UNIVERSITÄT OSNABRÜCK
LV Geostrategie und Geopolitik
Fachbereich 1
49069 Osnabrück

Cyberwar

Grundlagen-Methoden-Beispiele

07.07.2019

Zusammenfassung

Der Cyberwar (Cyberkrieg) ist die kriegerische Auseinandersetzung mit den Mitteln der Informationstechnologie. Dieses Arbeitspapier unternimmt eine aktuelle Bestandsaufnahme und geht auf die theoretischen und praktischen Probleme ein. In der Praxis ist der Cyberwar ein integraler Bestandteil militärischen Handelns, lässt sich jedoch nicht ganz von der Spionage trennen, da das Eindringen in und Aufklären von gegnerischen Systemen wesentlich für das weitere Vorgehen ist.
Nach einem Überblick über Angriffsmethoden, Angreifer (Advanced Persistent Threats), Spionagetools, Cyberwaffen und der Cyberverteidigung liegt ein besonderes Augenmerk auf der Einordnung von Cyberangriffen (Attribution) und der Smart Industry (Industrie 4.0). Anschließend werden die Cyberwar-Strategien der USA, Chinas, Russlands und weiterer führender Akteure besprochen. Ein abschließendes Kapitel befasst sich mit biologischen Anwendungen.

Inhalt

1. Grundlagen

1.1 Einführung

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].
Der Cyberwar (Cyberkrieg) ist die kriegerische Auseinandersetzung mit den Mitteln der Informationstechnologie. Dieses Arbeitspapier unternimmt eine aktuelle Bestandsaufnahme und geht auf die theoretischen und praktischen Probleme ein. In der Praxis ist der Cyberwar ein integraler Bestandteil militärischen Handelns, lässt sich jedoch nicht ganz von der Spionage trennen, da das Eindringen in und Aufklären von gegnerischen Systemen wesentlich für das weitere Vorgehen ist.
Nach einem Überblick über Angriffsmethoden, Angreifer (Advanced Persistent Threats), Spionagetools, Cyberwaffen und der Cyberverteidigung liegt ein besonderes Augenmerk auf der Einordnung von Cyberangriffen (Attribution) und der Smart Industry (Industrie 4.0). Anschließend werden die Cyberwar-Strategien der USA, Chinas, Russlands und weiterer führender Akteure besprochen. Ein abschließendes Kapitel befasst sich mit biologischen Anwendungen.

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.
Ein erhöhtes Risiko für Cyber-Attacken ergibt sich insbesondere aus:

- Exponentielles Wachstum von Schwachstellen durch schnellen Anstieg von digitalen Geräten, Anwendungen, Updates, Varianten, Netzwerken und Schnittstellen
- Computer und Geräte sind keine isolierten Systeme, denn für technische, kommerzielle und Überwachungszwecke müssen digitale Technologien von außen zugänglich bleiben
- Datenschutz und Privatsphäre erodiert durch freiwillige, unwissentliche oder erzwungene (z.B. durch Nutzungsbedingungen) Datenfreigabe an Dritte
- Professionelle Suche nach Lücken und Exploits durch Hacker, Hacktivisten, Cyberkriminelle, Sicherheitsfirmen und Forscher, aber auch durch staatliche Behörden oder mit dem Staat verknüpften Gruppen.

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

[1] vgl. USAF 2010a, DoD 2011

- 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].
- 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]), siehe Abschnitt 7.10.
- 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)'** und des **'company owned, personally enabled (COPE)'–**

[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.

[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.

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

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]

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 bei konventionellen Angriffen (sog. **Attributionsproblem**), so dass auch die Abschreckung durch Bestrafung oder Gegenwehr erschwert wird.

Auch gibt es einen signifikanten Trend zu immer aggressiveren und größeren Angriffen, wie im Abschnitt 2.3.1.1 dargestellt.
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*.

---

[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
[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. In Deutschland hat das Innenministerium 1.700 Objekte als geschützten Kernbereich definiert, die nur noch Kern sind, die geschützt werden müssen, darunter 110 Krankenhäuser, die mindestens 30.000 Fälle pro Jahr behandeln, vgl. Osterloh 2017, S.
[11] vgl. Megill 2005, DoD 2011

1.3 Cyberwar Definition

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[12].

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[13].

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[14].
Jedoch gehen die meisten Autoren davon aus, dass groß angelegte und komplexe Cyberangriffe wegen der benötigten Ressourcen und der möglichen Folgen nicht ohne Rückendeckung staatlicher Organisationen stattfinden, so dass eine Reihe von Vorfällen, bei denen sich der Urheber nicht klären ließ, in der Literatur dem Cyberwar zugeordnet werden.
Der erste Chef des *US Cyber Command Cybercom,* General Keith Alexander, sah die Notwendigkeit einer erweiterten Definition, die klarstellt, dass es auch um den Schutz der eigenen Systeme und der Handlungsfreiheit (**freedom of action**) geht[15].
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[16].

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[17]. 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

[12] vgl. Wilson 2008, S.3ff.
[13] vgl. Beidleman 2009, S.9ff. and S.24
[14] vgl. auch CSS 2010, Libicki 2009, S. XIV
[15] 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."
[16] vgl. Alexander 2007, S.60
[17] vgl. IT Law Wiki 2012a, S.1-4

Gegner die effektive Nutzung seiner Computer, Informationssysteme und Netzwerke zu verwehren“ definiert[18].

Diese Überlegungen spiegeln sich in der aktuellen **Cyberwar-Definition** der US Army wider[19]:

„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[20].
Die Cyber-Kriegs-Konzepte der USA und Chinas stimmten von Anfang an dahingehend überein, dass der Einsatz von Computern im militärischen Bereich nur ein Teil anderer militärischer Aktivitäten ist. Die Debatte über die Frage, ob ein Krieg durch Computerangriffe allein entschieden werden kann, ist rein theoretischer Natur, für die militärische Praxis wurde diese Option niemals in Betracht gezogen.

Manchmal wird auch diskutiert, ob Computer wirklich ein Teil eines Krieges sein könnten, da Computerangriffe Menschen nicht töten konnten, aber in der militärischen Praxis ist diese Debatte irreführend. Computer sind einfach technische Werkzeuge wie z.B. Radarsysteme. Radarsysteme töten die Feinde nicht direkt und in der Tat retten sie viele Leben im zivilen Luftverkehr, aber niemand würde daran zweifeln, dass Radarsysteme auch ein Teil anderer militärischer Aktivitäten sind.

Die Russen schließen in ihrer Cyberwar-Definition den Informationskrieg mit ein, wobei die Verbreitung von Meinungen und Informationen im Netz politischen und gesellschaftlichen Zwecken dient und nicht wie der eigentliche Cyberwar militärisch-technischen Zielen, siehe auch Kapitel 2.2.6.

---

[18] 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”.

[19] 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.

[20] vgl. auch Beidleman 2009, S.10

1.4 Cyberwar und Spionage

Es ist wichtig, sich den Unterschied zwischen Spionage und Cyberwar nochmal genauer anzuschauen. Hacker versuchen mit Schadsoftware, englisch **Malware** in ein digitales Gerät wie Computer oder z.B. auch Smartphones einzudringen, um dann Aktionen zur Spionage, Manipulation, Sabotage, Diebstahl/Erpressung und Missbrauch auszuführen.

Hacker müssen nicht nur in die Computer/Geräte rein, sondern die Informationen dann auch wieder raus, zum sogenannten **Command and Control**-Server. Diese Zweigleisigkeit ermöglicht oft erst die Entdeckung einer Infektion und auch die Rückverfolgung des Angreifers.

Um einen Computer oder System beschädigen zu können, muss man also erstmal drin sein. Es gibt umfangreiche Spionageaktivitäten und wenig Cyberwar, aber man muss sich aber im Klaren darüber sein, dass der Cyberwar oft nur einen zusätzlichen Mausklick erfordern würde.

So gesehen ist es einerseits verständlich, warum Sicherheitskreise die Gefahr eines Cyberwars für hoch halten und entsprechende Maßnahmen fordern, während anderen die Sache aufgebauscht vorkommt, weil man noch keinen großen Cyberwar beobachten konnte. Die Grenzen zwischen Spionage und Cyberwar sind fließend, da das eine das andere voraussetzt, was sich auch in der oft ungenauen Berichterstattung widerspiegelt. Eine in der CIA geführte Diskussion zur Digitalisierung der Spionage kam laut US-Medien zu dem Schluss, dass digitale Spionage letztlich die bisherige Arbeit nur ergänzen, aber keinesfalls den Agenten vor Ort ersetzen kann.

1.5 Terminologie

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[21].

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

[21] vgl. auch Mehan 2008, CSS 2010

aufdecken würde[22]. Großangelegte Spionageangriffe können jedoch auch zu Computer- und Netzwerkstörungen führen und werden dann mitunter in der Literatur ebenfalls dem Cyberwar zugerechnet.

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[23].

Dazu gehört neben bereits etablierten Anwendungen

- wie dem Radarflugzeugsystem **Airborne Early Warning and Control System (AWACS)**, das der großräumigen Radarüberwachung aus der Luft dient,
- der Einsatz der vernetzten Kriegführung (**Network based warfare NBW**), bei der die **C4ISR** (Command, Control, Computers, Communications, Information for intelligence, surveillance, and reconnaissance) im Zentrum steht, d.h. die Vernetzung aller Führungs-, Informations- und Überwachungssysteme zur Gewinnung eines genauen Lagebildes und zur Verbesserung der Entscheidungsfindung und Führungsfähigkeit
- der Einsatz von **Lenkwaffen** wie smart bombs (intelligente Bomben)
- der Einsatz unbemannter Systeme wie der **Drohnen** (Unmanned Aerial Vehicles UAV) oder auch Bombenentschärfer (PackBots[24])
- 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[25]. Drohnen eignen sich generell für alle Arten von Operationen, die „dull, dirty, dangerous or difficult“ sind[26]. Der operative Erfolg der Drohnen hat die Nachfrage entsprechend steigen lassen[27][28].

Bei der **integrierten Kriegführung** werden zivile Ziele und Organisationen in die Planung und Durchführung des Krieges mit eingebunden und die

[22] vgl. Libicki 2009, S.23
[23] vgl. Neuneck/Alwardt 2008
[24] vgl. Hürther 2010, S.33-34
[25] vgl. Rüb 2010, S.5
[26] vgl. Jahn 2011, S.26: also alles, was „langweilig, schmutzig, gefährlich, schwierig oder anders“ ist
[27] vgl. FAZ 2010b, S.6
[28] 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.

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.[29] Ziel der IO ist die Erlangung und Optimierung von 5 Kernfähigkeiten (core capabilities), nämlich

- der erfolgreichen psychologischen Kriegsführung (**psychological operations PSYOP**) zur Erringung der Informationsüberlegenheit, wobei man noch die Gegenspionage (**Counterintelligence CI**), Gegenpropaganda und öffentliche Information (**Public Affairs PA**) abgrenzen kann[30]
- der Irreführung des Gegners (**military deception MILDEC**), z.B. der gegnerischen Luftabwehr wie während des Irakkrieges[31]
- 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[32], die Entwendung von Informationen als **computer network exploitation (CNE)** und die Schutzmaßnahmen gegen beides als **computer network defence (CND)**[33]
- die klassische elektronische Kampfführung (**electronic warfare EW**) mit Hilfe der Schädigung des Gegners durch Störsignale und ähnliche Maßnahmen.

1.6 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,

[29] vgl. Wilson 2007
[30] vgl. USAF 2010b, S.5
[31] vgl. USAF 2010b, S.32
[32] vgl. Wilson 2008
[33] vgl. CSS 2010

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[34].

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[35] und China[36] 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*[37].

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[38].
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[39]. Die Staaten sollten zusammenarbeiten, um die Sicherheit und Stabilität der Nutzung der Informations- und

[34] Gleichwohl gibt es Überlegungen zu voll automatisierten Gegenantworten bei Cyberattacken, Nakashima 2012b
[35] vgl. Nakashima 2012a
[36] vgl. Spiegel online 2012
[37] vgl. ITU 2012
[38] vgl. auch Fayutkin 2012, S.2
[39] UN 2015

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[40].

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 [41].

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 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) [42]. Laut einer Mitteilung des CCD CoE im Februar

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

2016 waren 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[43].

1.7 Die Geostrategie des Cyberspace

Inzwischen haben sich die Strukturen im Cyberspace verfestigt und professionalisiert.
Es werden immer mehr spezialisierte Cybereinheiten errichtet, sei es auf nachrichtendienstlicher Ebene oder im militärischen Bereich.
Damit einhergehend richtet sich der Blick vermehrt auf die Sicherung der eigenen nationalen IT-Infrastruktur, was mit einem wachsenden Risiko der Fragmentierung des Internets einhergeht.
Nachdem lange Zeit die Vorstellung des Cyberspace als virtueller Welt dominierte, setzt sich in Sicherheitskreisen ein immer physischeres Verständnis durch: wer die Geräte und die Leitungen kontrolliert, der kontrolliert auch die darin befindlichen Daten.

1.7.1 Die physische Kontrolle über die Datenflüsse

Die langfristigen Strategien zielen darauf ab, trotz der weltweiten Vernetzung die **physische Kontrolle über die Datenflüsse** zu sichern bzw. wieder zurück zu erlangen.
Tatsächlich hat sich die Vorstellung, man könnte seine Bevölkerung und die Gegner langfristig virtuell kontrollieren, in der Praxis aus drei Gründen als problematisch erwiesen:

- War früher der Zugang zu Informationen oft vertikal-hierarchisch gegliedert, hat die Vernetzung dazu geführt, dass aggressive Hacker selbst Präsidenten angreifen und ihre Informationen freigeben können. Leaks werden immer häufiger und schwerwiegender.
- Virtuelle Überwachung ermöglicht eine nie dagewesene Kontrolle der eigenen Bevölkerung. Dies gilt auch für gegnerische Angreifer, wie bei dem sogenannten 'OPM-Breach', bei dem Hacker die Personalakten und digitale Fingerabdrücke sicherheitsüberprüfter Amerikaner kopierten.
- Drittens kann virtuelle Kontrolle nur bei technischer Überlegenheit zur Machtgewinnung und –sicherung beitragen, denn wenn der Vorsprung schmilzt, ist es praktisch unmöglich, sich gegnerische Angreifer noch vom Leibe zu halten.

---

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.
[43] vgl. Gebauer 2016

Die **physische Datenkontrolle** soll auf verschiedene Weise (wieder)-erlangt werden, nämlich durch

- physischen Systemzugang
- Bildung von Cyberinseln
- und Herausdrängen von ausländischen Firmen aus der eigenen Sicherheitsarchitektur.

Langfristige Kontrolle gewährt einem stets der **physische Systemzugang**, z.B. Zugang zu Servern, zu Internetknoten, das Anzapfen von Tiefseekabeln usw. oder leitet mit strategisch platzierten Knotenrechnern den Datenverkehr um mit dem sogenannten **Border Gateway Protocol hijack**. US-Studien haben gezeigt, dass der gesamte Datenverkehr von Staaten auf diese Weise schon wochenlang umgeleitet und kopiert wurde, im Prinzip aber auch vernichtet werden könnte.

Zunehmend verlangen Staaten, dass Server von international agierenden Providern im eigenen Land aufgestellt werden, so dass die Behörden direkten Zugriff auf das System haben können.
Noch weitergehend verlangen einige Staaten, dass bestimmte Daten nur noch national gelagert werden und das Land nicht verlassen dürfen. Das mag gegen Spionage nicht wirklich helfen, aber es steigert die Angriffsrisiken und -kosten des Angreifers.
Frühere Versuche der physischen Kontrolle durch Abtrennung von Teilsystemen vom Netz konnten den gegnerischen Zugriff jedoch meistens nicht verhindern, sondern nur verzögern.

Trotz der Zunahme des Hackens aus sicherer Entfernung sind **physisch präsente Abhör- und Datensammeleinrichtungen** in Zielnähe immer noch das Rückgrat einer nachhaltigen und erfolgreichen nachrichtendienstlichen Tätigkeit.

- **Bildung von Cyberinseln**

Zugriffssperren auf Inhalte ausländischer Provider, in Verbindung mit Blockaden von Virtual Private Network VPN-Tunneln[44] ermöglichen die **Schaffung von nationalen Netzen bzw. Cyberinseln.**
Eine ‘weiche’ Inselbildung ist das Anbieten nationaler Services und Plattformen, wodurch die Attraktivität für die eigene Bevölkerung gesteigert und gleichzeitig sprachliche und ggf. auch technische Eingangshürden für Ausländer geschaffen werden.
Einen Sonderfall stellt Russland dar, dessen Netz sich in Sowjetzeiten eigenständig entwickelte und heute auch als *Runet* bekannt ist. Die lange Abstinenz des Westens

[44] China plante Mitte 2017 ein VPN-Verbot. In China gibt es für Suchmaschinen und Social Media längst chinesische Äquivalente wie *Baidu* oder *Wechat*, die auch intensiv genutzt werden.

ergab eine bis heute anhaltende Dominanz russischer Anbieter[45]. Aus dem ursprünglichen sowjetischen Internetsystem *Relkom* entwickelte sich der russische Teil des Internets. Schon früh entwickelte sich die Suchmaschine *Yandex (Yet another index)* und das Soziale Netzwerk *VKontakte*, die beide nach wie vor den Markt beherrschen.

- **Herausdrängen von ausländischen Firmen aus der eigenen Sicherheitsarchitektur**

Staaten achten zunehmend darauf, dass sich keine ausländischen Anbieter in ihre kritische Infrastruktur einkaufen können und so in den Verteidigungsperimeter des jeweiligen Staates gelangen. Auch gelangen ausländische Sicherheitsfirmen zunehmend in das Visier von Ermittlern.

1.7.2 Die Kontrolle kritischer Komponenten

1.7.2.1 Rohstoffe

China besaß 2010 einen 97%igen Marktanteil[46] an seltenen Erden (speziellen Industriemetallen wie Niob, Germanium, Indium, Palladium, Kobalt und Tantal), 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 zunehmend das Exportvolumen ein[47]. 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 sinkenden Preisen geführt[48].
Die USA haben im Jahr 2019 35 Rohstoffe als kritisch identifiziert, aber weisen bei 14 dieser Rohstoffe keine eigene Produktion auf. Bei den seltenen Erden hat China im Jahr 2019 71% Marktanteil und 37% der Reserven, wobei Vietnam und Brasilien mit je 18% Reserven zukünftige Ausweichförderstaaten darstellen könnten[49].

1.7.2.2 Die Verflechtung USA - China

Sowohl die USA als auch China sind wichtige Cyber-Mächte: China ist der wichtigste Produzent von physischer Elektronik in Computern und Smartphones, selbst US-Firmen lagern ihre Produktion oft nach China aus. Das ist sinnvoll, da

[45] vgl. Limonier 2017, S.1, 18-19
[46] vgl. Büschemann/Uhlmann 2010, S.19
[47] 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
[48] vgl. FAZ 2010d, S.12, Bierach 2010, S.11, FAZ 2013d, S.24
[49] vgl. FAZ 2019b, S.17

China der Haupteigentümer von computerrelevanten Metallen ist. Daher produziert China 75 Prozent der Mobiltelefone und 90 Prozent aller PCs weltweit, da selbst US-Unternehmen diesen Produktionsschritt nach China auslagern.

Auf der anderen Seite dominieren die USA das Infrastrukturniveau der zentralen Server und der Tiefseekabel. In der physischen Welt ist das Internet immer noch an ein physisches Netzwerk mit einem signifikanten Zentralisierungsgrad gebunden.
Das US-amerikanische Unternehmen *Equinix* steuert laut Firmenwebseite mit eigenen IXPs und Co-Location von Client-Computern in ihren Rechenzentren rund 90% (!) der Datenübertragung des Internets.

1.7.2.3 Der Huawei-Konflikt

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. Die US-Behörden wiesen *Huawei* wegen Sicherheitsbedenken an, ihre Anteile an der Cloud computing Firma *3Leaf* zu verkaufen[50].

Wie in den Vorjahren wurden Sicherheitsbedenken gegen das chinesische Unternehmen *Huawei* im Jahr 2018 von westlichen Ländern geäußert, da dieses mittlerweile einer der größten globalen Smartphone-Hersteller und auch einer der größten Infrastrukturanbieter, insbesondere von Funkmasten für Smartphones und anderen Datenverkehr ist[51]. In Deutschland lieferten sie fast 50 Prozent aller Funkmasten, während *Huawei*-Komponenten im deutschen Regierungsnetz trotz Protesten bereits verboten waren. Während die deutsche IT-Sicherheitsorganisation BSI in der technischen Analyse bisher nichts fand, ist die Technik sehr komplex, was eine Verunsicherung hinterlässt.

Die *Huawei*-Problematik eskalierte aus zwei Gründen: Die nächste Internet-Kommunikationsgeneration **5G** kommt, die erstmals eine breite Umsetzung des **Internets der Dinge** und intelligenter Home- und Smart City-Lösungen, insbesondere durch deutlich höhere Datenströme, Echtzeitübertragung, massiv reduzierte Latenzzeiten (Übertragungsverzögerungen) unter 1 Millisekunde und einem reduzierten Energiebedarf für die Übertragung pro Bit ermöglichen wird. Der andere Punkt war die Verhaftung der Finanzchefin von *Huawei* in Kanada wegen vermuteter Verstöße gegen die US-Sanktionen gegen den Iran am 01. Dezember 2018.[52]

[50]vgl. Mayer-Kuckuck/Hauschild 2010, S.28, Wanner 2011, S.8
[51] vgl. Giesen/Mascolo/Tanriverdi 2018
[52] vgl. Giesen/Mascolo/Tanriverdi 2018

In Großbritannien arbeitet *Huawei* mit dem eigens eingerichteten behördlichen *Huawei Cyber Security Evaluation Centre (HCSEC)* zusammen. Während die Zusammenarbeit zwischen Huawei und HCSEC seitens des HCSEC 2019 insgesamt als positiv und transparent bewertet wurde, ist die Anzahl der Schwachstellen in ihren Systemen auf mehrere hundert angestiegen (Punkt 3.11), und selbst bekannte Schwachstellen wurden aufgrund einer raschen Produktentwicklung und -aktualisierung erneut ausgenutzt. Die HCSEC schlug Änderungen von Software bis hin zu Chips vor (Punkt 3.16). Das Problem lag also in einer (zu) schnellen Produktentwicklung[53].

Die Sanktionen der USA gegen *Huawei* 2019 sollen den wachsenden Einfluss von *Huawei* zurückdrängen, so dass die USA auch anderen Ländern raten, Produkte nicht mehr in sicherheitsrelevanten Bereichen einzubauen. *Huawei* ist inzwischen der weltweit führende Mobilfunkausrüster bei der Infrastruktur mit über 30% Marktanteil und hat *Apple* bei den Smartphones überholt. Huawei hat 92 Zulieferer, davon 33 aus den USA, hierzu gehört das Android-System von Google, *Qualcomm*-Chips und *Microsoft*-Anwendungen[54].

1.7.3 Der Trend zur Zentralisierung

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[55]. 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[56], aber auch Gegenstand klassischer Spionage und konventioneller physischer Angriffe sein können[57].

---

[53] vgl. HCSEC 2019
[54] vgl. Müller 2019, S.9
[55] ENISA 2009, S.2; vgl. auch Dugan 2011, S.8
[56] 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.
[57] Zudem können Probleme mit der Stromversorgung Großrechner schwer beschädigen wie im Oktober 2013 im *Utah Data Center*, vgl. Spiegel online 2013b

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.

In der Regel beginnen die Staaten die Verwaltung von Cyber-Angelegenheiten mit der Einrichtung von Cyber-Behörden. In einem zweiten Schritt werden neue Fragen mit der Einrichtung weiterer Behörden angesprochen, die dann zu überlappenden oder unklaren Verantwortlichkeiten führen. Der letzte Schritt ist dann Umstrukturierung und Zentralisierung.

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).[58]

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[59]. 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. Eine Studie des *Electric Power Research Institute* zum EMP ergab jedoch in Simulationen, dass die Explosion einer 1,4 Megatonnen-Bombe in 400 Kilometern Höhe nur regionale Zusammenbrüche des Stromnetzes zur Folge hätte, kein Szenario würde zu einem landesweiten Kollaps führen[60].

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.

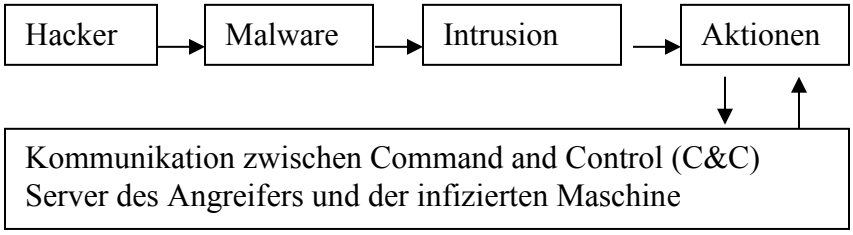
---

[58] vgl. Wilson 2008, S.11
[59] vgl. Morschhäuser 2014, S.1-2
[60] vgl. Rötzer 2018

2.2 Der Angriff auf Computer

2.2.1 Die Grundlagen einer Cyberattacke

Cyber-Angriffe erfordern das Eindringen (**Intrusion**) in das digitale Gerät, d.h. den Computer, Smartphone oder andere Arten von digitalen Geräten mit einem Schadprogramm (Malware) und die Kommunikation mit den intrudierten Geräten, um Aktionen zu starten. Abhängig von der Art der Aktion wird die Kommunikation für eine längere Zeit aufrechterhalten, mitunter auch über Jahre; komplexe Angriffe erfordern in der Regel eine *bidirektionale* Kommunikation, die vielfältige Möglichkeiten zur Erkennung und Zuordnung bietet.



Derzeit sind die häufigsten und herausragenden Cyber-Attacken:

- Malware-Installation für alle Arten von Cyber-Spionage (Militär, Politik, Industrie, Finanzsektor, Forscher, internationale Organisationen etc.). Manchmal ist dies mit der Verwendung von Cyber-Waffen wie **logischen Bomben** und **Wiper-Malware** kombiniert
- Errichtung von Botnetzen, d.h. Gruppen von infizierten und kontrollierten Maschinen, die missbraucht werden, um automatisierte und sinnlose Anfragen an einen Zielcomputer oder -system zu senden, das dann zusammenbricht (verteilte = distributed Denial-of-Service-Angriffe, kurz **DDoS-Angriffe**). Dies kann aus politischen Gründen geschehen, aber auch, um das Opfer im Rahmen der Cyberkriminalität zu erpressen
- Die Installation von Crimeware wie **Ransomware**, die das Gerät verschlüsselt, woraufhin vom Opfer Geld für den Entschlüsselungscode verlangt wird, und Banking-Trojaner, um Zugang zu Online-Banking-Konten zu erhalten.

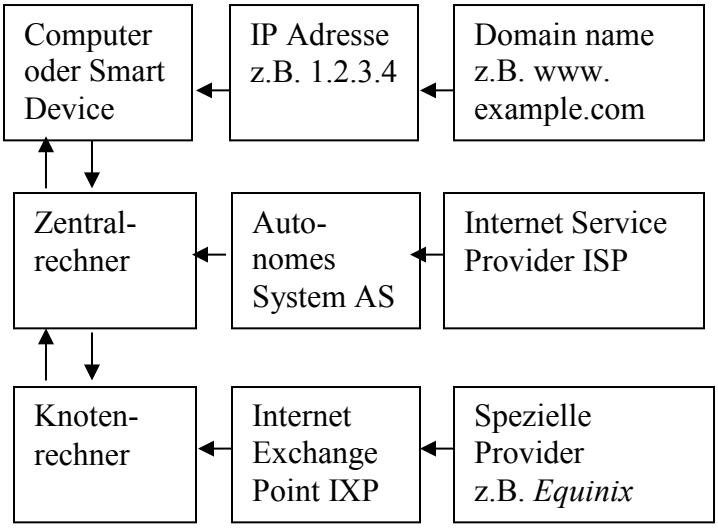
2.2.2 Kommunikationswege der Cyberattacken

Daten, d.h. Bits und Bytes sind nicht vollständig virtuell, sondern sind immer noch physikalisch als definierter elektromagnetischer Zustand auf Speichermedien und Gerätespeichersystemen vorhanden[61]. Die drahtlose Übertragung führt zu elektromagnetischen Wellen und schließlich enden diese Wellen am Ende wieder

[61] Dies mag trivial erscheinen, aber bedeutet das gelöschte Daten auf einem Gerät **nicht ausradiert** sind. Das Gerät markiert die Datei nur als 'gelöscht' und sie erscheint nicht mehr auf dem Bildschirm. In Wirklichkeit befinden sich die Daten weiterhin auf dem Speichermedium, so dass "gelöschte" Daten mit Hilfe forensischer und Spionage-Techniken wiederhergestellt werden können.

physisch in Geräten. Dieser Befund ist für die Erkennung und Zuordnung essentiell. Da die Kommunikation über Computer-Netzwerke erfolgt, ist es hilfreich, die allgemeine Infrastruktur des Internets im Auge zu behalten: Diese Struktur bildet auch das 'digitale Ökosystem' der Hacker, das im nächsten Abschnitt dargestellt wird.

Vereinfachtes Modell der Internetkommunikation



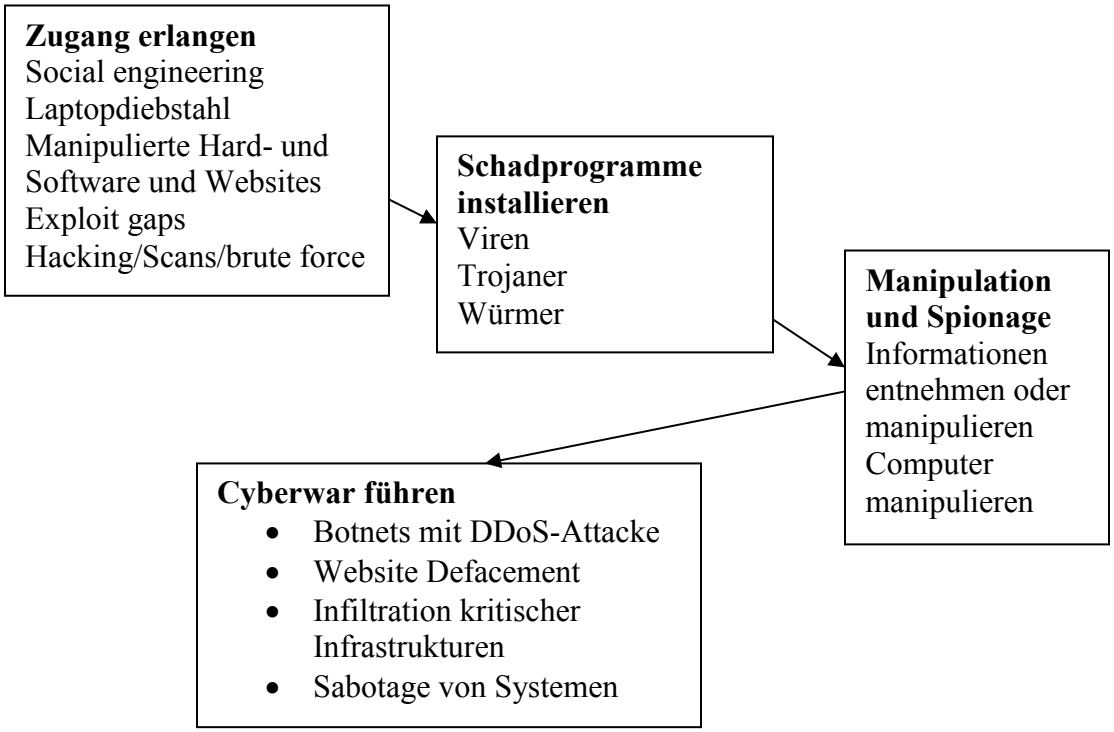
Typischerweise startet eine Internetkommunikation bei einem bestimmten Computer und die Daten werden dann an den zentralen Rechner eines **Internet Service Providers (ISP)** übertragen. Dieser zentrale Computer wird offiziell als **Autonomes System (AS)** bezeichnet und große Anbieter können viele davon haben. Allerdings müssen die Internet Service Provider miteinander verbunden sein, dies geschieht über Knotencomputer, die offiziell als **Internet Exchange Point (IXP)** bezeichnet werden. In Wirklichkeit sind dies große Rechenzentren und nicht nur einzelne Computer.

Jeder Computer, der mit dem Internet verbunden ist, hat eine **IP-Adresse (IP = Internetprotokoll)**, eine nach bestimmten Regeln strukturierte Zahl. Das alte 4-stellige System der IP-Version 4 wird nun durch größere Bausteine der IP-Version 6 ersetzt, aber das Prinzip, dass eine Domain mit einer IP-Adressnummer zu einem bestimmten Zeitpunkt verknüpft ist, bleibt gleich. Dies hat die gleiche Funktion wie Telefonnummern für Telefone, d.h. die technische Möglichkeit, Sender und Ziel richtig zu verbinden.
Webseiten haben auch IP-Adressen, aber stattdessen werden normalerweise **Domain-Namen** verwendet, z.B. www.example.com. Zu einem definierten Zeitpunkt beziehen sich Domainnamen jeweils auf bestimmte IP-Adressen, um Kommunikationsverwechslungen zu vermeiden.

Infolgedessen mag das Internet im Alltag dezentral und virtuell erscheinen und es scheint fast sinnlos, herauszufinden, woher ein Cyberangriff kam.
In der physischen Welt ist das Internet jedoch am Ende an ein physisches Netzwerk mit einer signifikanten Zentralisierung gebunden. Das US-amerikanische Unternehmen *Equinix* steuert mit eigenen IXPs und Co-Location von Client-Computern in ihren Rechenzentren rund 90% (!) der Datenübertragung des Internets[62]. Wie im folgenden gezeigt wird, bietet dies Möglichkeiten, Einblick in die Infrastruktur des Gegners zu bekommen.

2.2.3 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[63].



[62] vgl. Müller 2016, S.7
[63] vgl. Northrop Grumman TASC 2004

2.2.3.1 Einführung

Die Expansion der Angriffsziele

Früher	Heute
Computer	Zubehör: Maus, Drucker, Router, USB-Sticks Smartphones/iPhones Smart home: Internet der Dinge Infrastruktur: Zugang zu nationalen Servern, Anzapfen von Internetknoten, Umleitung und Kopieren des Datenverkehrs, Tiefseekabel anzapfen, Attacken auf Clouds, 5G-Sendemasten
Software	Hardware (Fuzzing), Firmware, Add-on Chips
Hacken/Virus	Interdiction (Abfangen), Diebstahl, ‚Virus ab Werk'
User	Datensammlung auf Vorrat („alles von allen")
	Höhere Ebenen: Bankkunden > Bank > Interbankensystem
	Attacken auf Drittfirmen, Zulieferer und Wartungssysteme, Help Desks und Vertragsmitarbeiter

In der Zeit um 2000 beschränkten sich Computerattacken oft darauf, dass ein Hacker einen Computer angriff, um dessen Software (Programme) beeinflussen zu können, um so an einen User heranzukommen. Die Angriffsziele sind seither massiv expandiert. Heute werden neben dem Computer auch Zubehörteile infiziert, selbst die Maus. Der Trend geht vom Computer zum Smartphone als neues digitales Key-Gerät (E-Mail, *Smart House, BYOD, COPE*, Smart Car, Online-Zahlung). Die Schwachstellenfunde bei Smartphones und iPhones nehmen ständig zu, bösartige Apps sind ein besonderes Problem. Im *Smart Home* wird vom Kühlschrank bis zu den Babyphonen alles attackiert. Neben der Software stehen nun auch Chips, die fest eingebauten Programme der sogenannten **Firmware**, aber auch die Platinen im Vordergrund, wo es Berichte über heimlich zusätzlich eingebaute Elemente als **Add-on**-Minichips gab, die von der betroffenen Firma *Apple* dementiert wurden, die aber zumindest technisch machbar erscheinen (Details und Literatur siehe folgende Abschnitte).

Nachdem lange Zeit die Vorstellung des Cyberspace als virtueller Welt dominierte, setzt sich in Sicherheitskreisen ein immer physischeres Verständnis durch: wer die Geräte und die Leitungen kontrolliert, der kontrolliert auch die darin befindlichen Daten. Deshalb verlangt man die Aufstellung von Computern im eigenen Land, zapft Tiefseekabel an oder leitet mit strategisch platzierten Knotenrechnern den Datenverkehr um mit dem sogenannten **Border Gateway Protocol hijack**. US-Studien haben gezeigt, dass der gesamte Datenverkehr von Staaten auf diese Weise schon wochenlang umgeleitet und kopiert wurde, im Prinzip aber auch vernichtet werden könnte. Große Speicherrechner, die Clouds, werden auch schon angegriffen, und in Zukunft wird die **Resilienz**, also die Aufrechterhaltung der Funktionsfähigkeit bei Störungen oder Angriffen gerade bei der kommenden 5G-Technologie von herausragender Bedeutung sein.

