufs iPhone. 26.08.2016, 2 S.

FDA (2013a): FDA safety communication: Cybersecurity for medical devices and hospital networks (June 2013). http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

FDA (2013b): Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Draft Guidance for Industry and Food and Drug Administration Document issued on: June 14, 2013

Finkle, J. (2012): Exclusive: Insiders suspected in Saudi cyber attack. Reuters 07.09.2012, S.1-4

Finsterbusch, S. (2013): Big Data steht unter Beschuss. In: Frankfurter Allgemeine Zeitung Nr. 31, 06.02.2013, S.15

Finsterbusch, S. (2015): Behörden räuchern Hacker-Nest aus. Frankfurter Allgemeine Zeitung Nr. 163/2015, S.26

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

Flegr, J. (2013): Influence of latent Toxoplasma infection on human personality, physiology and morphology: pros and cons of the Toxoplasma–human model in studying the manipulation hypothesis. The Journal of Experimental Biology 216, 127-133 doi:10.1242/jeb.073635

Flückiger, J. (2014): Staatstrojaner mit Risiken und Nebenwirkungen. Neue Zürcher Zeitung 03.07.2014, S.27

Focus online (2012): Staatlicher Cyberangriff: Gauss-Trojaner späht Bankkunden aus. Focus online 09.08.2012

Focus (2013): Drohnentechnik ausspioniert? Focus 14/2013, S.16

Focus online (2013): Millionenfach installierte Android-App schnüffelte Nutzer aus. 06.12.2013

Focus Online (2016): NSA knackte verschlüsselte Befehle für Anschläge in Bayern 13.08.2016, 1 S.

Franz, T. (2010): The Cyber Warfare Professional. Air & Space Power Journal Summer 2011, S. 87-99

Frei, H. (2015): Effizient – aber überhaupt nicht städtisch. Neue Zürcher Zeitung Nr. 158 vom 11.07.2015, S.27

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, Nr. 1, October 2008, S.28-80

Fromm, T., Hulverschmidt, C. (2016): Totalschaden. Süddeutsche Zeitung Nr. 151/2016, S.25

Fromme, H. (2015): Der Spion kommt ins Auto. Süddeutsche Zeitung Nr. 150, 03.07.2015, page 17

Fuchs, C., Goetz, C., Obermaier, P und Obermayer, B. (2013a): Deutsche Aufträge für US-Spionagefirmen. Süddeutsche Zeitung Nr.265, 16/17.11.2013, S.1

Fuchs, C., Goetz, C., Obermaier, P und Obermayer, B. (2013b): Berlin, vertrauensselig. Süddeutsche Zeitung Nr.265, 16/17.11.2013, S.8

Fuest, B. (2011): Attacke auf die Wolke. Welt Online article 13401948

Fuest, B. (2012): Drohnen für alle. Welt am Sonntag Nr.51/2012, S.37

Fuest, B. (2014a): Uroburos –Russisches Supervirus greift die Welt an. Welt am Sonntag online 10.03.2014, 3 Seiten

Fuest, B. (2014b): Der übliche Verdächtige. Welt Am Sonntag Nr. 52/2014

Fuest, B. (2015): Fremdgesteuert. Welt Am Sonntag Nr. 26 vom 28.06.2015, S.34-35

Future of Life Institute (2015): Autonomous weapons. An open letter vom AI and Robotics Researchers. 27 July 2015

GAO (2015): GAO Highlights January 2015 FAA needs to address weaknesses in air traffic control systems, S.1

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

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

Gebauer, M. (2016): Nato erklärt Cyberraum zum Kriegsschauplatz. Der Spiegel online 14.06.2016, 2 S.

Gebhardt, U. (2013): Bakterielle Waffen zum Schweigen bringen. Neue Zürcher Zeitung Nr.264, S.38.

Genkin, D., Pachamanov, L., Pipman, I., Tromer, E. (2015): Stealing keys vom PCs using a radio: cheap electromagnetic attacks on windowed exponentiations. www.tau-ac.il, Juli 2015

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

Gerstein, DM (2015): Strategies for Defending U.S. Government Networks in Cyberspace. RAND Office of External Affairs Document CT-436 Juni 2015, 7 S.

Gierow, H. (2016): NSA legt Angriff und Abwehr zusammen. Zeit online 05.02.2016, 2 S.

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

Goebbels, T. (2011): Wurmfortsatz von Stuxnet entdeckt. Financial Times Deutschland, 20.10.2011, S.8

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

Goetz, J. Leyendecker, J. (2014): Das Problem mit der Wirklichkeit. Süddeutsche Zeitung Nr. 130, 7-9.06.2014, S.5

Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., Fu, K. (2011): They can hear your heartbeats: non-invasive security for implantable medical devices. Paper presented at the SIGCOMM 2011, 11 Seiten.

Gostev, A. (2012): Interview in: Der Feind hört mit: Wie IT-Experten die Spionage-Software entdeckten. Welt online, 30.05.2012

Graf, J. (2012): Stuxnet und Flame haben die gleichen Väter. Financial Times Deutschland, 12.06.2012, S.9

Graff, B. (2014): Sie sind da. Süddeutsche Zeitung Nr. 107, 10/11.05.2014, S.13

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

Graw, A. (2013): Freundschaft war gestern. Welt am Sonntag Nr.43, 27.10.2013, S.4-5

Grimmer, R., Irmler, W., Neiber, G., Schwanitz, W. (2003): Sicherheitspolitik der SED, staatliche Sicherheit der DDR und Abwehrarbeit des MfS. In: Die Sicherheit – zur Abwehrarbeit des MfS, Band I von 2, S. 44-239, edition ost

GSMA (2015): Remote SIM provisioning for machine to machine. GMSA Website Connected/Living/embedded-sim, 2 Seiten

Gujer, E. (2012a): Würmer und andere Computer-Parasiten. Neue Zürcher Zeitung, 01.09.2012, S.30

Gujer, E. (2012b): Medizinische Gutachten zum Datendieb. Neue Zürcher Zeitung, 05.10.2012, S.24

Gujer, E. (2013): Verfeindete Freunde. Neue Zürcher Zeitung, 03.07.2013, S.5

Guerrero-Saade, J.A., Raiu, C. (2016): Operation Blockbuster revealed. Securelist. https://securelist.com/blog/incidents/73914, 10 Seien