Man muss auch nicht mehr unbedingt hacken, man kann auch Postpakete mit Geräten abfangen und diese manipulieren (**Interdiction**) oder Computer, CDs und USB Sticks einfach klauen, das britische Verteidigungsministerium vermisste in den letzten Jahren gleich mehrere hundert[64], manche Firmen liefern bei Billighandys das Virus gleich mit. Der einzelne User ist kaum noch interessant, heute sammelt man lieber alles von allen, inzwischen auch Hacken und Datensammeln auf Vorrat für zukünftige Aktivitäten (Smartphones, Internet der Dinge, Krankenhäuser, Bankkonten usw.)[65] Statt Einzelkunden raubt man lieber die Bank selber aus, so wie die *Carbanak*-Gruppe, die ca. 1 Milliarde Euro erbeutete oder man manipuliert den Austausch zwischen Banken, wie es die nordkoreanische Hackergruppe *Lazarus* vormachte1, siehe Abschnitt 5.
Für die Unternehmen ist wesentlich, dass Hacker zunehmend auf Zulieferer und Wartungssysteme sowie auf Serviceprovider zielen, so dass man sich mit der anderen Firma auch gleich den Infekt mit ins Haus holt.
Nicht alle Methoden haben sich gewandelt: automatische Kontaktversuche mit Suche nach offenen Kommunikationskanälen (**Portscans**) sind nach wie vor bedeutsam. Das wäre so, als wenn man alle Telefonnummern ausprobiert und mal schaut, wer drangeht. Passwortraten übernehmen Maschinen, diese Brechstangenmethode heißt auch **brute force**.

2.2.3.2 Zugang erlangen

Der Zugang kann auf verschiedenste Weise erlangt werden, insbesondere durch:

- **Phishing** in Verbindung mit **Social Engineering**
- **Infizierte Websites**
- **Backchannels**
- **Exploits**, d.h. Gebrauch von Schwachstellen, **Backdoors** und **Bugdoors**
- **Infizierte Speichermedien** und digitale Geräte wie Router
- **Infizierte Software** zum Download wie Apps und Updates
- **Hacken von Passwörtern**
- **Physikalische Maßnahmen** wie **Interdiction** und **Diebstahl** von Computern und Smartphones
- **Gefälschte Mikrochips**
- **Firmware-Infektionen**
- **Veränderte Platinen (motherboards)**
- **Fuzzing**
- **Vorverschlüsselungszugriff** auf Server

[64] vgl. Zeit online 2016b
[65] So wie der MySpace Hack mit 360 Millionen Passwörtern im Jahr 2016 und der Yahoo Hack im Jahr 2014 mit 500 Millionen Benutzerkonten, vgl. Hern/Gibbs 2017

- Falsch konfigurierte Internet-Server **(BGP Hijacking)**

- **Phishing** in Verbindung mit **Social Engineering**

Immer häufiger versucht man, durch manipulierte e-Mails mit präparierten Anhängen oder Internetseiten Zugang zu erlangen. 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.

Irreführung von Computernutzern erfolgt durch **social engineering**, bei denen man den Nutzern unter einem Vorwand z.B. als falscher ‚Administrator' Zugangsdaten wie das Passwort entlockt (oder z.B. auch falsche CEOs/Top-Manager, die um Ausführung von Geldtransfers bitten, bekannt auch als '**CEO fraud**'). Social engineering mittels Telefonanrufen wird auch als **Vishing (Voice Phishing)** bezeichnet. Ein ehemaliger NSA-Agent hat in Studien gefunden, dass 14% der Phishing-Angriffe erfolgreich sind, manchmal sogar mehr. Ein Trick ist, minimale Variationen echter Namen von Webseiten zu machen, z.B. ein Buchstabe groß statt klein, eine Methode, die als **typosquatting** bekannt ist. Bei größeren Angriffen wurde die erste E-Mail nach 2 Minuten geöffnet und der erste Anhang wurde nach 4 Minuten geöffnet.[66]

Aber auch **Insider**, insbesondere solche mit IT-Kenntnissen, können die Sicherheitsmaßnahmen einer Organisation überwinden, was später noch näher diskutiert wird.
Eine zunehmend verwendete Technik besteht im Angriff auf einfache Angestellte, um von da aus an Administratorenrechte zu gelangen (**lateral movement**). Infolgedessen sammeln Cyberangreifer inzwischen immer systematischer Personaldaten, um relevante und/oder verwundbare und/oder mit Sicherheitsfragen befasste Zielpersonen zu identifizieren.[67]

[66] vgl. Schmieder 2017, S.74

[67] 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 Vergabe von sensiblen Aufträgen an externe IT-Anbieter birgt Risiken durch Bildung zusätzlicher Schnittstellen, die von Angreifern ausgenutzt werden können[68]. Zudem droht der Verlust interner IT-Kompetenz.

- **Infizierte Websites**

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.

- **Backchannels**

Die *Efail*-Verwundbarkeit wurde 2018 entdeckt und verwendet HTML-basierte Backchannels. Ein **Backchannel** ist hier eine Methode, um den E-Mail-Client zu zwingen, eine externe URL aufzurufen, z.B. um ein Bild herunterzuladen. *Open Pretty Good Privacy (PGP)* verwendet ausschließlich den *Cipher Feedback-Modus (CFB)* und die *Encryption Methods Secure/Multipurpose Internet Email Extensions (S/MIME)* und den *Cipher Block Chaining Mode (CBC)* für den Betrieb. Bösartige CFB/CBC-Tools können für Angriffe verwendet werden. Der Angreifer muss die verschlüsselte Nachricht in Klartext-MIME-Teile mit einem HTML-basierten Backchannel einbetten, der entschlüsselte Text wird dann über einen HTML-Link an die Angreifer zurückgegeben, wenn HTML im E-Mail-Programm erlaubt ist[69]. Dies funktionierte nicht bei allen, aber vielen getesteten E-Mail-Clients.

- **Exploits**, d.h. Gebrauch von Schwachstellen, **Backdoors** und **Bugdoors**

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 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].

---

[68] 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

[69] vgl. Siegel 2018a, S.20, Poddebniak et al. 2018

[70] Ein Portscanner überprüft, welche Dienste ein System über das Internetprotokoll anbietet, und welches Antwortverhalten es zeigt.

[71] vgl. Kurz 2013, S.31

Es gibt immer wieder Debatten wegen schon vorher eingebauter Hintertüren (‘**backdoors**’[72]), 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[73]. 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.

- **Infizierte Speichermedien** und digitale Geräte wie Router

Die Platzierung von Schadprogrammen kann aber auch durch das Einlegen **infizierter Datenträger** (früher Disketten, heute insbesondere infizierte DVDs und USB-Sticks) geschehen, so geschahen die Infektionen mit *agent.btz* und mit *Stuxnet* durch USB-Sticks. Auch die **IT-Umgebung** kann für Eindringversuche genutzt werden, wie z.B. Router[74], kabellose Mäuse und Drucker. Zunehmend werden Netzwerkdrucker und Multifunktionsdrucker (MFPs) angegriffen, was das Abfangen der Daten oder das erneute Ausdrucken von Dokumenten ermöglicht[75]. Router wurden z.B. während der *Mirai*-Attacke Ende 2016 angegriffen.
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[76], 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[77]. Auch wenn die technischen Details unbekannt sind, haben Forscher gezeigt, wie ein akustisches, auf hochfrequenten Audiosignalen beruhendes verdecktes Computernetzwerk errichtet werden kann, das sogar keylogging über mehrere Stationen erlaubt[78]. 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 [79] als Einfallstor genutzt werden.

---

[72] 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
[73] Die Welt 10 Januar 2007
[74] vgl. Handelsblatt 2014 b, S.23
[75] vgl. Dörfler 2015, S.P4
[76] vgl. Betschon 2013b, S.34
[77] vgl. Winker 2014a, S.3
[78] vgl. Hanspach/Goertz 2013, S.758 ff.
[79] Durch manipulierte Videodateien, vgl. Schmundt 2014, S.128

- **Infizierte Software** zum Download wie Apps und Updates

Ein weiteres 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[80].

- Ausprobieren (**Hacken**) von Passwörtern, wobei dies inzwischen auch automatisiert unter Einsatz großer Rechnerkapazitäten (brute force) erfolgt

- **Physikalische Maßnahmen** wie **Interdiction** und **Diebstahl** von Computern und Smartphones

Eine weitere Methode ist die **interdiction**, d.h. der Austausch von verschickten CD-ROMs und anderen physischen Medien durch infizierte Datenträger.
Das britische Verteidigungsministerium berichtete über den unerklärlichen Verlust von 759 Laptops und Computern und 32 Computer wurden definitiv innerhalb von 18 Monaten gestohlen. Von Mai 2015 bis Oktober 2016 gingen 328 CDs, DVDs und USB-Sticks verloren[81].

- **Gefälschte Mikrochips**

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. 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[82]. Nicht nur Hersteller, sondern auch die globalen Lieferketten bilden mögliche Angriffspunkte[83]: eine Studie des US-Senats von 2012 berichtete, dass in US-Waffen mehr als eine Million gefälschter Chips installiert wurden, 70% der Chips kamen aus China, aber relevante Mengen stammten auch aus Großbritannien und Kanada[84]. Da jeder Chip minimale Konstruktionsunterschiede aufweist, können diese Unterschiede gemessen und als einzigartiger Fingerabdruck genutzt werden, als sogenannte **Physically Unclonable Function (PUF)** [85].

---

[80] vgl. T-online 2015
[81] vgl. Zeit online 2016b
[82] 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
[83] vgl. USAF 2010a, S.5
[84] vgl. Fahrion 2012, S.1
[85] vgl. Betschon 2016, S.39

- **Firmware-Infektionen**

Die Anti-Diebstahl-Software *LoJack* der Firma *Absolute Software*, implementiert ein UEFI/BIOS-Firmware-Modul, um seine Entfernung zu verhindern und erschien in trojanisierten Versionen seit mindestens Anfang 2017. Die bösartigen Versionen sind jetzt als *LoJax* bekannt, die wie *LoJack* sehr tief in das Computersystem eingebettet sind und deshalb persistieren[86].

- **Veränderte Platinen (motherboards)**

Die Firma *Super Micro* ist ein Anbieter von Server-Motherboards (Platinen). Während einer Evaluation des Software-Unternehmens *Elemental Technologies* durch *Amazon Web Services (AWS)* wurde ein winziger Mikrochip gefunden, ein bisschen größer als ein Reiskorn, und der nicht Teil des ursprünglichen Designs war. [87]. Das war kritisch, denn *Elemental Technologies*, die seit 2009 Entwicklungspartner der CIA-Firma *In-Q-Tel* ist, stellte Server für die DoD-Rechenzentren, die Drohnenoperationen der CIA und für Kriegsschiffe zur Verfügung. Auch Tausende Apple-Server wurden kompromittiert.
Außerdem produziert China 75 Prozent der Mobiltelefone und 90 Prozent aller PCs, da selbst US-Unternehmen diesen Produktionsschritt nach China auslagern. Laut dem *Bloomberg*-Bericht könnten Subunternehmer in China von der Hardware-Hacking-Einheit der chinesischen PLA unter Druck gesetzt worden sein, diese zusätzlichen Chips einzubauen, die eine totale Hintergrundkontrolle ermöglichen würden[88]. Alle Akteure, darunter *Amazon* und *Super Micro*, dementierten energisch. *Bloomberg* bestand jedoch auf der Richtigkeit des Berichts, denn sie stünden in Kontakt mit 17 Insidern, darunter auch nationale Sicherheitsbeamte, *Amazon*- und *Apple*-Insider. Konkrete Diskussionen innerhalb des Weißen Hauses begannen 2014 und Apple tauschte stillschweigend mehr als 7.000 Server aus (Apple dementierte dies).

- **Fuzzing**

Beim Fuzzing werden systematisch mögliche Befehle an die Software bzw. an die Hardware abgearbeitet, auch ohne konkreten Anhaltspunkt für irgendwelche Schwachstellen. Die Zahl der gefundenen Schwachstellen, Dokumentations- und Konstruktionsfehler war bei ersten Tests 2017 erheblich, insbesondere bei den Zentralprozessoren (**Central Processing Unit CPU**), also den Computerchips.

Die 2017 entdeckten und 2018 publizierten CPU-Schwachstellen *Meltdown* und *Spectre* sind nur ein kleiner Teil des Problems. Die USA vermeiden, wie schon erwähnt, die Nutzung chinesischer Chips in der Waffentechnologie, dennoch

[86] vgl. ESET 2018
[87] vgl. Robertson/Riley 2018
[88] vgl. Robertson/Riley 2018

kursieren zahlreiche gefälschte Chips, d.h. was beim echten Chip in Ordnung ist, kann in der gefälschten Version noch weitere absichtliche oder unabsichtliche Schwachstellen enthalten.

Als **Superbugs** bezeichnet man solche Schwachstellen, die wesentliche Teile des Internets betreffen können und die häufig wegen des damit verbundenen Aufwandes nicht mehr völlig geschlossen können.
Bekannte Superbugs neben *Meltdown* und *Spectre* sind[89] die *Heartbleed Open SSL Lücke* von 2014, die immer noch aktiv ist, ebenso *Shellshock* von 2014 im Linux-Betriebssystem, die auf hunderten Millionen Geräten immer noch aktiv ist. Ebenso kann der im Oktober 2017 gefundene sogenannte *Krack error* in dem für Router wichtigen *WPA2-encrytion standard* wohl nicht auf allen Geräten geschlossen werden.

Software Fuzzing: Beim **grammar-based software fuzzing** werden zur Programmiersprache passende Befehle der Reihe nach abgearbeitet, um mögliche Fehler bzw. Fehlreaktionen zu erkennen. Seit 2011 hat der Software Fuzzing-Forscher Holler rund 4.000 Schwachstellen entdeckt[90].

Hardware Fuzzing: Während *Meltdown* und *Spectre* aufgrund theoretischer Überlegungen und Selbsthackversuche von Grazer Forschern gefunden wurden, wurden parallel dazu zahlreiche weitere Fehler entdeckt. [91]
Der Hardware-Fuzzer *Sandsifter* kann 100 Millionen Bytekombinationen an einem Tag abarbeiten[92]. In einem ersten Test fand er in drei Chips (*Intel Core, Advanced Micro Devices AMD-Athlon, Via Nano*) zahlreiche undokumentierte Befehle und zahlreiche Hardware-Bugs, insbesondere einen Befehl "*halt and catch fire*", der den Prozessor zur Einstellung seiner Arbeit zwingt. Forscher der Universität Bochum zeigten außerdem, dass es möglich ist, CPUs der Marke AMD nachträglich mit Trojanern zu infizieren und diese über Updates einzuschleusen, eine Entdeckung ist danach selbst durch Fuzzing kaum möglich.

Meltdown/Spectre
Der spätere *Meltdown*-Patch *Kaiser (Kernel Address Isolation)* wurde bereits im Mai 2017 aufgrund theoretischer Vorüberlegungen entwickelt durch dasselbe Grazer Forscherteam, das später *Meltdown* und *Spectre* entdeckte. Die Forscher hatten sich selber gehackt und konnten problemlos auf Server, Clouds, Passwörter, Fotos usw. zugreifen[93].

[89] vgl. Fuest 2018
[90] vgl. Asendorpf 2017
[91] vgl. Schmidt 2017, FAZ 2018a
[92] vgl. Schmidt 2017
[93] vgl. FAZ 2018, RP online 2018

Die Entdeckung wurde 2017 zunächst geheim gehalten, um den Herstellern die Möglichkeit zum Lückenschluss zu geben, jedoch fiel Fachleuten die Hektik bei den Updates auf. [94]
Die Lücke *Meltdown*, die nur *Intel*-Prozessoren betrifft, erlaubt u.a. das unprivilegierte Auslesen von Kernel Memory, d.h. Zugriff auf die innersten Informationen, und das Ausbrechen aus virtuellen Maschinen. Die Abwehrmethode **Page Table Isolation (PTI)** bzw. der spätere Meltdown-Patch *Kaiser (Kernel Address Isolation)* trennen die einzelnen Bereiche besser und schützen so die Information[95].
Die Lücke *Spectre* betrifft Prozessoren der Computer und Smartphones von *Intel, Advanced Micro Devices (AMD)* und *ARM Holdings*. Bei der **speculative execution** stellen die Prozessoren vorab Berechnungen an, um diese im Bedarfsfall sofort bereithalten zu können, was die Rechengeschwindigkeit deutlich steigert. Durch eine **Seitenkanalattacke**, z.B. ein malignes Javascript im Browser, ist der Zugriff auf die Informationen möglich, die im Rahmen der speculative execution bereitgehalten werden, wenngleich auch nur in sehr engen Zeitfenstern (**Timing-Attacke**). Die Schutzmaßnahmen umfassen zahlreiche Einzeländerungen, die die Prozesse besser trennen und die getimten Attacken auf die speculative execution erschweren[96].

Bei Spectre handelt es sich strenggenommen um zwei Lücken, *Spectre-1* CVE-2017-5753 (*bounds check bypass, spectre-v1*) und *Spectre-2* CVE-2017-5715 (*branch target injection, spectre-v2*), die jeweils mit gesonderten Gegenmaßnahmen behandelt werden müssen. *Spectre-2* erfordert auch Änderungen an der Firmware.

Die bisher erfolgten Lückenschlüsse für *Meltdown/Spectre* bergen das Risiko einer Verlangsamung der CPUs[97].

Das US-CERT berichtete im März 2018 über neue Varianten von *Meltdown* (ein Fehler, der erzwungene Sicherheitsgrenzen in Hardware zusammenschmilzt), während *Spectre* ein Fehler ist, der eine CPU zwingen kann, ihre Informationen preiszugeben. *SpectrePrime* und *MeltdownPrime* sind keine wirklich neuen Lücken, aber einige Chips erlauben automatisierte Angriffe mit *Meltdown* und *Spectre*, für *Spectre* wurde dies bereits erfolgreich getestet[98].
2018 wurden weitere Lücken entdeckt mit einer eigenen **CVE (Common Vulnerability Enumerator)**-Nummer, bis August 2018 waren es insgesamt zehn Lücken, u.a. *Spectre Next Generation (Spectre NG)*; diese betreffen Intel. Eine der

[94] vgl. Weber 2018
[95] vgl. Weber 2018
[96] vgl. Weber 2018
[97] vgl. Leyden/Williams 2018
[98] vgl. Scherschel 2018

Lücken erlaubt es, von der virtuellen Maschine auf die Cloud vorzudringen, oder andere virtuelle Maschinen direkt zu attackieren, bekannt als *Spectre NG*[99].
Speculative bypass ist eine neue Variante, bei der ein Angreifer ältere Speicherwerte in einem CPU-Stack oder einem anderen Ort lesen kann. Die *Foreshadow-Lücke (L1 Terminal Fault)* erlaubt es, Daten aus dem Intel-Level-1-Cache zu extrahieren, der die Berechnungsprozesse koordiniert.[100]

Hacker haben 2019 Zugriff auf den in Intel-Chips integrierten Logikanalysator *Visualization of Internet Signals Architecture (Visa)* erlangt, der Möglichkeiten zu tiefergehenden Analysen des Chips ermöglicht[101].

- **Vorverschlüsselungszugriff** auf Server

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[102].

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[103]. 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[104] *eventuell* auch indirekt für die Dienste anderer Staaten gilt und ein zero day-exploit in Wirklichkeit eventuell keineswegs ‘zero’ ist. Zusammen mit der Überwachung des Informationsflusses[105] 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

[99] vgl. CT2018
[100] vgl. Betschon 2018b, S.37
[101] vgl. Grüner 2019
[102] vgl. Schlüter/Laube 2010, S.8
[103] vgl. FAZ 2013a, S.1
[104] 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.
[105] 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.

könnten die eigenen User und Firmen nehmen[106]. Im Jahr 2015 publizierte die NSA 91% der gefundenen Schwachstellen[107].

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[108]. Die nationalen Zugriffsrechte haben aber zur Folge, dass man sich mit einer ausländischen oder internationalen IT-Plattform auch die anderen Nachrichtendienste ins Haus holt[109].
In Überstimmung mit den jeweils gültigen nationalen Gesetzen, wie z.B. dem 1994 *Communications Assistance for Law Enforcement Act (CALEA),* das mit der Öffnung des Internets für die Allgemeinheit 1994 in Kraft trat, und dem *Foreign Intelligence Surveillance Act (FISA)* in den USA, geben Provider ggf. Zugang zu Daten oder Systemen. Der *US Patriot Act* enthält weitere Vorgaben für Internetprovider.
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.

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 [110] 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[111].

---

[106] Daniel zitiert von Abendzeitung 2014
[107] vgl. Perloth/Sanger 2017
[108] 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.
[109] vgl. Scheidges 2010, S.12-13
[110] 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
[111] 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.

- **Falsch konfigurierte Internet-Server (BGP Hijacking)**

Wie in Abschnitt 2.2.2 oben gezeigt, spielen **Autonome Systeme (AS)** eine Schlüsselrolle, da es sich um die zentralen Server von **Internet Service Providern (ISPs)** handelt und jedes AS eine Reihe von IP-Adressen kontrolliert, die in konsekutiven Blöcken zugewiesen werden. Jeder Router überprüft die Ziel-IP-Adresse in einem übertragenen Datenpaket und leitet sie an die nächstgelegenen AS weiter, basierend auf Weiterleitungstabellen, die den besten (nächsten) AS-Server für ein bestimmtes Datenpaket anzeigen. Diese Tabellen werden von den AS-Administratoren mit dem **Border Gateway Protocol (BGP)** erstellt und zeigen, ob ihr AS-Server ein geeignetes Ziel oder ein Transit-Knoten sein kann.

Wenn ein AS durch das BGP den Besitz eines IP-Blocks anzeigt, der in Wirklichkeit einem anderen AS gehört, wird zumindest ein Teil der Daten auf und über das falsche AS geleitet. Dies kann durch Fehler geschehen oder böswillig, was dann als **BGP-Hijack** bezeichnet wird[112]. Das Umleiten ermöglicht das unentdeckte Kopieren der Daten oder sogar deren Beseitigung aus dem Verkehr. Die Umleitung und das Kopieren können ggf. nur zu minimalen und wahrscheinlich unentdeckten Verzögerungen bei Datenverbindungen führen.

China Telecom verfügt in Nordamerika über zehn Internet-**Points of Presence (PoPs)**, d.h. wichtige Verbindungsstellen, an denen sich ein Fernkommunikationsträger mit einem lokalen Netzwerk verbindet[113], davon acht in den USA und zwei in Kanada; dazu kommen weitere Server in Europa, wie in Frankfurt/Deutschland.

Mehrere temporäre Ereignisse wurden beobachtet, die viel zu lang und zu groß waren, um technische Fehler zu sein, darunter eine Übernahme von 15% des Internetverkehrs für 18 Minuten durch China Telecom am 08. April 2010 und weitere Umleitungen des Datenverkehrs über China von Kanada nach Korea und USA nach Italien in 2016, sowie von Skandinavien nach Japan und Italien nach Thailand in 2017 als klassische Fälle von **Man-in-the-middle (MITM)**-Angriffen[114].

Jedoch könnte eine geplante Umleitung des Datenverkehrs zwischen nationalen Internetknoten eine defensive Abkopplung des nationalen Internets vom globalen Netz erlauben; Russland plant einen Test in 2019[115].

[112] Vgl. Demchak/Shavitt 2018
[113] vgl. Demchak/Shavitt 2018
[114] vgl. Demchak/Shavitt 2018
[115] vgl. Ma 2019

2.2.3.3 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.

Typische Ziele sind:

- Malware-Installation für alle Arten von Cyber-Spionage (Militär, Politik, Industrie, Finanzsektor, Forscher, internationale Organisationen etc.). Manchmal ist dies mit der Verwendung von Cyber-Waffen wie **logischen Bomben** und **Wiper-Malware** kombiniert
- Errichtung von Botnetzen, d.h. Gruppen von infizierten und kontrollierten Maschinen, die missbraucht werden, um automatisierte und sinnlose Anfragen an einen Zielcomputer oder -system zu senden, das dann zusammenbricht (verteilte = distributed Denial-of-Service-Angriffe, kurz **DDoS-Angriffe**). Dies kann aus politischen Gründen geschehen, aber auch, um das Opfer im Rahmen der Cyberkriminalität zu erpressen
- Die Installation von Crimeware wie **Ransomware**, die das Gerät verschlüsselt, woraufhin vom Opfer Geld für den Entschlüsselungscode verlangt wird, und Banking-Trojaner, um Zugang zu Online-Banking-Konten zu erhalten.

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.

Cyberwaffen sind demnach Softwareprogramme, mit deren Hilfe man andere Computer angreifen, infiltrieren, ausspionieren und manipulieren kann und die ihre Ausbreitung selbsttätig steuern können. Der Ausdruck ‚Cyberwaffe' soll nicht suggerieren, dass es sich um ein militärisches Instrument handelt, denn auch hier gibt es keinen substantiellen technischen Unterschied zu der Software, die im Bereich der Cyberkriminalität eingesetzt wird.

2.2.3.4 Cyberspionage-Tools

Hochentwickelte Cyberspionage-Programme nehmen an Häufigkeit zu, so dass die bisherige Einteilung in Viren, Würmer und Trojanern langsam an Bedeutung verliert.

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[116] und **Rootkits** (Programme, die dem Angreifer das heimliche Einloggen und Steuern des Computers ermöglichen).
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.

[116] vgl. Stark 2009, Schmitt 2009, S.83

2.2.3.5 Offensive Cyberwaffen

Was?	Wofür?
falsche Signale	GPS Spoofing: Irreführung von Drohnen, Schiffen etc.
	Täuschkörper: Attrappen zur Irreleitung autonomer Systeme, neue Form der Tarnbemalung mit großen kontrastarmen Pixeln
	20 kHz-Befehle: Ultraschallbefehle zur Fern-Manipulation von Heimlautsprechern
Botnetze	Überflutung mit Anfragen und Daten kann Computer bzw. Netzwerke lahmlegen
logische Bomben	Schadprogramme, die erst nach einer bestimmten Zeit oder bestimmten Handlung aktiv werden
Textbomben	Schwer zu interpretierende Symbole, die den Chip überlasten und zum Absturz bringen
Wiper-Malware	Löschprogramme, die Dateien des infizierten Computers löschen
Bricking	Programme, die bei smarten Geräten wichtige Steuerdateien mit Nullen überschreiben und so das Gerät unbrauchbar machen
Ransomware	Sperrbildschirme, für deren Entsperrung Geld verlangt wird (Ransom=Erpressung): Immer häufiger als destruktive Ransomware, d.h. der Bildschirm lässt sich gar nicht mehr entsperren
Fuzzing	Zufallskommandos an Chips, die diesen aufgrund von Designlücken zur Datenfreigabe bringen oder gar endgültig abschalten (halt and catch fire)
	=> digitaler Rettungsschuss ist technisch möglich, latente Gefahr der ‚Abschaltung' durch Gegner im Gefechtsfall

Offensive Cyber-Waffen mit Zerstörungspotential sind:

- **Spoofing:** Irreführung von GPS-gesteuerte Systemen, indem sie ein falsches GPS-Signal senden, das das richtige Signal überlagert, z.B. gegen Drohnen oder Schiffe
- **Home Assistants** erwiesen sich dagegen für stille Befehle im nicht mehr hörbaren 20 Kilohertz-Bereich anfällig, Täuschkörper wie Aufkleber oder Bilder eignen sich zur Verwirrung autonomer Fahrzeuge. Kleine Aufkleber auf der Straße reichten aus, um den Autopiloten eines *Tesla*-Fahrzeuges auf die Gegenfahrbahn zu lenken[117]. Geeignete Attrappen würden sicherlich auch autonome Kampfdrohnen irreführen können, um sie in Ruhe auszuschalten können. Inzwischen finden sich gepixelte Tarnbemalungen zum Beispiel auf modernen chinesischen Militärfahrzeugen, aber auch auf russischen Helikoptern[118].
- **Distributed Denial of Service (DDoS)-Attacken** mit **Botnetzen,** d.h. manipulierte Computer, Smartphones und andere smarte Geräte werden genutzt, um einen Zielcomputer oder Netzwerk mit sinnlosen Anfragen zu überfluten
- **Logikbomben:** Malware, die bis zum Erreichen eines vordefinierten Zeitpunktes ruht, was gleichzeitige Angriffe auf eine große Anzahl von Zielen ermöglicht

[117] vgl. FAS 2019, S.21
[118] vgl. Marquina 2019

- **Textbomben:** Das Versenden von Nachrichten oder Symbolen, die schwer zu interpretieren sind und zu Computerabstürzen führen. Ein Beispiel ist der *Black Dot-Bug*, bei dem ein großer schwarzer Punkt in Klammern zum Absturz der iOS11-News-App führt. Ein ähnlicher Fehler wurde bereits bei *Android* beobachtet[119]. Eine spezielle Nachricht kann einen Absturz des *Play Station4*-Systems verursachen[120].
- **Wiper-Malware**: zerstört Daten durch Löschung, kann das Zielsystem beschädigen, wenn wesentliche Daten und Funktionen betroffen sind
- **Bricking:** Angriffe auf smarte Geräte, gibt Anweisungen, um Einstellungen zu ändern und oder überschreibt die Firmware, was zu einer faktischen Zerstörung des Gerätes führt
- **Ransomware:** Malware, die Dateien verschlüsselt. Die Opfer werden typischerweise aufgefordert, Lösegeld für die Entschlüsselung zu zahlen, aber Anfang 2017 wurde Ransomware in Pakistan bei einem Angriff ohne das Angebot zur Entschlüsselung verwendet, d.h. nur um den Computer unbrauchbar zu machen
- **Kombinierte Waffen:** Bei Smart Grid-Attacken wurden Kombinationen von Beachheads, Manipulationssoftware und Wipern von *BlackEnergy* und *Industroyer/CrashOverride* verwendet
- **Fuzzing:** Die vielleicht stärkste Cyberwaffe ist das Fuzzing, das Verschicken von Zufallscodes an Chips, das militärisch weitreichende Konsequenzen hat: die USA haben um 2007 die Verwendung chinesischer Chips in den Waffensystemen gestoppt, aus Furcht im Gefecht abgeschaltet werden zu können. Weiter oben wurde bereits gezeigt, dass viele Chips störanfällig durch Fuzzing sind. Die Chiphersteller versuchen, die Lücken zu schließen, es werden aber ständig neue entdeckt. So sollten Chips in der existierenden Militärtechnik intensiv getestet werden, damit nicht plötzlich die Lichter ausgehen, wenn sie dem Feind zu nahe kommen. Einer dieser Zufallsbefehle trägt den Namen „*halt and catch fire*“ der den Computerchip irreparabel abschaltet. Auch wenn dieser Befehl nur bei bestimmten Chips zur Ausführung gebracht werden konnte und Einzelheiten verständlicherweise geheim blieben, zeigt er, dass ein ‚**digitaler Rettungsschuß**‘ zumindest technisch möglich ist[121].

Der Linux-Kernel eines Computers kann zum Absturz gebracht werden, wenn man einen speziellen Puffer für das Versenden von Datenpaketen überfüllt (TCP-*Funktion Selective Acknowledgement*), diese Attacke wird wegen der Fähigkeit, den gegnerischen Rechner übers Netz abstürzen zu lassen, auch als **Ping of Death**

[119] vgl. Becker 2018
[120] vgl. Welch 2018
[121] Man muss aber anmerken, dass in der Fuzzing-Forschung schon früher Befehle auffielen, die die Chipfunktionen störten, wobei dies wohl zunächst eher als lästiges Testhindernis betrachtet wurde.

bezeichnet. Der Rechner wird aber anders als beim Fuzzing nicht dauerhaft beschädigt[122].

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**[123].

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).
Beim Distributed Denial of Service-Angriff wird ein Computer(system) von mehreren Rechnern oder smarten Geräten koordiniert angegriffen, was selbst leistungsfähige oder gut gesicherte Computersysteme funktionsunfähig machen kann[124].
Das Werkzeug, um mit einer DDoS-Attacke anzugreifen, ist das **Botnetz**.
Man kann Computer mit Hilfe eingeschleuster Programme[125] 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[126].

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[127].

---

[122] vgl. Böck 2019
[123] vgl. Schmundt 2015, S.120-121, Langer 2014b, S.1
[124] 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.
[125] 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.
[126] 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.
[127] 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

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[128].

DDoS-Angriffe waren im Jahr 2017 häufige Ereignisse. Mega-Attacken, die 100 Gigabit pro Sekunde (Gbps) übersteigen, traten jedes Quartal auf; die Hälfte aller Angriffe ist zwischen 250 Mbps und 1,25 Gbps stark. [129]
Am Nachmittag des 28.02.2018 wurde die Plattform *Github* mit einer DDoS-Attacke mit einer Spitze von 1,35 Terabit/Sek angegriffen, indem das *Memcached*-Tool zur Vervielfachung von Datenmengen benutzt wurde[130]. *GitHub* entlastete sich durch eine Datenumleitung auf *Akamai*, woraufhin wenige Tage später ein anderer Provider mit derselben Methode und 1,7 Terabit pro Sekunde angriffen wurde[131].

Weitere tatsächlich praktizierte Methoden sind

- das **Website Defacement**, bei dem man das Aussehen (face) einer Internetseite zu propagandistischen Zwecken verändern. Ein aktuelles Beispiel sind Dutzende Defacements durch Unterstützer des Islamischen Staates mit dem Namen *System DZ Team.*
- 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[132]. Gleichwohl ist zumindest vorläufig davon auszugehen, dass der Einsatz von Botnetzen vorerst ein Kernelement massiver Angriffe bleiben wird.

---

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.

[128] WhiteWolfSecurity 2007
[129] vgl. Akamai 2017
[130] vgl. Beiersmann 2018b
[131] vgl. Beiersmann 2018c
[132] vgl. Gaycken 2009

2.2.5 Insider-Threats

Mittlerweile sind Insider-Bedrohungen selten, aber bei weitem die gefährlichste Methode, einen Akteur zu beschädigen:

Die wichtigsten Vorfälle waren:

- Weitergabe vertraulicher Daten an *WikiLeaks* vom geschützten US-Netz *Secret Internet Protocol Router Network SIPRNET* am 28.11.2010 durch Bradley/Chelsea Manning.
- Im Jahr 2012 hatte ein IT-Administrator innerhalb des Schweizer Geheimdienstes, des *Nachrichtendienstes des Bundes NDB*, eine nicht autorisierte Datensammlung eines Volumens von 500 Gigabyte vom gesicherten internen Netzwerk SI-LAN 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[133].
- *Snowden leaks*: Die öffentliche Enthüllung der Überwachungsprogramme PRISM der NSA und Tempora der britischen GCHQ mit der Einbeziehung großer Internetfirmen wie auch von Telekommunikationsanbietern[134] 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[135].
- *Harold T. Martin/Shadow Brokers Leak*: Details sind in Abschnitt 5 dargestellt. Das Leck bestand aus einer nicht autorisierten Sammlung von Cyberwaffen aus der NSA und anderen Dateien, die seit 2016 geleakt wurden
- *Vault 7 Leck*: Wie in Abschnitt 5 gezeigt, wurden im Jahr 2017 mehr als 8600 CIA-Dokumente vermutlich von ehemaligen Auftragnehmern an die Wikileaks-Plattform ausgeliefert
- *Michailow*-Vorfall: wie in Abschnitt 6 gezeigt, wurden mehrere Personen, die mit einem russischen Geheimdienstbeamten namens *Michailow* in Verbindung stehen, inhaftiert, einige Cyber-Operationen und auch hundert IP-Adressen des Verteidigungsministeriums wurden offenbart.

---

[133] Vgl. Gujer 2012a, S.30, Gujer 2012b, S.24, Häfliger 2012a, S.29, Gyr 2016, 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.

[134] vgl. Tomik 2013b, S.2.

[135] 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

Das gesicherte *Secret Internet Protocol Router Network SIPRNET* der USA ist inzwischen zu groß geworden und hat zu viele Zugangsberechtigte[136], wie die Debatten nach den aus dem SIPRNET stammenden WikiLeaks-Enthüllungen vom 28.11.2010 gezeigt haben[137].
Tatsächlich haben in den USA 1,5 Million Personen eine Sicherheitsstufe für Cyberangelegenheiten, davon arbeiten 480.000 in privaten Firmen[138]. 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[139]. Es wurde auf der anderen Seite darauf verwiesen, dass die Zusammenarbeit mit Privatfirmen schon lange besteht[140] und es notwendig ist, Expertenwissen für den rapide wachsenden Cybersektor nutzen zu können.
Das US-Verteidigungsministerium hat konstatiert, dass ihr eigenes Netzwerk immer noch aus tausenden von Netzwerken weltweit bestehen würde[141]

Mögliche Gegenmaßnahmen gegen die umfangreiche Entwendung von Daten, sei es von innen wie beim Wikileaks-Vorfall oder durch Cyberangriffe von außen sind z.B. die **Segmentierung** durch ein vertikal nach Dienstgraden und horizontal nach Zuständigkeiten gestuftes System von Zugangsberechtigungen, Blockaden von Druck- und Downloadfunktionen z.B. durch **Dokumentenmanagement**-Systeme, und die heute technisch einfach realisierbare Nachverfolgung von Zugriffen und downloads (**tracking**). Auch die Übermittlung von Nachrichten über gesonderte Kanäle trägt dem bewährten **need to know-Prinzip** (jeder bekommt nur die Informationen, die für die Aufgabe notwendig sind) Rechnung[142]. In einem ersten Schritt haben die USA die Zahl der Zugangsberechtigten verkleinert[143].
Auch die regelmäßige Überprüfung der Zugriffsrechte ist erforderlich. Schließlich wird keine Cyber-Verteidigung helfen, wenn die Menschen vor dem Bildschirm nicht ausreichend überwacht werden.