Gupta, S. (2012): Implantable Medical Devices – Cyber Risks and Mitigation Approaches NIST Cyber Physical Systems Workshop April 23-24, 2012, 28 Seiten

Guterl, F. (2013): Warten auf die Katastrophe. Spektrum der Wissenschaft November 2013, S.46-52

Gutscher, Th. (2013a): Sensibler Sensenmann. Frankfurter Allgemeine Sonntagszeitung Nr.22 02.06.2013, S.4

Gutscher, Th. (2013b): Menschenrechte hochhalten, nach Daten tauchen. Frankfurter Allgemeine Sonntagszeitung Nr.26 30.06.2013, S.7

Hafliger, M. (2012a): Datendieb wollte geheime Daten ins Ausland verkaufen. Neue Zürcher Zeitung, 29.09.2012, S.29

Hafliger, M. (2012b): Staatsschutz will private Computer ausspionieren. Neue Zürcher Zeitung, 05.11.2012, S.23

Haller, O. (2009): Angeborene Immunabwehr. In: Doerr, H.W., Gerlich, W.H. (2009): Medizinische Virologie. Thieme Verlag Stuttgart New York, S.48-58.

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

Handelsblatt (2014a): Das Ende von Herkules. Handelsblatt vom 09.05.2014, S.13, 16-17

Handelsblatt (2014b): Viele Wege führen in die Fritzbox. Handelsblatt vom 19.02.2014, S.23

Handelszeitung online (2014): Finnischer Teenager prahlt mit Sony Hack. 29.12.2014, S.1

Hanke, T. (2012): Erfolgreicher Probeflug der europäischen Kampfdrohne. Handelsblatt 03.12.2012, S.14-15

Hanspach, M., Goetz, M. (2013): On covert Mesh Networks in Air. Journal of communication Vol. 8 No 11, Nov 2013, S.758-767

Hawranek, D., Rosenbach, M. (2015): Rollende Rechner. Der Spiegel 11/2015, S.64-66

Hayes, B. (2007): Terroristensuche in Telefonnetzen? Spektrum der Wissenschaft 2/2007, S.108-113

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

Heider, D. (2006): Drohnen im zivilen und militärischen Einsatz. Universität Münster 01.02.2006, 10 S.

Heil, G., Mascolo, G. (2016): Eine Behörde gegen das "going dark". Tagesschau online, 22.06.2016, 2 S.

Hein, C., Schubert, C. (2016): Datenleck setzt französische Staatswerft unter Druck. Frankfurter Allgemeine Zeitung 25.08.2016, S.22

Heinemann, M. (2013): Global unterwegs – global vernetzt. Mobilität von morgen. Dezember 2013

Heller, P. (2016): Kanonen gegen Drohnen. Frankfurter Allgemeine Sonntagszeitung vom 24.04.2016, S.68

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

Heute (2016): Mit Funksender: Autoklub knackt 25 Autos. Heute.at online 17.03.2016

Hevelke, A., Nida-Rümelin, J. (2015): Intelligente Autos im Dilemma. Spektrum der Wissenschaft Oktober 2015, S.82-85

Hickmann, C. (2013): Kopien nicht erlaubt. Süddeutsche Zeitung Nr.124, 01/02.06.2013, S.6

Hildebrand, J. (2010): Ein Land schottet sich ab. Welt aktuell, S.6

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

Hofmann, N. (2012): Herumstochern im Genom. In: Süddeutsche Zeitung Nr. 179/2012 vom 04/05.08.2012, S.14

Hoppe, T., Osman, Y. (2015): Cybersturm auf Berlin, Handelsblatt Nr.110/2015 vom 12 to 14.06.2015, S.1

Huber, M. (2013): Der entkernte Staat. Der Spiegel 25/2013, S.18-19.

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

Hummel, P. (2014a): RoboRoach: Smartphone steuert Schabe 13.03.2014 Zeit online, S.1-3

Hummel, P. (2014b): Die Ankunft der Bioroboter Neue Zürcher Zeitung Nr. 59 vom 12.03.2014, S.42

Humphreys, T./Wesson, K. (2014): Drohnen auf Abwegen. Spektrum der Wissenschaft (German edition of Scientific American) März 2014, S.82-86

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

ICS-CERT (2016a): ICS-ALERT-14-281-01E: Ongoing Sophisticated Malware Campaign Compromising ICS (Update E). Original release date: 10.12.2014, last revised 02.03.2016

ICS-CERT (2016b): Alert (IR-ALERT-H-16-056-01). Cyber-Attack Against Ukrainian Critical Infrastructure. Original release date: 25.02.2016

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.

Isselhorst, H. (2011): Cybersicherheit in Deutschland. Präsentation von Dr. Hartmut Isselhorst, Abteilungspräsident des BSI am 16.06.2011, 27 S.

IT Law Wiki (2012a): Cyberwarfare - The IT Law Wiki, S.1-4 http://itlaw.wikia.com/wiki/Cyberwarfare

IT Law Wiki (2012b): Cyberwarfare - The IT Law Wiki, S.1 http://itlaw.wikia.com/wiki/European_Government_CERTs_Group

ITU (2012): FAQs on Flame. Paper of the International Telecommunications Union, 5 S.

Jäger, T, Daun, A. (2009): Intelligence in der EU. In: Geheimdienste in Europa. Transformation, Kooperation und Kontrolle VS Verlag für Sozialwissenschaften, S.213-239.

Jahn, T. (2011): Das Milliardengeschäft mit den Drohnen. Handelsblatt vom 25.11.2011, S.26

Jansen, J., Lindner, R. (2016): Der Spion in meinem iPhone. Frankfurter Allgemeine Zeitung 27.08.2016, S.28

Jennifer (2014): Breaking the Code on Russian Malware. The Recorded Future Blog Posted in Cyber Threat Intelligence 20.11.2014

Jones, S. (2014): NATO holds largest cyber war games. Financial Times FT.com 29.11.2014, 3 Seiten.

Jones, S. (2016): Cyber espionage: A new cold war? 19.08.2016 Financial Times online, 7 S.