2.2.6 Informationskrieg

Das Konzept des Informationskrieges ist gut etabliert, z.B. in der *psychologischen Kriegsführung*, bei der gezielte Informationen oder Propaganda wurde an die freigegeben wurde, um das Verhalten zu beeinflussen.

---

[136] Es handelte sich um 2,5 Millionen Zugangsberechtigte und 280.000 Personen für die höhere Geheimhaltungsstufe; vgl. Schneider 2011, S.9
[137] vgl. Schaaf 2010, S.9
[138] vgl. Gartmann/Jahn 2013, S.24
[139] vgl. Huber 2013, S.18-19
[140] BAH knackte die Codes deutscher U-Boote im zweiten Weltkrieg, vgl. Gartmann/Jahn 2013, S.24. Andere Sicherheitsfirmen sind z.B. Xe und USIS.
[141] vgl. DoD 2015, S.7
[142] vgl. Sattar et al. 2010, S.3
[143] vgl. Schneider 2011, S.9

Der moderne Informationskrieg ist etwas anderes gelagert, denn dies ist die **kombinierte Manipulation von digitalen Technologien und Informationen**, um Gegner zu beeinflussen.

Eine neue Variante 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**)[144].
Ein neuer Trend der Bot-Kommunikation ist der *Bot-Journalismus*, bei denen ohne menschliches Zutun Wetter- und Sportnachrichten erstellt werden[145].

Falsche Kommunikation und gefälschter Verkehr (fake traffic) sind Werkzeuge, die zur Beeinflussung politischer Gegner eingesetzt werden können, sind aber mittlerweile auch im Marketing weit verbreitet, z.B. **Fake-Follower** auf Twitter, **gefälschte Likes** auf Facebook, manipulierte Kommentare zu Produkten und Dienstleistungen etc. etc. Ein neues Beispiel aus dem Jahr 2017 ist das *Star Wars Botnet* (da Begriffe aus *Star Wars* in der gefälschten Kommunikation verwendet werden) mit 350.000 gefälschten *Twitter* User Accounts, wahrscheinlich gesteuert von einem einzelnen Benutzer[146].

Die **Social Me**dia dienen auch zur Kontaktanbahnung über **Fake Profile**. Mutmaßliche chinesische Agenten bieten über *LinkedIn* Geld für Informationen gegen Geld und im Erfolgsfall nachfolgende Einladungen zu Kongressen nach China. Dieses Vorgehen wurde in der Schweiz, Deutschland, aber auch anderen Ländern beobachtet[147].

Die NATO und die EU sind besorgt darüber, dass Russland den politischen Prozess in den europäischen Ländern durch gefälschte Kommunikationen beeinflussen könnte. Insbesondere wurde eine Gruppe von sogenannten **Cyber-Trollen** in St. Petersburg verdächtigt, die westliche Diskussion zu beeinflussen. Seit 2014 analysiert das *Nato Strategic Communication Center of Excellence*, das kurz als *StratCom* bekannt ist, in Riga die russischen Aktivitäten und sammelt Beweise für die gezielte Freigabe von gefälschten Nachrichten und Cyber-Trolle[148]. Die EU hat eine Task Force gegründet, die gefälschte Nachrichten erkennen, sie korrigieren und

[144] vgl. Graff 2014, S.13.
[145] Anbieter dieses neuen Service sind z.B. die Firmen Narrative Science und Automated Insights, vgl. Dörner/Renner 2014, S.18-19
[146] vgl. Wolfangel 2017, S.27-29
[147] vgl. Häuptli 2018
[148] vgl. Wüllenkemper 2017, S.15

auch eine positive Wahrnehmung der EU in den östlichen Staaten unterstützen sollte.[149].

Es gab eine Diskussion, ob gefälschte Nachrichten (**fake news**) das Ergebnis der Präsidentschaftswahlen im Jahr 2016 in den USA beeinflusst haben. Forscher der Universitäten von Stanford und New York führten eine detaillierte Analyse der fake news während der US-Wahlen 2016 durch. Die Auswirkungen von fake news, die übrigens oft von den Lesern nicht für wahr gehalten wurden, waren begrenzt. Die meisten Wähler bevorzugen immer noch das Fernsehen als primäre Informationsquelle, während das Internet nur von einem kleinen Teil der Wähler bevorzugt wird[150]. Insgesamt nannten 14 Prozent der Amerikaner die Social Media ihre wichtigste Informationsquelle. Der durchschnittliche Amerikaner sah und erinnerte sich an 0,92 pro-Trump gefälschte Geschichten und 0,23 pro-Clinton fake stories[151].

Im Sommer 2017 wurde von der University of Oxford eine Studie über **Computational Propaganda** veröffentlicht. Ein Team von 12 Forschern bewertete die Situation in 9 Ländern[152]. Die Autoren definieren die Computational Propaganda als den Einsatz von Algorithmen, Automatisierung und menschlicher Bearbeitung, um irreführende Informationen über soziale Mediennetze gezielt zu verteilen" [*„as the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks"*.] Derzeit sind Facebook und Twitter die wichtigsten Plattformen für diese Aktivitäten. Während der US-Wahl von 2016 war die Zahl der Bots, die Trump unterstützten, dreimal höher als Pro-Clinton-Bots, was im Einklang mit der oben beschriebenen fake news-Studie steht.

Insbesondere wird *Twitter* zunehmend von Social Bots bevölkert, die zusammen mit dem Ergebnis in Abschnitt 4 unten, dass Tweets auch eine neue Form der verdeckten Kommunikation von Kontrollservern mit gehackten Computern sind, zeigt, dass Twitter jetzt generell eine Hauptplattform der Bot-Kommunikation ist.

Ein weiteres Problem ist, ob die oben beschriebenen Methoden auch missbraucht werden können, um elektronische Abstimmungen zu untergraben.
Die einzige offiziell bestätigte Manipulation einer Abstimmung war bisher die "*Second referendum petition*", die nach dem Brexit-Votum für eine Wiederholung des Referendums im Juni 2016 plädiert hatte[153]. Der britische Petitionsausschuss entfernte offiziell 77.000 gefälschte Unterschriften aus der Petition am 27. Juni 2016. Jedoch war die Menge der gefälschten Signaturen am Ende viel größer, wie

[149] vgl. Stabenow 2017, S.3
[150] vgl. NZZ 2017a, S.32
[151] vgl. Hunt/Gentzkow 2017, S.1
[152] vgl. Woolley/Howard 2017
[153] vgl. Heighton 2016

z.B. aus dem Vatikanstaat, aus dem bei 1.000 Einwohnern 42.000 Unterzeichner gemeldet wurden. Später übernahmen Hacker von *4chan* die Verantwortung und sagte, das sei ein Streich (prank) gewesen.

Die Hacks während der US-Wahlkampagne auf Abstimmungssysteme und der DNC-Hack werden später in Kapitel 5 erörtert.

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[154]. Es folgte eine Explosion von ca. 3 Kilotonnen Stärke, immerhin einem Fünftel der Hiroshima-Bombe[155]. 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[156].

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[157]. 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[158].

[154] vgl. Kloiber/Welchering 2011, S. T6
[155] vgl. Falliere 2010, Herwig 2010
[156] vgl. Vistica 1999
[157] vgl. Hegmann 2010
[158] 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[159].

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[160], 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[161]. 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[162].
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[163].

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

[159] vgl. Fritz 2008 und Nazario 2009, der in seinem Papier einen Überblick über politisch motivierte DoS-Attacken gibt.
[160] 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
[161] vgl. Fischermann/Hamann 2010
[162] vgl. Fritz 2008, S.55 und auch Stokes 2005
[163] 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[164]. Operation Aurora wird inzwischen der *Axiom/APT17 Group* zugeschrieben, siehe Kapitel 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[165][166]. 2011 wurden weitere Angriffe dieser Art, u.a. auf die Rüstungsfirma *Lockheed Martin* und Googles Mailservice *Gmail* berichtet[167].

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[168]. Estlands Netz wurde daraufhin von Russland aus mit gewaltigen Datenmengen bombardiert, wobei dies nicht vom russischen Staat ausging, sondern 'nur' von nationalistisch gesinnten Kreisen[169][170]. 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[171].

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

[164] vgl. Markoff/Barbosa, 18.02.2010
[165] Alperovitch 2011, McAfee 2011. RAT steht für remote administration tool.
[166] vgl. FAZ 2011b, S.7.
[167] 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
[168] vgl. Busse 2007
[169] Später bekannte sich die russische patriotische Jugendorganisation **Naschi** (die Unsrigen) zu dem Angriff, vgl. Frankfurter Allgemeine Zeitung 11.03.09
[170] vgl. Koenen/Hottelet 2007, S.2
[171] vgl. Wilson 2008, S.7ff.

sprächen die Angriffsmuster für die Aktivitäten patriotischer **script kiddies**, d.h. Angreifern, die mit im Internet erhältlichen Standardwerkzeugen operiert hätten[172].

3.2.6 Der Angriff auf Syrien 2007

Bei dem Angriff auf eine mutmaßliche Atomanlage in Ostsyrien am 06.09.2007 mussten israelische Flugzeuge den gesamten syrischen Luftraum durchfliegen. Um dies zu ermöglichen, hatten die Israelis den Computern der syrischen Luftabwehr einen leeren Himmel vorgegaukelt, so dass die Flugzeuge unbehelligt einfliegen und angreifen konnten. Dies ist ein klassisches Beispiel für die Idee des Cyberwars als operativer Ergänzung zu konventionellen Maßnahmen[173].

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[174]. 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. Inzwischen wird die Attacke *APT28/Fancy Bear/Sofacy* zugeschrieben[175].

3.2.8 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[176]. 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 hatte dies jedoch keinen Einfluss auf die Einsatzfähigkeit der Drohnen[177]. Der Iran brachte 2011 eine US-Drohne vom Typ RQ-170 in seinen Besitz[178].
Die US Navy hat 2012 entschieden, die Kontrollsysteme der Drohnenbasen auf Linux umzurüsten, was von der Rüstungsfirma *Raytheon* mit einem Budget von 28

[172] vgl. Luschka 2007, S.1-3
[173] vgl. Herwig 2010, S.60
[174] vgl. die Stellungnahme der georgischen Regierung von 2008
[175] vgl. Beuth 2017, S.14
[176] vgl. Ladurner/Pham 2010, S.12
[177] vgl. Los Angeles Times 13 October 2011
[178] vgl. Bittner/Ladurner 2012, S.3. Als Eindringmethode wurde die Verwendung eines manipulierten GPS-Signals (GPS spoofing) diskutiert, aber das konnte nicht belegt werden.

Million US-Dollar durchgeführt werden sollte[179]. Die Verwundbarkeit von Drohnen ist aber auch typabhängig, da diese mit unterschiedlichen Kontrollmethoden und verschieden großer Systemautonomie gesteuert werden[180].

3.2.9 Attacken in der Ukraine

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[181].

Am 23.12.2015 kam es zu Stromausfällen in der Ukraine durch Cyberattacken bei drei regionalen Stromanbietern, die insgesamt ca. 225.000 Kunden betrafen[182]. Drei weitere Anbieter waren betroffen, hatten aber keine Stromausfälle. Die Eindringlinge[183] waren in der Lage, Stromverbindungen aus der Distanz zu öffnen, was zum Stromausfall führte, was in koordinierter Form in einem kleinen Zeitfenster geschah[184]. **Telephone denial of service-Attacken (TDoS attacks)** wurden genutzt, um die Anbieter–Hotlines mit Anrufen zu fluten, so dass die Kunden die Stromausfälle nicht telefonisch weitermelden konnten[185].
Am Schluss wurde die Wiper-Malware *KillDisk* benutzt, um die Systeme zu beschädigen. Die *Sandworm/Quedagh-Gruppe* wurde als Angreifer vermutet, aber ihre Malware *Black Energy* schien die Ausfälle nicht herbeigeführt zu haben, siehe auch Kapitel 7.

Am 17. Dezember 2016 verursachte die Malware *Industroyer/CrashOverride* einen Blackout in Kiew, der einer neuen APT namens *Electrum* zugeschrieben wurde, die mit der *Sandworm/Quedagh-Gruppe* verbunden ist. Dies wird im Abschnitt 7 im Kapitel Smart Grid ausführlich besprochen.

Die IT-Sicherheitsfirma *CrowdStrike* entdeckte Ende 2016 einen Angriff auf ukrainische Artilleriegeschütze des *Howitzer*-Typs.
Die *APT 28/Fancy Bear/Sofacy-Malware X-Agent* wurde verdeckt in ein Android-Paket implantiert, das von einem ukrainischen Offizier namens Sherstuk entwickelt wurde und 9.000 User hatte. Diese App unterstützt D-30/122mm *Howitzer* Artillerie-Waffen, um Ziel-Daten in kürzester Zeit zu verarbeiten. *CrowdStrike* nahm an, dass dies zu einem Verlust von 80% der Artilleriegeschütze im Vergleich

[179] vgl. Knoke 2012
[180] vgl. Heider 2006, S.9
[181] vgl. FAZ online 2014
[182] vgl. ICS-CERT 2016b
[183] Die Nutzung von BlackEnergy lässt die Urheberschaft der Sandworm/Quedagh-Gruppe zwar plausibel erscheinen, einen eindeutigen Beweis hierfür gibt es aber nicht.
[184] vgl. ICS-CERT 2016b
[185] vgl. Zetter 2016

zu einem durchschnittlichen Waffenverlust 50% in den letzten zwei Jahren beigetragen hat, diese Analyse blieb aber umstritten[186].

3.2.10 Nord-Korea

Die *New York Times* berichtete, dass die NSA in der Lage gewesen sei, in nordkoreanische Netzwerke über Malaysia und Südkorea vorzudringen, so dass sie in der Lage gewesen sei, nordkoreanische Hackeraktivitäten zu beobachten und nachzuverfolgen, aber eine offizielle Bestätigung dieser Darstellung wurde nicht gegeben[187].
Während des so genannten *Sony Hacks* (siehe Kapitel Lazarus-Gruppe in Abschnitt 5) fand ein Netzwerkversagen in Nordkorea statt, was zu Spekulationen führte, dass dies eine **Cybervergeltung** der USA für den Druck war, dem Sony und der Film *The Interview* ausgesetzt war.
Im Jahr 2014 befahl US-Präsident Obama, Cyber- und elektronische Schläge gegen das nordkoreanische Raketenprogramm zu verstärken. Während es eine hohe Ausfallrate bei den Raketentests gibt, hat das Programm dennoch Fortschritte gemacht. Die aktuelle Diskussion geht davon aus, dass das nordkoreanische Programm möglicherweise widerstandsfähiger als erwartet ist[188].

3.2.11 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[189]. Wichtige Beispiele unter vielen sind die Konflikte von Indien und Israel mit Akteuren aus den Nachbarstaaten[190].

Nachdem vermutlich Hacker aus Pakistan erfolgreich die Website der indischen *National Security Guard* gehackt hatten, wurden am 02.01.2017 Computer der Islamabad, Multan und Karachi Flughäfen wurden von indischen Hackern mit Vergeltungs-Ransomware angegriffen, was den Flugverkehr beeinträchtigte. Im Gegensatz zu früheren Attacken wurde kein Code gegen Lösegeld angeboten, stattdessen wurde die Ransomware verwendet, nur um die Computer nur zu beschädigen. Im Gegensatz zu anderen Cyberwars wurden wenig Anstrengungen unternommen, um den Ursprung des Angriffs zu verbergen oder etwas zu verweigern, stattdessen wird dies als *shooting over the virtual border* betrachtet[191].

---

[186] vgl. CrowdStrike 2016
[187] vgl. FAZ 2015, S.5
[188] vgl. Sanger/Broad 2017
[189] vgl. Saad/Bazan/Varin 2010
[190] vgl. Saad/Bazan/Varin 2010, Valeriano/Maness 2011, Even/Siman-Tov 2012, S.37
[191] vgl. Shekhar 2017

3.2.12 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[192]. Die Aktivitäten wurden in die allgemeinen militärischen Maßnahmen eingebettet. Während der IS formal kein Staat war (da er vom Ausland nicht als solcher anerkannt wurde),[193] kam 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[194], 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[195]. 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[196].

Um die Überwachung von e-Mails zu umgehen, werden zunehmend Messengerdienste mit Verschlüsselung benutzt[197]. 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[198].

---

[192] vgl. Paletta/Schwartz 2016, S.1-2
[193] vgl. Kurz 2016, S.14
[194] vgl. Anonhq 2014
[195] vgl. Chip.de 2015
[196] vgl. DW online 2016
[197] vgl. Langer 2015b, S.5
[198] vgl. Dörner/Nagel 2016, S.37

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.

In Januar 2016 gab der IS ein Cyberwar-Magazin namens *Kybernetiq* heraus mit Cyberwar-Informationen[199]. 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[200]. 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[201]. 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[202].
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[203].
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[204]. 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. [205] 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[206].

Das US-Verteidigungsministerium DoD befand, dass die NSA und die Intelligence Community im Kampf gegen den IS die Informationsgewinnung aus den IS-Netzwerken gegenüber der Bekämpfung priorisierten, also ein Zielkonflikt aus verdeckter nachrichtendienstlicher Arbeit und offensiven militärischen

[199] vgl. Cyberwarzone 2016
[200] vgl. DW 2016
[201] vgl. Strobel 2016, S.2
[202] vgl. Lange 2016, S.5
[203] vgl. Strobel 2016, S.2
[204] vgl. Strobel 2016, S.2, Rötzer 2016, S.2
[205] vgl. Rötzer 2016, S.2
[206] vgl. FOCUS Online 2016

Erfordernissen existierte[207]. In Zukunft sollen Cybersoldaten direkt an der Front mit der Infanterie zusammenarbeiten, eine Taktik, die schon im Kampf gegen den IS erprobt wurde[208].

Um die Cyberwarfähigkeiten der USA weiter zu stärken, plante Präsident Obama 2016 die Aufwertung von Cybercom zu einem eigenständigen militärischen Kommando mit einem Fokus auf die militärischen Aspekte des Cyberspace. Die Verbindung zur NSA sollte aufgehoben und die NSA dann von einem Zivilisten geführt werden[209]. Präsident Trump führte die Aufwertung 2017 durch und unterstellte *Cybercom* direkt dem DoD[210].

Ein 20-jähriger Hacker aus dem Kosovo lieferte im Jahr 2015 die Adressen von 1.300 US-Militärs und stellte sie online. Im September 2016 plädierte er auf schuldig und wurde zu 20 Jahren Gefängnis verurteilt[211].

Eine weitere Aktivität waren Dutzende von Website-Defacements durch die Unterstützer des islamischen Staates mit dem Namen *System DZ Team*. In den letzten drei Jahren seit Oktober 2014 weisen die IP-Adressen auf einen Standort in Algier hin. Im Juni 2017 wurde die Website des Gouverneurs des US-Bundesstaates Ohio, John Kasich, mit einer Pro-ISIS-Nachricht des *System DZ-Team* defaced[212].

Europol und US-Polizeibehörden konnten in einer zweitägigen Aktion im April 2018 IS-Plattformen stilllegen. Betroffen davon waren die Nachrichtenagentur *Amaq*, Radio *Al-Bayan* und die Nachrichtenseiten *Halumu* und *Nashir*. *Nashir* veröffentlichte *Amaq* News jedoch weiter über den Messenger-Dienst *Telegram*[213].

3.2.13 Cyberkonflikte im Jahr 2019

Neben anderen militärischen Unterstützungsmassnahmen (Luftverteidigungs-systeme, Hubschrauber usw.) wurden Ende März 2019 von Russland einige Cybersoldaten nach Venezuela entsandt. Dies ist zwar kein Beweis dafür, dass die

[207] vgl. The Australian 2017
[208] vgl. Sokolov 2017
[209] vgl. Strobel 2016
[210] vgl. Sokolov 2017
[211] vgl. Rohde 2016
[212] vgl. Fox News 2017
[213] vgl. Tagesschau 27 Apr 2018

USA in den Wochen zuvor die großen Stromausfälle in Venezuela verursacht hatten (die USA sagten, das Kraftwerk sei durch ein natürliches Lauffeuer beschädigt worden), aber es könnte eine Warnung Russlands gewesen sein, nichts in diese Richtung zu unternehmen[214].

Anfang Mai 2019 kombinierte die Hamas ihre Raketenangriffe vom Gaza-Streifen mit Cyberangriffen, woraufhin Israel das Gebäude der Hackereinheit gezielt bombardierte, so dass erstmals Hacker während eines Konflikts ums Leben kamen[215].

Die USA haben laut eigenen Angaben am 18 Juni 2019 Raketenkontrollsysteme der iranischen Revolutionsgarden und ein Spionagenetzwerk angegriffen[216]. Dies war auch eine Reaktion auf eine Zunahme iranischer Cyberattacken auf US-Regierungseinrichtungen, den Wirtschafts- und Finanzsektor sowie Öl- und Gasfirmen, wobei die Attacken typischerweise mit Spearphishing ausgeführt wurden[217].

Im Juni 2019 wurde bekannt, dass die USA seit mindestens 2012 Aufklärungsprogramme in Steuerungssystemen des russischen Stromnetzes einsetzen. Zusätzlich zur *Wolf Creek*-Attacke waren nämlich Versuche unternommen worden, die *Cooper Nuclear Station* des *Nebraska Public Power Districts* zu infiltrieren, wo die Angreifer die Kommunikationsnetze erreichten, jedoch nicht das Reaktorsystem[218].

[214] vgl. Spetalnick 2019
[215] vgl. Wired 2019
[216] vgl. Welt online 2019
[217] vgl. Abdollah 2019
[218] vgl. Sanger/Perloth 2019

4. Attribution

4.1 Einführung

Attribution bezeichnet die Zuordnung einer Cyberattacke zu einem bestimmten Angreifer bzw. Angreifergruppe im ersten Schritt und die Aufdeckung der tatsächlichen Identität des Angreifers in einem zweiten Schritt. Während sich die Methodik der Zuordnung einer Cyberattacke zu bestimmten Angreifern in den letzten Jahren deutlich weiterentwickelt hat, erlauben Digitaltechnologien oft nicht den eindeutigen Nachweis der tatsächlichen Identität des Angreifers.
Die Situation sieht anders aus, wenn die Attribution als cyber-physischer Prozess gehandhabt wird, d.h. als Kombination aus digitaler Forensik und Beweisführung in der physischen Welt.
Bits und Bytes sind nämlich nicht wirklich virtuell, sondern nach wie vor an eine physische Infrastruktur in der realen Welt gebunden, was verschiedene Möglichkeiten zur Erkennung von Gegnern bietet. Lücken in der Beweisführung können auch mit Mitteln der Human Intelligence (HumInt) geschlossen werden.

4.2 Attribution von Cyberangriffen

Theoretisch kann ein Hacker einen einzigen Angriff von "irgendwo" starten und es mag unmöglich sein, diesen zurück zu verfolgen. Auf der anderen Seite ist die Erfolgsquote dieses Ansatzes recht niedrig.
Angreifer, die einen bedeutenden Erfolg erzielen wollen, greifen typischerweise in einem größeren Maßstab an, d.h. als Gruppen, mit anspruchsvoller Malware und agieren manchmal über Jahre. Je länger und je intensiver der Angriff ist, desto höher ist das Risiko für Erkennung und Attribution.

Der Datenverkehr des Computers erfolgt über sogenannte **Ports**. Ein Supervisor (IT-Administrator) kann die Ports und den Datenverkehr mit handelsüblichen Tools überprüfen. Diese Tools zeigen auch, an welche IP-Adresse die Daten gehen oder gegangen sind.
Nun gibt es spezialisierte Suchmaschinen, die automatisch überprüfen, was hinter einer IP-Adresse steht. Ein Beispiel für solche Maschinen ist *Robtex.com*. Die Anbieter dieses Dienstes erklären auf ihrer Website, dass dieses Tool "nicht nur" von der *National Security Agency NSA* verwendet wird, was darauf hinweist, dass diese Dienste auch als Intelligence-Tools dienen.

Durch die Eingabe der IP-Adresse in die Suchmaske zeigt *Robtex* Datenströme mit anderen IP-Adressen sowie den Weg zum autonomen System AS oder dem Internet Service Provider ISP. *Robtex* kombiniert IP-Adressen und Domains sowie alle existierenden Subdomains. Außerdem zeigt es die Mail-Server im Zusammenhang mit dem Domain-Namen.

Dies ist aus folgenden Gründen wichtig:

- Angreifer behalten oft eine gewisse Angriffsstruktur bei, denn wie jedes Konstrukt hat eine Angriffsumgebung sowohl Aufbau- als auch Ausstiegskosten. Infolgedessen werden Mailadressen, Domainnamen, Server und IP-Adressen zumindest teilweise von einem Angriff zum nächsten recycelt. Diese Überlappungen erlauben die forensische Verknüpfung von Angriffen.
- Angreifer benötigen Computer als Verteiler (distribution hubs) für ihre Malware, was zur Verwendung mehrerer Domainnamen führt. Jeder bekannte Domain-Name kann den Weg zurück zur IP-Adresse geben und gleichzeitig zum Besitzer des Computers verweisen, wie unten gezeigt.

Es ist zu beachten, dass AS-Computer mit dem IANA-System nummeriert sind und jeder AS-Computer registriert ist. AS-Computer und die registrierten Personen/Organisationen können mit weiteren kostenlosen Tools wie *Ultratools* und vielen anderen Maschinen leicht abgefragt werden.
Für Domains und IP-Adressen existiert eine so genannte WHOIS-Registrierung, die oftmals mit kostenlosen Suchmaschinen verfügbar ist. Die Registrierungsangaben zeigen Firmennamen, Adressen, Telefonnummern und E-Mail-Adressen an. Dadurch wird der Schritt von der digitalen Welt zur physischen Welt gemacht, von Daten zu Personen und Organisationen. Damit kann der Forscher Einblick in das "digitale Ökosystem" von Servern, Adressen, Registrierungen, Domains etc. der Angreiferidentität erhalten.

Auch gefälschte Registrierungsinformationen werden in Wirklichkeit oft wiederverwendet und ermöglichen es, Verbindungen zwischen bestimmten Angriffen herzuleiten. Überraschenderweise führt die Eingabe der Daten in Google oder jede andere Suchmaschine oft zu weiteren Erkenntnissen, die massiv die Chance erhöhen, Informationen zu finden, die sich auf eine Person mit einer realen Identität beziehen.

Weiterhin reservieren größere Organisationen **IP-Blöcke**, z.B. Pakete mit aufeinander folgenden IP-Nummern[219]. Wenn eine vermutete IP-Adresse Teil eines solchen Blocks ist, kann dies helfen, auch alle anderen IP-Adressen in Domain-Suchmaschinen etc. zu überprüfen.

Der Sicherheitsforscher *Krebs* wurde über eine IP-Adresse der *Carbanak*-Gruppe informiert, die 1 Milliarde US-Dollar durch Intrusion von Bankensystemen erbeutet

[219] Es gibt noch weitere technische Optionen, wie z.B. die Vergabe virtueller **IP-Adressen** in Cloudbasierten Systemen und das Vortäuschen falscher IP-Adressen (**IP spoofing**), aber zumindest in den veröffentlichten Analysen von großen Cybercrime-Gruppen und Advanced Persistent Threats APT stellte dies kein Kernproblem dar.

hatte[220]. Seine Analyse der IP-Adress-Registrierung zeigte, dass der Firmenname auch für vergangene Cyber-Angriffe mit zwei anderen Arten von Malware verwendet wurde. Die E-Mail-Adresse führte ihn zu weiteren IP-Adressen der *Carbanak*-Gruppe. Die Telefonnummer erlaubte es *Krebs*, eine Person mit potenziellen Beziehungen zur *Carbanak*-Gruppe zu identifizieren; er war sogar in der Lage, diese Person zu kontaktieren[221].

Spezialisierte Angreifer haben schon darauf reagiert. Eine Strategie ist, IP-Adressen und Server schnell mit der sogenannten **Fast-Flux-Technologie** abzuwechseln. Auch das Herunterfahren bestimmter Server kann dann den Angreifer nicht stoppen. Eine Gegenstrategie ist jedoch die Verwendung von **Sinkhole-Servern**.
Wenn jemand eine Domain wie *www.example.com* in den Browser eingibt, muss der Computer die IP-Adresse des Ziels kennen. So genannte Domain Name Server (**DNS Server**) helfen dem Computer, die IP-Adresse zu finden.
Sinkhole-Server geben jetzt absichtlich falsche Hinweise (z. B. indem sie angeben, dass *www.example.com* die IP-Adresse 4.5.6.7 hat, während die wahre Adresse 1.2.3.4 ist) und damit den Datenverkehr von dem "echten" Computer wegleiten.
Der Sinkhole-Server kann die fehlgeleiteten Daten *erfassen und analysieren*. Da bei größeren Angriffen die Kommunikation für eine Weile im Gange ist, können sowohl Daten des Angreifers als auch die des Opfercomputers gesammelt werden, was hilft, die Probleme durch die sich ändernden IP-Adressen zu überwinden. Sinkholing wurde z.B. von der russischen Sicherheitsfirma *Kaspersky* gegen die vermutlich US-amerikanische *Equation Group* eingesetzt[222], die ihrerseits *Kaspersky* mit der anspruchsvollen Spionage-Malware *Duqu 2.0* infiziert hat[223].

Eine weitere Strategie ist die Verwendung von **Domains mit schwer nachverfolgbarer Registrierung**, die 2017 von der Sicherheitsfirma *Kaspersky* Labs für vermutete "Überlebende" der *Carbanak*-Gruppe gemeldet wurde. Einige Länder erlauben den freien Verkauf von Domains mit ihrer Länderkennung wie Gabun (.ga) durch Anbieter wie *Freenom*. Jedoch hat jeder Provider das Risiko, von der nationalen oder ausländischen Polizei oder Nachrichtendiensten angegangen zu werden, um Zugang zu ihren Daten zu erhalten. Es gibt eine enorme weltweite Variabilität der Cybersicherheitsgesetze und Strafverfolgungsverfahren, und es gibt u.a. eine nie endende öffentliche Debatte und von Gerichtsverfahren in den USA, wer unter welchen Umständen befugt ist, Informationen über User von Privatunternehmen zu erfragen.

[220] vgl. Kaspersky Lab 2015c
[221] vgl. KrebsonSecurity 2016
[222] vgl. Kaspersky Lab 2015a, S.34-35. Unerwarteterweise wiesen frühe Versionen der *Equation Group*-Malware hartcodierte (fest verankerte) IP-Adressen in ihren Programmen auf.
[223] vgl. Kaspersky Lab 2015b

Der Dienst der Europäischen Kommission *European Commission Service* hat im Dezember 2016 einen Überblick über die aktuelle Rechtslage in den EU-Mitgliedstaaten veröffentlicht. Die Umfrage zeigte ein enormes Spektrum der Rechtsauffassungen, z.B. ob ein Anbieter mitwirken *kann* oder kooperieren *muss*, welches Ausmaß an Informationen angefordert wird, welche Arten von Strafverfolgungsmaßnamen verwendet werden (bis hin zum Fernzugriff auf Anbieter) und ob die Zusammenarbeit zwischen den Behörden praktiziert wird oder nicht[224].
Allerdings arbeitet die EU auf einen gemeinsamen Rechtsrahmen mit einem gemeinsamen Rechtsverfahren hin, der Europäischen Ermittlungsanordnung **European Investigation Order EIO** und die Europäische Union sieht Cybersicherheitsfragen als dringende politische Angelegenheit an.

Smart-Geräte haben eigene IP-Adressen. Die Analyse von Vorfällen mit intelligenten Geräten im Internet der Dinge (IoT) ermöglicht die Identifizierung des Herstellers und der beteiligten Produkte.

4.3 Hacker

Die Cyberwelt kann in mehrere Akteursgruppen unterschieden werden:

- Der Staat mit Zivilbehörden, Militär- und Zivilgeheimdiensten. Hacker können für diese Organisationen arbeiten, in einigen Staaten auch in staatlich verknüpften Hackergruppen.
- Cyber-Sicherheitsfirmen, die an der Erkennung, Attribution und Verteidigung beteiligt sind, aber auch am Bau von Cyberwaffen und Spionagewerkzeugen. Hacker können auch als **Penetrationstester** fungieren, um Sicherheitsmaßnahmen einer bestimmten Einheit zu überprüfen.
- Im wissenschaftlichen und privatwirtschaftlichen Bereich können Hacker als **White Hat Hacker** arbeiten, um Sicherheitslücken zu finden und zu schließen, aber auch als **Black Hat Hacker** für kriminelle Zwecke oder zur Industriespionage der Industrie.
- **Hacktivisten** nutzen ihre Fähigkeiten für politische Aktivitäten.

Die oben genannten Sphären sind nicht vollständig getrennt. In Wirklichkeit kann ein begabter Hacker während eines Hacking-Contests prämiert werden, der dann vom Staat angestellt wird, um später irgendwann in den privaten Sicherheitsbereich zu wechseln[225].

[224] vgl. EU 2016
[225] vgl. Rosenbach 2016, Kramer 2016

Während das ursprüngliche Image der Hacker mehr anarchisch war, sind mittlerweile Staaten intensiv und routinemäßig auf der Suche nach erfahrenen Hackern, um sie zu anzuwerben. **IT-Summer Camps, Hackerwettbewerbe, Hackathons** (Hacker-Marathons, wo ein bestimmtes Problem gelöst werden muss) sind typische Aktivitäten. Die Suche nach Hackern ist aber nur ein kleiner Teil der Suche nach qualifizierten IT-Mitarbeitern im Allgemeinen: Qualifizierte IT-Studierende können auch direkt von Staaten und Sicherheitsfirmen kontaktiert werden.

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[226]. Im Ergebnis konnten die Rekrutierungsmethoden in der Cybersicherheit inzwischen einfacher gestaltet werden[227].

Der typische Hacker ist ein jüngerer Mann, der - wenn er in größere Cyber-Attacken involviert ist - dies als regelmäßigen Job macht. Die Dominanz der jüngeren Männer im Hacking spiegelt die Dominanz der jüngeren Männer im IT-Bereich im Allgemeinen wider. Dies wird mittlerweile als ein Problem gesehen, da dies die unzureichende Resourcennutzung von Frauen im IT-Bereich anzeigt. Der britische Cyber-Nachrichtendienst *Government Communication Headquarter GCHQ* ist nun systematisch auf der Suche nach qualifizierten Frauen durch die Initiierung der *CyberFirst Girls Competition* für 13 bis 15 Jahre alte Mädchen mit Tests in Kryptologie, Logik und Codierung. Ende Februar 2017 starteten 600 Teams den Wettbewerb. Derzeit sind nur 37% der 12.000 Mitarbeiter im britischen Geheimdienstsektor Frauen.[228]

Der typische Hacker ist kein Einzelkämpfer, sondern interagiert mit Freunden und anderen Hackern, um Werkzeuge und Erfahrungen auszutauschen, Einblicke und Neuigkeiten aus der Szene zu bekommen usw. Dies geschieht mit Decknamen in **Hackerforen**, auf dem **Schwarzmarkt** und im **Darknet**[229]. Diese drei Bereiche

---

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

[227] 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 NSA wartete 2017 mit einer neuen Stellenanzeige auf: *NSA Cyber Careers – For a Safer Digital World – intelligencecareers.gov. Protect the nation against cyberattacks using state of the art tools & tactics.* Die NSA erhält über 140.000 Bewerbungen im Jahr, vgl. Shane/Perloth/Sanger 2017. 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.

[228] vgl. Wittmann 2017

[229] Eine Übersicht findet sich bei Chiesa 2015

überlappen sich gegenseitig. Manchmal gibt es auch **defacement websites**, wo Hacker Screenshots der gehackten und beschädigten (verunstalteten) Webseiten als eine Art Trophäe posten.

Dies öffnet den Weg zur Attribution: Decknamen können in mehreren Angriffen erscheinen, auch die verwendeten E-Mail-Adressen. Wenn ein einzelner Hacker einen Angriff öffentlich für sich beansprucht, steigt das Risiko, gefasst zu werden, wie z.B. der Hacker mit dem Decknamen *Anna Sempai*, der an den *Mirai*-Botnet-Attacken beteiligt war und der wahrscheinlich schon identifiziert wurde[230].
Wieder kann es hilfreich sein, den Decknamen eines Hackers in eine Suchmaschine einzugeben, um weitere Hinweise zu erhalten. Die Praxis zeigt, dass Hacker manchmal mehrere Decknamen verwenden, *aber nicht zu viele*, denn sonst verlieren sie ihr "Profil" in der Insider-Szene[231].

Reales Praxisbeispiel[232]**:** In der *Winnti 2.0*-Attacke trug eine Bot-Kommunikation via *Twitter* als Header den Decknamen eines der Hacker, der sich dann auch in Hacker-Foren finden ließ. Dort hatte er E-Mail-Kommunikation mit einem Freund, der eine reguläre Social-Media-Website mit allen Kontaktdaten hatte. Auch eine Abkürzung im Malware-Programm führte zu weiteren Treffern in Suchmaschinen und führte zu einem Hacker-Team, von dort wiederum zu einer Mail-Adresse, die dann wieder zu einer jungen männlichen Person führte.