Jüngling, T. (2013): Big Data! Die nächste Revolution Welt am Sonntag 03.03.2013, S.52

Jüngling, T. (2014): Unter die Haut. Welt am Sonntag Nr. 23 08.06.2014, S.62-63

Jüngling, T. (2015): Die Geiselnahme. Welt am Sonntag Nr. 41/2015, S.67

Jürgensen, N. (2016): Mehr als 20 Gigabyte Daten entwendet. Neue Zürcher Zeitung 25.05.2016, S.28

Jürisch, S. (2013): Intelligenz für mehr Lebensqualität. In: Implantate Reflex Verlag Dezember 2013, S.10

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

Karabasz, I. (2013): Gemeinsame Spionageabwehr im Netz. Handelsblatt 29 May 2013, Nr. 101, S.14-15

Karabasz, I. (2014): Angst vor dem Kontrollverlust. Handelsblatt 06.01.2014, Nr. 3, S.14-15

Kash, JC et al. (2011): Lethal synergism of 2009 Pandemic H1N1 Influenza Virus and Streptococcus pneumonia Coinfection Is Associated with Loss of Murine Lung Repair Responses. mBio 2(5):e00172 doc10.1128/mBio.00172-11

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

Kaspersky (2013): Kaspersky Lab identifies Operation “Red October”, an advanced Cyber-espionage campaign targeting diplomatic and government institutions worldwide. Kaspersky Lab Press Release 14.01.2013, S.1-3

Kaspersky (2014): Unveiling Careto – The masked APT February 2014

Kaspersky Lab (2015a): Equation Group Questions and Answers. Version 1.5, February 2015, 32 Seiten

Kaspersky Lab (2015b): The Duqu 2.0 Technical details. Version 2.0, 9 June 2015, 45 Seiten

Kaspersky Lab (2015c): Der große Bankraub: Cybergang “Carbanak” stiehlt eine Milliarde US-Dollar von 100 Finanzinstituten weltweit, Moskau/Ingolstadt, 15.02.2015, 3 Seiten

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

Kleinwächter, W. (2012): Sollen Staaten künftig das Internet kontrollieren? Frankfurter Allgemeine Zeitung Nr. 255/2012, S.31

Kloiber, M., Welchering, P. (2011): Militärs suchen Strategien gegen Cyberattacken. Frankfurter Allgemeine Zeitung Nr.38/2011, S.T6

Klüver, R. (2013): Automaten des Todes. Süddeutsche Zeitung Nr. 187/2013, S.2

Knocke, F. (2012): Indien rüstet zum Cyberwar. Spiegel online 11.06.2012

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

Koch, M. (2011): Die Spur führt nach China. Süddeutsche Zeitung vom 03.06.2011, S.20

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

Köpke, J., Demmer, U. (2016): Bundeswehr im Visier von Hackern. Neue Westfälische 16.03.2016, 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

Kremp, M. (2011): Elite-Hacker führen Cyberwar für China. Spiegel online 26.05.2011

Krohn, P. (2014): Der Schaden durch Hackerangriffe wird immer größer. Frankfurter Allgemeine Zeitung vom 20.12.2014, S.24

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

Kuhn, J. (2010): Deep Brain Stimulation for Psychiatric Disorders. Deutsches Ärzteblatt International 2010; 107(7): 105–13

Kunze, A. (2013): Die Stunde der Bio-Punks. Die Zeit Nr. 19/2013, S.19-20

Kurz, C. (2012): Die ganz normale Unterwanderung des Netzes. Frankfurter Allgemeine Zeitung Nr. 286/2012, S.33

Kurz, C. (2013): Die Angriffsindustrie. Frankfurter Allgemeine Zeitung Nr. 254/2013, S.31

Kurz, C. (2016): Wir erklären den Cyberwar für eröffnet. Frankfurter Allgemeine Zeitung 07.03.2016, S.14

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

Lakshmi, B. (2012): India signs the new ITR at WCIT: 80 countries including U.S. refuse to sign. Article vom 14.12.2012 on Mediauama.com

Lambrecht M., Radszuhn, E. (2011): Game over. Financial Times Deutschland, 29 April 2011, S.25

Lange, A.M. (2016): Mit Cyberbomben gegen den IS. Neue Zürcher Zeitung 28.04.2016, S.5

Langer, M.A. (2014a): Das Netz als Entwicklungshelfer. Neue Zürcher Zeitung Nr.271, S.7

Langer, M.A. (2014b): Geheimes Wettrüsten. Neue Zürcher Zeitung Nr.290, S.1

Langer, M.A. (2015 a): Spionage für jedermann. Neue Zürcher Zeitung Nr.6, S.6

Langer, M.A. (2015b): Hinter dem Rücken der Geheimdienste. Neue Zürcher Zeitung, 08.12.2015, S.5

Latif, T. and Bozkurt, A. (2012): Line Following Terrestrial Insect Biobots. IEEE 2012, Paper 4 Seiten

Leithäuser, J. (2015a): Der virtuelle Krieg. Frankfurter Allgemeine Zeitung vom 28.07.2015, S.8

Leithäuser, J. (2015b): Aufrüstung für den Krieg der Zukunft. Frankfurter Allgemeine Zeitung Nr. 217/2015, S.4

Leithäuser, J. (2016): Fortgeschrittene ständige Bedrohung. Frankfurter Allgemeine Zeitung Nr.48/2016, S.8

Lemos, R. (2015): NFC security. 3 ways to avoid being hacked. PC World online 26.06.2015

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

Lewicki, M. (2014): Hacker am Steuer. Welt am Sonntag 14.09.2014, S.62

Leyden, J. (2014): Nuke Hack fears prompt S Korea cyber-war exercise Reactor blueprints leaked on social media. The Register 22.12.2014, S.1-3

Li, C., Yang P., Zhang Y., Sun Y., Wang W. et al. (2012): Corticosteroid Treatment Ameliorates Acute Lung Injury Induced by 2009 Swine Origin Influenza A (H1N1) Virus in Mice. PLoS One 7(8): e44110, doi:10.1371/journal.pone.0044110

Li, C. et al. (2012): IL-17 response mediates acute lung injury induced by the 2009 Pandemic Influenza A (H1N1) virus. Cell Research 2012, 22:528-538

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

Lichtblau, E., Weiland, N. (2016): Hacker releases more Democratic Party Documents. New York Times online, 12.08.2016

Lindner, R. (2016): Drohnen – und wie sie unschädlich gemacht werden. Frankfurter Allgemeine Zeitung Nr.7/2016, S.24

Löwenstein, S. (2013): Geheimdienste sind geheim – auch in Österreich. Frankfurter Allgemeine Zeitung Nr.169/2010, S.5

Lohse, E., Sattar, M., Wehner, M (2015): Russischer Wissensdurst. Frankfurter Allgemeine Nr. 24/2015, S.3

Los Angeles Times (2011): Air Force says drone computer viruses pose ‘no threat’. Los Angeles Times online 13 October 2011, 11:26 am

Luschka, K. (2007): Estland schwächt Vorwürfe gegen Russland ab. Spiegel online 18.05.2007, S.1-3

Mähler, M. (2013): TV Total. Süddeutsche Zeitung Nr. 253/2013, S.38

Mahaffey, K. (2016): Warum ich das Tesla Model S gehackt habe. Frankfurter Allgemeine Zeitung Sonderbeilage ITK 2016, S.V6.

Maliukevicius, N. (2006): Geopolitics and Information Warfare: Russia’s Approach. University of Vilnius, S.121-146

Mandal SM. et al (2014): Challenges and future prospects of antibiotic therapy: vom peptides to phages utilization. Front Pharmacol. 2014 May 13;5:105

Mandiant (2013): APT 1 Exposing One of Chinas Cyber Espionage Units, 74 S.

Market Wired (2014): Proofpoint uncovers Internet of Things (IoT) Cyberattack. Market Wired 16 Jan 2014, S.1-2

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

Marsiske, HA (2016): Bei Strahlenwaffen liegt Deutschland vorn. Artikel 3117433 Heise.de 25.02.2016, 2 Seiten

Martin-Jung, H. (2008): Die Schlagadern des Internets. Süddeutsche Zeitung Nr. 34, S.22

Martin-Jung, H. (2014): Digitale Super-Wanze. Süddeutsche Zeitung Nr. 271, 25.11.2014, S. 17

Mascolo, G., Richter, N. (2016): Bundesbehörde soll Verschlüsselungen knacken. Süddeutsche Zeitung online, 23.06.2016, 3 S.

Matthews, E. (2013): Cyberspace Operations: HAF Cyber Matrix and Force Development, HAF/A3C/A6C 27.06.2012, S. 8

Mayer, M. (2015): Wir wissen, wen Du triffst. Frankfurter Allgemeine Zeitung vom 23.07.2015, S.13

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

Mayer-Kuckuck, F., Koenen, J., Metzger, S. (2012): Hacker werden immer dreister. Handelsblatt 15.02.2012, S.20-21

Maure, F. et al. (2013): Diversity and evolution of bodyguard manipulation The Journal of Experimental Biology 216, 36-42 doi:10.1242/jeb.073130

McAfee (2011): Global Energy Cyberattacks: “Night Dragon”. McAfee White Paper 10.02.2011, 19 S.

McAfee Labs (2013): Dissecting Operation Troy: Cyberespionage in South Korea. McAfee Labs White Paper. By Ryan Sherstobitoff and Itai Liba, McAfee® Labs and James Walter, Office of the CTO, 29 Seiten

McDonald, G., O’Morchu, L., Doherty, S., Chien, E. (2013): Stuxnet 0.5: The Missing Link. Symantec Report 2013, 18 Seiten

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

Medtronic (2013): Media backgrounder Activa® PC+S: sensing the future of Deep Brain Stimulation, 4 Seiten

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

Meier, L. (2011): Super-Sarko im Cyberkrieg. Financial Times Deutschland 08.03.2011, S.9

Melton, K.H. (2009): Der perfekte Spion (Deutsche Ausgabe von The ultimate spy). Coventgarden, aktualisierte Ausgabe von 2009

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

Mertins, S. (2012): Cyberkrieg zwischen Iran und USA eskaliert. Financial Times Deutschland 17.10.2012, S.10

Mertins, S. (2015): Feindliche Übernahme. NZZ am Sonntag 14.06.2015, S.5

Metzler, M. (2015): Hacker legen deutschen Hochofen lahm. NZZ am Sonntag 11.01.2015, S.34

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

Miller, T. (2013): Drohnen über Amerika. Le Monde Diplomatique Deutsche Ausgabe Oktober 2013, S.12-13

Morschhäuser, T. (2014): Heftiger Sonnensturm verfehlt Erde nur knapp. Frankfurter Rundschau online 25.07.2014, S.1-2

Müller, G.V. (2014): Die Schatten-IT wird zum Problem. Neue Zuercher Zeitung 11.04.2014, S.16

Nakashima, E. (2012a): In U.S.-Russia deal, nuclear communication system may be used for cyber security. The Washington Post 26.04.2012

Nakashima, E. (2012b): With Plan X, Pentagon seeks to spread U.S. military might to cyberspace. The Washington Post 30.05.2012

Nakashima, E., Miller, G., Tate, J. (2012): U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. The Washington Post online 19.06.2012, S.1-4

Nakashima, E. (2016a): Russian government hackers penetrated DNC, stole opposition research on Trump. Washington Post online, 14.06.16, 6 S.

Nakashima, E. (2016b): Russian hackers targeted Arizona election system. 29.08 Aug 2016. Washington Post online, 29.08.16, 4 S.

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

NATO (2014): Hybride Kriegsführung – hybride Reaktion? Nato Brief Magazine online

NATO (2015): Cyber security. Nato.int/cps/en/natohq/topics last updated 09 Jul 2015

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

NCSA (2009a): The Mission Priority 1: Support to NATO operations: Combating Cyber attacks. 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

NCSA (2009c): NATO Communication and Information Systems Services Agency (NCSA), Sector Mons (Formerly Regional Signal Group SHAPE – RSGS) Unit History (As of: March 2005)

Neubacher, A. (2013): Spion im Keller. Der Spiegel 49/2013, S.82.

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

Nligf (2012): Structure of Iran’s Cyber Warfare (Source: the BBC Persian). PDF-file on nligf.nl 7 Seiten

Northrop Grumman TASC (2004): Cyber Warrior Hacker Methodology. Presentation, 44 S.

Novetta (2015): Operation-SMN-Report Juni 2015, 31 Seiten

Novetta (2016): Operation-Blockbuster-Report Februar 2016, 59 Seiten

NTV online (2013): USA schaffen neue Kriegsmedaille. 14.02.2013

NZZ (2012): Wirbel in den USA um Indiskretionen. Neue Zürcher Zeitung, 07.06.2012, S.1

NZZ (2014): Virtueller Gegenangriff auf Nordkorea? Neue Zürcher Zeitung Nr.300, S.3

Oparus (2010): Oparus Overview and Objectives. Website of the OPARUS project, 3 Seiten, oparus.eu

Opfer, J. (2010): IT-basierte Informationsgewinnung durch Angriffe auf die Mobilkommunikation – Gefährdungen und Schutzmaßnahmen. In: Proaktiver Wirtschaftsschutz: Prävention durch Information 4. Sicherheitstagung des BfV und der ASW am 18. März 2010 in Köln

Paletta, D.Ä, Schwartz, F. (2016): Pentagon deploys cyberweapons against Islamic State. Wall Street Journal online 29.02.2016, article 1456768428, 4 S.