Das Darknet wurde in den Medien 2016 und 2017 als großes Problem thematisiert. Das TOR-System (abgeleitet von *The Onion Router*) gilt in den Medien als Rückgrat des Darknet, weil es die Aufteilung von Datenpaketen über mehrere Strecken und damit einen hohen Grad an Anonymität im Netz ermöglicht.

Allerdings gerät TOR zunehmend unter Druck. Eine neuere Arbeit des *Naval Research Laboratory*, das das TOR-System ursprünglich erfunden hat, zeigt, dass die Übernahme eines autonomen Systems oder eines IXP-Knotencomputers (siehe oben) durch einen Gegner genügend Informationen zur Erfassung eines Nutzers innerhalb von Wochen oder manchmal sogar innerhalb von Tagen bereitstellen würde[233]. Während dieses Erkennungsverfahren nur als statistische Modellierung präsentiert wurde, zeigt die Arbeit, dass das TOR-System wohl nicht auf Dauer eine Barriere gegen Erkennung und Attribution bleiben wird.
TOR ist besonders anfällig, wenn der Exit-Knotenserver von einem Gegner kontrolliert wird und es können auch bestimmte Daten während der

[230] vgl. KrebsonSecurity 2017
[231] Die Erforschung der Benutzeridentifikation ist permanent im Gange, z.B. mit der *Bio-Catch*-Methode, bei der das Cursor-Bewegungsmuster (Geschwindigkeitsrichtung, Pausen) etc. die Identifizierung des Nutzers eines Online-Bankkontos ermöglicht, vgl. Gebauer/Wolfangel 2017.
[232] vgl. Kaspersky 2013, S.53ff.
[233] vgl. Johnson et al. 2013

Datenübertragung über das TOR-Netzwerk extrahiert werden, da theoretisch jedermann einen TOR-Server einrichten kann.

In Bezug auf das Darknet[234] sollte man bedenken, dass die Akteure auch Undercover-Ermittler sein können[235].
Da mittlerweile viele Behörden verdeckte Agenten für mannigfaltige Ermittlungen im Darknet einsetzen verwenden, besteht ein zunehmendes Interferenzrisiko oder eine unbeabsichtigte Wechselwirkung zwischen ihnen, z.B. sie arbeiten dann unabsichtlich gegeneinander statt ihre Gegner zu untersuchen.

Schätzungen zeigen, dass das **Darknet** Mitte 2017 aus ca. 5200 Webseiten besteht, von denen 2700 aktiv sind und die Hälfte illegale Inhalte haben[236]. Es ist zu beachten, dass das Darknet faktisch der (weitgehend) anonyme Bereich des Internets ist, was nicht mit dem weit aus größeren **tiefen Internet (Deep Web)** zu verwechseln ist, was jene Webseiten umfasst, die von Suchmaschinen normalerweise nicht erfasst werden.

Im Juli 2017 wurden zwei der größten Darknet-Plattformen für illegalen Drogen- und Waffenhandel *AlphaBay* und *Hansa* in enger Zusammenarbeit des FBI, der *Drug Enforcement Agency (DEA)* und der niederländischen Polizei mit Unterstützung von *Europol* geschlossen[237].

Alphabay war die größte Plattform mit 200.000 Nutzern und 40.000 Anbietern und einem Umsatz von 1 Milliarde Dollar seit 2014. Im Juli 2017 wurden im Zuge der *Operation Bayonet* des FBI und der DEA die Server sichergestellt und die zentrale Person von Alphabay verhaftet, ein in Thailand lebender Kanadier.
Die Plattform *Hansa* wurde mit Hilfe des Cybercrimecenters E3C am 20 Juni 2017 sichergestellt, jedoch noch einen Monat undercover weiter betrieben, um die von *Alphabay* wechselnden Nutzer einfangen zu können[238].

Im Messenger-Dienst *Telegram* finden sich Angebote von 1000 Dollar im Tag für Angestellte von *Moneygram* oder *Western Union* für eine Zusammenarbeit mit Hackern. Generell findet 2018 eine Abwanderung vom Darknet in verschlüsselte Messengersysteme mit Apps und Plattformen wie *Amir Hack* und *Dark Job* statt, die Ermittlungsbehörden begannen bereits mit der Infiltration[239].

---

[234] Eine einzige Darknet-Plattform, die von der Polizei im Juni 2017 geschlossen wurde, hatte 20.000 Benutzer für Aktivitäten wie den Handel mit Drogen, Waffen, Kreditkarten, Falschgeld und falschen Ausweisen, vgl. FAZ 2017c. Später im Juli konnte eine weitere kriminelle Plattform (Missbrauch von Kindern) genannt *Elysium* mit 87.000 Nutzern gestoppt werden, vgl. Steinke 2017, S.6.
[235] vgl. Tellenbach 2017, S.31
[236] vgl. Steinke 2017, S.6
[237] vgl. Europol 2017
[238] vgl. Europol 2017
[239] vgl. FAZ 2018e

4.4 Attribution im Cyberwar

Die Zuordnung im Cyberkrieg ist aus theoretischer und rechtlicher Perspektive das wichtigste Attributionsproblem, da die Frage "*Wer war es?*" zur Vergeltung oder gar Krieg führen kann, wenn ein bestimmtes Schadensausmaß überschritten wird. Allerdings ist die praktische Relevanz der Sache fraglich, da es ein **Attributions-Paradoxon** gibt.

Die US- und chinesischen Cyberwar-Konzepte zeigen deutlich, dass ein konventioneller Schlag gleichzeitig oder sehr kurz nach dem Cyber-Angriff durchgeführt werden muss, wenn die militärische Aktion erfolgreich sein soll. Dies bedeutet, dass die Zuordnung des Cyber-Angriffs innerhalb von Minuten möglich ist, weil der Zielstaat gleichzeitig dem feindlichen Feuer ausgesetzt sein wird, d.h. der Angreifer *identifiziert sich selbst*.

Reales Praxisbeispiel: Bei dem Angriff auf eine mutmaßliche Atomanlage in Ostsyrien am 06.09.2007 mussten israelische Flugzeuge den gesamten syrischen Luftraum durchfliegen. Um dies zu ermöglichen, hatten die Israelis den Computern der syrischen Luftabwehr einen leeren Himmel vorgegaukelt, so dass die Flugzeuge unbehelligt einfliegen und angreifen konnten. Dies ist ein klassisches Beispiel für die Idee des Cyberwars als operativer Ergänzung zu konventionellen Maßnahmen[240].

Wenn ein massiver Cyber-Angriff ohne einen konventionellen Schlag durchgeführt wird, hat der Zielstaat Zeit, die Systeme zuerst wiederherzustellen und die Attribution in der Zwischenzeit zu beginnen, die mit aggressivem Gebrauch von nachrichtendienstlichen Methoden weniger Zeit in Anspruch nehmen kann, als die Angreifer erwarten.
Auf der anderen Seite ergibt sich eine Art **reverse attribution**, d.h., von der physischen zur digitalen Welt. In der Ära der Spionage-Satelliten wird die Vorbereitung eines großen Militärschlags nicht unentdeckt bleiben und er kommt typischerweise nach massiven politischen Spannungen, d.h. es gibt klare Warnzeichen in der physischen Welt für Angriffe in der digitalen Welt.

[240] vgl. Herwig 2010, S.60

5. Hochentwickelte Hackereinheiten und Malware-Programme

Mittlerweile wurden mehrere hochentwickelte Hackergruppen und Malwarefamilien entdeckt und berichtet, die in den folgenden Abschnitten dargestellt werden.

5.1 Hochentwickelte Malware-Programme

Hochentwickelte Schadprogramme (Malware) sind 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. Die höchstentwickelten Programme weisen technische Gemeinsamkeiten auf.

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. Derartige Fälschungen bergen ein hohes Fehlerrisiko, in größeren Malwareprogrammen kann es passieren, dass einzelne Zeitstempel oder Spracheinstellungen nicht durchgehend geändert wurden.
Zudem hinterlassen Hacker auch **digitale Fingerabdrücke**, womit man charakteristische Zugriffsmuster oder Programmcodes bezeichnet. Diese erlauben eine Differenzierung zwischen Angreifergruppen[241].
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 [242]. Informationen können auch in kleinen Bildern verborgen werden, einer als **Steganographie** bekannten Methode. benutzte Manchmal benutzen Angriffsserver *Twitter* oder e-mail zur Kommunikation mit dem Zielcomputer.

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

[241] vgl. Mayer-Kuckuck/Koenen/Metzger 2012, S.20-21
[242] vgl. Mandiant 2013

von Verschleierungssoftware (**obfuscation software**) zur Ersetzung von Namen und Veränderung von Klammern zu[243]. 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.

Viele Menschen betrachten Intrusion als statisches Ereignis: Sobald die Malware installiert ist, kann sich der Angreifer zurücklehnen und der Datenfluss läuft von allein.
In Wirklichkeit ist ein Cyberangriff ein **dynamischer Prozess**. Der Angreifer kann versuchen, die Zugangs- und Kontrollrechte zu erweitern oder durch eine **lateral movement**, d.h. zu anderen Computern der eingedrungenen Organisation zu gelangen. Es müssen Updates erstellt und maßgeschneiderte Module hochgeladen werden. Anleitungen müssen an den Zielcomputer gesendet werden.
Eindringlinge müssen darauf achten, dass sie nicht entdeckt werden, z.B. durch Veröffentlichung eines von ihnen verwendeten Exploits. Die extrahierten Daten müssen sorgfältig analysiert werden, um weitere Bedürfnisse zu identifizieren oder zu realisieren, wenn ein weiterer Angriff eine Verschwendung von Zeit und Ressourcen ist.
Deshalb ist es schwierig, den Angriff einer APT zu imitieren, auch wenn die Malware der jeweiligen Hackergruppe auf dem Schwarzmarkt verfügbar ist. Der Angreifer muss sich bewusst sein, dass die Cyber-Security-Unternehmen ihr Wissen nicht zur Gänze veröffentlichen, dass die Nachrichtendienste des Mitgliedsstaates auch mehr über die Nutzung wissen und natürlich die ursprüngliche Hackergruppe ihre Malware besser als jeder andere kennt und daher nicht nur am besten weiß, *was* benutzt wird, sondern auch *wie* und *wann*.

Allerdings könnte eine Angreifergruppe natürlich Malware verwenden, die auf dem Schwarzmarkt verfügbar ist, aber selbst dann kann die Gruppe **typische Charakteristika** und Programme im Einsatz zeigen.

Spezialisierte Hacker-Einheiten (z.B. die *Equation Group* and *Waterbug Group*) können Computer **auf bereits vorhandene Infektionen** mit ihrer Malware **überprüfen** und wenn sie Infektionen von Computern erkennen, die bisher weder angegriffen noch infiziert wurden, werden sie benachrichtigt. Die Hacker-Einheiten könnten sogar in der Lage sein, den Angriff unter falscher Flagge direkt zu untersuchen und dann hat der imitierende Angreifer sowohl in der digitalen als auch in der physischen Welt massive Probleme.

Zusätzlich zu den obigen Analysen ist die **Chronologie** der Malware-Entwicklung wichtig, um zu erkennen, welche Malware aus Vorläufern abgeleitet werden und damit mit denselben Angreifern zusammenhängen könnte. Für alle anspruchsvollen

[243] vgl. Welchering 2016, S. T4

Malware-Gruppen existiert eine solche Chronologie. Es ist erwähnenswert, dass z.B. die Stuxnet-Malware nicht nur eine lange Versionsgeschichte hatte, sondern dabei auch massive Veränderungen ihrer Struktur und Ziele (ursprünglich Klappenschluß, später Urangaszentrifugen) erfuhr. [244]

Im Bereich der Cyerkriminalität endet ein Cyber-Angriff nicht mit der Computer-Kommunikation, sondern das Geld, das durch die Angriffe gewonnen wird, muss übertragen und versteckt werden. Diese **Geldwäsche** wird in der Regel mit mehreren Transfers zwischen Bankkonten durchgeführt, um den Ursprung des Geldes zu verschleiern. Die **Verwendung von digitalen Bitcoins** löst das Problem nicht wirklich, denn am Ende müssen die Bitcoins dann doch wieder in echtes Geld umgetauscht werden. Die Übertragung von großen Geldsummen und schnelle Konto-Bewegungen sind Warnsignale.
Menschen, die ihr Bankkonto für Geldtransfers nutzen, sind die sogenannten **money mules**, d.h. neben den Hackern sind weitere Personen Teil der Cyberkriminalität. Experten identifizierten die Geldwäsche bei Cyber-Verbrechen als eine wichtige Schwachstelle der Angreifer[245].

5.2 Advanced Persistent Threats (APTs)

Die größten Hackergruppen werden auch als **Advanced Persistent Threat (APT)**, d.h. als fortschrittliche anhaltende Bedrohung bezeichnet. Bisher gilt eine klassische Definition, nach der APTs längerfristig agierende Angreifergruppen mit definierten Techniken, Taktiken und Programmen (TTPs) sind.
Die letzten Jahre haben jedoch gezeigt, dass folgende Definition für Spionage und Cyberwar präziser ist: Eine APT ist eine Projektgruppe innerhalb eines Nachrichtendienstes, die ihre Techniken, Taktiken und Programme (TTPs) sowie die Angriffsziele entlang der operativen Vorgaben ihres Dienstes entwickelt und anwendet.
Sicherlich ist es so, dass Hacker am Anfang ihrer Entwicklung erst einmal schauen, wie weit sie kommen und was sie mit ihren Erfolgen anfangen können, aber APTs bilden sich nicht von selber, sie werden durch Zusammenstellung geeigneter Leute gebildet und ihre Cyberaktivitäten an den Zielvorgaben ausgerichtet.

Typischerweise geht man daher 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

[244] vgl. McDonald et al. 2013, S.1-2
[245] vgl. Baches 2016, S.15

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 macht.246. 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**.

Die Angriffstaktik variiert: Führende Techniken sind **Phishing-E-Mails** mit infizierten Anhängen oder Links zu infizierten Websites. Wie in der *APT28/Fancy Bear*-Analyse der Sicherheitsfirma *FireEye* skizziert, können solche E-Mails auch zur Spurensuche verwendet werden, wie z.B. "spezifische E-Mail-Adressen, bestimmte Muster, spezifische Namensdateien, MD5-Hashes, Zeitstempel, benutzerdefinierte Funktionen und Verschlüsselungsalgorithmen"[247].

Die Verwendung **gestohlener Sicherheitszertifikate** und die Verwendung von **Zero-Day-Exploits** sind typische Indikatoren für eine anspruchsvolle Angreifergruppe.

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 Organisation 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 über hundert Gruppen geschätzt, die folgende Übersicht zeigt die bekanntesten Gruppen.

[246] Siehe auch Jennifer 2014
[247] vgl. FireEye 2014, S.29

Führende APTs

Land	Zuordnungen durch führende Cybersicherheitsfirmen
Russland	APT28/FancyBears/Sofacy/Strontium/Sednit (GRU)
	APT 29/Cozy Bears/Dukes (FSB oder SWR)
	Waterbug/Turla/Ouroburos/Venomous Bear/Krypton Gruppe (FSB)
	Sandworm/Quedagh (GRU)*
	Energetic Bear/Dragonfly (unklar, welcher Geheimdienst)
	Trisis/Triton/Temp Veles (Central Scientific Research Institute of Chemistry and Mechanics)
China (ca. 20 APTs)	APT 1/Comment Group (PLA)
	APT 10/Cloud Hopper (Staatssicherheit MSS)
USA	Equation Group (NSA)
	Longhorn/The Lamberts (CIA)
Nordkorea	Lazarus-Gruppe und Ableger
Israel	Unit 8200 (IDF)

Alle führenden Gruppen haben mehrere Namen, denn Analysten weisen einer Gruppe typischerweise einen Arbeitsnamen zu und es erweist sich erst später, dass dieselbe Gruppe von verschiedenen Analysten adressiert wurde. *Microsoft* benennt sie nach chemischen Elementen wie *Strontium, Potassium, Barium* usw., andere Firmen sprechen von *Bears* für russische Gruppen und *Pandas* für chinesische APTs, andere nummerieren die APTs, wieder andere beziehen sich auf Namen im Code, z.B. der Name *Sauron* in der APT *Project Sauron* (das all-sehende böse Auge aus *Herr der Ringe*), *Quedagh* oder *Ouroburos*.

Für die Smart Industry ist vor allem wichtig, dass Russland drei darauf spezialisierte APTs hat, nämlich *Triton* auf der Entwicklungsebene, *Dragonfly* für die Spionage und *Sandworm* für Angriffe (in der Ukraine). Es ist denkbar, dass alle drei APTs nur Teil eines umfassend angelegten Cyberproduktionsprozesses sind. In China gilt die APT10 als zurzeit erfolgreichste Industrie-APT, in Nordkorea steht die sogenannte *Lazarus*-Gruppe im Fokus der Debatte.

Aus amerikanischer Sicherheitsperspektive hat Russland innerhalb der letzten Jahrzehnte erhebliche Fortschritte mit der Errichtung hochspezialisierter Einheiten gemacht. Die APTs stehen unter Kontrolle der Geheimdienste. Russland hat vier Dienste als Nachfolger des ehemaligen sowjetischen Geheimdienstes KGB[248]:

- FSO – Föderaler Schutzdienst, auch für den Schutz des Präsidenten im Kreml
- FSB – Inlandsgeheimdienst, aber auch zum Teil im Ausland aktiv
- SWR - Auslandsgeheimdienst, auch für Intelligence Cooperation zuständig[249]
- GRU oder GU - militärischer Nachrichtendienst.

[248] vgl. Ackert 2018a, S.7
[249] vgl. Ackert 2018a, S.7

Im Jahr 2018 zeigte das *Mueller Indictment* (Anklageschrift), dass die USA offenbar in der Lage waren, Computeraktivitäten von *APT28/Fancy Bears*-Mitgliedern in zwei Gebäuden des russischen Militärgeheimdienstes GRU (jetzt GU) zu überwachen und zu protokollieren[250]. Die Industrial Control System (ICS)-fokussierte Gruppe *Sandworm/Quedagh* wird auch der GRU zugeordnet, die *Waterbug/Turla/Ouroburos/Venomous Bear/Krypton Gruppe*, dem FSB, während die *APT29/Cozy Bears* dem FSB oder SWR zugeordnet wird, aber der niederländische Geheimdienst berichtete, die *Cozy Bears*-Mitglieder identifiziert zu haben[251].

Die Niederländer haben eine gemeinsame *SigInt Cyber Uni*t mit etwa 300 Mitgliedern, die aus dem *Geheimdienst AIVD* und dem *Militärischen Geheimdienst MIVD* kommen, darunter eine offensive Cyber-Einheit von 80-100 Personen und eine Cyberdefense-Einheit. Die *SigInt Cyber Unit* war in der Lage, die Kontrolle über eine Überwachungskamera eines Universitätsgebäudes in der Nähe des Roten Platzes zu übernehmen, wo sich *Cozy Bears/APT29* mit einem durchschnittlichen Team von 10 Personen physisch befindet[252].

Aus historischen Gründen führt der FSB noch ausländische Operationen durch eine spezielle Abteilung durch. Analysten glauben, dass dies getan wird, um den Wettbewerb anzukurbeln, aber auch, um das Kräfteverhältnis zwischen den Diensten zu halten[253]. Die genauen Verbindungen nach Russland werden noch für die systemorientierte Gruppe *Energetic Bear/Dragonfly* diskutiert. Eine neue Gruppe *Temp.Veles* wurde im Jahr 2018 gemeldet, aber da es sich um ein staatliches Forschungsinstitut handelt, ist es fraglich, ob es sich um eine eigene APT oder nur um einen Malware-Anbieter für bereits bekannte APTs handelt.

Für die *Comment Crew/APT1* und die *Axiom/APT17 Group* werden Verbindungen zu China diskutiert, während die *Lazarus*-Gruppe vom FBI in Zusammenarbeit mit der Sicherheitsfirma *Mandiant* analysiert wurde: Die Gruppe benutzte nordkoreanische IP-Adressen und eine Menge gemeinsamer Infrastruktur, Techniken, Codes etc. bei verschiedenen Angriffen, die mit der *Lazarus*-Gruppe in Verbindung stehen[254].
Die *Equation Group* wird der US *National Security Agency (NSA)* zugeschrieben, was auf den Leaks der *Shadow Brokers*-Gruppe aus dem Jahr 2016 basiert, die mit einer nicht autorisierten Datenerhebung von NSA-Software durch einen

[250] vgl. Mueller 2018
[251] vgl. Paganini 2018a
[252] vgl. Paganini 2018a
[253] vgl. Ackert 2018a, S.7
[254]vgl. Shields 2018, S.56, 134 und 138

Auftragnehmer namens Harold T. Martin identisch waren[255]. Und 2017 konnte die als *Longhorn Group/The Lamberts* bekannte APT mit der CIA auf Basis der *Vault-7*-Lecks in Verbindung gebracht werden.
Aber es gilt unbedingt zu beachten, dass alle angesprochenen Regierungen solche Verbindungen verneint bzw. nicht kommentiert haben.

In der Praxis zögerten die Vereinigten Staaten lange, Angreifer offiziell zu benennen, weil dadurch Geheimdienstwissen der Öffentlichkeit zugänglich gemacht werden müsste. Dies führte zu dem sogenannten *Grizzly-Steppe*-Bericht 2016/2017 über die Beteiligung russischer Akteure an den US-Präsidentschaftswahlen, der für seine vagen Äußerungen kritisiert wurde. Unterdessen wurde beschlossen, einige Geheimdiensterkenntnisse zu enthüllen, die es erlauben, Angreifer offen und präzise zu benennen. Dies resultierte im *Mueller-Indictment* aus dem Jahr 2018, das die Erkenntnisse aus der Überwachung und Protokollierung von Computern der russischen Geheimdienstoffiziere als Mitglieder von *APT28/FancyBears* zeigt[256], einschließlich der organisatorischen Einteilung (GRU Units 26165 und 74455), die Namen der Offiziere und detaillierte Protokolle, wie, von wem und wann die Demokratische Partei angegriffen wurde, die gestohlenen Daten übertragen und durchsickern ließ (*spearphishing, DNC-Hack, DCLeaks, Guccifer 2.0*).

Nachdem Google im Jahr 2014 in einem Bericht mit dem Namen "*Peering into the Aquarium*" erhöhte Cyber-Aktivitäten des russischen Militärgeheimdienstes GRU festgestellt hatte, wurde nicht nur die Überwachung und Protokollierung von Computern von GRU-Offizieren durchgeführt, sondern von westlichen Diensten auch konventionelle nachrichtendienstliche Maßnahmen eingesetzt. Die Aktivitäten wurden massiv verstärkt, nachdem vier Russen, die als GRU-Mitglieder identifiziert wurden, in den Hauptsitz der OPCW in der Schweiz gereist waren, um ihre Untersuchungen zu chemischen Waffen zu beobachten. Dazu gehörten eine Beratung des ehemaligen GRU-Mitglieds Skripal und anderer ehemaliger Agenten, das Abhören von Telefonaten und Kontakte zum russischen Passamt und der Verkehrspolizei. [257][258] Die Kombination dieser Quellen erlaubte es, die Adresse eines GRU-Gebäudes und dazu 300 GRU-Mitglieder zu identifizieren, da ihre Autos mit der Adresse dieses Gebäudes gemeldet wurden[259].

In gleicher Weise wurde die *Lazarus*-Gruppe vom FBI in Zusammenarbeit mit der Sicherheitsfirma *Mandiant* analysiert, um einen nordkoreanischen Offizier Park Jun Hyok als Schlüsselmitglied zu identifizieren. Die Gruppe benutzte nordkoreanische

[255] vgl. Perloth/Shane 2017
[256] vgl. Mueller 2018
[257] vgl. Rüesch 2018, S.4-5
[258] vgl. Ackert 2018b, S.3
[259] vgl. Ackert 2018b, S.3

IP-Adressen und eine Menge gemeinsamer Infrastruktur, Techniken, Codes etc. bei verschiedenen Angriffen, die mit der *Lazarus*-Gruppe in Verbindung stehen[260], und untermauerte so die Ergebnisse der *Operation Blockbuster* mit soliden Beweisen.

5.2.1 Die Equation Group

Das erste 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.

Forscher von *Kaspersky Labs* entdeckten die *Equation Group* im September 2014, 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 *Stuxnet*versionen 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.

Mittlerweile wird die Existenz einer gesonderten *Equation Group* in Frage gestellt, da es sich nur um einen Arbeitsbegriff für die NSA selbst handeln könnte[261]. Diese Vermutung wird dadurch gestützt, dass die im *Shadow Brokers*-Vorfall gesammelte Malware im *Harold T. Martin-Prozess* von 2017/2018 als originäre NSA-Software behandelt wird.

5.2.1.1 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 Programm 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.

[260] vgl. Shields 2018, S.56, 134 und 138
[261] vgl. Perloth/Shane 2017

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 Acquisition SCADA*[262]) 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[263].
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[264].
Stuxnet wurde mit Hilfe von infizierten USB-Sticks in Computer eingebracht. In Windows existierte eine Schwachstelle in LNK-Dateien, die als Eintrittspforte genutzt wurde[265]. 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[266].
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[267]. 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[268]. 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[269].
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[270]. Es kamen

[262] vgl. Shea 2003
[263] vgl. Welt online 2010b. Siemens baut daher seine Cyberwarforschung aus, vgl. Werner 2010, S.7
[264] Da Stuxnet sehr viele (Dutzende) Funktionen hat, wird es in der Literatur auch als Trojaner oder als Virus bezeichnet, vgl. auch FAZ2010a.
[265] Am 13.10.2010 gab Microsoft deshalb 16 Updates heraus, die insgesamt 49 Sicherheitslücken schlossen, vgl. Handelsblatt 2010, S.27.
[266] vgl. Rieger 2010, S.33, der auch den Begriff des digitalen Erstschlags prägte.
[267] vgl. Krüger/Martin-Jung/Richter 2010, S.9
[268] vgl. Schultz 2010, S.2
[269] vgl. Kaspersky 2010
[270] vgl. Falliere 2010

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[271], die daraufhin vom Iran auch bestätigt wurden[272][273].
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[274] ergab sich in den Medien das Bild einer gezielten Superwaffe, die möglicherweise von Geheimdiensten konstruiert wurde, um das iranische Atomprogramm zu sabotieren[275].

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[276].

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[277].

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[278]. Die Berichte der New York

[271] vgl. FAZ2010c, S.6
[272] 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.
[273] 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.
[274] vgl. Schultz 2010, S.2
[275] vgl. Ladurner/Pham 2010, S.12
[276] vgl. McDonald et al. 2013, S.1-2
[277] vgl. Broad/Markoff/Sanger 2011, S.4
[278] vgl. Sanger 2012, S.3

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[279].

Durch einen technischen Fehler hatte Stuxnet den Computer eines Ingenieurs infiziert und sich dadurch im Internet in andere Länder ausgebreitet[280]. 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[281]. 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 aufrechterhalten, d.h. der Angriff wurde im Bezug auf die Software sehr präzise ausgeführt, nicht jedoch im Bezug auf Zeitpunkt und Ort[282].

Es muss aber auch der Schaden betrachtet werden, den Stuxnet für die Zukunft anrichtet, denn mit Stuxnet wurde auch das Know-How allgemein preisgegeben[283]. 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[284]. 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[285].

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*[286]. *DuQu* benutzte ein gestohlenes Sicherheitszertifikat eines taiwanesischen Unternehmens zum Eindringen und konnte z.B. screenshots machen, Tastatureingaben protokollieren (keylogging) und

[279] vgl. NZZ 2012, S.1, FAZ 2012b, S.7
[280] vgl. Sanger 2012, S.6
[281] vgl. Handelsblatt 2010, S.27, Symantec 2010, S.5-7
[282] 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
[283] vgl. Rosenbach/Schmitz/Schmundt 2010, S.163, Rieger 2011, S.27
[284] vgl. Iran Daily 26 July 2010
[285] vgl. Knop/Schmidt 2010, S.20
[286] vgl. Goebbels 2011, S.8. Der Name stammte von dem im Programmiercode verwendeten Präfix DQ.

Informationen aus den befallenen Computern verschicken und wie Stuxnet verfügte es auch über ein Verfallsdatum mit Selbstzerstörung[287]. Es wurde vermutet, dass *DuQu* evtl. dazu dienen sollte, Informationen aus den Zielsystemen zu gewinnen, die für die Schaffung von *Stuxnet* genutzt wurden[288].

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'[289] namens *Flame*, das sehr detaillierte Informationen über die infizierten Systeme weitergibt und das wiederum eine technische Verwandtschaft zu *Stuxnet* aufwies[290].

Die *Washington Post* berichtete, dass *Flame* bereits im Jahre 2007 entwickelt wurde und Teil der Cyberaktivitäten gegen den Iran war[291]. Der Programmteil, der die Infektion durch USB-Sticks ermöglichte, wurde zuerst in *Flame* und dann in *Stuxnet* verwendet[292].
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*[293].

5.2.1.2 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.[294]

Der *Kaspersky*-Virenschutz schlug im September 2014 bei einem massiv Malware-verseuchten Privatcomputer an, wobei sich der Computerbesitzer als NSA-Kontraktor entpuppte[295]. Kaspersky hatte am 11 Sep 2014 die Equation Group-Malware gefunden, aber nur, weil der Besitzer des Computers auch andere Malware

[287] vgl. Goebbels 2011, S.8
[288] vgl. Welchering 2012, S. T1
[289] 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.
[290] vgl. Welchering 2012, S. T1, Graf 2012, S.8, Gostev 2012, S.1
[291] vgl. Graf 2012, S.9, was aber offiziell ebenfalls nicht bestätigt wurde.
[292] Nakashima/Miller/Tate 2012, S.1-4
[293] vgl. Focus 2012, Symantec 2012, Mertins 2012, S.10
[294] vgl. Kaspersky Lab 2015, S.3
[295] vgl. Kaspersky Lab 2017

auf dem Computer hatte. Ein *7zip*-Archiv, das von *Kaspersky* Antivirus geprüft wurde enthielt *Equation Group*-Tools, die der Mitarbeiter vorschriftswidrig mit nach Hause genommen hatte[296]. Die Entdeckung war also nur ein Beifang.

Der Computerbesitzer hatte 121 weitere Malwareprogramme auf dem Rechner[297], u.a. die Backdoor *Mokes/SmokeBot/Smoke loader*, die seit 2011 in russischen Untergrundforen bekannt war, deren Command and Control-Server jedoch 2014 von einer chinesischen Gruppe namens *Zhou Lou* registriert waren, so dass auch weitere Akteure im Rechner der Zielperson gewesen sein könnten[298].
Die Israelis waren jedoch bereits im Rechnersystem von Kaspersky mit der Spionagesoftware *Duqu 2.0* und konnten die Aktivitäten beobachten[299].

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[300].

Grayfish infiziert den boot record des Betriebssystems und übernimmt die totale Kontrolle, d.h. betreibt den gesamten Computer[301]. Es sammelt Daten und legt sie verschlüsselt als **encrypted Virtual File System** in der Registry des Computers ab, wo es für Antivirus-Produkte unsichtbar ist[302]. *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.[303]

Die *EquationGroup*-Malware wird durch interdiction verbreitet, bei der versandte CD-ROMs und andere physische Medien während des Transportes entnommen und

[296] vgl. Kaspersky Lab 2017
[297] vgl. Kling 2017c, Weidemann 2017a
[298] vgl. Kaspersky Lab 2017
[299] vgl. Weidemann 2017a
[300] vgl. Kaspersky Lab 2015, S.5, 8
[301] vgl. Kaspersky Lab 2015, S.10. Schon EquationDrug war in der Lage, die volle Kontrolle zu erlangen, siehe S.8
[302] vgl. Kaspersky Lab 2015, S.10-12
[303] vgl. Kaspersky Lab 2015, S.13

durch infizierte ersetzt werden. *EquationDrug* und *Grayfish* können auch noch die Firmware infizieren, d.h. die in die Hardware eingebetteten essentiellen Programme eines Computers[304]. 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 *EquationGro*up Malware-Familie und der *Stuxnet*-Familie sind die folgenden[305]: *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[306]. 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[307]. Die Programmierer setzten ‚**false flags**', d.h. nutzten Codeelemente, die auf andere Hackergruppen verweisen sollten[308]. Auch Zeitstempel wurden manipuliert.

DuQu 2.0 wird inzwischen Israel und der *Unit 8200* zugerechnet[309]. Dieses gegenüber *DuQu* weiter entwickelte Programm richtete sich auch gegen US-Ziele. Aufgrund der mit *DuQu 2.0* gesammelten Hinweise beobachtete der israelische Geheimdienst, dass russische Geheimdienstler *Kaspersky*-Zugänge wohl im piggybacking-Verfahren dazu nutzten, US-Ziele auszuspähen, weshalb eine diesbezügliche Warnung an die NSA erging[310]. Dieser Vorgang wurde dann 2017 vom *Wall Street Journal* publiziert[311] zu dem Zeitpunkt, wo Kaspersky seine kostenlose Antivirusversion *Kaspersky Free* auf den Markt brachte, was einen erheblichen Nutzungszuwachs erwarten ließ. Das *Department of Homeland Security DHS* verbot den internen Einsatz von Kaspersky-Software[312]-

[304] vgl. Kaspersky Lab 2015, S.15-16
[305] vgl. Kaspersky Lab 2015, S.5
[306] vgl. Kaspersky Lab 2015b, S.3
[307] vgl. Kaspersky Lab 2015b, S.4
[308] vgl. Kaspersky Lab 2015b, S.43
[309] vgl. Perloth/Shane 2017
[310] vgl. Perloth/Shane 2017, Beiersmann 2017e
[311] vgl. Lubold/Harris 2017
[312] vgl. Beiersmann 2017e

Dies wurde auch mit der Entdeckung der *Equation Group* 2014/2015 in Verbindung gebracht; *Kaspersky* bestritt dies jedoch energisch und verwies darauf, dass die Aufdeckung nur dadurch erfolgte, dass der Kaspersky-Virenschutz im September 2014 bei einem massiv Malware-verseuchten Privatcomputer anschlug, also der Virenschutz lediglich seine Arbeit tat und der Computerbesitzer sich als NSA-Kontraktor entpuppte[313].

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 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[314]. Ähnlich wie bei der *Equation Group* wurden encrypted virtual file system containers und eine RC5-Verschlüsselung benutzt[315]. *Regin* hat viele Eigenschaften wie die Überwachung des Datenflusses, die Entnahme von Informationen und das Sammeln von Daten[316]. Wie bei den anderen beschriebenen Schadprogrammen wurden wieder nur wenige ausgewählte Ziele attackiert[317].

Im Februar 2014 wurde eine weitere spezielle Cyberattacke von *Kaspersky Labs*[318] 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.

5.2.1.3 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)[319]. Die Auktion wurde jedoch ganz schnell abgeschaltet, das letzte

[313] vgl. Kaspersky Lab 2017, Beiersmann 2017e
[314] vgl. Symantec 2014a, S.3
[315] vgl. Symantec 2014a, S.3
[316] vgl. Symantec 2014a, S.11
[317] vgl. Martin-Jung 2014, S.17
[318] vgl. Kaspersky 2014
[319] vgl. Jones 2016

Gebot lag bei 0,12 Bitcoins (60 Euro). [320] 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[321].

Die Analyse der öffentlichen Datei zeigte Software von 2013[322]; 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.
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[323]. 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 NSA-Tools bezeichnet hatte, wie z.B. *Epicbanana, Buzzdirection, Egregiousblunder, Bananaglee, Jetplow* und *Extrabacon*[324]. 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[325].

Am 31. Oktober 2016 veröffentlichten die *Shadow Brokers* eine Liste von Servern mit 352 IP-Adressen, die von der Equation Group genutzt wurden, darunter 32 *edu*-Domains aus verschiedenen Ländern und dazu sieben weitere Tools wie *Orangutan* (die z. B. in Deutschland gefunden wurde) und *Patchicillin*[326].

---

[320] vgl. Beuth 2016b, Spiegel online 2016
[321] vgl. Jones 2016
[322] vgl. Shane/Perloth/Sanger 2017
[323] vgl. Ragan 2016
[324] vgl. Steier 2016b, Spiegel online 2016, Solon 2016
[325] vgl. Steier 2016b
[326] vgl. Spiegel online 2016b. In einer weiteren Botschaft mit dem Namen *Black Friday/Cyber Monday sale* wurde ein Screenshot mit der Dateistruktur der Cybertools veröffentlicht.