Park, S.J. et al. (2016): Phototactic guidance of a tissue-engineered soft-robotic ray. Science 08 Jul 2016: Vol. 353, Issue 6295, pp. 158-162

Perlroth, N. (2013): U.S. seeks young hackers. New York Times international Weekly 28.03.2013, S.1 und S.4

Perlroth, N. (2014): 2nd China Army Unit Implicated in Online Spying. New York Times online 10.06.2014

Perrot-Minnot, MJ. und Cézilly, F. (2013): Investigating candidate neuromodulatory systems underlying parasitic manipulation: concepts, limitations and prospects The Journal of Experimental Biology 216, 134-141 doi:10.1242/jeb.074146

Pofalla, B. (2013): Datenfüchse von morgen. Frankfurter Allgemeine Sonntagszeitung 11.08.2013, S.44

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 Seiten

Postinett, A. (2008): Wolken-Reich. Handelsblatt Nr.245/2008, S.12

Postinett, A. (2011): Lauschangriff in Amerika. Handelsblatt Nr.234/2011, S.32

Postinett, A. (2013a): Auf die kleine Art. Handelsblatt Nr. 248/2013, S.30

Postinett, A. (2013b): Aus allen Wolken gefallen. Handelsblatt Nr. 249/2013, S.12-13

Prawda (2012): USA starts anti-Russian drills, Russia hires nation’s best hackers. Prawda English online 18.10.2012, 2 Seiten

Puhl, J. (2013): Im Silicon Savannah. Der Spiegel 48/2013, S.118-122.

Quirin, I. (2010): Vorfahrt fürs Netz. FTD Dossier Intelligente Netze 15.10.2010, S.2-7.

Ragan, S. (2016): Salted Hash – Top Security News. Hackers say leaked NSA tools came from a contractor at Red Seal. CSO online article 3109936, 6 Seiten

Raiu, C., Baumgartner, K., Kamluk, V. (2013): The MiniDuke Mystery. PDF 0-day Government Spy Assembler 0x29A MicroBackdoor, 20 S.

Reder, B., van Baal A. (2014): Wenn Hacker den Strom abstellen. Frankfurter Allgemeine Zeitung Verlagsspezial IT-Sicherheit 7.10.2014, S.V2

Rees, J. (2016): Volvo schafft den Zündschlüssel ab. Handelsblatt online 20.02.2016, S.1-4

Rieger, F. (2010): Du kannst Dich nicht mehr verstecken. Frankfurter Allgemeine Zeitung Nr. 43/2010, S.5

Rieger, F. (2011): Angriff ist besser als Verteidigung. Frankfurter Allgemeine Zeitung Nr. 14/2011, S.27

Robertson, J., Lawrence, D., Strohm (2014): Sony's breach stretched vom Thai Hotel to Hollywood. 07 Dec 2014, www.bloomberg.com

Rößler, C. (2016): Ab in den Süden. Frankfurter Allgemeine Zeitung 02.03.2016, S.6

Rötzer, F. (2016): Der vom Pentagon angekündigte Cyberwar gegen den IS dümpelt vor sich hin. Telipolis 19.07.2016, 2 S.

Rogers, J. (2009): From Suez to Shanghai: the European Union and Eurasian maritime security. Occasional Paper - n°77, March 2009

Rõigas, H., Minárik, T. (2015): 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law. Incyder news, 31.08.2015

Rosenbach, M., Schmitz, G.P., Schmundt, H. (2010): Mord ohne Leiche. Spiegel 39/2010, S.163

Rosenbach, M, Traufetter, G. (2015): Der Computerabsturz. Der Spiegel 22/2015, S.72-73

Rüb, M. (2010): Jenseits der Partnerschaftsrhetorik. Frankfurter Allgemeine Zeitung Nr. 129/2010, S.5

Rühl, L. (2012): Was nur Soldaten leisten können. Frankfurter Allgemeine Zeitung Nr. 248/2012, S.10

Ruggiero, P., Foote, J. (2011): Cyber Threats to Mobile Phones. Carnegie-Mellon University, 6 Seiten

Russell, J.R. et al. (2011): Biodegradation of Polyester Polyurethane by Endophytic Fungi. Applied and Environmental Microbiology, Sep 2011, pp.6076-6084

RWE (2013): Wohnen in der Zukunft, S.5 RWE-Unternehmensbeitrag RWE-Effizienz in: Smart Building 2013

Saad, S., Bazan, S.B., Varin, C. (2010): Asymmetric Cyber-warfare between Israel and Hezbollah: The web as a new strategic battlefield. University of Beirut, 4 S.

Sanger, D.E. (2012): Obama order sped up wave of cyber attacks against Iran. New York Times online. 01.06.2012, 9 S.

Sanger, D.E., Shanker Th. (2014): NSA devises radio pathway into computers. NYTimes 14.01.2014

Sanger, D.E. (2015): US and China seek arms deal for cyberspace. New York Times online 20.09.2015, 5 S.

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

Schanz, M.V. (2010): Building better cyber warriors. Air Force Magazine September 2010, S.50-54.

Scheidges, R. (2010): Bundesamt misstraut US-Firmen. Handelsblatt 02.12.2010, S.12-13

Scheidges, R. (2011): Schlechte Noten für deutsche Kryptographen. Handelsblatt 18.07.2011, S.17

Schelf, S. (2013): Stromlobby will im Notfall Kühlschränke abschalten. Neue Westfälische 23/24 Feb 2013, S.1.

Scheren, M. (2009): Vernetzte Sicherheit – Zusammenarbeit der Inlandsnachrichten- und Sicherheitsdienste in Europa. In: Geheimdienste in Europa. Transformation, Kooperation und Kontrolle VS Verlag für Sozialwissenschaften, S.168-181.

Scheubeck, Th. (2014): Über Prioritäten nachdenken. Spektrum der Wissenschaft (German edition of Scientific American) June 2014, S.7.

Schlüter, N., Laube, H. (2010): Der RIM-Code. Financial Times Deutschland 03.08.2010, S.8

Schmid, G. (2001): Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 INI)

Schmidt, M.S., Perlroth, N., Goldstein, M. (2015): FBI says little doubt that North Korea hit Sony, New York Times online 08 Jan 2015

Schmitt, J. (2009): Virtuelle Spürhunde. Der Spiegel 10/2009, S.83

Schmitt, M.N. (2013): International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.

Schmundt, H. (2014): Glotze glotzt zurück. Der Spiegel 8/2014, S.128

Schmundt, H. (2015): Tödlich wie eine Granate. Interview with Luciano Floridi. Der Spiegel 8/2015, S. 120-121

Schneider, W. (2011): Das Unheimliche am Internet. Neue Zürcher Zeitung NZZ Folio Januar 2011, S.9

Schneider, MC. (2014): Wie die Autobauer sich gegen Angriffe aus dem Netz wehren. Bilanz November 2014

Schönbohm, A. (2012): Interview in: 50 Prozent mehr Angriffe. Afrikas Cyber-Piraten greifen Deutschland a. Bild online 24.06.2012

Schöne, B. (1999): Der „große Lauschangriff“ im Internet. Die Welt 22.06.1999, S.32

Schöne, B. (2000): Ein Netz aus 120 lauschenden Satelliten. Die Welt 17.05.2000, S.39

Schröder, T. (2008): Was Du siehst, sehe ich auch. Frankfurter Allgemeine Sonntagszeitung Nr.3, S.58

Schröm, O. (1999a): Verrat unter Freunden. Die Zeit Nr. 40, S.13-14

Schröm, O. (1999b): Traditionell tabu. Die Zeit Nr. 40, S.15

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

Schulz, T. (2013): Frust beim Filtern. Süddeutsche Zeitung 6/7.04.2013, S.6

SEC (2011): Commission Staff Working Paper. Determining the technical and operational framework of the European Border Surveillance System (EUROSUR) and the actions to be taken for its establishment. Brussels, 28 Jan 2011, SEC (2011) 145 final 11 S.

Shah, S. (2014): Die Rückkehr der Pocken Spektrum der Wissenschaft (German edition of Scientific American) Februar 2014, S.24-29

Shane, S. (2013): No morsel too small for a US spy agency. New York Times International 8 Dec 2013, S.1/4

Singer, P.W. (2010): Der ferngesteuerte Krieg. Spektrum der Wissenschaft Dezember 2010, S.70-79

Spehr, M. (2015): Ausgespäht mit Android. Frankfurter Allgemeine Zeitung 04.08.2015, Nr. 187/2015, S.T4

Solon, O. (2016): Hacking group auctions 'cyber weapons' stolen from NSA. The Guardian online, 16 August 2016, 2 pages

South Africa (2010): Note of Intention to make national cyber security policy for South Africa. In Government Gazette Vol. 536, No. 32963, 16 S.

South Africa (2012): Statement on the approval by Cabinet of the Cyber Security Policy Framework for South Africa 11.03.2012

Spiegel online (2011): Deutschland probt den Cyber-Ernstfall http://www.spiegel.de/netzwelt/netzpolitik/0,1518,801114,00.html

Spiegel online (2012a): Internet-Sicherheit USA und China wollen Cyberkrieg verhindern. Bericht vom 08.05.2012

Spiegel online (2012b): Wie Syrien das Internet verlor. Artikel vom 30 November 2012

Spiegel online (2013a): Briten gründen riesige Cyberarmee. Artikel vom 27.09.2013

Spiegel online (2013b): Stromschwankungen bringen NSA-Technik zum Schmelzen. Artikel vom 08.10.2013

Spiegel (2012): Badrnejad, K., Dworschak, M., von Mittelstaedt, J., Schnepp, M., Schmundt, H.: Ansteckende Neugier. Der Spiegel 23/2012, S.121-124

Spiegel (2013a): Neues Drohnenprojekt. Der Spiegel 25/2013, S.11

Spiegel (2013b): Das chinesische Problem. Der Spiegel 9/2013, S.22

Spiegel (2013c): Abwehrschlacht gegen Cyberspionage, Der Spiegel 13/2013, S.15

Spiegel (2013d): Verdacht statt Vertrauen, Der Spiegel 26/2013, S.111

Spiegel (2014): BND ausgebremst. Der Spiegel 24/2014, S.18

Spiegel online (2016): Gruppe "Shadow Brokers" Hacker erbeuteten offenbar NSA-Software. 17.08.2016, 1 S.

Stamoulis, C. and Richardson, AG. (2010): Encoding of brain state changes in local field potentials modulated by motor behaviors. J Comput Neurosci. 2010 December; 29(3): 475–483. doi:10.1007/s10827-010-0219-6

Standard (2015): Sicherheitslücke: Hacker kapern Jeep während Fahrt auf Autobahn derStandard.at 22.07.2015, 2 Seiten

Stark, H. (2009): Digitale Spionage. Der Spiegel 11/2009, S.33

Stegemann-Koniczewski, S. et al. (2012): TLR7 contributes to the rapid progression but not to the overall fatal outcome of secondary pneumococcal disease following influenza A virus infection. Journal of Innate Immunity, doi: 10.1159/000345112; 2012

Steier, H. (2016a): Wer nicht zahlt, muss frieren. Neue Zürcher Zeitung 17.08.2016, S.36

Steier, H. (2016b): Riskantes Horten von Sicherheitslücken. Neue Zürcher Zeitung online, 18.08.2016, 2 Seiten

Steinitz, D. (2014): Großes Drama. Süddeutsche Zeitung Nr. 296 vom 19.12.2014, S.11

Steinmann, T. (2010): Deutschland im Visier der Cyberkrieger. Financial Times Deutschland 29.12.2010, S.10

Steinmann, T., Borowski, M. (2012): Deutschland wird im Netz verteidigt. Financial Times Deutschland 05.06.2012, S.1

Steler, H. (2015): Google Geräte als Wanzen. Neue Zürcher Zeitung online vom 28.07.2015

Stingl, K. et al. (2013): Artificial vision with wirelessly powered subretinal electronic implant alpha-IMS Proc. R. Soc. B 2013 280, 20130077, published 20.02.2013

Stokes, G. (2005): Cyber Security Fundamentals: What You Should Know About Protecting Data & Systems Orus Group LLC, Orus Group Cyberwar Institute

Storm, D. (2016): SWIFT: More banks hacked; persistent, sophisticated threat is here to stay. Computerworld 31.08.2016

Storn, A. (2016): Plötzlich sind 81 Millionen Dollar weg, Die Zeit Nr.20, 04.05.2016, S.29

Striebeck, UB. (2014): Fabriktore stehen für Hacker offen. Industrie 4.0 Reflex Verlag 2014

Strobel, W. (2016): Obama prepares to boost U.S. military's cyber role: sources. Reuters 07.08.2016, 3 S.