Am 08.04.2017 wurde das lange und komplexe Passwort zu den verschlüsselten Dateien von 2016 veröffentlicht, was die vorher geleakten Dateien zugänglich machte[327].
Am 14.04.2017 wurden weitere Instrumente veröffentlicht, darunter *DoublePulsar, EternalBlue* und *EternalRomance*, die dann vermutlich von anderen Akteuren zur Vorbereitung von drei großen Cyber-Attacken namens *WannaCry/WanaDecryptor 2.0, Adylkuzz* und *Petya/Not-Petya/Petya2017* verwendet wurden (vgl. später zur Lazarus-Gruppe im selben Abschnitt).
Im Mai 2017 sagten die *Shadow Brokers*, dass sie über Daten zur Überwachung von SWIFT-Servern durch die NSA und zu nuklearen Programmen verfügen würden[328].
Im September 2017 gaben die *Shadow Brokers* ein älteres NSA-Manual für Angriffe auf Windows, *Unitedrake*, frei.[329]

Um mögliche Verbindungen zu den *Shadow Brokers* zu klären, wurden diverse NSA-Mitarbeiter einem Lügendetektortest (Polygraphen) unterzogen, einige wurden suspendiert, einige mussten ihren Pass abgeben, wobei jedoch die Verbindungen zu den *Shadow Brokers* nicht geklärt werden konnten.[330]
Ein besonderer Fokus lag auf jenen Mitarbeitern, die auch schon für die CIA gearbeitet hatten, um zu prüfen, ob eine Verbindung zwischen den *Vault7*-Releases auf Wikileaks und den *Shadow Brokers* bestehen könnte[331].

Harold T. Martin III leak
Untersuchungen u.a. durch das FBI nach den *Shadow Brokers-Leaks* führten im August 2016 zur Entdeckung des nicht autorisierten Kopierens von Daten durch Harold T. Martin.
Die gefundenen Dateien würden 500 Millionen gedruckten Seiten an Material entsprechen. Er lagerte sie in seinem Haus in Maryland auch an unsicheren Orten, wie der Garage und auf dem Rücksitz seines Autos, das trotzdem offen auf der Straße stand. Die Speicherung bestand aus Festplatten, Computern, USB-Sticks und Ausdrucken[332].

Er arbeitete für sieben private Unternehmen bei verschiedenen Agenturen, darunter die CIA, Cybercom und ODNI und war zuletzt bei *Booz Allen Hamilton* beschäftigt, wo er von 2012-2015 als Auftragnehmer in der *Tailored Access Operations Group TAO* der NSA arbeitete[333]. Dann war Mr. Martin in ein Cyber-Security-

[327] vgl. Kramer 2017
[328] vgl. Brinkmann 2017
[329] vgl. Shane/Perloth/Sanger 2017
[330] vgl. Shane/Perloth/Sanger 2017, Mikelionis 2018
[331] vgl. Shane/Perloth/Sanger 2017
[332] vgl. Ammann 2016, S.3
[333] vgl. Marimov 2017

Doktorandenprogramm an der University of Maryland eingeschrieben, für das er weitere Forschung betrieb[334].
Es ist nicht klar, wie die *Shadow Brokers* die Hackerwerkzeuge erhielten, die - wie von der *Washington Post* berichtet - *identisch* sind mit denen, die von Harold T Martin entwendet wurden, nach Aussagen ehemaliger Beamter[335]. Auch scheint es praktisch die *gesamte* Bibliothek der NSA zu sein (‚virtually the entire library')[336].
Er hat über Jahre eine riesige Menge an Daten aus verschiedenen Agenturen gestohlen, d.h. auch *außerhalb* der NSA.
Ursprünglich galt die Arbeit der *NSA-Tailored Access Group TAO* als *Exceptionally Controlled Information*, die nur in Safes gelagert werden durfte. Die Regeln wurden später gelockert, als die Mengen an Informationsmaterial immer mehr anwuchsen[337].

Zu Harold Martin wurde berichtet, Zugang zu vertraulichem Material seit 1996 seit seiner Zeit an der US-Marine zu haben;[338] und am Gericht plädierte er zunächst auf nicht schuldig[339], die Untersuchung und der Prozess sind noch im Gange.
Harold T. Martin wollte sich im Januar 2018 für den ersten von 20 Anklagepunkten schuldig bekennen, 19 weitere Punkte werden noch verhandelt. Eine Verbindung zu den *Shadow Brokers* konnte bisher nicht gezeigt werden. Er hatte Dateien von der *NSA, US Cybercom*, der CIA and des NRO gesammelt[340].

5.2.2 Die Longhorn Group/Lamberts/Der Vault 7-Vorfall

Im März 2017 begann die Plattform *Wikileaks*, Informationen über die Cyber-Fähigkeiten der *Central Intelligence Agency CIA* unter dem Namen *Vault 7* zu veröffentlichen Das Leck umfasste 7818 Webseiten und 943 Anhänge aus dem *CIA Cyber Center of Intelligence*[341].
Digitale Spuren führten Ermittler zu einem Team von Entwicklern, die früher mit der CIA Engineering Development Group zusammenarbeiteten. Allerdings haben diese Vertragspartner die Projekte verloren und waren deshalb unzufrieden, was der Grund für das Leck gewesen sein könnte[342].
Von der Organisationsseite aus hatte das bereits bekannte *CIA Cyber Center of Intelligence* im Jahr 2016 eine geschätzte Mitarbeiterzahl von 5.000 Personen und 1.000 Programmen[343].

---

[334] vgl. Ammann 2016, S.3
[335] vgl. Nakashima et al. 2017
[336] vgl. Nakashima et al. 2017
[337] vgl. Shane/Perloth/Sanger 2017
[338] vgl. Ammann 2016, S.3
[339] vgl. Marimov 2017
[340] vgl. Mikelionis 2018
[341] vgl. Derespins 2017, Shane/Mazetti/Rosenberg 2017
[342] vgl. Harris/McMillan 2017, Deutschlandfunk 2017
[343] vgl. Derespins 2017

Es gibt eine Vielzahl von spezialisierten Gruppen (branches), wie zum Beispiel die Embedded Development branch für die Einbettung von Implantaten in VoIP-Telefone, Smart-TVs etc., die Network-Devices branch für Router und die Mobile Development branch für Mobiltelefone. Das *Cyber Center of Intelligence Europe (CCI Europe)* ist verantwortlich für Europa, die MENA-Region und Afrika.[344]. Allerdings scheint es, dass die Bemühungen auf Einzelpersonen statt auf Massenspionage gerichtet waren [345].

Die von *Vault7* offenbarten Cyber-Tools wie Malware-Archive, Verschleierungs (obfuscation) software, Spyware, interdiction etc. spiegeln den Stand der Technik der Cyber-Intelligenz wider.

Die wichtigsten Ergebnisse waren bisher:

- Umgehung der Verschlüsselung von Messenger Services und Smartphones.[346]. Car Hacking wurde nur ausprobiert, Erfolgsberichte waren nicht verfügbar.
- *Weeping Angel*-Spyware kann Smart-TVs (Samsung Modell F-8000) infizieren, wenn Agenten physischen Zugang zu ihnen haben, was es ermöglicht, TV-Zuschauer zu beobachten, da der Fernseher nur in einem gefälschten Off-Modus ist.[347]
- Die Sammlung ausländischer Malware hat den Namen *Umbrage*[348]
- Im April 2017 wurde die Verschleierungsoftware *Marble* geleakt, die auch für die **Entschleierung (de-obfuscation)** verwendet werden kann, d.h. die zuvor getroffenen Schritte wiederherzustellen. *Marble* ist in der Lage, Code-Fragmente zu verstecken, liefert auch Textbeispiele in Fremdsprachen, die Analysten verwirren können. *Marble* Version 1.0 wurde im Jahr 2015 veröffentlicht.[349]
- Im Mai 2017 wurde die Spyware *Athena* (zusammen mit der Betriebsanleitung *Hera*) bekannt gegeben, die alle Windows-Versionen mit oder ohne Internet-Zugang infizieren kann und seit August 2015 aktiv war [350]
- Im Juni wurde berichtet, dass eine fortschrittliche CIA-Firmware seit dem Jahr 2007 Wi-Fi-Router infiziert hat. Ein Exploit-Code namens *Tomato* kann Passwörter auslesen, wenn der Plug-and-Play-Modus aktiviert ist. Die Malware *CherryBlossom* steuert die Router, bei Routern von 10 Herstellern

[344] vgl. BfV 2017
[345] vgl. Shane/Mazetti/Rosenberg 2017
[346] vgl. Shane/Mazetti/Rosenberg 2017
[347] vgl. Shane/Mazetti/Rosenberg 2017
[348] vgl. Goetz/Steinke 2017
[349] vgl. Beiersmann 2017a
[350] vgl. Kolokhytas 2017

sind bekannt, dass sie infiziert sind[351]. *Brutal Kangooro* ist eine fortschrittliche USB-Stick-Malware, die über das Internet versendet werden kann, dannach infiziert sie den ersten USB-Stick. Einmal installiert, baut es verdeckte Netzwerke innerhalb eines geschlossenen Netzwerks auf.[352]

- *Highrise* ist Teil einer größeren technischen Plattform und ist ein SMS-Proxy, der SMS-Nachrichten des Ziels zu einem Abhörpunkt umleiten kann[353].
- Im *Vault 8* genannten *Wikileaks*-Release von Ende 2017 wurde berichtet, dass die CIA den Nachrichtenverkehr mit ihren Command und Control-Servern durch gefälschte Kaspersky-Sicherheitszertifikate als unverdächtig erscheinen ließ. Das Ganze ist auch als *Project Hive (Bienenkorb)* bekannt[354].

Darüber hinaus entdeckte *Symantec*, dass die seit 2011 bekannte *Longhorn Group/The Lamberts*, eine APT, mit den Dateien von *Vault7* verknüpft ist[355].
Longhorn Group/The Lamberts ist eine seit 2011 bekannte APT mit Angriffen in 16 Ländern auf Ziele von strategischem Interesse. Die Malware *Fluxwire* hat starke Ähnlichkeiten zu Daten von *Symantec* für den Trojaner *Corentry*, für die Malware *Archangel* mit *Trojan.Plexor*. *Longhorn Group/The Lamberts* benutzt zwei weitere Backdoors namens *LH1* und *LH2*. Die *Longhorn*-Gruppe hat auch ein Programm geschrieben, das definiert, an welchem Tag der Woche die Malware Kommunikation mit dem Kontroll-Server hat.
Im Oktober 2014 wurde ein Zero-day-Exploit (Hintertür) von *FireEye* entdeckt und von Kaspersky *Black Lambert* genannt. Weitere Varianten wurden entdeckt, die seit 2016 *White, Blue, Green, Pink* und *Gray Lambert* heißen. Die Lamberts-Malwarevarianten teilen sich Codes, Stile, Datenformate, Kommando-und Steuerungsserver und Ziele und verwenden Namen aus Filmen (*Flash Gordon*), Computerspielen, TV-Serien (*Star Trek*) in ihren Codes, was eine interessante Parallele zur *Sauron* und *Slingshot* APT ist. Die Angriffe wurden nur auf einer kleinen Anzahl von Computern ausgeführt und auf die Opfer zugeschnitten.[356]

5.2.3 Sauron/Strider und Slingshot

Die neue APT *Project Sauron* (auch bekannt als *Strider*) wurde im Jahr 2016 entdeckt, aber die Malware-Eigenschaften zeigen an, dass die Programmierer von anderen anspruchsvollen Malwareprogrammen gelernt haben, insbesondere von *Duqu, Flame* (Verwendung der Programmiersprache *Lua*), *Equation* und *Regin*,

[351] vgl. Goodin 2017
[352] vgl. Beiersmann 2017b
[353] vgl. Beiersmann 2017d
[354] vgl. Borchers 2017
[355] vgl. Samnite 2017
[356] vgl. Kaspersky 2018b

aber schon zu einer Zeit, wo diese Malware-Typen noch nicht entdeckt waren, was auf eine Beziehung zwischen den APTs hindeuten kann[357].
Kaspersky berichtete über die neue *Slingshot* APT, die die gleiche Komplexität wie *Sauron* oder *Regin* hatte, die seit mindestens 2012 aktiv ist und dabei eine Schwachstelle von *Mikroti*k-Routern (lettischer Netzwerk-Hardware-Anbieter) nutzte, um Opfer vor allem im Nahen Osten und in Afrika zu infizieren[358]. Im Code gab es Verweise auf das Buch "Herr der Ringe" (*Gollum, Smeagol*). *Slingshot* ist auch der Name eines Loaders, der versucht, modulare Malware zu platzieren, insbesondere die *Gollum*-App und ihr unterstützendes *Cahndr (Ndriver)*-Modul, das z.B. Debugging-Aktivitäten des angegriffenen Computers blockiert, um eine Datenexfiltration zu ermöglichen.

Es ist zu beachten, dass die *Sauron* und *Slingshot* APTs die Verwendung von Popkultur-Begriffen in ihren Codes mit *The Lamberts* teilen. Andererseits bezog sich auch die offenbar russische APT *Sandworm/Quedagh* auf den Science-Fiction Roman *Dune*.

5.2.4 APT28 und APT29

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

APT 28 (alias Sofacy, Pawn Strom, Csar Team, Sednit, Fancy Bear, Strontium) ist eine Gruppe, die sich auf Ziele mit politischer Relevanz für Russland richtet und die seit 2004 beobachtet wird[359]. 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.[360] APT 28 nutzt eine Vielfalt an Malware (*Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer and DownRange*) und verfügt auch über Malware für Smartphones[361].

APT28 hat eine typische Angriffsstrategie[362]:

- Sie beginnen mit einer gut ausgearbeiteten, gezielten Phishing-E-Mail.
- •Dies kann auch eine Verknüpfung zu einem interessanten Thema beinhalten. Die URL-Adresse (URL) unterscheidet sich jedoch etwas von der ursprünglichen URL (**Tabnabbing**), so dass das Opfer auf einer bösartigen

[357] vgl. Kaspersky 2016, S.21, Symantec 2016b
[358] vgl. Kaspersky 2018a
[359] vgl. ESET 2016
[360] vgl. Weedon 2015, S.71-72
[361] vgl. Alperovitch 2016
[362] vgl. Hacquebord 2017

Webseite landet. Manchmal wird der Nutzer aufgefordert, die Login-Daten neu einzugeben. Was ein harmloser technischer Fehler zu sein scheint, wird in Wirklichkeit verwendet, um Passwörter (**Credential Phishing**) zu bekommen. Die Anzahl der gefälschten URLs ist hoch: Die Sicherheitsfirma *ESET* entdeckte eine irrtümlich öffentliche Liste mit rund 4.400 URLs, die zwischen März und September 2015 durch die *Bitly*-Methode verkürzt wurden[363]. Mehrere der Domains, die APT28 registrierte, imitierten NATO-Domainnamen, einschließlich der *NATO Special Operations Headquarters* und der *NATO Future Forces Exhibition*[364]

- Auch wurden manchmal **watering hole**-Angriffe verwendet. Hier werden potenziell interessante Webseiten infiziert, z.B. mit dem *Browser Exploitation Framework (BeEF)* und während des Besuchs wird der Browser der Zielperson angegriffen.

Die Malware kann in drei Gruppen aufgeteilt werden: im ersten Schritt Software für die Aufklärung, im zweiten Schritt Software wie *X-Agent* für Spionage, während im dritten Schritt die finale Software wie *X-Tunnel*, um andere Computer zu erreichen[365]. *FireEye* nannte 2014 den Downloader *Sourface, das* Spionage-Tool *Eviltoss* und das modulare Implantat *Chopstick.*[366].

5.2.4.2 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-phishing 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[367].

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

[363] vgl. ESET 2016
[364] FireEye 2014, S.14
[365] vgl. ESET 2016
[366] vgl. FireEye 2014, S.14
[367] vgl. Raiu/Baumgartner/Kamluk 2013

benutzt werden, die als *The Dukes* oder auch als *APT29* bezeichnet wird[368]. Die Attacken zeigen ein zweistufiges Vorgehen mit einem initialen Einbruch in das attackierte System, dem, falls es sich um ein relevantes Ziel handelt, der Übergang zu einer Langzeitüberwachung folgt[369]. Für dieses Vorgehen sind mehrstufige Ladevorgänge und Backdoors verfügbar. Zugangswerkzeuge (Remote Access Tools RATs) waren u.a. *AdobeARM*, *ATI-Agent* und *MiniDionis*[370]. 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, was 2018 bestätigt werden konnte.

5.2.4.3 Der Cyberangriff auf den Bundestag

Der deutsche Bundestag ist seit Jahren ein primäres Angriffsziel[371], jedoch stehen auch Regierungsbehörden im Fokus wie das Außenministerium und die Botschaften.

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[372]. Der Server für die Satellitensignale wurde angegriffen und da dieser von einem Drittanbieter gewartet wurde, konnte ein längerer Ausfall des Signals erreicht werden[373].

Der *Verfassungsschutz BfV* bekam einen Hinweis aus dem Ausland, dass ein Cyberangriff mit Datenaustausch zwischen zwei Bundestagscomputern mit einem osteuropäischen Server im Gange sei[374]. Untersuchungen bestätigten das Eindringen in mehrere Computer durch infizierte emails[375], einschließlich der Übernahme von Administratorenrechten[376].

[368] vgl. Weedon 2015, S.70-71
[369] vgl. F-Secure Labs 2015
[370] vgl. Alperovitch 2016
[371] vgl. Lohse/Sattar/Wehner 2015, S.3
[372] vgl. FAZ online 2015, S.1
[373] vgl. Wehner 2016a, S.6
[374] vgl. Baumgärtner/Röbel/Schindler 2015, S.28.
[375] vgl. Mertins 2015, S.4
[376] vgl. Hoppe/Osman 2015, S.1

Im Jahr 2017 wurde eine eingehende Analyse veröffentlicht [377]. Am 30. April 2015 erhielten die Abgeordneten eine E-Mail mit einem Artikel „Ukraine conflict with Russia leaves economy in ruins“. Nach dem Herunterladen wurden mehrere Programme von den Angreifern ausgeführt, darunter das Programm *Mimikatz*, das nach Admin-Passwörtern sucht. Ein paar Tage später waren 5 von 6 Administratorpasswörtern unter Kontrolle der Angreifer.
Eine Person bemerkte am 08.05.2017 die Unmöglichkeit, den französischen Accent aigu zu benutzen. Das BSI wurde benachrichtigt und fand später die Malware *X-Tunnel*. Weitere Analysen zeigten eine IP-Adresse, die von einer Firma in Pakistan gemietet wurde und später auch im DNC-Hack, dem WADA-Hack und der CDU verwendet wurde.
Ein anderer Server konnte einer russischen Person namens *Roschka* zugeordnet werden, die auch scheinbar in den Macron-Hack involviert zu sein schien und für *Eureka CJSC* arbeitet, die als Sicherheitspartner des russischen Militärgeheimdienstes GRU bekannt ist. Auch bei einem älteren Angriff von *Fancy Bears* führte ein technisches Problem zu einer Umleitung des Datenflusses und konnte in Moskau zu einem Gebäude der GRU verfolgt werden. Das Programm, das bei diesem älteren Angriff verwendet wurde, war das gleiche für den Bundestag und den DNC-Hack.

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[378]. Der Angriff wies Ähnlichkeiten zum Angriff auf den französischen TV-Sender TV5Monde auf[379].
Einer der für die Attacke auf den Bundestag genutzten Server war identisch zu denen der DNC-Attacke von 2016 und ebenso ein gefälschtes Sicherheitszertifikat[380].
Auch der OSZE-Hack (der nur einer von vielen gemeldeten Fällen wie Tschechien, Polen, Norwegen usw. war), den man Ende 2016 entdeckte, wies Ähnlichkeiten auf[381].

Anfang 2017 stellte das BSI einen ungewöhnlichen Verkehr fest und erkannte einen weiteren Angriff auf die Bundestagsmitglieder, mindestens 10 Mitglieder wurden angegriffen [382]. Dazu gehörte das Mitglied der Grünen, Marielouise Beck, deren Computer bereits 2014 von der Malware *Miniduke* von *APT 29/CozyBears* infiziert wurde[383].

[377] Beuth 2017, S.13-15
[378] vgl. Erk et al. 2015, S.2
[379] vgl. FAZ online 2015, siehe auch Wehner 2015, S.1
[380] vgl. Baumgärtner/Neef/Stark 2016, S.90-91
[381] vgl. Deutsche Welle 2016
[382] vgl. Tanriverdi 2017
[383] vgl. Wehner 2016b, S.9

Der Angriff wurde durch die Präsentation bösartiger Online-Werbung von einem Dritten auf der Website der *Jerusalem Post* durchgeführt, eine Methode namens **Malvertising**[384].
In 2017 waren **malvertising-Kampagnen** ein globales Problem, insbesondere durch die Malware *RoughTed*, die Adware, Exploit kits und Ransomware verbreitete[385].

5.2.4.4 Der DNC hack/Angriff auf die Wahlsysteme

Entdeckungsgeschichte
Das *Democratic National Committee (DNC)*, das formelle Leitungsgremium der Demokratischen Partei, alarmierte die Sicherheitsfirma *Crowd Strike* wegen eines Angriffs auf ihre Systeme[386].
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 protokollieren zu können[387]. Einer der für die DNC-Attacke genutzten Server war identisch zu dem der Attacke auf den Bundestag und ebenso ein gefälschtes Sicherheitszertifikat [388].

Später bekannte sich ein vorgeblich rumänischer Hacker mit dem Namen *Guccifer 2.0* zu den Angriffen, der aber bei Anfragen nicht in der Lage war, auf Rumänisch adäquat zu antworten und er benutzte einen russischen Kommunikationskanal[389].
Infolgedessen verdächtigen die US-Ermittler *Guccifer 2.0*, wenn existent, ein Mitarbeiter der russischen Nachrichtendienste zu sein, der später auch noch Kontaktdatenlisten von führenden Mitgliedern der demokratischen Partei veröffentlichte[390].
Ende August 2016 wurde ein erfolgreiches Eindringen in Onlinewahlsysteme von Illinois und Arizona berichtet, in Illinois wurden Daten von 200.000 Wählern kopiert[391].
Das FBI fand russische Versuche, in 21 Staaten in Wahlsysteme einzudringen, und als Warnung wurde eine Cyber-Operation von der NSA mit dem Implantieren von Computercode in sensiblen Computersystemen durchgeführt, die Russland finden

[384] vgl. Reuters 2017a
[385] vgl. Check Point Research 2017, S.7
[386] vgl. Alperovitch 2016, Nakashima 2016a
[387] vgl. Alperovitch 2016
[388] vgl. FAZ online 2015, siehe auch Wehner 2015, S.1
[389] vgl. Baumgärtner/Neef/Stark 2016, S.90-91
[390] vgl. Lichtblau/Weiland 2016
[391] vgl. Nakashima 2016b, Winkler 2016, S.4

sollte[392]. Allerdings wurde auch der *Surkov*-Vorfall im Abschnitt 6.2.3 als Teil der Vergeltung diskutiert.
Der *US Intelligence Community Report on Cyber incident Attribution* von 2017 und die vorherige Beurteilung durch das *Department of Homeland Security* der Angriffe von *APT28/Fancy Bears* und *APT29/Cozy Bears* als *Operation Grizzly Steppe* unterstützte die Zuordnung der Angriffe nach Russland. [393]
Im April 2017 wurde ein Russe auf dem Flughafen von Barcelona festgenommen, der vermutlich während des US-Wahlkampfes in den russischen Hack verwickelt war [394].

Das Mueller indictment von 2018[395]
Die Mueller-Anklageschrift (Indictment) hat Beweise dafür vorgelegt, dass *Fancy Bears* GRU-Mitglieder sind, die in GRU-Einrichtungen arbeiten. Der russische Militärgeheimdienst GRU hat mehrere Einheiten, die sich an Cyberoperationen beteiligen, darunter die Einheiten 26165 und 74455. 12 namentlich bekannte Offiziere dieser Einheiten werden verdächtigt, an den russischen Aktivitäten des Jahres 2016 während der Präsidentschaftswahlkampagnen beteiligt gewesen zu sein, insbesondere am Democratic National Committee (DNC) Hack. Die Einheit 26165 ist in erster Linie verantwortlich und befindet sich in Moskau, während die Einheit 74455 in einem anderen Moskauer Gebäude befindet, das die GRU den Turm nennt. Im März 2016 startete der Angriffe mit Spearphishing. Von einem gehackten Computer eines Mitarbeiters des *Democratic Congressional Campaign Committee (DCCC)* konnten die Angreifer in das DNC-Netzwerk gelangen.
Im April 2016 wurden Akten des DCCC, des DNC und des Clinton-Wahlkampfteams gestohlen und dann im Juni 2016 vom fiktiven Akteur *Guccifer 2.0* und der Plattform *DCLeaks* veröffentlicht. Innerhalb der Einheit 26165 ist eine Abteilung für die Entwicklung und Verwaltung von Malware zuständig, einschließlich *X-Agent*, das dann auf DCCC und DNC-Computern eingesetzt wurde. Auch die *Fancy Bears/APT28*-Malware *X-Tunnel* wurde implementiert. Eine Linux-basierte Version von *X-Agent*, die sich mit der GRU-registrierten Domain linuxkrnl.net verständigen konnte, war bis Oktober 2016 aktiv. Die erste *Guccifer 2.0*-Nachricht wurde auf einem Computer von GRU Einheit 74455 erstellt. *DCLeaks* wurde auf einem gepachteten malaysischen Server gehostet, der mit Bitcoin-mining finanziert wurde. Die gleiche Bitcoin-Adresse wurde für andere GRU-Operationen verwendet, um Server und Domains zu kaufen, z.B. die

[392] vgl. Miller et al. 2017. Details der Befunde waren durch die Whistleblowerin Reality Winner, einer NSA-Linguistin, auf der Plattform *The Intercept* durchgesickert. Da nur eine sehr begrenzte Gruppe von Personen auf die Dateien zugreifen und sie ausdrucken konnte, wurde sie nach der Veröffentlichung schnell identifiziert, vgl. Gruber/Reinhold 2017, Shane/Perloth/Sanger 2017.
[393] vgl. ODNI 2017, JAR 2016 of the *Department of Homeland Security DHS* and the *Federal Bureau of Investigation FBI*.
[394] vgl. Zeit online 2017
[395] vgl. Mueller 2018

gefälschte Website account-gooogle.com und US-Server. Auch der Link linuxkrnl.net wurde durch das Bezahlen mit diesen Bitcoins erneuert.

5.2.4.5 Der WADA hack

Die neu gegründete *Fancybear.net* Website im Sommer 2016 veröffentlichten Informationen der World Anti-Doping Agentur WADA zeigen, dass bestimmte Sportler Ausnahmeregelungen z.B. zur Verwendung von Steroiden bekamen. Der Hack geschah nach Doping-Vorwürfen gegen russische Sportler. [396]

5.2.4.6 Der Macron-Hack

Der Wahlkampf des neuen französischen Präsidenten Macron wurde angegriffen und bestimmte Dokumente wurden geleakt. Am 15. März 2017 entdeckte die Sicherheitsfirma TrendMicro Phishing-Emails an Mitarbeiter des Wahlkampfteams und anderen, die sie zu gefälschten Webseiten lotsen sollten. Am 15. April 2017 wurden auch gefälschte Webseiten, die die Namen der Macron-Partei (En Marche!) nachahmen, wie mail-enmarche.fr registriert. Die IP-Nummern hinter den Webseiten waren Teil eines IP-Adressblocks, der von *TrendMicro* bereits APT 28 zugeschrieben wurde[397].

5.2.4.7 Die Angriffe auf Yahoo

Die Internetfirma *Yahoo* berichtete über das Hacken von 1 Milliarde Benutzerkonten im Jahr 2013 und 500 Millionen E-Mail-Konten im Jahr 2014. Die Vereinigten Staaten identifizierten 4 Personen, zwei Mitglieder des russischen Geheimdienstes FSB und zwei weitere Hacker, von denen vermutet wird, dass sie den 2014er Hack mit durchgeführt haben. Ein besonderer Schwerpunkt lag auf den Konten von Diplomaten, Militärs und Cybersicherheitsfachleuten. Einer der Verdächtigen ist bereits in Russland inhaftiert, wahrscheinlich als Teil des *Michailow*-Vorfalls. Allerdings konnte ein Link zu APT28 oder 29 bisher nicht hergestellt werden[398]. Eine erneute Untersuchung des Hacks von 2013 zeigte jedoch 2017, dass alle drei Milliarden *Yahoo*-Konten geknackt worden waren[399].

5.2.4.8 Die LoJax firmware-Attacke

Die Anti-Diebstahl-Software *LoJack* der Firma *Absolute Software*, implementiert ein UEFI/BIOS-Firmware-Modul, um seine Entfernung zu verhindern und erschien in trojanisierten Versionen seit mindestens Anfang 2017. Die bösartigen Versionen sind jetzt als *LoJax* bekannt, die wie *LoJack* sehr tief in das Computersystem

[396] vgl. WADA 2016
[397] Perloth 2017a
[398] FAZ 2017a, S.23
[399] vgl. DW 2017

eingebettet sind und deshalb persistieren[400]. *LoJax* erschien typischerweise mit anderen *APT28/Fancy Bears*-Modulen, wie dem Backdoor *SedUploader*, *X-Agent* und dem Netzwerk-Proxy-Tool *X-Tunnel*[401].

5.2.4.9 Weitere Aktivitäten

Weitere Aktivitäten der *APT28*/*Fancy Bears* 2017 betrafen die Freigabe von Dokumenten der englischen *Football Association* und einen Einbruch in das Mailsystem der UNO[402].
Kaspersky-Experten stellten im Jahr 2018 fest, dass *APT28*/*Fancy Bears* jetzt den Fokus auf ehemalige sowjetische Saaten setzt. Sie aktivieren mehrere Server, verwenden für Domain-Registrierung gefälschte Telefonnummern, nutzen Services mit Datenschutz für die Registrierung und solche, die Bitcoins akzeptieren.[403]
Microsoft berichtete im August 2018, dass *APT28*/*Fancy Bears* gefälschte Webseiten konservativer Think Tanks eingerichtet hatte, um Nutzerdaten einzufangen, Microsoft konnte dies blockieren.[404].

5.2.5 Die Waterbug Group (Turla/Snake/Ouroburos/Venomous Bear/Krypton/Group88)

Waterbug ist der Name für die Gruppe, die die Malware *Wipbot/Tavdig/Epic Turla, Uroburos/Turla/Snake/Carbon* und *agent.btz/Minit* einsetzt.
In einem Quellcode wurde der Begriff UrObUr()s verwendet, alternative Schriften zu Uroburos sind *Ouroburos* und *Uroboros*. Westliche Geheimdienste schreiben diese APT dem russischen Zivilgeheimdienst FSB zu.

5.2.5.1 Die agent.btz-Attacke 2008

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[405]. 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[406].

---

[400] vgl. ESET 2018
[401] vgl. ESET 2018, S.7
[402] vgl. The Telegraph 2017, Bild 2017
[403] vgl. Paganini 2018b
[404] vgl. Tagesschau 2018
[405] vgl. Glenny 2010, S.23
[406] vgl. Brown/Poellet 2012, S.131

Die Multifunktionsmalware namens Ou*roburos/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*[407] 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[408]. Angreifer setzten die *Snake/Ouroburos/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[409].

5.2.5.2 Die RUAG-Attacke 2014-2016

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[410].

5.2.5.3 Die IVBB-Attacke 2016-2018

Der *Informationsverbund Berlin-Bund (IVBB)* ist seit 1999 in Betrieb und wird von der Deutschen Telekom betrieben. Er umfasst den Internet- und Telefonverkehr des Bundespräsidialamts, Bundeskanzleramts, von Bundesministerien, Bundesrechnungshof, Sicherheitsbehörden und Teilen von Bundestag und Bundesrat. Es dient der sicheren Übermittlung von Informationen der Stufe VS-NfD (Verschlusssache-nur für den Dienstgebrauch). Die Sicherheit des IVBB wird durch das BSI betreut. Schon nach der Attacke auf das Computernetz des Bundestags 2015 kam es zu längeren nicht aufgeklärten Unregelmäßigkeiten im Telefonnetz. Inwieweit IVBB-Telefonate mitgehört werden konnten oder wurden, ist unklar[411].

Es gibt nur zwei Ausgänge, je einen in Berlin und Bonn. Übergänge zum IVBB-Internet und IVBB-Sprachnetz werden mit Paketfiltern der hohen Evaluierungsstufe EAL4 geschützt. Es gibt eine doppelte Firewall mit Inhaltsfilter und formalen Filter (IP-Adressblockaden) und *Sichere Netzwerkarchitektur (SINA)*-Box. iPhones und iPads dürfen nur mit der Sicherheitslösung *SecurePIM* arbeiten, Sprach- und

[407] vgl. Symantec 2016, S.10-11
[408] vgl. Fuest 2014a, S.1-3
[409] vgl. Weedon 2015, S.72-73
[410] vgl. Jürgensen 2016, S.28
[411] vgl. Gräfe/Link/Schulzki-Haddouti 2018

Faxdaten werden mit *Elcrodat 6-2* verschlüsselt[412]. Zur Zeit sind auch Schutzprogramme der Sicherheitsfirma *TrendMicro* aktiv[413].
Vor 2 Jahren hatten die Hacker von *Snake/Turla/Ouroburos* eine eLearning-Lernplattform der *Bundesakademie für öffentliche Verwaltung* mit Spähsoftware manipuliert, 17 Mitarbeiter hatten sich die Spähsoftware dann auf den eigenen Rechner geladen, 6 Dokumente wurden entwendet[414].

Ziel war die Abteilung 2 (Referat 205) des Auswärtigen Amtes, zuständig u.a. für Russland. Im Dezember 2017 erfolgte dann ein Hinweis an die Deutschen durch einen ausländischen Nachrichtendienst[415], das *Mobile Response Incident Response Team MIRT* des BSI und das ZITIS analysierten die Lage. Dann berichtete jedoch die deutsche Presseagentur Ende Februar 2018 über den Vorgang und daraufhin zog sich der Angreifer zurück. Die APT versuchte jedoch nochmals im November 2018, an Email-Adressen von Bundestagsabgeordneten zu gelangen.

5.2.5.4 Die Attacke auf die französische Marine 2017-2018

Turla griff gezielt 12 Beamte an, um die Ölversorgungskette der französischen Marine in den Jahren 2017 und 2018 zu enthüllen, die Franzosen bevorzugten jedoch die diskrete Klärung von Vorfällen statt öffentlicher Anklagen[416].

5.2.6 Die Sandworm/Quedagh APT (Black Energy/Telebots/Voodoo Bear)

Der britische Geheimdienst GCHQ assoziiert *Sandworm* und *Black Energy* with dem russischen Militärgeheimdienst GRU[417] (Russland dementierte).

5.2.6.1 Die Black Energy-Attacke

The *Sandworm* or *Quedagh*-Gruppe (die Namen beziehen sich auf gefundene Referenzen zur Science-Fiction Welt *Dune* – der Wüstenplanet) nutzt die ursprünglich als Crimeware entwickelte und dann modifizierte Malware *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

[412] vgl. Gräfe/Link/Schulzki-Haddouti 2018
[413] vgl. FAZ 2018c, S.2
[414] vgl. FAS 2018, S.7
[415] vgl. FAS 2018; Pinkert/Tanriverdi/Von Bullion 2018
[416] vgl. Lawfareblog 2019
[417] vgl. Technology review 2018

Funktionen ergänzt wie das Kapern inaktiver Laufwerke und die Fähigkeit zum umfangreichen Informationsdiebstahl[418].
Das *US ICS-CERT* hat eine Malwarekampagne entdeckt, die mindestens seit 2011 läuft, verschiedene ICS-Systeme betraf und bei denen eine Variante von *BlackEnergy* bei vernetzten Benutzerschnittstellen (auch Mensch-Maschine-Schnittstellen bzw. *human-machine interfaces HMIs*) eingesetzt wurde[419]. Unter anderem waren die Systeme *GE Cimplicity, Advantech/Broadwin WebAccess*, und *Siemens WinCC* betroffen.
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[420]. Jedoch bestätigte die NATO, dass die geheimen operativen Netzwerkbereiche nicht betroffen waren, da diese vom Internet abgetrennt sind[421].

Am 23.12.2015 kam es zu Stromausfällen in der Ukraine durch Cyberattacken bei drei regionalen Stromanbietern, die insgesamt ca. 225.000 Kunden betrafen[422]. Drei weitere Anbieter waren betroffen, hatten aber keine Stromausfälle. Die Eindringlinge waren in der Lage, Stromverbindungen aus der Distanz zu öffnen, was zum Stromausfall führte, was in koordinierter Form in einem kleinen Zeitfenster geschah[423]. **Telephone denial of service-Attacken (TDoS attacks)** wurden genutzt, um die Anbieter–Hotlines mit Anrufen zu fluten, so dass die Kunden die Stromausfälle nicht telefonisch weitermelden konnten[424].
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[425].

5.2.6.2 Die Industroyer-Attacke

Am 17. Dezember 2016 verursachte die Malware *Industroyer/CrashOverride*, die speziell für Angriffe auf intelligente Netze entworfen wurde, einen Blackout in Kiew, der einer neuen APT namens *Electrum* zugeschrieben wurde, die mit der Sandworm/Quedagh Gruppe verbunden ist[426].