Süddeutsche Online (2013): Hacker aus China klauen Google Datensätze. 21.05.2013. www.sueddeutsche.de/ digital/gegenspionage aus China google gehackt spione gecheckt-1.1677106

Symantec (2010): W32.Stuxnet Dossier by Nicolas Falliere, Liam O Murchu, and Eric Chien. Version 1.3. November 2010, 64 S.

Symantec (2011): W32.Duqu The precursor to the next Stuxnet, Dossier, 14 S.

Symantec (2012): W32.Gauss Technical Details, Dossier, 13 Seiten

Symantec (2013): Security Response Symantec Four Years off DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War Created: 26 Jun 2013 Updated: 23 Jan 2014

Symantec (2014a): Regin: Top-tier espionage tool enables stealthy surveillance. Symantec Security Response Version 1.0 – November 24, 2014, 22 Seiten

Symantec (2014b): Emerging Threat: Dragonfly/Energetic Bear – APT Group. 30.06.2014, 5 Seiten

Symantec (2016): The Waterbug attack group. Security Response Version 1.02 Symantec, 14.01.2016, 44 Seiten

SZ (2014a): Der BND will soziale Netzwerke ausforschen. Süddeutsche Zeitung Nr 130, 31.05./01.06.2014, S.1

SZ (2014b): Nordkorea vom Internet abgeschnitten. Süddeutsche Zeitung Nr. 296 vom 24-26.12.2014, S.1

SZ (2014c): Cyber-Angriff auf Filmkonzern War der Sony-Hack das Werk eines Ex- Mitarbeiters? http://www.sueddeutsche.de/digital/2.220/cyber-angriff-auf-filmkonzern-war-der-sony-ha... 30/12/2014

SZ online (2013): Fernseher schaut zurück. Artikel vom 21.11.2013

SZ online (2016): Lücke bei Facebook. Zugriff auf die Welt. Article 1.2901048 10.03.2016

T-online (2015): Apple löscht über 250 Spionage-Apps aus App-Store, 2 S. Artikel id_75824954

Tagesschau (2015): Umbaupläne vorgestellt: Bei der CIA soll vieles anders werden. Tagesschau.de 07.03.2015, 1 Seite.

Talos Cooperation (2012): Transportable Autonomous Patrol for Land Border Surveillance D.10.3 4th Workshop 25.05.2012

TAZ online (2013): China testet das “scharfe Schwert”. 23.11.2013, 4 Seiten

The Economist (2013): War on terabytes. The Economist 02.02.2013, S.59

The SecurityLedger online (2014): New Clues in Sony Hack point to insiders, away from DPRK, page 1 18 Dec 2014

Thibaut, M., Alich, H. (2010): Paris und London besiegeln Militärkooperation. Handelsblatt Nr.213/2010, S.15

Thiel, T. (2012): Auf der sicheren Seite. Frankfurter Allgemeine Zeitung Nr. 281/2012, S.Z1-Z2

Tiesenhausen, F. von (2011): Zehn Beamte gegen den Internetkrieg. Financial Times Deutschland 24.02.2011, S.11

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, S.228-233

Tomik, S. (2013a): Pufferspeicher, Volumenreduktion und Community Detection. Frankfurter Allgemeine Zeitung Nr. 156/2013, S.6

Tomik, S. (2013b): Enthüllungen am laufenden Band. Frankfurter Allgemeine Zeitung Nr. 148/2013, S.2

Touré, H.I. (2012): Statement from Dr. Hamadoun I. Touré Secretary General of the ITU. Dubai, 13.12.2012

Ulfkotte, U. (1998): Im Visier der Datenjäger. Frankfurter Allgemeine Zeitung Nr.125, S.16

UN (2015): Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, adopted in July 2015, 17 Seiten

United Nations letter (2011): Letter dated 12 September from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, 5 Seiten mit einem 3-seitigen Annex mit dem Code of conduct

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

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.

Valeriano, B., Maness, R. (2011): Cyberwar and Rivalry: The Dynamics of Cyber Conflict between Antagonists 2001-2011, 25 S.

Verbeken, G. (2014): Call for a Dedicated European Legal Framework for Bacteriophage Therapy. Arch. Immunol. Ther. Exp. (2014) 62:117–129

Vistica, G. (1999): We're in the Middle of a Cyberwar. Newsweek 13.09.1999

Vitzum, Th. (2013): unbekanntes Flugobjekt. Welt Am Sonntag Nr. 22, 02.06.2013, S.6

Wanner, C. (2011): Das Phantom von Shenzen. Financial Times Deutschland 28.02.2011, S.8

WCIT (2012): Official Powerpoint Presentation of the ITU

WCIT Final Acts (2012): Final Acts of World Conference on International Telecommunications, 23 Seiten

WCIT Resolution Plen/3 (2012): Resolution Plen/3 to foster an enabling environment for the greater growth of the Internet. In: Final Acts of World Conference on International Telecommunications, S.20

WCITleaks (2012): Document DT-X 05 December 2012. Russia, UAE, China, Saudi-Arabia, Algeria, Sudan, and Egypt. Proposals for the Work of the Conference in track change modus

Weber, M., Weber, L. (2016): Die smarte Kapitulation. Frankfurter Allgemeine Zeitung Nr.3/2016, S.T1

Wechlin, D. (2016): Auf Orwells Spuren. Neue Zürcher Zeitung 27.06.2016, S.6

Weedon, J. (2015): Beyond ‚Cyber War': Russia's use of strategic espionage and information operations in Ukraine. In: Geers, K. Cyberwar in Perspective Russian aggression against Ukraine. Nato CCD COE Publications. Tallinn 2015, S.67-77

Wehner, M. (2015): Cyber-Krieg im Bundestag. Frankfurter Allgemeine SonntagsZeitung Nr.24 vom 14.06.2015, S.1

Wehner, M. (2016): Cyberkrieg. Frankfurter Allgemeine Sonntagszeitung vom 07.08.2016, S.6

Welchering, P. (2011): Wie Ägypten das Internet gezielt abschaltete. Frankfurter Allgemeine Zeitung Nr. 32/2011, S.T2

Welchering, P. (2012): Wege in den digitalen Abgrund. Frankfurter Allgemeine Zeitung Nr. 134/2012, S.T1

Welchering, P. (2013a): Digitale Überwachungsaugen an jeder Ecke. Frankfurter Allgemeine Zeitung Nr. 110/2013, S.T6

Welchering, P. (2013b): Mit Vierkantschlüssel und Biege-Koppler. Frankfurter Allgemeine Zeitung Nr. 156/2013, S.6

Welchering, P. (2013c): Geheimdienste lesen auch bei verschlüsselten Daten mit. Frankfurter Allgemeine Zeitung Nr. 216/2013, S.T2

Welchering, P. (2014a): Das Stromnetz verrät nicht nur Kriminelle. Frankfurter Allgemeine Zeitung vom 01.07.2014, S.T4

Welchering, P. (2014b): Arbeiten am Trojaner-Abwehrschirm. Frankfurter Allgemeine Zeitung vom 09.09.2014, S.T4

Welchering, P. (2016): So fahndet der Geheimdienst NSA nach Programmierern. Frankfurter Allgemeine Zeitung Nr. 136/2016, S.T4

Welt (2013): Und alle hören mit. Welt am Sonntag Nr.43, 27.10.2013, S.3

Welt online (2013): Teheran führt Aufklärungsdrohnen vor. Welt am Sonntag Nr.43, 28.09.2013

Welt online (2014): Forscher entwickeln Herzschrittmacher ohne Batterie. Welt online 20 Jan 2014

Werner, K. (2010): Siemens zieht in den Cyberkrieg. Financial Times Deutschland 21.12.2010, S.7

White House (2011): International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World, 25 S.

White House (2013): The White House (2013): Executive Order – Improving Critical Infrastructure Cybersecurity 12.02.2013, 6 S.

White Wolf Security (2007): Estonia and Cyberwar – Lessons Learned and Preparing for the Future By White Wolf Security, 3 Seiten, 6 April 2007

Whitlock, C. (2014): When drone fall from the sky. Washington Post online from 20.06.2014

WHO (2014): WHO's first global report on antibiotic resistance reveals serious, worldwide threat to public health New WHO report provides the most comprehensive picture of antibiotic resistance to date, with data from 114 countries, News release, 30 April 2014

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

Winkler, P. (2013): Die Affäre Edward Snowden schreckt Washington auf. Neue Zürcher Zeitung International Nr.133, 12 Jun 2013, S.3

Winkler, P. (2014a): Die NSA kann Computer auch offline ausspähen. Neue Zürcher Zeitung 17.01.2014, S.3

Winkler, P. (2014b): Designierter NSA-Chef will mehr Transparenz. Neue Zürcher Zeitung 14.02.2014, S.3

Winkler, P. (2015): Die Mutter aller Datendiebstähle. Neue Zürcher Zeitung, Nr. 139, S.3

Winkler, P. (2016): Russische Hacker in Amerikas Wahlregistern. Neue Zürcher Zeitung, 01.09.2016, S.4

Wong, E. (2013): Espionage Suspected in China`s drone bid. New York Times international Weekly 27 Sep 2013, S.1 and S.4

Wysling, A. (2013): Spione im Mobilfunknetz. Neue Zürcher Zeitung 07.12.2013, S.5

Wysling, A. (2014): Luftraum frei für Drohnen. Neue Zürcher Zeitung 04.01.2014, S.5

Xu, F., Qin, Z., Tan, C.C., Wang, B., and Qun, L. (2011): IMDGuard: Securing Implantable Medical Devices with the External Wearable Guardian. Paper of the College of William and Mary, 9 Seiten

Y.2770 (2012): ITU-T Study Group 13. Future networks including mobile and NGN. Draft New Recommendation ITU-T Y.2770 Proposed For Approval At The World Telecommunication Standardization (WTSA-12). Requirements for Deep Packet Inspection in Next Generation Networks, 90 Seiten

Yang, S.H. et al. (2013): Assembly of Bacteriophage into Functional Materials Challenges and future prospects of antibiotic therapy: from peptides to phages utilization. The Chemical Record, Vol. 13, 43–59 (2013)

Yannakogeorgos, P.A. (2012): Internet Governance and National Security. In: Strategic Studies Quarterly. Volume 6 Fall 2012 Number 3, S.102-121.

Yoshida, S. et al. (2016): A bacterium that degrades and assimilates poly(ethylene terephthalate) Science 11 Mar 2016:Vol. 351, Issue 6278, pp. 1196-1199 DOI: 10.1126/science.aad6359

Young, S. (2013): Brain radio records and emits electrical pulses MIT Technology Review 09.08.2013

Zeit online (2015a): Sieben Wege, ein Handy abzuhören. 20.02.2015, 2 Seiten

Zeit online (2015b): Apple and Samsung arbeiten am Ende der SIM-Karte. 17.07.2015, 2 Seiten

Zeng Guang (2013): Gefährliche Experimente mit Vogelgrippe-Viren. RP online 16.08.2013, 2 Seiten

Zepelin, J. (2012): Länder lahmlegen. Financial Times Deutschland 06.07.2012, S.27

Zetter, K. (2016): Everything we know about Ukraines power plant hack www.wired.com 20.01.2016

Zhanga, X. (2012): Structure of Sputnik, a virophage, at 3.5-Å resolution. PNAS, 06 Nov 2012 vol. 109, no. 45, S.18431–18436

Zhou, J. et al. (2012): Diversity of Virophages in Metagenomic Data Sets. J. Virol. 2013, 87(8):4225. DOI: 10.1128/JVI.03398-12. Journal of Virology S.4225–4236

Zoll, P. (2015): Donnerwetter aus Nordkorea. Neue Zürcher Zeitung vom 05.01.2015, S.1

Zucca, M., Savoia, D. (2010): The Post-Antibiotic Era: Promising Developments in the Therapy of Infectious Diseases. International journal of Biomedical science. Int J Biomed Sci vol. 6 no. 2 June 2010, S.77-86