[418] vgl. F-Secure Labs 2014, S.2, 10-11
[419] vgl. ICS-CERT 2016a
[420] vgl. BBC 2014, S.1, F-Secure Labs 2014, S.2
[421] vgl. BBC 2014, S.2
[422] vgl. ICS-CERT 2016b
[423] vgl. ICS-CERT 2016b
[424] vgl. Zetter 2016
[425] vgl. ICS-CERT 2016a
[426] vgl. Scherschel 2017a, Dragos 2017

Die Malware beeinflusste eine einzelne Übertragungs-Unterstation durch die Installation einer Hintertür, der ein Launcher folgte, danach Payloads einschließlich IEC104-Protokollbefehlen und schließlich eine Wiper-Malware. Die Malware verwendete hartcodierte Proxyserver einschließlich TOR-Knoten[427].

5.2.6.3 Die Petya/Not-Petya/MoonrakerPetya-Attacke

Es ist zu beachten, dass der vorhergehende *MoonrakerPetya*-Angriff erst nach dem NotPetya-Angriff entdeckt wurde. Während die Zuordnung zur GRU durch die CIA vom GCHQ bestätigt (und von Russland dementiert) wurde, ist aus dem Angriff von *MoonrakerPetya* erkennbar, dass dies der *Sandworm/Quedagh*-Gruppe zugeschrieben werden konnte.
Der MoonrakerPetya-Angriff war nur ein kleiner Angriff auf ein paar Computer, erst der NSA-Exploit *EternalBlue* erlaubte dann einen großen Angriff.

Der *Sandworm/Quedagh* APT hat 2017 einen *NotPetya*-Vorläufer namens *MoonrakerPetya* veröffentlicht. Im Dezember 2016 setzten die Angreifer den Wurm *MoonrakerPetya* ein, der vermutlich ein Vorläufer von NotPetya (auch bekannt als *Petya, ExPetr, Nyetya, EternalPetya*) war. Der Wurm ist eine DLL-Datei, die unter dem Namen msvcrt120b.dll im Windows-Verzeichnis angelegt wird, während der interne Name moonraker.dll ist. *MoonrakerPetya* enthält Code, der den Computer unbootbar macht, aber nur in einer kleinen Anzahl von Fällen verwendet wurde[428].

Wie für *WannaCry*, wurde am 23. Mai 2017 zunächst ein Angriff mit NSA-Exploits gestartet, der wenig Aufmerksamkeit erregte, da kein Schaden sichtbar war.[429].
Der NSA-Exploit *Eternal Rocks* kombinierte 7 NSA-Exploits (*EternalBlue, DoublePulsar, EternalRomance, EternalChampion, EternalSynergy, ArchiTouch* und *SMB Touch*). Die Malware *Petya* nutzte die *EternalBlue* und *EternalRomance*-Exploits Ende Juni 2017. Bevor sie aktiv wird, lädt sie den TOR-Browser herunter, um eine verdeckte Kommunikationsleitung zu errichten, um den Server zu steuern.

Die Malware, die anfangs wie die bereits bekannte Ransomware *Petya* aussah, war anders, auch gegenüber anderer Ransomware wie *Mischa* und *Goldeneye*. Zusätzlich zu *EternalBlue* und *EternalRomance* benutzte es die ukrainische Buchhaltungssoftware *Me-doc*, indem sie ein bösartiges Update injizierte[430]. Dies war aufgrund eines verfälschten Microsoft Sicherheitszertifikats möglich. Diese Unterschiede erklären, warum einige Autoren es *Not-Petya* oder *Petya2017* nannten.

[427] vgl. Dragos 2017, S.11 und 14
[428] vgl. Cherepanov 2018
[429] vgl. Kling 2017
[430] vgl. Kaspersky 2017b/Scherschel 2017b

Sobald das ‚neue' Petya einen Computer infiziert hatte, suchte es automatisch nach anderen Computern im Netzwerk, die auch infiziert werden sollten[431].
Obwohl die attackierten Nutzer aufgefordert wurden, Geld zu bezahlen, scheint es, dass die UserID, die für die Anfrage gezeigt wurde, nur eine sinnlose Zufallszahl war und die Malware scheint eine Wiper Malware zu sein, die den Master Boot Record [432] und andere Dateien überschreibt. Aus diesem Grund hatte die Sperrung des *Posteo*-Mail-Kontos, die als Kontaktadresse zur Zahlung präsentiert wurde, keine Auswirkung mehr.
Eine große Anzahl von Unternehmen wurde getroffen, z.B. *Merck* in den USA, *Maersk* in Dänemark, *Milka* in Deutschland (die dann an mehreren Tagen Produktionsstopp litten), aber auch russische Unternehmen und das Atomkraftwerk Tschernobyl.

Die Verwendung eines verfälschten Sicherheitszertifikats, die Komplexität der Malware und die mangelnde Rentabilität, da die Opfer ohnehin nicht bezahlen konnten, deuteten stark auf einen Angriff eines Staatsakteurs hin.
Ende 2017 berichtete die CIA, dass sie die *Petya/NotPetya*-Attacke mit ziemlicher Sicherheit ('with high confidence') dem militärischen Nachrichtendienst GRU zuordnen konnte[433].

5.2.6.4 Grey Energy/Bad Rabbit/Telebots

Im Oktober 2017 nutzte die Gruppe auch die *BadRabbit*-Malware-Familie für Anschläge. Ihre *Telebots*-Malware wurde nur in der Ukraine eingesetzt[434].
Das Design und die Architektur der *GreyEnergy*-Malware, die seit 2015 zu existieren scheint, ähneln sehr der *BlackEnergy*-Malware, aber eine der *GreyEnergy*-Proben wurde mit einem gültigen digitalen Zertifikat der taiwanesischen Firma *Advantech* unterzeichnet, die ICS und IoT-Komponenten herstellt[435], so dass das Zertifikat möglicherweise gestohlen wurde.

5.2.6.5 Die VPN Filter-Attacke 2018

Das neue modulare Malware-System *VPNFilter* betraf 2018 mindestens 500.000 Netzwerkgeräte in mindestens 54 Ländern, insbesondere aber in der Ukraine, indem es eine spezifische C2-Infrastruktur für dieses Land nutzte[436].
Die Malware hat Überschneidungen mit *BlackEnergy* und infiziert *Linksys, MikroTik, Netgear* und *TP-Link* Netzwerkgeräte und *QNAP*-Netzwerk-angeschlossene Speichergeräte.

---

[431] vgl. Kaspersky 2017b/Scherschel 2017b
[432] vgl. Beiersmann 2017c
[433] vgl. Nakashima 2018
[434] vgl. Cherepanov 2018, S.22-24
[435] vgl. Cherepanov 2018, S.2-3
[436] vgl. Talos 2018

Es handelt sich um eine dreistufige Malware. Stufe 1 ist die erste IoT-Malware, die nach einem Neustart fortbestehen kann und Befehls-und Kontrollmechanismen nutzt, um den Stage 2 Malware-Einsatzserver zu kontaktieren. Die Malware der Stufe 2 ist für die Datenerfassung, wie Dateien, die Befehlsausführung, die Datenexfiltration und das Gerätemanagement zuständig. Einige Versionen der zweiten Stufe haben eine Bricking-Fähigkeit, die einen kritischen Teil der Firmware des Geräts mit Nullen überschreibt und das Gerät neu startet, was es unbrauchbar macht. Darüber hinaus gibt es verschiedene Stage 3 Module als Plugins für Stufe 2.Diese Plugins können z.B. die Modbus SCADA-Protokolle überwachen und die Stufe 2-Malware über TOR kommunizieren lassen. Die C2-Kommunikation und zusätzliche Malware-Downloads können über TOR oder SSL-verschlüsselte Verbindungen erfolgen und ein Programmierfehler in der Entschlüsselungsroutine ähnelten Befunden in *Black Energy*.

5.2.7 Die Dragonfly/Energetic Bear APT

Die Hackergruppe *Dragonfly (Energetic Bear/Crouching Yeti Koala/Group 24/Iron Liberty)* drang bei den Anbietern von ICS-Programmen ein, so dass alle Nutzerunternehmen die Malware automatisch mit dem nächsten Update in ihre Programme luden[437]. 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[438]. Als weiteres Werkzeug diente *Trojan.Karagany*, der aber auch auf dem Schwarzmarkt verfügbar ist. Die Arbeitszeiten (Progammierzeitstempel der Malware) lassen die Gruppe in Osteuropa (GMT plus 4 Stunden) vermuten [439].

Im Mai und Juni 2017 war der US-Energiesektor Ziel von Cyberangriffen. Die US-Behörden DHS und FBI untersuchten dies; unter den Zielen war das Kernkraftwerk *Wolf Creek* bei Burlington in Kansas, aber seine Operationen waren nicht betroffen. Die Angriffe waren die gleichen wie die Taktik der APT *Dragonfly (Energetic Bear/Crouching Yeti/Koala)*. Zum Angriff wurden **gefälschte Lebensläufe** für Kontrollingenieur-Jobs, watering hole-Attacken und Man-in-the-Middle-Attacken angewendet[440]. so dass diese Attacke auch *Dragonfly 2.0* genannt wurde. Beide Angriffswellen *Dragonfly* und *Dragonfly 2.0* nutzten exklusiv die Schadsoftware *Trojan.Heriplor*. Es wurden Bedenken laut, dass die Angriffe dazu dienten, die Kontrolle zu erlangen, um in Zukunft ggf. Sabotageakte durchführen zu können.

437 vgl. Metzler 2015, S.34, Perloth 2017b
438 vgl. Campbell 2015, S.11
439 vgl. Symantec 2014b
440 vgl. Perloth 2017b

5.2.8 Die Triton/Temp.Veles/Trisis-Attacke

Ende 2017 wurde bei einem Ziel im mittleren Osten eine neue ICS-Malware entdeckt, die *Triton* oder *Trisis* genannt wird [441] Die Malware *Triton/Trisis* richtet sich speziell gegen das *Schneider Electric's Triconex Safety Instrumented System (SIS)*. SIS-Systeme führen Notabschaltungen bzw. Produktionsstops in kritischen Situationen aus, die Intrusion kann von außen solche Abschaltungen anlaßlos erzwingen oder auch im Notfall verhindern und so die Produktion beschädigen[442].

Der Schutz eines solchen SIS-Systems durch eine gesonderte Firewall kann eine Fernwartung (**remote access engineering**) behindern, so dass oft kein solcher gesonderter Schutz vorliegt[443]. Die israelische Cybersicherheitsfirma *Cyber X* berichtete, dass es sich um ein saudisches Ziel gehandelt hätte, das vom Iran aus angegriffen worden sei und die Malware schon gegen mehrere Ziele zum Einsatz kam.[444]

Ende 2018 konnte *FireEye* die Malware Russland zuordnen. Die Entwicklung von *Triton* wurde höchstwahrscheinlich *vom Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM)* unterstützt, aus folgenden Gründen: Eine Person mit Verbindungen zu dem Institut war in die Malware-Entwicklung eingebunden, Malwaretests des CNIIHM hingen wiederum sehr wahrscheinlich mit den Aktivtäten der Gruppe *Temp.Veles* zusammen, einem Arbeitsbegriff für die Gruppe, die *Triton* nutzt; zudem wurde eine IP-Adresse des CNIIHM für Aktivitäten rund um die *Triton*-Attacke verwendet, und das Institut verfügt über Forschungssektionen zur kritischen Infrastrukturen und Waffenentwicklung. Weitere einzigartige Dateien und Tools wurden gefunden, zudem testete *Temp.Veles* Eindringversuche schon seit 2013, was schließlich in die hochentwickelte *Triton*-Attacke mündete[445]. Zudem passen Spracheinstellungen und Artefakte (Sprachfehler in Programmen) sowie die primären Arbeitszeiten sehr gut zu dieser Zuschreibung.
Da es sich um ein staatliches Forschungsinstitut handelt, ist es fraglich, ob es sich um eine eigene APT oder nur um einen Malware-Anbieter für bereits bekannte APTs handelt.
In der Zwischenzeit (2019) wurden neue *Triton*-Varianten entdeckt, die eine breitere Palette an SIS-Systemen gefährden. Sie wurden auch im Nahen Osten und in den USA gefunden[446].

[441] vgl. Johnson et al. 2017
[442] vgl. Dragos 2017
[443] vgl. Dragos 2017, S.5-6
[444] vgl. Weidemann 2017b
[445] vgl. Fireeye 2018b
[446] vgl. Miller 2019

5.2.9 Mutmaßlich chinesische APTs

Sowohl der Zivil- als auch der Militärsektor von China stehen unter der Kontrolle der Kommunistischen Partei Chinas. Chinas Volksbefreiungsarmee PLA wird verdächtigt, große Cybereinheiten an mindestens einem halben Dutzend Standorten zu unterhalten[447].

Der zuständige PLA-Bereich ist das *General Staff Department GSD*, das aus 4 Abteilungen besteht. Dies besteht aus der Abt. Operationen in der 1. Abteilung, Abt. Intelligence in der 2. Abteilung, Signals Intelligence und Netzwerk-Verteidigung in der 3. Abteilung und elektronische Gegenmaßnahmen und offensive Cyber-Operationen in der 4. Abteilung [448]. Die NSA verfolgte im Jahr 2014 20 Gruppen aus China, von denen sie über die Hälfte der PLA zuschrieb[449] (so dass von den anderen angenommen werden kann, dass sie dem zivilen Sektor angehören).

Während es offensichtlich ist, dass alle APTs einen spezialisierten Tätigkeitsbereich haben, ist wenig über die Koordination zwischen den APTs bekannt. So müssen alle Annahmen mit Vorsicht durchgeführt werden, weitere Untersuchungen könnten zeigen, dass bestimmte APTs nur Teile von anderen sind oder aktuelle APTs in neue aufgeteilt werden müssen oder eine erneute Zuordnung erfolgen muss.

Unterdessen sind die USA der Ansicht, dass das Ministerium für Staatssicherheit 2015 die Koordination von Cyber-Operationen von der PLA übernommen hat. [450]

Im Jahr 2018 stand die APT10 im Verdacht, mit dem Ministerium für Staatssicherheit in Verbindung zu stehen.

5.2.9.1 APT1/Comment Crew/Comment Panda/TG-8223

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 *Putter Panda/APT2/TG-6952* genannt und ihre Cyberaktivität konnte mit der *Unit 61398* wegen der Nutzung gemeinsamer Infrastruktur verknüpft werden[451].

2013 hat die IT-Sicherheitsfirma *Mandiant* eine tiefgreifende Analyse chinesischer Cyberaktivitäten vorgelegt[452]. 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

[447] vgl. Finsterbusch 2013, S.15
[448] vgl. Mandiant 2013, Sharma 2011, S.64
[449] vgl. Perlroth 2014
[450] vgl. Langer 2018b
[451] vgl. Novetta 2015, S.15, Perlroth 2014
[452] vgl. Mandiant 2013

Energieversorger durchgeführt und *Mandiant* vermutete, 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. Diese Person hatte sowohl eine von APT1 genutzte IP-Adresse registriert wie auch ein im Netz zugängliches Personenprofil als Armeeangehöriger. China wies die Beschuldigungen zurück, aber US-Medien spekulierten, dass dieser Vorgang zu dem vorübergehenden deutlichen Rückgang mutmaßlicher chinesischer Aktivitäten in den Jahren danach beigetragen hatte[453].
Andere US-chinesische Cyber-Aktivitäten gehen jedoch weiter. Chinesische Hacker sollen im Januar 2018 im Auftrag der chinesischen Regierung in die Rechner einer US-Firma eingedrungen sein, die für das *Naval Undersea Warfare Center* in Rhode Island arbeitet. Die Dateien lagen in einem ungesicherten Netz, die 614 Gigabyte umfassen auch ein Überschall-Raketensystem, das ab 2020 eingesetzt werden soll.[454]
Die Daten von 500 Millionen Besucher der *Starwood*-Hotelgruppe[455], zu der auch die *Marriot*-Hotelgruppe gehört, wurden seit 2014 kopiert, einschließlich Kreditkarten-und Passnummern etc. Die US-Regierung glaubt, dass dieser Angriff von China durchgeführt wurde, da die *Marriot*-Hotels in häufig von Mitarbeitern der US-Regierung und des Militärs genutzt werden. [456]

5.2.9.2 APT17/Winnti/Axiom/Barium

Die *APT17/Winnti/Axiom/Barium Group* ist auch unter vielen anderen Namen bekannt, wie *DeepPanda, Shell_Crew, Group 72, Black Vine, HiddenLynx, KungFu Kittens, Winnti Group, Tailgater, Ragebeast, Blackfly, Lead, Wicked Spider, Dogfish, Deputy Dog, Wicked Panda* etc.
Die Gruppe führt hochentwickelte Phishingattacken durch Aufsatteln auf laufende reale Konversationen (**piggybacking**) durch, um das Opfer zum Anklicken von infizierten Links zu motivieren[457].

---

[453] vgl. Mandiant 2013, Jones 2016, S.5, Nakashima 2016. Jedoch erhoben die USA 2017 Klagen gegen drei chinesische Hacker, die zwischen 2011 und 2017 in US-Firmen eindrangen, u.a. die US-Niederlassung von Siemens, so daß dieser Frieden gefährdet erscheint, vgl. NZZ 2017b
[454] vgl. Spiegel 2018
[455] vgl. Langer 2018a
[456] vgl. Langer 2018b
[457] 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.

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[458]. 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*[459]. Die Malware *Zox* und *Hikit* wurden nur bei Axiom beobachtet, während andere verwendete Malwareprogramme auch von anderen Organisationen genutzt werden[460] Angriffsziele waren eine große Bandbreite an Regierungseinrichtungen, Unternehmen der Technologiebranche und akademischen Institutionen.
Sie greift u.a. auch ausgewählte Ziele mit der *Blackcoffee*-Malware an, um z.B. Daten zur militärischen Intelligence zu gewinnen[461].

Im Jahr 2019 wurde deutlich, dass diese APT zunehmend auf Methoden setzt, mit der eine große Anzahl von Usern gleichzeitig angegriffen werden kann.
So infizierten sie im Rahmen der *Operation Shadowhammer* ein Update der Firma ASUS, so dass zehntausende von Computern durch das *ASUS Live Update* befallen werden konnten[462].
Zudem hat die Winnti–Gruppe (also Axiom/APT17) den IT-Service Provider *Teamviewer* von 2014-2016 infiltriert, das *Teamviewer*-Programm wird für Fernzugriffe z.B. von IT-Admins genutzt[463].

5.2.9.3 APT10/Red Apollo/CVNX/Stone Panda/menuPass/Potassium

APT10 hat eine massive Spionage-Kampagne gegen *Managed Service Provider MSPs* (z. B. Unternehmen, die IT-Services, Help Desks und andere Dinge anbieten), durchgeführt, um durch die Überlappung mit firmenspezifischen Infrastrukturen eine große Anzahl von westlichen Unternehmen zu infiltrieren.
Die Angriffe und der neue Operation *Cloud Hopper* werden wie folgt durchgeführt: Die taktische Malware, *EvilGrab* und jetzt *ChChes*, wird durch Spear-Phishing

[458] vgl. Markoff/Barbosa, 18.02.2010
[459] vgl. Novetta 2015, S.12-13
[460] vgl. Novetta 2015, S.20. Jedoch wies *Novetta* in der Analyse der *Winnti-Gruppe* im Rahmen der Operation SMN darauf hin, dass *Hikit* nun genutzt wurde, um *Winnti*-Attacken zu unterstützen. Ob dies nun bedeutet, dass die *Hikit*-Malware nicht mehr exklusiv ist oder *Winnti* (deren Fokus von der Spieleindustrie zu anderen Branchen gewechselt hat wie *ThyssenKrupp*) nun mit *Axiom* verbunden ist, war nicht klar, jedoch nimmt man inzwischen an, dass es sich um dieselbe APT handelt.
[461] FireEye 2017
[462] vgl. Securelist 2019
[463] vgl. Rosenbach 2019

eingeführt, um dann im Falle eines relevanten Ziels dauerhafte Malware, *PoisonIvy* (bis 2013) und ab 2014 *PlugX* und *Quasar* zu installieren.[464]

Im Jahr 2018 wurden zwei Gruppenmitglieder von den USA offiziell angeklagt. Zhu Hua (alias *Afwar/CVNX/Alayos/Godkiller*) und Zhang Shilong (alias *Baobeilong/Zhang Jianguo/Axtreep*) wurden als Mitglieder der APT10 identifiziert; beide sind Mitarbeiter der *Huaying Haitai Science and Technology Development Compan*y in Tianjin und mit dem lokalen Büro des Ministeriums für Staatssicherheit liiert[465]. Die Gruppe ist mindestens seit 2006 aktiv. Sie führten mehrere Angriffskampagnen durch wie das Eindringen bei *Managed Service Providern (MSPs)*, um auf zahlreiche Firmen in mehreren Ländern Zugriff zu erlangen, sie infiltrierten zudem Dutzende von Technologiefirmen und Regierungseinrichtungen in den USA während der *Technology Theft Campaign* und stahlen Daten von mehr als 100.000 Mitgliedern der US Navy.[466] Die Anklageschrift präsentierte nur Bespiele und Highlights der Befunde zur APT10, wohl um sensitives Wissen zu schützen; jedoch wird ein sehr viel weitergehendes Detailwissen angedeutet, z.B. durch Nennung der genauen Zahl der infizierten Computer, die Nutzung von Spearphishing und 1,300 einzigartigen malignen Domänen.

Laut Berichten vom Juni 2019 wurde das *Jet Propulsion Laboratory JPL* der NASA durch das Anschließen eines *Rapsberry Pi*-Geräts infiltriert, das es dann u.a. ermöglichte, Daten von Mars-Missionen zu stehlen[467]. Im Jahr 2018 wurde auch das *JPL Deep Space Network* als System von Satellitenschüsseln für die Kommunikation mit Raumschiffen infiltriert. Im Dezember 2018 wurden zwei Mitglieder der APT10 wegen Eindringens in das JPL angeklagt, es wurde jedoch nicht angegeben, ob dieser spezifische Angriff gemeint war.

5.2.9.4 APT 40 (Temp.Periscope/Temp.Jumper/Bronze Mohawk/Leviathan) und Thrip

Satellitenhacks von US-Satelliten wurden bereits seit einem Jahrzehnt gemeldet und China wurde bereits seit längerer Zeit von der *US-China Economic and Security Review Commission* verdächtigt[468]. Im Juni 2018 meldete *Symantec* erfolgreiche Vorstöße gegen Satelliten- und Verteidigungsunternehmen durch eine neue APT namens *Thrip*, der seit 2013 aktiv ist. Diese APT weist möglicherweise Überschneidungen mit der APT40 (*Temp.Periscope/Temp.Jumper/Bronze Mohawk/Leviathan*) auf.

[464] vgl. PwC/BAE Systems 2017, S.18
[465] vgl. DoJ 2018
[466] vgl. DoJ 2018
[467] vgl. Cimpanu 2019
[468] vgl. Menn 2018

Die APT40 ist seit 2013 aktiv und konzentriert sich vorzugsweise auf Firmen, die im militärischen Schiffsbau tätig sind. Die Gruppe nutzt eine Vielzahl an Tools, wie Spearphishing, Spoofing (der domain von *Thyssen Krupp Marine Systems*) und hat in den Jahren 2017 und 2018 unerwartet TTPs der russischen Gruppen *Dragonfly* und *APT28* übernommen. Die Gruppe benutzte das *Foxmail*–System, das zuvor im Jahr 2012 von einer anderen chinesischen Gruppe namens *Luckycat* genutzt wurde[469].

Im Dezember 2016 erlangte die Marine der chinesischen Armee PLA ein unbemanntes Unterwasserfahrzeug (**unmanned underwater vehicle UUV**) der US Navy und parallel dazu wurden die Cyberaktivitäten gegen Marineforschungseinheiten und -unternehmen erheblich verstärkt.
Die APT40 ist chinesischen IP-Adressen, Befehls- und Kontrollservern in China, chinesischen Arbeitszeiten und mit China zusammenhängenden WHOIS-Registrierungen zugeordnet. Sie verwendet Dutzende neuer und unterschiedlicher Malware-Programme für das Eindringen, um dauerhaft Fuß zu fassen, die Aufrechterhaltung der Präsenz, das lateral movement, die Eskalation von Zugriffsprivilegien und die Aufklärung[470].

5.2.9.5 Weitere mutmaßlich chinesische APTs

Weitere mutmaßlich chinesische APTs sind:

- *APT3/Gothic Panda/UPS Team/Pirpi/Clandestine Fox TG-0110/Buckeye*[471]: seit 2014 gezielte Angriffe auf ausgewählte Branchen mit Spearphishing und Zeroday-Exploits
- *APT12/Ixeshe/DynCalc/DNSCalc/Numbered Panda/JoyRAT* zielt auf Journalisten und militärische Auftragnehmer aus den USA und dem Pazifischen Raum ab, dies seit 2012 durch Spearphishing und die Installation von Malware wie *Riptide.* Kürzlich wurde der *Etumbot*-Angriff in Europa entdeckt, das jetzt ein neuer Schwerpunkt der APT ist[472]
- *APT 15/Mirage/Vixen Panda* konzentriert sich nun auf Regierungs- und Diplomaten in Russland und ehemaligen Sowjetrepubliken [473]
- *APT18/Dynamite Panda/Wekby/TG-0416*: Auf Daten von bis zu 4,5 Millionen Mitgliedern der US-amerikanischen Gesundheitsorganisation *Community Health Systems*, wurde während eines Eindringens zugegriffen [474].

[469] vgl. Insikt Group 2018
[470] vgl. Plan 2019
[471] vgl. FireEye 2017/Reuters WorldNews 2017
[472] vgl. FireEye 2017/Reuters WorldNews 2017
[473] vgl. Reuters World News 2017
[474] vgl. PwC/BAE Systems 2017, S.14

- *APT 19:* Mehrere Gesundheitsfirmen wurden angegriffen, *Anthem, Premera Blue Cross* und *CareFirst,* alle im Jahr 2015[475]
- *APT 27/Emissary Panda/TG-3390: ThreatConnect* hat im Jahr 2016 die APT 27-Aktivitäten in Europa entdeckt[476].
- *APT30/PLA unit 78020/Naikon*[477]: aktive Spionage seit 2004, z.B. auf ASEAN-Gipfeln, modulare Malware wie *Backspace* zur Überwindung von airgaps
- *APT31*: Operation *Iron Tiger* im Jahr 2013 war ein Angriff, wo US-Regierungsvertragspartner in den Bereichen Technologie, Telekommunikation und Energie attackiert wurden[478].

5.2.10 Die Lazarus-Gruppe (BlueNoroff, Andariel, Hidden Cobra)

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 von 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*[479]. Die gemeinsame Analyse ergab starke Hinweise, dass zumindest zwei der drei großen Wiperattacken und der Sony/SPE-Hack von derselben Gruppe durchgeführt wurden, die nun Lazarus Group[480] 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*[481] in 2015.

[475] vgl. PwC/BAE Systems 2017, S.14
[476] vgl. Threat Connect 2016
[477] vgl. FireEye 2015
[478] vgl. FireEye 2017
[479] vgl. Novetta 2016
[480] vgl. Novetta 2016
[481] vgl. Guerrero-Saade/Raiu 2016, S.2

Im Sommer 2016 wurde diskutiert, ob die *Lazarus Group* hinter den Angriffen auf das Interbankensystem SWIFT steht, siehe unten.

Allerdings war der SPE-Hack eine der umstrittensten Debatten in der Cyber-Attributions-Geschichte, die sich aus unerwarteten Fakten wie der anfänglichen Geldforderung, Datenverteilung von Computern außerhalb Nordkoreas usw. ergab.[482][483]. Auch die Mischung aus Cyberspionage und verdächtigen cyberkriminellen Aktivitäten wie der Angriff auf das Interbanken-System SWIFT war irritierend[484].
Allerdings könnten die meisten Widersprüche gelöst werden, wenn die folgenden Annahmen richtig sind:
1. Der SPE-Hack war zunächst ein Fall von Cyber-Kriminalität, der zu einem späteren Zeitpunkt zur politischen Materie eskalierte. Dies würde dem Kommunikations- und Angriffsmuster entsprechen.
2. Die *Lazarus*-Gruppe hat einen Kern von staatlich gebundenen Hackern, die Hacker in Südostasien koordinieren. Dies würde seltsame Befunde wie die langen Arbeitszeiten, die Angriffsorte, aber auch die Frage der begrenzten Netzwerkkapazitäten usw. erklären.

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[485]. 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[486]. Die Zeitstempel der Programme deuten auf eine Gruppe in der Zeitzone GMT+8 oder GMT+9 hin, was auf Korea passen würde[487].

Der Lazarusgruppe konnten inzwischen zwei weitere spezialisierte Gruppen zugeordnet werden, *Bluenoroff*, die sich auf ausländische Finanzinstitutionen konzentrieren, während sich die Gruppe *Andariel* mindestens seit Mai 2016 auf

[482] vgl. Fuest 2014b, S.31
[483] vgl. The Security Ledger online 2014, S.1
[484] vgl. Brächer 2016, S. 26-27
[485] vgl. Novetta 2016
[486] vgl. Guerrero-Saade/Raiu 2016
[487] vgl. Guerrero-Saade/Raiu 2016, S.6

Ziele in Südkorea konzentriert und es dabei u.a. auf Bankkarten, OnlinePoker und andere Onlinespiel-Seiten abgesehen hat[488].

5.2.10.1 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[489]. Die kommerziell verfügbare Software *EldoS RawDisk*[490] wurde benutzt, um die Windows-Laufwerke zu erreichen. In allen Fällen fungierte die Malware als **logische Bombe**, d.h. sie wurde erst zu einem vordefinierten Zeitpunkt aktiv[491].

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[492] (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[493], diese waren *Cutting Sword of Justice* (Aramco), *Whois/NewRomanic Cyber Army Team* (im *Darkseoul* hack[494]) 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[495]

---

[488] vgl. Kim 2017

[489] 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

[490] vgl. Baumgartner 2014, S.2, 4

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

[492] Zuvor wurden wie bereits erwähnt im April 2012 iranische Ölterminals von einer datenvernichtenden Wiper-Schadsoftware getroffen.

[493] vgl. McAfee 2013

494 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.

[495] vgl. Novetta 2016

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[496]. 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[497]. 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.

5.2.10.2 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[498]. 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[499]. 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*

[496] vgl. auch Baumgartner 2014, S.4-6
[497] vgl. Novetta 2016, S.15
[498] vgl. McAfee 2013, S.28
[499] vgl. Symantec 2013, S.1-2

Co (KHNP) wiederholt angegriffen und eine Reihe von Personal- und technischen Daten geleakt[500].

5.2.10.3 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.[501] und im Dezember 2014 wurde Sony auch von der Hackergruppe *Lizard Squad* angegriffen[502][503].

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[504]. 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.[505]
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[506].

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*[507] war. 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.[508] An Weihnachten 2014 wurde der Film *Das Interview* in einer begrenzten Anzahl von Kinos publiziert. Zudem wurden Sanktionen gegen einige nordkoreanische

---

[500] vgl. Leyden 2014, S.1-3. KHNP bestätigte, dass keine kritischen Daten abgeflossen sind und ließ Cyberübungen zur Erhöhung der Sicherheit durchführen.
[501] vgl. Lambrecht/Radszuhn 2011, S.25, Betschon 2014, S.34
[502] 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.
[503] vgl. Handelszeitung online 2014, S.1
[504] vgl. Fuest 2014b, S.31
[505] vgl. Betschon 2014, S.34
[506] vgl. Steinitz 2014, S.11
[507] 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
[508] vgl. SZ2014b, NZZ 2014

Personen Anfang 2015 verhängt, diese standen aber mit militärtechnologischen Angelegenheiten, nicht mit dem Sony-Hack in Verbindung[509].

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[510]. 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[511].Der Sony-Hack und die anderen Angriffe auf Südkorea verwendeten einen gemeinsamen Command and Control-Server, der sich in Bolivien befand[512]

Außerdem wurde über Nordkoreas wichtigsten Nachrichtendienst, das *General Reconnaissance Bureau*, berichtet, dass dieser über Cyberfähigkeiten verfügt, insbesondere zwei Einheiten mit den Namen *Unit 121 (Einheit 121)* und *No. 91 office (Büro Nr.91)*. Das *General Reconnaissance Bureau* wurde um 2009-2010 zur Bündelung der Cyberaktivitäten gegründet.[513] Es gibt einige wenige Berichte, nach denen einige dieser Personen aufgrund der begrenzten Internetkapzitäten des Landes vom Ausland aus operieren sollen[514].
Dies würde mit den Ergebnissen eines kürzlich veröffentlichten Berichts übereinstimmen, dass Nordkorea mittlerweile mehrere spezialisierte Einheiten hat, darunter auch die *Unit 180* für Cyber-Operationen im Finanzsektor. Cyber-Spezialisten würden aus dem Ausland wie China und Malaysia operieren, um die Zuordnung zu blockieren und die größere Internet-Infrastruktur nutzen [515]. Die russische Firma *Russian TransTeleCom* betreut seit Oktober 2017 60% des nordkoreanischen Internetverkehrs, während der bisherige Alleinanbieter *China Unicom* weiterhin 40% betreut. Schätzungen zufolge hat Nordkorea immer noch nicht viel mehr als 1000 Internetverbindungen ins Ausland[516].

[509] vgl. Zoll 2015, S.1
[510] 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.
[511] vgl. Fuest 2014b, S.31
[512] vgl. Robertson/Lawrence/Strohm 2014, S.1
[513] vgl. FAZ 2017d, S.6
[514] vgl. Robertson/Lawrence/Strohm 2014, S.2
[515] vgl. Park/Pearson 2017
[516] vgl. Reuters 2017c

Es wurde außerdem argumentiert, dass Nordkorea ein klares politisches Motiv gehabt hat[517], jedoch hat Nordkorea jede Beteiligung an dem Angriff auf das Schärfste zurückgewiesen[518].

Alternative Theorien wurden diskutiert, denn die Angreifer haben anfangs nach Geld gefragt[519] 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[520]. 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[521]. Die genutzten IP-Adressen wären auch von anderen Hackergruppen genutzt worden und die Schadsoftware wäre auf dem Schwarzmarkt verfügbar gewesen[522][523].

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[524]. Deshalb hielt das FBI an seinen Schlussfolgerungen zur Angriffsquelle fest[525]. 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, nordkoreanische Hackeraktivitäten zu beobachten und nachzuverfolgen, aber eine offizielle Bestätigung dieser Darstellung wurde zunächst nicht gegeben[526][527].

5.2.10.4 Die SWIFT-Attacken

Im Sommer 2016 vermuteten Sicherheitsexperten von *BAE Systems* die Lazarus Group hinter dem Eindringen in das globale Finanznetzwerk **SWIFT** *(Society for*

[517] vgl. Fuest 2014b, S.31
[518] vgl. NZZ 2014
[519] vgl. Fuest 2014b, S.31
[520] vgl. SZ 2014c, Bernau 2014, S.1
[521] vgl. The Security Ledger online 2014, S.1
[522] Siehe z.B. Bernau 2014, S.1
[523] 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).
[524] vgl. Zoll 2015, S.1
[525] vgl. SZ 2014c
[526] 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 Systeme half, Aramco wollte dies jedoch nicht kommentieren, Finkle 2012, S.1
[527] vgl. FAZ 2017d, S.6

Worldwide Interbank Financial Telecommunication), wodurch am 04.02.2016 der Transfer von 81 Millionen Dollar von der Zentralbank in Bangladesch zu anderen Konten möglich war[528]. 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[529]. Mittlerweile wurden weitere Attacken auf das SWIFT System für Banken in Ecuador, der Ukraine und Vietnam berichtet[530]. Der WiperCode, der zur Spurenverwischung genutzt wurde, war derselbe wie beim Sony/SPE-Hack[531].

Der SWIFT-Interbanking-Angriff ist von besonderer Bedeutung, denn inzwischen hat sich gezeigt, dass sowohl die *Lazarus*-Gruppe als auch zu *Carbanak*-gehörende Hacker **unabhängig voneinander das gleiche Ziel** angegriffen haben. Der Wiper-Code, der von der *Lazarus*-Gruppe benutzt wurde, um die Bankhacks zu verschleiern, war identisch zu dem, der im SPE-Angriff verwendet wurde[532], während die mutmaßlichen *Carbanak*-Hacker letztere eine neue Malware namens *Odinaff* benutzten[533].

Die polnische Finanzaufsichtsbehörde wurde gehackt, um ihre Webseite als Watering Hole zu nutzen, die Kampagne begann im Oktober 2016, wurde anscheinend von der *Lazarus/BlueNoroff* Gruppe durchgeführt und im Februar 2017 entdeckt[534].
2017 berichtete *BAE Systems*, dass die Lazarusgruppe wohl auch für die Entwendung von 60 Millionen Dollar von der taiwanesischen Bank *Far Eastern International Bank* verantwortlich war. [535]

5.2.10.5 Die WannaCry/Wanna Decryptor und Adylkuzz-Attacken

Wie bereits erwähnt, wurden am 14. April 2017 weitere Tools von den *Shadow Brokers* einschließlich *DoublePulsar, EternalBlue* und *EternalRomance* geleakt, die dann vermutlich von anderen Akteuren zur Vorbereitung von drei großen Cyberangriffen namens *WannaCry/WanaDecryptor 2.0*, *Adylukzz* und *Petya/Not-Petya/Petya2017* verwendet wurden.

---

[528] vgl. Brächer 2016, S. 26-27
[529] vgl. Storn 2016, S. 29
[530] vgl. FAZ 2016b, S.23, Storm 2016
[531] vgl. Storm 2016
[532] vgl. Storm 2016
[533] vgl. Symantec 2016c
[534] vgl. Kaspersky 2017a
[535] vgl. Boey 2017

Bereits am 24. April 2017 wurden 183.107 Computer mit *DoublePulsar* nach Angaben von Binary Edge infiziert[536].
Anfänglich wurde dem Phänomen nur wenig öffentliche Aufmerksamkeit geschenkt, jedoch begann am gleichen Tag (24. April 2017) der *Adylkuzz*-Malware-Angriff[537]. Diese Malware überprüfte Computer auf eine bereits vorhandene Infektion mit *DoublePulsar* und wenn nicht, wurde eine Infektion mit *EternalBlue* durchgeführt, wenn möglich [538].

Dies ermöglichte die Erstellung eines Botnetzes für die Schaffung virtuellen Geldes, das **virtual money mining**.
Virtuelles Geld, wie **Bitcoin**, wird durch eine Folge komplexer Berechnungen erzeugt, die mathematisch mit den zuvor erzeugten Bitcoins verknüpft sind, einem Validierungsverfahren, das als Blockchain bekannt ist. Da eine entsprechende Rechenleistung erforderlich ist, sind diejenigen, die ein neues Bitcoin berechnen, die Besitzer des neuen Bitcoins. Zusammenfassend ist das Bitcoin mining der Berechnungsaufwand für die Schaffung eines neuen Bitcoins.
Die illegale Nutzung fremder Computer zum bitcoin mining ist auch als **cryptojacking** or **collective mining** bekannt. Eine 2017 verbreitete mining-Malware war *Coinhive*[539].

Adylkuzz nutzt jetzt infizierte Computer für das Bitcoin mining, überträgt aber das Ergebnis an den Kontrollserver und löst hiermit das virtuelle Geld von den erschaffenden Computern. Virtuelles Geld ist auch als **digitales Geld** oder **Krypto-Währung** bekannt. Aus mathematischen Gründen ist das Maximum von Bitcoins begrenzt, weitere Arten von virtuellem Geld sind in der Entwicklung.

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*[540].

---

[536] vgl. WinFuture 2017
[537] vgl. PandaSecurity 2017
[538] vgl. Kling 2017a
[539] vgl. Betschon 2017
[540] 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

Am 12. Mai 2017 begannen Masseninfektionen von mehr als 200.000 Computern in über 150 Ländern mit der Ransomware *WannaCry*. Es wurde auch *WannaCry 2* genannt, sowie *Wanna Decryptor 2.0, WanaCrytOr 2.0 und Wanna Decryptor 2*[541]. Wie *Adylkuzz* überprüft diese Malware Computer auf eine bereits vorhandene Infektion mit *DoublePulsar* und *nur* wenn der Computer nicht mit DoublePulsar infiziert ist, wurde eine Infektion mit *EternalBlue* durchgeführt, wenn möglich[542]. Dies könnte zur schnellen Masseninfektion beigetragen haben, obwohl der *EternalBlue*-Exploit von Microsoft bereits nach einer Warnung von der NSA an einem Patch-Day im März 2017 geschlossen wurde [543].
Die Ransomware-Ausbreitung wurde durch die Registrierung und Aktivierung einer hartcodierten IP-Domain, die im Malware-Code erwähnt wurde, durch einen IT-Forscher blockiert, weil die Aktivierung einen vorprogrammierten Stopp der Malware-Verbreitung induzierte[544].
Die Analyse zeigte, dass *WannyCry* relevante Ähnlichkeiten mit einer Funktionalität eines Trojaners hatte, der bei SWIFT -Attacken verwendet wurde.[545] Technische Überschneidungen wurden zum SPE- und SWIFT-Hack gefunden, auch für den polnischen Bankangriff vom Februar 2017[546].

Nach dem Angriff wurde diskutiert, warum so viele alte Windows-Systeme noch aktiv sind, da insbesondere Windows XP anfällig war. Allerdings sind oft Windows-Systeme in ein institutsspezifisches digitales Ökosystem von Anwendungen eingebettet und Updates tragen das Risiko von Schäden oder Kollaps, die in Wirklichkeit hohe Hürden für die Erneuerung darstellen.[547]

Über Phishing emails wird von den nordkoreanischen Hackern eine Malware verschickt, die laut des *südkoreanischen Computer Emergency Response Team (CERT)* eine *Adobe Flash-Player* Lücke nutzt[548].

In einem Fall hatte das Bitcoin-Mining den attackierten Server überlastet, so dass eine Spur nach Nordkorea gesichert werden konnte. Zusätzlich zum Bitcoin-Mining werden zunehmend digitale Tauschbörsen angegriffen. Der Schaden wird vom britischen Geheimdienst GCHQ auf bis zu 1 Milliarde Dollar pro Jahr geschätzt[549].

---

typischerweise mit TOR-Browsern zugänglich ist, Überlappungen zum Cyberwar finden sich z.B. in der Anwendung von DDoS-Attacken.
[541] vgl. Bodkin/Henderson 2017
[542] vgl. Lee et al. 2017
[543] vgl. Perloth/Sanger 2017
[544] vgl. Bodkin/Henderson 2017
[545] vgl. O'Neill/Bing 2017
[546] vgl. Perloth/Sanger 2017
[547] vgl. Steier 2017
[548] vgl. Kant 2018
[549] vgl. Freidel 2018

Bei einem Angriff auf die japanische Börse *Coincheck* 2018 wurden 523 Millionen Einheiten der Kryptowährung *XEM* gestohlen mit einem Schätzwert von 430 Millionen Euro, die Urheber konnten noch nicht geklärt werden. Das Geld war in einer "heissen", d.h. online ans Internet angeschlossenen Börse aufgehoben worden, statt in einer sichereren offline "kalten" Börse (cold wallet)[550].

Der südkoreanischen Krypto-Börse *Coinrail* wurden 2018 bei einem Hackerangriff 31 Millionen Euro gestohlen[551]. Kleinere Währungen wie *NXPS* waren betroffen. Das Geld war nicht in einer *cold wallet* gesichert, d.h. die Gelder waren vom Internet aus direkt zugänglich.
Die Sicherheitsfirma *Proofpoint* berichtete 2018 vom Mining Botnetz *Smominru*, das ebenfalls den *EternalBlue*-Exploit auf Windows-Servern ausnutzt und ca. eine halbe Million Computer zum Kryptomining nutzt. Seit Mai 2017 wurden rund 8900 Einheiten der Kryptowährung *Monero* generiert, was Anfang Februar 2018 ca. 24 Monero am Tag = ca. 8900 Dollar pro Tag entsprach[552].

5.2.10.6 Die Olympic Destroyer (false flag)-Attacke 2018

Lazarus wurde verdächtigt, einen Netzwerk-Wurm-Angriff mit der Malware *Olympic Destroyer* auf die Olympischen Winterspiele in Pyeongchang in Südkorea durchgeführt haben, die zu verschiedenen unzugänglichen Olympia-Websites führte, aber *Kaspersky* zeigte, dass dies ein false-flag-Angriff war, bei dem ein unbekannter Dritter einen digitalen Fingerabdruck von *Lazarus* im Angreifercode platzierte[553]. Außerdem verwendet *Lazarus* lange und zuverlässige Passwörter und hartkodiert keine Passwörter in der Malware. Ein *Wiper*-Element wurde zu spät hochgeladen, also zwei Stunden nach der Eröffnungsfeier.

5.2.10.7 Das Park Jin-hyok indictment 2018

Experten von *Mandiant* (der gleichen Firma, die APT1 analysierte) unterstützten die FBI-Ermittlungen zur *Lazarus*-Gruppe. Eine fiktive Person namens *Kim Hyon Woo* nutzte die Konten der staatlichen Firma *Chosun Expo* und wurde als *Park Jin-hyok* identifiziert, der als ein nordkoreanischer Geheimdienstoffizier des *Lab 110* des Militärgeheimdienstes RGB gilt[554]. Er benutzte eine Reihe von E-Mail-Accounts mit dem Cover-Namen *Kim Hyon Woo*, die von Computern aufgerufen wurde, die in mehreren Angriffen der *Lazarus*-Gruppe verwendet wurden, wie z.B. im SPE-Hack, der *Lockheed*-Angriffe und dem Angriff auf die Zentralbank von

[550] vgl. Welter 2018, S.8
[551] vgl. FAZ 2018f
[552] vgl. Beiersmann 2018a
[553] vgl. GReAT 2018
[554] vgl. Cimpanu 2018

Bangladesch[555] Die nordkoreanischen IP-Adressen wurden als Befehls- und Steueradresse für verschiedene Malware-Arten verwendet, z.B. für den Angriff auf *Lockheed Martin*[556].
Zu beobachten waren unter anderem eine Wiederverwendung von Code-Schnipseln und die Verwendung von FakeTLS. Die **Transport Layer Security TLS** ist ein kryptografisches Protokoll und ein FakeTLS imitiert authentisch verschlüsselten TLS-Verkehr, so dass Computerwarnsysteme nicht reagieren. Dies wurde bei *WannaCry, Macktruck (SPE Hack), Nestegg* und *Contopee* (Bank-Attacken in Asien) usw. verwendet.[557] Darüber hinaus gibt es mehrere technische Beziehungen zu den Malwaretypen *Destover*, dem *Brambul*-Wurm und *Wannacry*[558].

5.2.10.8 APT37 und APT 38

Im Bezug auf Nordkorea hat *FireEye* eine Differenzierung der Aktivitäten innerhalb der *Lazarus*-Gruppe festgestellt, die zur Entstehung von zwei neuen APTs, der APT37 (auch bekannt als *Reaper, Group 123* oder *Scarcruft*) und APT 38 geführt haben, die beide spezifische Taktiken, Techniken und Verfahren haben und damit ein spezifisches Profil. Beide APTs sind auf die Finanzoperationen spezialisiert, aber APT 38 ist einzigartig darin, Beweismittel oder Zielnetzwerke im Rahmen ihrer Operationen zu zerstören[559].

5.2.11 Iran

FireEye berichtete 2017 über die neue APT33, die mit der iranischen Regierung in Verbindung steht, unterstützt durch Erkenntnisse, dass Werkzeuge wie *Nanocore, Netwire* und *AlfaShell* typischerweise von iranischen Hackern verwendet werden, die auf iranischen Hacking-Webseiten und bei anderen iranischen Cyber-Akteuren präsent sind[560]. Die *Dropshot* (auch bekannt als *Stonedrill*) Malware wird verwendet, um die *Turnedup*-Backdoor zu etablieren, die dann manchmal an die zerstörerische Malware *Shapeshift* verwendet wird, die konfiguriert werden kann, um Dateien zu löschen, ganze Volumen zu löschen oder Festplatten zu säubern. *Dropshot und Shapeshift* Codes weisen einige Farsi-Sprachartefakte auf.

Eine Verbindung zum *Shamoon*-Angriff vor einigen Jahren konnte jedoch nicht hergestellt werden: *Shamoon* konzentrierte sich auf Regierungsziele und hatte Elemente arabisch-jemenitischer Sprache, während *Dropshot* auf kommerzielle Organisationen mit Farsi-Sprachreferenzen zielte. Die Tatsache, dass beide Saudi-

[555] vgl. Shields 2018, S.6, 134 und 138
[556] vgl. Cimpanu 2018, Shields 2018, S.13
[557] vgl. Cimpanu 2018
[558] vgl. Shields 2018, S.56
[559] vgl. FireEye 2018a
[560] vgl. O'Leary et al. 2017

Arabien angriffen, Wiper verwendeten und gegen virtuelle Maschinen gesichert waren (Anti-Emulation), war nicht ausreichend. Ein Mann von APT33 mit der Coveridentität xman_1365_x konnte mit dem *Nasr-Institut* in Verbindung gebracht werden, das von den USA verdächtigt wird, der iranischen Cyber-Armee identisch zu sein, und das auch verdächtigt wurde, von 2011 bis 2013 Angriffe auf US-Finanzinstitute in einer Operation namens *Ababil* ausgeführt zu haben.[561]. APT33-Angriffe wurden nun in den USA, Saudi-Arabien und Südkorea registriert, wobei der Schwerpunkt auf Firmen lag, die mit dem militärischen und dem Energie-Petrochemie-Bereich zusammenarbeiten.

Eine weitere iranische APT ist APT34, die seit 2014 tätig ist und iranische Infrastruktur nutzt, die zur Zuordnung zum Iran führte, womöglich identisch mit der Gruppe *OilRig*. Im Fokus stehen strategisch relevante Unternehmen im Nahen Osten. APT34 benutzte eine Reihe von speziellen Tools (*Powbat, Powrunner, Bondupdater*), um einen inzwischen gepatchten Microsoft Office-Exploit zu verwenden[562]. In eine ähnliche Richtung zielt die Gruppe *APT39/Chafer*, die auch seit 2014 aktiv ist und eine abgewandelte *Powbat*-Version einsetzt[563].

Das *US Department of Justice (DoJ)* gab im April 2018 einen großangelegten Angriff auf 320 Universitäten bekannt, u.a. 23 Universitäten in Deutschland, wo dann Papers, Dissertationen und Konferenzberichte veröffentlicht wurden[564]. Zuerst wurde die Uni Göttingen attackiert, dann 22 weitere Universitäten in Hessen und NRW mit phishing-Mails und falschen Bibliotheksseiten. Ein Institut namens *Mabna* in Teheran betrieb die website *Megapaper*, wo sich die Dateien wiederfanden.

5.2.12 Cybercrime-Gruppen

Im Augenblick sind die meist diskutierten Cybercrime-Gruppen die *Carbanak Gruppe* und das *Avalanche*-Botnetz.
Kaspersky Labs identifizierte im Jahr 2017 8 Gruppen, die auf Ransomware-Angriffe spezialisiert sind, wie *PetrWrap* und *Mamba.*
PetrWrap greift finanzielle Institutionen an und zielt darauf ab, sehr wichtige Dateien zu verschlüsseln, um die Wirkung und die Zahlungsbereitschaft zu erhöhen[565].

5.2.12.1 Carbanak/Fin.7

Eine der größten bekannten Aktivitäten der Cyberkriminalität, der Diebstahl von 1 Milliarde Dollar von insgesamt 100 Finanzinstituten durch die Carbanak-Gruppe

[561] vgl. O'Leary et al. 2017
[562] vgl. FireEye 2018
[563] vgl. FireEye 2019
[564] vgl. Diehl 2018, S.58-59
[565] vgl. Scholl-Trautmann 2017

wurde auf diese Weise durchgeführt[566]. Zudem übernahmen sie die Kontrolle über die Überwachungskameras und konnten so in Ruhe vorab die Abläufe in den Instituten studieren[567].
Die Carbanak-Gruppe benutzte ein lateral movement, um das Zugangslevel zu Bankennetzwerken zu eskalieren. Trotz massiver Anstrengungen z.B. der russischen Behörden, um die Gruppenmitglieder zu verhaften, bestanden Reste der Gruppe weiterhin und griffen SWIFT mit der *Odinaff-Malware* im Jahr 2016 an. Sie benutzten Domains mit schwer nachzuverfolgender Registrierung für ihre Aktivitäten. Zudem drang die Gruppe in Hotelnetzwerke ein, um Informationen über die Gäste zu bekommen, 2018 wurden drei Gruppenmitglieder dafür offiziell angeklagt[568].

5.2.12.2 Avalanche

Das Ransomware-freisetzende Botnetz *Avalanche* nutzte die **Fast-Flux-Technologie**, um die Erkennung zu vermeiden. Schließlich erlaubte das Sinkholing, 130 Terabyte Daten abzufangen. Die Analyse dieser Daten erlaubte es den Strafverfolgungsbehörden, das Botnetz zu stoppen und die Mitglieder der *Avalanche*-Gruppe zu verhaften. Die Kooperation des *Bundesamtes für Sicherheit in der Informationstechnik BSI*, der Forschungseinheit *Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE*, der deutschen *Polizei, Europol, Eurojust*, des *FBI* und der Sicherheitsfirma *Symantec* machten dies trotz des Missbrauchs von 800.000 (!) Domains möglich[569].
Avalanche nutzte auch den drive-by-exploit *Andromeda*, der jedoch nach dem Coup gegen *Avalanche* immer noch weiter verbreitet wurde; FBI, Europol und weitere Ermittler aus 25 Ländern konnten das *Andromeda*-Netzwerk jedoch Ende 2017 schließen[570].

5.2.12.3 Smart Contract Hacking/51% Attacken

Ethereum ist eine virtuelle Währung, deren Transaktionen an Ausführungsbefehle, die smarten Verträge (**Smart Contracts**) gebunden ist. Die Ausführung erfolgt über ein dezentrales Peer-to-Peer-Netzwerk von sog. Minern, die durch '*gas*' genannte Ausführungskosten von dem Transfer profitieren. Ethereum kann in kleinste Einheiten, *wei* genannt (1 Ether = 10^{18} wei) aufgeteilt werden, was eine präzise Ausführung sichert[571].
Manipulationen (**Smart Contract Hacking**) haben schon Schäden bis zu 60 Millionen Dollar bei einem Vertrag verursacht, in der sogenannten DAO-Attacke

[566] vgl. Bilanz 2015, S.50-57
[567] vgl. Kaspersky Lab 2015c, S.1
[568] vgl. Langer 2018a
[569] vgl. EUROPOL 2016
[570] vgl. Zeit online 2017
[571] vgl. Atzei/Bartoletti/Cimoli 2016

wurde eine Crowdfunding-Plattform am 18 Juni 2016 um diesen Betrag geschädigt. Vereinfacht gesagt erzeugte die Attacke eine Endlosschleife von Buchungen, bis das Geld weg war[572]. Es gibt zahlreiche weitere Schwachstellen, die die Contracts, das 'gas', die Adressen usw. betreffen können.

Eine neuartige Angriffsmethode sind **51 %-Attacken**. Dabei setzt ein crypto currency miner soviel Rechnerkraft ein, dass er kurzfristig die Mehrheit der Rechenkraft für eine Kryptowährung hat (was bei Bitcoins sehr teuer und aufwendig wäre, jedoch nicht bei kleinen Währungen). Dadurch kann er dann Zahlungen mit der Blockchain an andere vornehmen, aber danach eine andere Version derselben Blockchain erstellen (Fork = Aufgabelung), in der die Zahlungen nicht vorkommen. Der dominante Rechner kann dann bei der Aufgabelung „seine" Version für wahr erklären, so dass zukünftige Zahlungsflüsse an diese gefälschte Blockchain anknüpfen[573].

5.2.13 Weitere Gruppen

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* [574] bearbeitet wurden, zu extrahieren. Im Dezember 2014 tauchte eine ähnliche Malware für Smartphones unter dem Namen *Cloud Atlas/Inception*[575] wieder auf.

Die *APT32/Ocean Lotus Group* ist eine vermutlich vietnamesische APT, von der berichtet wurde, einen Fokus auf Firmen mit Geschäftstätigkeit in Vietnam zu haben. Social Engineering wird für den Einsatz von *ActiveMime*-Files and Malware wie z.B. *Soundbite* benutzt. [576]

[572] vgl. Atzei/Bartoletti/Cimoli 2016, S.14
[573] vgl. Orcutt 2019
[574] vgl. Kaspersky Labs 2013
[575] vgl. Dilger 2014
[576] vgl. FireEye 2017

6. Cyberverteidigung und Cyber-Intelligence

6.1 Cyberverteidigung

6.1.1 Einführung

Man kann auf verschiedenen Ebenen gleichzeitig ansetzen, wie die folgende Übersicht zeigt:

Ebene	**Verfahren**
User	Regelmäßige Updates, vorsichtiger Umgang mit Dateien, Virenschutz, Spamfilter, sichere Passwörter, 2 Faktor-Authentisierung mit Passwort und einem Gegenstand, Daten verschlüsseln, Firewalls (Kontrolle des Netzwerkzugriffs) Forschung: Tastendruckdauer- und stärke sowie Mausbewegungsmuster als nicht imitierbare individuelle Kennungen
Organisation	Whitelisting, segmentierte Netze, Need to know, Vier Augen-Prinzip für Administratoren
Sicherheitsfirmen	Threat Intelligence, Intrusion Detection, Penetration Testing, Honeypots, Sandbox Analysis, Datenkombination
Kooperationen	Nachrichtendienste (z.B. 5-/9-/14-eyes), Polizei (Europol), ENISA, AK KRITIS, Charter of Trust usw…
Recht	Straf- und Haftungsvorschriften, Sicherheitsstandards
Technik	z.B. DDoS-Abwehr: Daten ableiten, Provider einschalten, eigene IP abschalten, fremde IP sperren (geoblocking), Verlangsamung (tarpitting) Einbahnstraßentechnologien: Campusnetzwerke (Daten raus, aber nicht rein), Datendioden (rein, aber nicht raus)

Man kann zuerst bei sich selbst als User, aber auch auf den Ebene der Organisationen ansetzen, bei der Nutzung von Cybersicherheitsfirmen, durch Kooperation von Behörden und Firmen, durch gesetzliche Maßnahmen und im Falle einer Datenüberflutung auch mit rein technischen Mitteln.

Für die Nutzer ist das wichtigste, ihr System immer auf dem neuesten Stand zu halten und Vorsicht gegenüber unklaren Emails walten zu lassen. Bei der Passwortsicherheit sollte ein Passwort nicht zu simpel, aber auch nicht zu kurz sein. Im Zweifel ist das wichtigste, sich nicht von seiner Neugier hinreißen zu lassen, auch wenn dies manchmal schwerfällt. Organisationen können unter anderem das **Whitelisting** anwenden, d.h. was nicht ausdrücklich von der IT erlaubt wurde, ist auf Firmencomputern verboten, man kann wichtige Netzteile abtrennen, den Zugriff der Mitarbeiter auf das Nötigste beschränken (**need to know**), Administratoren können sich bei wichtigen Eingriffen gegenseitig überwachen.

Sicherheitsfirmen können Angriffe im Rahmen der **Threat Intelligence** mit Angriffsmuster-Datenbanken abgleichen, aber auch im Rahmen der **Intrusion**

Detection den Datenverkehr auf ungewöhnliche Vorgänge und statistische Auffälligkeiten abklopfen.
Threat Intelligence Repositories vergleichen eingehende Informationen mit bekannten IP-Adressen, Domainnamen, Webseiten und auch mit Listen bekannter bösartiger Attachments[577]. Dies ermöglicht eine sofortige Erkennung und manchmal sogar die Zuordnung eines eingehenden Angriffs. Neu entdeckte Malware kann mit so genannten **Indicators of Compromise IOC** integriert werden, d.h. Zahlenfolgen, die die Erkennung der Infektion in einem bestimmten Computer ermöglichen.

Die US-Regierung baut im Moment hochentwickelte Sensorsysteme aus[578]: 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[579].

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[580]. 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.

---

[577] vgl. Alperovitch 2014. Die IT-Sicherheitsfirma *CrowdStrike* 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.
[578] vgl. Gerstein 2015, S.4-5
[579] vgl. Welchering 2014b, S. T4
[580] vgl. Beuth 2016a, S.1-3

Administratoren können die Systemsicherheit durch Hacker als Penetrationstester prüfen, oder fremde Hacker durch **Honigfallen**, also scheinbar anfällige Computer anlocken, um ihr Treiben analysieren zu können. Man kann gefundene Schadprogramme in virtuellen Umgebungen, den sogenannten **sandboxes** laufen lassen, um ihre Funktion zu verstehen und schließlich, was immer häufiger vorkommt, das Wissen kombinieren.

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[581], 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.

Kooperationen können, um nur einige Beispiele zu nennen, z.B. zwischen den Nachrichtendiensten erfolgen, wobei Deutschland bei den USA zu dem erweiterten Kreis der 14-eyes gehört, die Polizei arbeitet sehr gut in Europol auch mit dem FBI zusammen, die Europäer in der *Netzwerkagentur ENISA*, deutsche Firmen und Behörden im *Arbeitskreis Kritische Infrastrukturen* und große deutsche Firmen haben sich zusammengeschlossen, um in der *Charter of Trust* Sicherheitsstandards für die Zulieferer zu etablieren.

Einen bedeutenden Fortschritt stellt die Bildung von weiteren großen **Cyber-Allianzen** dar, z.B. die *Cyber Threat Alliance* der Sicherheitsfirmen *Fortinet, Intel Security, Palo Alto Networks* und *Symantec* zur Bekämpfung von Ransomware. Eine wachsende Zahl privater Sicherheitsfirmen sammelt Daten und führt Langzeitanalysen zur Identifikation von Angreifern durch. In schwierigen Fällen tendieren die Firmen auch zur Kooperation und zur Kombination ihrer Analysen, z.B. in den großangelegten cyberforensischen Operationen *SMN* und *Blockbuster*, Einzelheiten folgen weiter unten.
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. Auch große Privatunternehmen koordinieren ihre Cyberverteidigung, wie z.B. in der *Deutschen Cyber Sicherheitsorganisation DCSO* mit *VW, BASF, Allianz und Bayer*.

[581] vgl. Dohmen 2015, S.75

6.1.2 Abwehr von DDoS-Angriffen

Die deutsche Sicherheitsbehörde BSI hat generelle Empfehlungen zur Abwehr von DDoS-Attacken herausgegeben[582]. Der attackierte Server kann die Antwortzeit zum angreifenden Computer verlängern, so dass letzterer sehr lang auf die 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 und umgeleitet 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.

6.1.3 Automatisierte Cyberabwehr

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[583]. Das Budget der Plan X-Forschung betrug 110 Millionen US-Dollar.

Die *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[584].
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 [585]

[582] vgl. BSI 2012
[583] vgl. DARPA 2012, Nakashima 2012b
[584] vgl. DARPA 2016
[585] vgl. Atherton 2016

Die DARPA war mit dem Ergebnis zufrieden, da es ein erster Schritt in Richtung vollautomatischer Abwehr- und Reaktionssysteme war.[586]. Da die Zahl der Sicherheitslücken inzwischen immens ist[587], 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 überzeugen, in den inaktiven Zustand überzugehen oder einen Patch zu konstruieren, der das Verteidigungssystem lahmlegt.

6.2 Human Intelligence (HumInt)

Die Identifikation der Angreifer ist mit rein digitalen Methoden manchmal unmöglich. Die Anwendung von Spionagemethoden der Human Intelligence kann dazu beitragen, den *missing link* zu finden.

Die folgenden Methoden sind in der Praxis der Attribution die wichtigsten:

- Cyber-Intelligence
- Intelligence Cooperation zum Informationsaustausch
- Konventionelle Anwendung von Intelligence.

6.2.1 Cyber-Intelligence

Cyber-Intelligence kann auf eine Vielzahl von Methoden zurückgreifen (siehe auch Kapitel 2):

Die Vorbereitung des Schlachtfeldes (*Preparing the battlefield*) gilt als wesentlich für erfolgreiche Strategien, in der Praxis werden vorsorglich Sender (**beacons**) oder Implantate in ausländischen Computernetzwerken platziert, das ist Computercode, mit dessen Hilfe die Arbeitsweise des Netzwerks untersucht werden kann[588]. Zum Beispiel hatte die NSA Implantate in iranischen Netzwerken versteckt (*Nitro Zeus*) [589] und wie schon beschrieben in russischen Netzwerken als Warnsignal.

Hack the hackers: Wenn die Angreifer identifiziert sind, kann es sich lohnen, diese ihrerseits zu infiltrieren, um mehr über ihre Arbeitsweise zu erfahren.

---

[586] vgl. DARPA 2016
[587] 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
[588] vgl. Sanger 2015, S.5
[589] Gebauer 2016, S.17

Datenanalyse: Große Serverfarmen können auch zur Analyse sehr großer Datenvolumina genutzt werden, man spricht auch von **big data**. Wie bereits dargelegt, ist das Hauptproblem nicht die Informationsgewinnung, sondern die Speicherung und zielgerichtete Analyse[590].
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[591].
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[592].
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[593]. Mehr als 90% dieser BND-Suchbegriffe sind formale Begriffe wie Telefonnummern, email- oder IP-Adressen von verdächtigen Usern oder Unternehmen[594].

Ein gezielterer Ansatz ist die Erstellung von **User-Profilen**. Im März 2012 hat Google bekanntgegeben, dass Profile durch Verknüpfungen von Suchmaschinennutzungen, *YouTube*, *Google plus* und *gmail* erstellt werden[595]. Ähnliche Prozeduren sind auch von Betreiberfirmen sozialer Netzwerke bekannt, aber Google und andere Firmen wurden 2013 von einem mutmaßlich chinesischen Hackerangriff betroffen bei dem Profile chinesischer Nutzer geprüft und exportiert wurden[596].

Ein weiterer Ansatz ist die **digital dust analysis**. Wenn in Russland oder China ein neues US-Botschaftsmitglied angekündigt wird, wird nicht nur die Menge, sondern auch die Verbreitung digitaler Informationen überprüft. Wenn der digitale Fußabdruck des Newcomers zu klein ist, wie Social Media-Beiträge, Handy-Telefonate, Kreditkarten-Zahlungen, dann wird der Diplomat als Undercover-CIA-Offizier markiert[597].

---

[590] Das diskutierte Speichervolumen für das NSA data Center bewegt sich im Bereich von Yottabytes, also 10^{24} bytes, Juengling 2013, S.52
[591] vgl. Hayes 2007. Die Identifikation von Netzwerken nennt man auch **community detection.**
[592] vgl. Tomik 2013a, S.6
[593] vgl. Amann 2013, S.17
[594] vgl. Schulz 2013, S.6
[595] vgl. Spiegel 2013d, S.111
[596] vgl. Süddeutsche Online 2013
[597] vgl. Rohde 2016

Nach 2010 wurden 18 bis 20 CIA-Quellen in China getötet oder eingesperrt. Die verschlüsselte Kommunikation zu CIA-Agenten wurde möglicherweise geknackt, dies konkurriert jedoch mit anderen Theorien wie Leaks durch einen Verräter oder Fehler (zu oft auf den gleichen Reiserouten, Essen in Restaurants mit Abhörgeräten und ‚Kellnern', die vom chinesischen Geheimdienst beschäftigt werden). [598]
Inzwischen wurde ein mittlerweile in Hongkong lebender ehemaliger CIA-Mitarbeiter namens Lee verhaftet, bei dem schon 2013 Informationen über chinesische CIA-Mitarbeiter vom FBI gefunden worden waren, man sich jedoch wohl erst jetzt hinreichend sicher war, um ihn 2018 bei einer Einreise in die USA zu verhaften[599]. Lees Fall war der dritte, an dem US-Agenten in weniger als einem Jahr in China beteiligt waren und hat gestanden[600].

6.2.2 Nachrichtendienstliche Kooperation

Die Berichterstattung in den Medien vermittelte den Eindruck, dass sich die nachrichtendienstliche Kooperation auf Computer und die Erfassung und Auswertung von allen Formen der 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 schon Jahrzehnte vor den Anschlägen des 11.September 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)[601].
Theoretisch ist Spionage zwar nicht legal, somit die Präsenz von Agenten ebenfalls[602], das Gewohnheitsvölkerrecht erkennt jedoch das Recht souveräner Staaten auf Spionage an, so dass die Zusammenarbeit möglich ist.
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

[598] vgl. Mazetti 2017
[599] vgl. Winkler 2018, S.3
[600] vgl. BBC 2019
[601] vgl. Best 2009
[602] vgl. Radsan 2007, S.623

Aktivitäten und Verantwortlichkeiten behaftet, zudem kann es zu Konkurrenzdenken und Kommunikationsdefiziten zwischen den Einrichtungen kommen. Die Standardlösung sind mehrere Dienste mit einer koordinierenden Ebene[603]. 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, sein office wird auch als ODNI bezeichnet, davon sind die 8 militärischen Dienste in der Dachorganisation **Defense Intelligence Agency DIA**[604] zusammengefasst.

Die zweite Ebene wird durch ein Geflecht von **bilateralen Kooperationen** gebildet, z.B. Deutschland verfügt über Kontakte zu mehr als 100 Staaten[605]. 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 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[606]:

- **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[607].

---

[603] vgl. Carmody 2005

[604] 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

[605] vgl. Daun 2009, S.72

[606] vgl. Jäger/Daun 2009, S.223

[607] vgl. Wetzling 2007

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[608] berichteten) erweiterten Kooperationen **9-eyes** mit Dänemark, Frankreich, den Niederlanden und Norwegen und **14-eyes** mit Belgien, Italien, Spanien, Schweden und Deutschland.
Bei näherer Betrachtung spiegelt dies nicht nur eine Präferenzordnung, sondern auch eine geographische Logik wider. Die 9-eyes-Partner befinden sich an der östlichen und südlichen Flanke des Vereinigten Königreichs, während die 14-eyes-Gruppe die umliegenden Nachbarn der 9-eyes-Staaten sind und zusammen einen territorialen Block bilden. Dies ermöglicht die Schaffung einer europäischen Plattform und die Sicherung der Überwachung und der physischen Präsenz in diesen Ländern.

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)[609] wertet die Informationen aus, die von Organisationen der Mitgliedsstaaten, Arbeitsgruppen zur Terrorbekämpfung usw. geliefert werden. [610]
Mittlerweile ist das *SitCen* Teil des *Europäischen Auswärtigen Dienstes EAD (European External Action Service EEAS)* und wird nun *Intelligence Center (INTCEN)* genannt, welches nach dem aktuellsten Organigramm vom 01.02.2019 in die 4 Einheiten *Intcen 1-4* für *Analysis, OSINT, Situation Room* und *Consular crisis management* gegliedert ist. Das EAD hat zudem einen Sicherheitsdienst für die eigene Sicherheit[611]. Das militärische Nachrichtenwesen wird im Militärstab der EU *(EU Military Staff EUMS)* koordiniert. Europäische Nachrichtendienste kooperieren auch seit 1972 im *CdB (Club de Berne)* [612].
Afrika hat inzwischen die multinationale Kooperation *Committee of Intelligence and Security Services of Africa CISSA* als Teil der Afrikanischen Union eingerichtet (siehe auch Kapitel 8).

[608] wie z.B. Shane 2013, S.4
[609] 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).
[610] vgl. Scheren 2009
[611] vgl. Tagesschau online 2019
[612] vgl. Scheren 2009

6.2.3 Konventionelle Anwendung von Intelligence

Ereignisse von 2016 veranschaulichen die Relevanz der konventionellen Spionage für die Zuordnung. Wie bereits erwähnt, waren die Spannungen zwischen Russland und den USA bereits im Gange, da die russische Sicherheitsfirma *Kaspersky* Sinkholing gegen die vermutlich US-amerikanische *Equation Group* eingesetzt hat[613], die ihrerseits *Kaspersky* mit der anspruchsvollen Spionage-Malware *Duqu 2.0* infiziert hat[614].

Im August 2016 gab eine bis dahin unbekannte Gruppe namens *Shadow Brokers* an, Cyberwaffen der *Equation Group* in ihrem Besitz zu haben und veröffentlichten Material.

Der **Michailow-Vorfall:** Ende August 2016 wurde ein erfolgreiches Eindringen in Onlinewahlsysteme von Illinois und Arizona berichtet, in Illinois wurden Daten von 200.000 Wählern kopiert[615]. Die Medien spekulierten darüber, dass dies Teil einer russischen Kampagne sei, definitive Beweise wurden bisher aber nicht gefunden.[616] Aber dann wurde festgestellt, dass eine Firma namens *King Server* sechs Server für diesen Angriff von einer Firma namens *Chronopay* mietete. Der russische Besitzer von *Chronopay* wurde bereits von *Sergej Michailow*, einem Mitglied der russischen Intelligence Cyber-Unit CIB des Nachrichtendienstes FSB untersucht, der (nach Berichten z.B. aus der Zeitung *Kommersant*) die US-Behörden über diese Angelegenheit informierte.[617]. *Russia Today* bestätigte, dass es einen Fall Michailow gibt, ohne die Einzelheiten des Informationslecks zu bestätigen und stellte klar, dass der Fall zusammen mit anderen Vorgängen noch von den russischen Behörden untersucht wird[618].Auch ein Cybersecurity-Experte namens *Ruslan Stojanow* von *Kaspersky Labs* war beteiligt. Während Details unklar sind, berichteten russische Zeitungen über eine Affäre mit unberechtigter Offenlegung von bis zu hundert IP-Adressen des russischen Verteidigungsministeriums gegen die Zahlung eines hohen Geldbetrags vermutlich durch einen ausländischen Geheimdienst. Allerdings war *Kaspersky Labs* als Organisation nicht beteiligt[619].

Der **Surkov-Vorfall**: Mitte Oktober 2016 gab US-Vizepräsident *Joe Biden* bekannt, dass die USA ernsthaft eine Cyber-Vergeltung gegen Russland aufgrund ihrer vermuteten Beteiligung am *DNC-Hack* und anderen Dingen erwägen würden[620]. Ein paar Tage später, d.h. noch vor den Präsidentenwahlen in den USA, präsentierte

[613] vgl. Kaspersky Lab 2015a, S.34-35. Unerwarteterweise wiesen frühe Versionen der *Equation Group*-Malware hartcodierte (fest verankerte) IP-Adressen in ihren Programmen auf.
[614] vgl. Kaspersky Lab 2015b
[615] vgl. Nakashima 2016, Winkler 2016, S.4
[616] vgl. Winkler 2016, S.4
[617] vgl. FAZ 2017, S.5
[618] vgl. Russia Today (RT Deutsch) online 27.01.2017
[619] Russia Today (RT Deutsch) online 27 Jan 2017
[620] vgl. Zeit online 2016a

eine ukrainische Gruppe namens *CyberHunta* den Hack der E-Mail-Box des Büros des wichtigen russischen Präsidentenberaters *Vladislav Surkov*. Zumindest Teile des Materials konnten als echt verifiziert werden, d.h. als nicht fabriziert. Allerdings bezweifelten US-Medien, dass eine solche Top-Level-Operation von einer ukrainischen Gruppe ohne eine entsprechende Hacking-Vorgeschichte durchgeführt werden könnte, sondern dass dies stattdessen eine Warnung der US-Nachrichtendienste war[621].

Der *US Intelligence Community Report on Cyber incident Attribution* von 2017, der im Einklang mit der vorherigen Bewertung der Operationen von *APT28/Fancy Bears* und *APT29/Cozy Bears* als Operation *Grizzly Steppe* stand, betonte stark die politische Motivation von Russland als Argument für die Zuordnung der Angriffe zu Russland[622].
Dies wurde in den Medien als begrenzte Beweislage kritisiert, aber die Vorfälle mit *Michailow* und *Surkov* deuten darauf hin, dass sich möglicherweise mehr hinter den Kulissen abspielte als nur eine digitale Zuordnung und Analyse politischer Motivationen.

[621] vgl. Shuster 2016
[622] vgl. ODNI 2017, JAR 2016 des *Department of Homeland Security DHS* und des *Federal Bureau of Investigation FBI*.

7. Cybersicherheit der Digitaltechnologie

7.1 Einführung

Die Zahl der intelligenten Geräte wächst rasant, aber die langfristige Entwicklung geht schon über das **Internet der Dinge** hinaus (IoT), es geht auf das **Internet von allem (IoX)**, das jeden und alles überall verbinden wird.
Im Jahr 2020 werden mindestens 50 Milliarden IPv6-Adressen reserviert sein und der Trend geht zu 8 bis 20 IP-Adressen für jeden einzelnen Menschen vor[623].

Die Anzahl der digitalen Geräte und Schwachstellen wächst. Die Sicherheitsfirma *Palo Alto* hat die Malware *Amnesia* (eine Variante der Malware *Tsunami*) entdeckt, die digitale Videorekorder infizieren und IoT-Botnets bauen kann. Um eine Analyse zu verhindern, kann sie virtuelle Maschinen (Sandboxen) erkennen und löschen.[624]

7.2 Drohnen

Drohnen bzw. unbemannte Luftfahrzeuge (**Unmanned Aerial Vehicles** UAVs) sind mittlerweile fortgeschrittene Waffen mit wachsender Systemautonomie. Auf der anderen Seite hat die Verteidigung gegen Drohnen auch deutliche Fortschritte gemacht.

Die vier wichtigsten Wege, um Drohnen anzugreifen, sind:

- **Drone hacking**: Mit der **Battle Management Language** werden Befehle auf vordefinierten Frequenzen gesendet. Die begrenzten Kosten und Anstrengungen, die für solche Angriffe erforderlich sind, sind ein wichtiges Sicherheitsrisiko für Militärs[625].
- **GPS-Spoofing** von Drohnen: Das Senden falscher Koordinaten an die Drohnen kann sie irreführen oder sogar zwingen, eine Notlandung zu machen
- **Jamming:** Überschwemmungen mit elektromagnetischen Signalen können eine Notlandung hervorrufen, die die Zerstörung oder sogar eine Sicherstellung der angegriffenen Drohnen ermöglicht.
- **Physische Angriffe:** Das Abschießen von Drohnen, aber auch die Erfassung von Drohnen, auch durch speziell ausgebildeten Tiere, bilden einen wachsenden Markt für Sicherheitsfirmen. Auch di Abwehr mit Lasern befindet sich in der Entwicklung.

Ein spezielles Cyberwar-Problem stellt der Fortschritt der Drohnen-Technologie dar. Drohnen können der Beobachtung, aber auch der gezielten Tötung von Gegnern dienen[626]. Der technische Fortschritt ermöglicht immer umfangreichere

[623] vgl. Chiesa 2017
[624] vgl. Kling 2017b
[625] vgl. Welchering 2017
[626] vgl. Thiel 2012, S. Z2

Assistenzfunktionen, d.h. die menschliche Entscheidung immer weitgehender von Computern unterstützt und beeinflusst[627]. In diesem Zusammenhang kam bereits die Frage einer **Haftbarkeit von Maschinen** auf[628]. 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 [629].
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[630].
Das Funktionieren autonomer Maschinen ist von der zugrunde liegenden Programmierung abhängig, was jedoch zu ethischen und praktischen Dilemmata führen kann[631]. Falls das programmierte Verhalten bekannt ist, könnten Drohnen (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[632]. 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[633].

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

[627] 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.
[628] 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
[629] 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).
[630] vgl. TAZ online 2013
[631] vgl. Hevelke/Nida-Rümelin 2015, S.82
[632] vgl. Gutscher 2013, S.4, Spiegel 2013a, S.11
[633] vgl. Whitlock 2014

(ADS-B). Auch hat man festgestellt, dass Drohnen unbeabsichtigt durch Signale, die an andere Drohnen gerichtet sind, abgelenkt werden können.[634]

Das Luftfahrtunternehmen *Airbus* entwickelt ein System zur Drohnenabwehr mit Radar und Infrarotkameras mit einem Erfassungsradius von 10 Kilometern[635]. 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[636]. 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 Abgrenzung von Vögeln), Signalerkennung und Infrarotkameras erkennen. Fortgeschrittene AUDS-Systeme kombinieren diese Methoden[637]. 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.

Der Verkauf eines bestimmten Drohnenmodells an mehr als einen Staat führt zu einer Verbreitung des Wissens um Fähigkeiten und Schwachstellen[638]. 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[639]. Dasselbe Prinzip wird für die indischen und australischen U-Boote der französischen Firma

[634] vgl. Humphreys/Wesson 2014, S.82
[635] vgl. Lindner 2016, S.24, Heller 2016, S.68
[636] vgl. Marsiske 2016
[637] vgl. Brumbacher 2016, S.5
[638] 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
[639] vgl. Löwenstein 2013, S.5, Hickmann 2013, S.6

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*[640].
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[641].

Die mittlerweile suspendierte[642] *EuroHawk*-Drohne kombinierte die Drohnentechnologie der *Global Hawk*-Drohne von Northrop Grumann mit dem neuartigen hochentwickelten Aufklärungssystem *ISIS (Integrated Signal Intelligence System)* 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.
Deutschland diskutierte 2018 die Anschaffung der *Triton Drohne* von der Navy und der NASA, die in einer Höhe von 18 Kilometern über 30 Stunden und 15000 Kilometern Flugstrecke operieren kann und die über ein Sense- und Avoid-Kollisionsdetektionssystem und das *ISIS-System (Integrated Signal Intelligence System)* verfügt, mit dem Signalaufklärung aus der Luft betrieben werden kann. Seit 2010 kann Deutschland das nicht mehr, da drei Flugzeuge des Typs *Breguet Atlantic* außer Dienst gestellt wurden, obwohl diese SigInt-Fähigkeiten aufwiesen.[643].

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[644] 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[645]:

---

[640] vgl. Hein/Schubert 2016, S.22
[641] vgl. FAZ 2016a, S.29
[642] 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.
[643] vgl. Seliger 2018
[644] 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.
[645] vgl. Oparus 2010, SEC 2011, S.7, Talos Cooperation 2012.

- 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 unten.

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[646]) und in einigen Abschnitten der US-Grenze entwickelt[647].

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[648].

7.3 Sicherheit von Smartphones

Das Abhören von Regierungshandys[649] 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**)[650], der Energieversorgung über intelligente Stromnetze (**smart grid**) und zukünftig auch für die Autosteuerung im Rahmen von **e-mobility**-Projekten[651]. Das Smartphone

[646] vgl. Hildebrand 2010, S.6
[647] vgl. Miller 2013, S.12-13
[648] vgl. Wysling 2014, S.5
[649] vgl. Graw 2013, S.4-5. Derartige Vorkommnisse wurden u.a. für Indonesien, Deutschland und Brasilien berichtet.
[650] vgl. RWE 2013
[651] vgl. Heinemann 2013, S.3

wird zunehmend als erster Internetzugang insbesondere in Afrika genutzt, wo deshalb die Internetnutzung rapide zunimmt.[652]
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. Ein anderer Ansatz ist **Company owned personally enabled (COPE),** bei dem Mitarbeiter ihre privaten Anwendungen auf Betriebsgeräten laufen lassen können. Die BYOD- und COPE-Philosophien produzieren eine Art **Schatten-IT** in Unternehmen, die sehr schwierig zu kontrollieren und zu sichern ist[653].

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) [654] sind das einfache Abfangen von Funkwellen durch Antennen (der GSM Standard ist nicht sicher[655]), Vortäuschen von Funkmasten durch **IMSI-Catchers**, Zugang zu Knotenrechnern oder deren Kabel[656], Einbringen von Trojanern oder Viren durch infizierte Apps, unzulässiger Datenfluss durch versteckte App-Funktionen[657], oder durch Zusendung unsichtbarer und stummer SMS (**stealth SMS**), um Spionagesoftware wie *Flexispy* [658] 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[659]. Die später entdeckte Variante Stagefright 2.0 nutzte MP3-Musikdateien anstelle von MMS.
Krypto-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[660].

Forscher der Deutschen Telekom haben gezeigt, dass das Eindringen in ein Smartphone einschließlich des Diebstahls aller Daten, Änderung der Einstellungen

[652] vgl. Langer 2014a, S.7
[653] vgl. Müller 2014, S.16
[654] vgl. Ruggiero/Foote 2011
[655] vgl. FAZ 2013c, S.14
[656] vgl. Wysling 2013, S.5
[657] vgl. Focus online 2013
[658] vgl. Welt 2013, S.3, Opfer 2010
[659] vgl. Steler 2015
[660] vgl. Drissner 2008, S.4, Opfer 2010

und der Installation eines Tools zum Fernzugriff in der Praxis nur rund 5 Minuten braucht[661]. Inzwischen wird deutschen Ministern die Nutzung von **Einweg-Handys** empfohlen, die einmalig während einer Reise gebraucht werden und dann zerstört werden.[662]

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.[663] 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[664].

Im Rahmen einer Untersuchung von Smartphones durch die französische Sicherheitsfirma *Eurecom* wurden 2000 Applications (Apps) für Android-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.[665]
Ein weiteres 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[666]. Im August 2017 konnten 500 infizierte Apps aus dem Google Playstore entfernt werden, die zusammen mehr als 100 Millionen downloads hatten[667].

[661] vgl. Dohmen 2015, S.75
[662] vgl. Der Spiegel 2015, S.18
[663] vgl. Der Spiegel online 2014, S.1, vgl. Zeit online 2014a
[664] vgl. 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.
[665] vgl. Spehr 2015, S. T4
[666] vgl. T-online 2015
[667] vgl. Janssen 2017, S.22

Apps können auch manchmal sensible Daten leaken, so der bei Soldaten beliebte Fitnesstracker *Strava*, der ungewollt Militärbasen offenlegte[668].

QR codes (Quick Response Codes), d.h. matrix-förmige oder zweidimensionale Barcodes können die Smartphones beim Scannen zu bösartigen Webseiten umleiten[669]. 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[670].

Anfang 2016 versuchte das FBI, ein iPhone eines Verdächtigen zu entschlüsseln, was dann mit Hilfe der israelischen Firma *Cellebrite* gelang[671].
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[672]. 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[673].
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[674].

Im Jahr 2017 wurde die Cyber-Sicherheitsfirma *Cellebrite* gehackt und Daten veröffentlicht. Diese zeigten, dass 40.000 lizenzierte Kunden (Nachrichtendienste, Grenzpolizei, Polizei, Militäreinheiten, Finanzorganisationen) z.B. das *Universal Forensic Extraction Device UFED* nutzten, die den Zugriff auf Smartphones durch die Nutzung von Sicherheitslücken (Exploits) ermöglicht. Weitere Exploit-Sammlungen für *iOS, Android* und *Blackberry* wurden veröffentlicht[675].

Masseninfektionen von Smartphones sind ein neuer Trend. Ein Motiv dafür ist das Erstellen von Smartphone-Botnets, die z.B. das Smartphone veranlassen, auf bestimmte Anzeigen zu klicken oder Websites im Hintergrund zu nutzen. Die Malware *Gooligan* wurde mehr als 1 Million Mal von App-Stores heruntergeladen und ermöglicht die Kontrolle über das Smartphone[676]. Weitere Masseninfektionen

[668] vgl. Holland 2018
[669] vgl. Beuth 2016a, S.1-3
[670] vgl. Lemos 2015
[671] vgl. FAZ online 2016
[672] vgl. Die Welt online 2016
[673] vgl. Die Welt online 2016, FAZ online 2016
[674] vgl. Jansen/Lindner 2016, S.28
[675] vgl. Kurz 2017, S.13
[676] vgl. NZZ 2016

von Smartphones wurden in den vorhergehenden Monaten berichtet, z.B. mit den Malwaretypen *DVMAP* und *VoVA*.

2018 bot die Sicherheitsfirma *Grayshift* großflächige iPhone-Cracking-Pakete an: 15.000 US-Dollar für 300 iPhones oder 30.000 Dollar für eine offline cracking-Blackbox mit unbegrenzter Nutzung[677].

7.4 Smart Industry (Industrie 4.0)

7.4.1 Überblick

Unter **Smart Industry (Industrie 4.0)** versteht man die digitalisierte (also vernetzte, computerisierte, intelligente) Industrie unter anderem mit Fernwartungs- und –Steuerungssystemen (*Industrial Control Systems ICS/Supervisory Control and Data Acquisition SCADA*) in der Produktion. Die Smart Industry ist ein Teilgebiet der smarten Technologien (smart home, smart cities, smart grid/smart meter, smart cars usw.) und somit des **Internets der Dinge** (**Internet of Things IoT**), also aller mit dem Internet verbundenen Geräte.
Verbunden wird dies in Zukunft durch die neue **5G-Technologie**, deren energiesparendes Arbeiten, deren Leistungskraft mit ca. 1 Million Geräten pro km2 und deren minimale Latenzzeit bei der Signalübertragung überhaupt erst das volle Potential smarter Anwednungen entfalten wird.
In Deutschland wurde als sichere Einbahnstraßentechnik das **5G-Campusnetzwerk** entwickelt, bei der der Anwender im sicheren Teil Daten an die Außenwelt schicken könnte, aber umgekehrt kein Zugang möglich ist. Zuvor wurde schon die **Datendiode** als Einbahnstrassentechnik entwickelt (Daten können nur rein, aber nicht raus).

Für die Cybersicherheit ist das aber nicht einfach, weil sich Nutzer und Firmen einem exponentiellen Wachstum von Geräten, Schnittstellen, Updates und Varianten gegenübersehen, das man kaum noch überblicken geschweige denn kontrollieren kann. Ein weiteres Problem sind die offenen Systeme: Um Aufgaben wie Monitoring, Wartung und Updates durchführen zu können, müssen die Systeme von außen zugänglich sein. Zudem wollen die Firmen für die Produktentwicklung auch das Nutzerverhalten studieren können und schließlich verlangen zuweilen auch Geheimdienste Hintertüren im System. Vernetzung bedeutet letztlich immer, dass einem ein System in der Regel nicht alleine gehört, weil es Dritte gibt, die es warten, schützen, updaten und administrieren müssen, so dass die eigene Sicherheit auch immer von dritten Personen abhängig ist.

[677] vgl. Betschon 2018a, S.7

Am gefährlichsten ist aber die **unnötige Vernetzung**. Die Suchmaschine *Shodan* sucht vernetzte smarte Geräte aller Art und Sicherheitsforscher fanden schon bei ersten Tests frei zugängliche Steueranlagen in Firmen, Bahnhöfen und Flughäfen, die man direkt anklicken und verändern konnte, sahen aber auch Babys in ihren Bettchen, die von ungeschützten Webcams überwacht werden. Wenigstens kann man Shodan benutzen, um die eigene Organisation auf ungeschützte Geräte abzuklopfen. Ein anderes Problem ist der **geringe Passwortschutz** durch werkseitig voreingestellte oder gar hartkodierte (unveränderliche) Passwörter, die geradewegs zum Missbrauch des Gerätes einladen.

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[678].

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[679]. SCADA-Systeme haben oft keine automatischen Sicherheitsupdates bzw. Virusscans und Firewalls können oft nicht implementiert werden, ohne die Haftung des Maschinenherstellers entfallen zu lassen[680].

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[681].
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[682].

---

[678] 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
[679] vgl. Betschon 2013a, S.38
[680] vgl. Striebeck 2014
[681] vgl. Reder/van Baal 2014, S. V2
[682] vgl. Krohn 2014, S.24

Das US *Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)* empfiehlt[683] 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.

7.4.2 Cyber-Attacken in der Smart Industry

7.4.2.1 Grundlagen

- Infiltration > lateral movement > Eskalation > Manipulation
- Entwicklung des Angriffs dauert Jahre (inkl. Tests) und erfordert die Zusammenarbeit von Informatikern und Ingenieuren
- Hacken allein reicht nicht, man muss auch das System genau kennen (sonst Entdeckung, versehentliche Sabotage)
- In der Regel wird nur spioniert, nicht sabotiert
  (im Cybercrime jedoch Ransomware und Botnetze)
- Das Primärziel ist die (Industrie)Spionage, der Cyberwar eine Option

Einige wichtige Grundregeln von Angriffen auf die smarte Industrie sind: Man muss nicht direkt die Produktion angreifen. Man kann sich auch -wie in einem wahren Vorfall geschehen- im lateral movement (Seitwärtsbewegung) vom infizierten Bürocomputer in die Steuerung des Hochofens vorarbeiten.
Die Entwicklung eines großen Angriffs dauert Jahre (inkl. Tests) und erfordert die Zusammenarbeit von Informatikern und Ingenieuren. Der Hacker weiß zwar, wie man in einen Computer reinkommt, aber was er vor sich hat, wissen letztlich nur die Ingenieure. Drückt ein Hacker nur aus Versehen den falschen Knopf, kann der Schaden immens sein und er sich nebenbei auch noch enttarnt haben.
In der Regel wird nur spioniert, nicht angegriffen. Das erklärt die exzessive Spionage, aber die nur wenigen Angriffe. Der Gegner könnte einem sonst auch mal den Strom abdrehen oder ein Kernkraftwerk lahmlegen, deshalb wird in der Praxis Zurückhaltung geübt.
Die typischen Industrie-Angreifer sind Cyberkriminelle, die Geld mit Hilfe von Blockaden erpressen wollen, sei es durch Ransomware (Sperrbildschirme) oder durch Botnetze (Überflutung der Systeme mit Anfragen).
Das Primärziel ist also die (Industrie)Spionage, der Cyberwar aber immer eine Option. Die Infiltration einer Steuerung liefert nicht nur wertvolle Informationen über die Steuerung selbst, sonst gibt auch Einblicke in den Produktionsprozess, einschließlich möglicher Probleme, aus denen man dann schon vorab lernen kann.

[683] vgl. ICS-CERT 2016a

7.4.2.2 Wichtige Cyber-Attacken

Die folgende Liste zeigt die wichtigsten Attacken in der Smart Industry, die Einzelheiten und Hintergründe werden im Abschnitt 5.2 beschrieben.

- *Stuxnet (2005-2010)*: Erst Lüftungsklappen, dann Frequenzen von Uranzentrifugen durch gezielte Attacke auf *Simatic S7-SPS* und die *Prozessvisualisierung WinCC*
- Immer noch ungeklärt: Shamon-Attacke auf *Aramco* (2012), Wiper-Attacke auf den Iran 2012
- *Cloud Hopper* (2006-2016): Angriff auf *Managed Service Providers MSP*s (Clouds, IT Services, Help Desks etc.), daneben auf Technologiefirmen und die US Navy
- *Lazarus-Gruppe* (2012-heute): Seit Jahren Angriffe mit Wipern als logische Bomben oder zur Spurenverwischung, Einsatz destruktiver Ransomware (*WannaCry*) 2017
- *Triton/Trisis/Temp.Veles* (2017): Malware *Triton/Trisis* gegen Schneider Electrics *Triconex Safety Instrumented System (SIS)* in Saudi-Arabien, Manipulation von Notabschaltungen
- *Dragonfly/Energetic Bear*: infiziert Anbieter von ICS-Programmen mit Malware *Havex* zur Überwachung und Manipulation von ICS/SCADA-Systemen (ca. 2000 Fälle)/*Wolf Creek*-Vorfall 2017 durch Spearphishing mit falschen Lebensläufen
- *Sandworm/Quedagh* (seit 2011): Modifizierte multifunktionale Malware *BlackEnergy3* gegen vernetzte Benutzerschnittstellen (**Human-Machine-Interfaces HMI**)
  - 2015 Stromausfälle in der Ukraine durch Trennen von Stromverbindungen mit Telephone Denial of Service (TDoS)-Angriffen zur Hotline-Blockade und Einsatz von Wipern (*Killdisk*)
  - 2016 *Industroyer*-Angriff Falsche IEC-104 Protokollbefehle an eine einzelne infiltrierte Übertragungs-Unterstation führten zu Stromausfall in Kiew
  - 2017 *Petya/Not-Petya/Moonraker-Petya* Nutzung von NSA-Exploits für destruktive Ransomware
  - 2018 *VPN-Filter* Neustartresistente IoT-Malware für Netzwerkgeräte zur Überwachung von SCADA-Protokollen mit Bricking

7.5 Internet of Things (IoT, Internet der Dinge)

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.[684]

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 Schnittstellen beiträgt[685].
Eine erhebliche neue Bedrohung sind Heimassistenten (**Home Assistant Systems** wie *Alexa, Siri, Google Assistant* etc.). Ein häufiges Problem ist die **unbeabsichtigte Befehlsausführung**, wenn die Systeme etwas hören, das nicht für sie bestimmt war, z.B. vom Fernsehen. Es können auch Datenschutzfragen auftreten.
Mittlerweile können Eindringlinge **unhörbare Befehle** (im Bereich über 20 kHz) von außerhalb des Gebäudes senden und dadurch die Kontrolle über den Heimassistenten übernehmen, und wenn es die Einstellungen erlauben, über die gesamte Smart-Home-Anordnung, z.B. das Öffnen von Türen. Die Detektion bestehender Smart-Home-Technologie ist technisch einfach[686].

Das Internet der Dinge (IoT)-Botnetz *Mirai* (benannt nach dem Anime *Mirai Nikki*) nutzte Webcams, Babyphones und andere Geräte, um einen DDOS-Angriff auf den US-Internet-Infrastrukturanbieter *Dyn* mit Datenflussraten von mehr als 1 Terabit pro Sekunde im Oktober 2016 auszuführen. Die IP-Adressen führten zum Hersteller *Xiong Mai*.
Einige Tage zuvor hat ein Hacker mit dem Decknamen *Anna Sempai* 62 Passwörter für den Zugriff auf die Geräte freigegeben. Mittlerweile wurden von dem Sicherheitsforscher *Krebs* starke Anhaltspunkte gefunden, dass *Anna Sempai* an den *Mirai*-Vorläufern beteiligt war, insbesondere *QBot*, während für den Dyn-Angriff eine andere Gruppe namens *New World Hacker* die Verantwortung übernahm[687].

[684] vgl. Market Wired 2014, S.1-2
[685] vgl. Weber 2016, S. T1
[686] vgl. Niewald 2018
[687] vgl. KrebsonSecurity 2017, Radio Free Europe 2016

Mirai wurde von Vorläufer-Botnets wie *QBot und Bashlite* abgeleitet. Diese Botnetze wurden ursprünglich verwendet, um *Minecraft* (ein beliebtes Online-Spiel)-Server anzugreifen, um sie aus dem attraktiven Minecraft Hosting Server-Markt zu drängen.
Später im Jahr 2016 wurde die deutsche Telekom massiv angegriffen. Hier wurde eine neue *Mirai*-Variante genutzt und die Analyse zeigte, dass wieder nur ausgewählte Geräte (sogenannte *Speedport*-Router) vom taiwanesischen Hersteller *Arcadyan* betroffen waren. Der Angriff schlug nur aufgrund eines Programmierproblems fehl[688].

Am 22.02.2017 wurde am Londoner Flughafen ein 29-jähriger Brite verhaftet, der verdächtigt wird, den Hack begangen zu haben. An der Aktion waren deutsche, britische und zypriotische Behörden beteiligt.
Der Angreifer war geständig. *Mirai* zielte auf den Fernwartungszugang den Port 7547. In Liberia wurde die Telekomfirma *Lonestar* attackiert, bei der deutschen Telekom deren *Speedport*-Router. Die Attacke auf die Telekomrouter schlug fehl, störte aber deren Funktion. Dennoch bekam er bis zu 600.000 Router in Deutschland, Großbritannien und Südamerika unter Kontrolle, um damit *Lonestar* zu attackieren. Die Telekom wurde attackiert, um mehr Router für spätere Angriffe zu haben[689].

Mirai-bezogene Attacken wurden jedoch fortgesetzt, wie die sogenannte **DNS Query Flood (Mirai DNS Water Torture Attack)** am 15 Jan 2017, bei der DNS-Server angegriffen wurden, also solche Computer, die die Zuordnung von IP-Adressen und Domains klären. An die Zieldomain werden von den angreifenden Computern zwölfstellige zufällige Subdomains angehängt und an lokale DNS-Server geschickt. Diese können die Anfrage naturgemäß nicht klären und leiten sie dann an den autoritativen DNS-Server, das eigentliche Ziel des Angriffs, weiter und der so mit Anfragen überflutet wird[690].

Eine neuartige IoT-Attacke ist das **Bricking**. Dabei geht es um Angriffe auf smarte Geräte, man gibt Anweisungen, um Einstellungen zu ändern und oder überschreibt die Firmware, was zu einer faktischen Zerstörung des Gerätes führt.
Die Malware *BrickerBot.1* und *BrickerBot.2* nutzte hartkodierte Passwörter von Kameras und Geräten der Firma *Dahua*, so dass die Angreifer leichten Zugang zu den Geräten hatten[691].

[688] vgl. Alvarez/Jansen 2016
[689] vgl. Jung/Jansen 2017, S.24
[690] vgl. Akamai 2017, S.8
[691] vgl. Böck 2017

7.6 Smart Grid

Das intelligente Netz (Smart Grid) ist die digitale Version des konventionellen Stromnetzes, das zur Stromerzeugung an Kraftwerken benötigt wird, um diese Energie an die örtlichen Stationen zu übertragen, wo die Spannung abgesenkt und der Strom an die Verteilungsnetze verteilt wird, um Kunden zu versorgen. Dominante intelligente Netznetzprotokolle sind *IEC 104*, ein TCP-basiertes Protokoll; dieses und sein serieller Protokollbegleiter IEC 101 werden in Europa und Asien verwendet, während das *Distributed Network Protocol 3 (DNP3)* typischerweise in US verwendet wird.
Ein spezifisches Risiko des Smart Grids sind **Dominoeffekte**, da die Spannung des übertragenen Stroms in einem sehr engen Bereich stabil gehalten werden muss. Jede Volatilität, z.B. verursacht durch einen Cyber-Angriff kann große Regionen bis hin zur gesamten Europäischen Union destabilisieren, die die intelligente Netzverteidigung zu einer Priorität der Cyber-Sicherheits-Bemühungen macht.

7.7 Kernkraftwerke

Schon beim großen Stromausfall von 2003 war der Verdacht aufgekommen, dass dieser durch ein Computervirus verursacht worden sein könnte[692].
Schon im August 2003 konnte der Internetwurm *Slammer* für einige Stunden in das zum Glück abgeschaltete Atomkraftwerk in David-Besse in Ohio eindringen[693]. Seit 2006 mussten zweimal Atomkraftwerke nach Cyberangriffen abgeschaltet werden[694]. Im April 2009 gelang es Hackern, in die Stromnetzkontrolle der USA vorzudringen[695] um dort Programme zu hinterlassen, mit denen das System bei Bedarf unterbrochen werden könnte, wobei China, das umgehend dementierte, und Russland verdächtigt wurden.

Im Oktober 2016 sagte der Direktor der *Internationalen Atomenergie-Organisation (IAEA)* Amano, dass vor zwei bis drei Jahren ein Atomkraftwerk von einem störenden Angriff getroffen wurde, eine Abschaltung wurde aber nicht nötig. Nach dem Cyber-Angriff in Südkorea 2014 (siehe Abschnitt 5 Lazarus-Gruppe) und einem Computervirus im deutschen Kernkraftwerk Grundremmingen im April 2014 (im Büro, nicht im Nuklearbereich). Ende Juni 2017 war das ukrainische Atomkraftwerk Tschernobyl von den *Petya-Attacken* betroffen[696].

Im Mai und Juni 2017 war der US-Energiesektor Ziel von Cyberangriffen. DHS und FBI untersuchen dies; unter den Zielen war das Kernkraftwerk *Wolf Creek* bei Burlington in Kansas, aber seine Operationen waren nicht betroffen. Die Angriffe

[692] vgl. Gaycken 2009 mit Abbildung des großen Stromausfalls in Northeast USA 2003
[693] vgl. Wilson 2008, S.22
[694] vgl. ArcSight 2009
[695] vgl. Goetz/Rosenbach 2009, Fischermann 2010, S.26
[696] vgl. Shalal 2016

waren die gleichen wie die Taktik der APT *Dragonfly (Energetic Bear/Crouching Yeti/Koala)*. Zum Angriff wurden **gefälschte Lebensläufe** für Kontrollingenieur-Jobs, watering hole-Attacken und Man-in-the-Middle-Attacken angewendet[697].

Das französische Bauunternehmen *Ingerop* war 2018 von einem Phishing-Angriff unbekannter Akteure betroffen, die 11.000 Dateien, u.a. mit Bezug auf Atommüllanlagen, Gefängnisse und andere kritische Infrastrukturen gestohlen hatten[698]. Eine Spur führte die Ermittler zu einem Server in Dortmund und es könnte sein, dass ‚Hacktivisten' beteiligt waren.

Im Juni 2019 wurde bekannt, dass die USA seit mindestens 2012 Aufklärungsprogramme in Steuerungssystemen des russischen Stromnetzes einsetzen. Zusätzlich zur *Wolf Creek*-Attacke waren nämlich Versuche unternommen worden, die *Cooper Nuclear Station* des *Nebraska Public Power Districts* zu infiltrieren, wo die Angreifer die Kommunikationsnetze erreichten, jedoch nicht das Reaktorsystem[699].

7.8 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[700]. Das wichtigste Angriffsziel ist das **controlled area network (CAN)**, ein serielles Bussystem zur Vernetzung von Steuergeräten[701].
2016 werden 80 Prozent aller neu zugelassenen Autos in Deutschland einen Internetanschluss haben[702]. 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[703].
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[704].

---

[697] vgl. Perloth 2017b
[698] vgl. Eckstein/Strozyk 2018
[699] vgl. Sanger/Perloth 2019
[700] vgl. Hawranek/Rosenbach 2015, S.65
[701] vgl. Fuest 2015, S.34-35
[702] vgl. Schneider 2014
[703] vgl. Fromme 2015, S.17
[704] vgl. Karabasz 2014, S.14-15

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[705]. 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[706]. Jedoch gelang Mitte 2015 der erste Autohack aus der Distanz, wobei ein *Cherokee Jeep*-Modell aus 15 Kilometern Entfernung angegriffen werden konnte[707].

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 Motor zu starten[708], aber solche Signale können von Angreifern mit Hilfe eines **Repeater**-Gerätes leicht abgefangen und reproduziert werden[709].

Das Automodell Tesla S wurde Ende 2015 mit Autopiloten-Funktionen für partiell autonomes Fahren ausgestattet, darüber hinaus können ab jetzt kabellose Updates via WLAN als **firmware over the air (FOTA)** erfolgen, was die Anfälligkeit für Hackerangriffe erhöht[710], aber auch rasche Sicherheitsupdates ermöglicht[711]. 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[712]. Mittlerweile zeigte eine Untersuchung, dass der Fahrer Warnungen des Autopiloten ignorierte[713].

In Zukunft werden Autos zusätzliche Features haben[714]. Eine Studie des Automobilverbandes FIA zeigte, dass die BMW Modelle 320 und i3 das Fahrverhalten, die Handykontakte, die Navigatorziele, die Nutzung von Sitzen, Standort- und Parkpositionen erfasst haben. Mercedes kommentierte, dass ihre Autos den Fahrstil, den Fahrerkalender und seine Musikpräferenzen kennen

[705] vgl. Lewicki 2014, S.62
[706] Mittlerweile engagieren Autohersteller Hacker, um die Sicherheit der Fahrzeuge zu prüfen, z.B. von der britischen Telekommunikationsfirma BT, vgl. FAZ 2015b, S.18
[707] 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.
[708] vgl. Rees 2016, S.2
[709] vgl. Heute 2016
[710] 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
[711] vgl. Becker 2016, S.78
[712] vgl. Fromm/Hulverschmidt 2016, S.25
[713] vgl. SZ online 2017
[714] vgl. Spehr 2017, S. T1

würden. Im öffentlichen Verkehr können E-Tickets jedoch auch ein Bewegungsprofil des Nutzers erstellen.

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[715]. 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.[716]

Die *Deutsche Flugsicherung DFS* baut ein Kontrollzentrum in Leipzig auf, von dem aus der Flughafen Saarbrücken ab 2019 als **Remote Tower Control (RTC)** ferngesteuert wird; ein Trend, der sich nach langer Pretestphase in Europa zu etablieren beginnt.[717]

7.9 Künstliche Intelligenz (KI)

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 des *Future of Life Institute* vom 27.07.2015 den Bann für autonome Waffen dieses Typs.

Allerdings wird die Entwicklung der KI eine Herausforderung sein:
Die aktuelle so genannte ‚künstliche Intelligenz' sind nur programmierte Maschinen, die schnelle Berechnungen durchführen können, die es ihnen ermöglichen, Handlungen zu interpretieren, nachzuahmen oder vorherzusagen, indem sie Datenbanken und statistische Modelle verwenden. Diese Einstellung macht sie jedoch anfällig für Manipulation und Angriffe.

Echte künstliche Intelligenz, d.h. ein System mit Bewusstsein, die Fähigkeit, nach dem Sinn von etwas zu fragen und mit einem eigenständigen Selbstverständnis (*cogito ergo sum*) wird - basierend auf überlegenem Wissen und Intelligenz - wahrscheinlich nicht eher der menschlichen Logik und Ethik folgen. Im DARPA-

[715] vgl. Rosenbach/Traufetter 2015, S.72f.
[716] vgl. GAO 2015, S.1
[717] vgl. FAZ 2018d

Wettbewerb 2016 hat die Maschine gewonnen, die sich selbst gerettet hat, anstatt die Verteidigungssysteme dauerhaft aktiv zu halten.

7.10 Cloud Computing

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.

Die Auslagerung von Daten und Anwendungen an Anbieter mit großen Zentralrechnern hat verschiedene Vorteile:

- Zum einen können die Programme und Computer der jeweiligen User stets auf dem neuesten und sichersten Stand gehalten werden, Updates werden sofort im ganzen System umgesetzt.
- Die Einrichtung neuer Computer und Standorte gestaltet sich unproblematisch, Organisationen werden so erheblich flexibler.
- Es muss deutlich weniger eigene IT-Infrastruktur vorgehalten werden.

Es gibt aber auch einige Sicherheitsaspekte zu beachten:

- Der Cloud-Anbieter hat die physische Kontrolle der Daten, so dass hohe Anforderungen an Vertrauenswürdigkeit und technische Zuverlässigkeit gestellt werden.
- Der Cloud-Provider muss in der Lage sein, die Daten gegen Angriffe zu verteidigen.
- Zudem können je nach Ort und Rechtslage auch Dritte legalen Zugriff auf die Daten erlangen.

Im Jahr 2019 gab es weltweit ca. insgesamt 3000-4000 Anbieter (**Cloud Service Provider**), die führenden Provider, die sogenannten **Hyperscaler**, sind sämtlich US-Firmen: *Amazon Webservices AWS, Microsoft Azure, Google Cloud Platform, IBM SoftLayer, Oracle Cloud, Salesforce* und *VMware*[718].

Der *US Cloud Act* ermöglicht seit 2018 unter bestimmten Umständen den Zugriff auf Daten aus Übersee, z. B. wenn dies zur Aufklärung von Verbrechen in den USA erforderlich ist.

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[719]. Der Cloud computing-Anbieter selbst stellt eine für die auslagernde Firma schwer

[718] vgl. Müller 2019, S.14
[719] vgl. FAZ 2010f, S.17

kontrollierbare zusätzliche Eintrittspforte für Angriffe dar[720]. Außerdem können Cloud-Anbieter ggf. die Daten einsehen, um sie zu scannen und zu analysieren, ggf. können sie unter bestimmten Umständen den Zugang sperren[721].

Eine verbreitete Lösung sind **Multicloud-Lösungen**, durch die die Firmen ihre Abhängigkeit verringern. Weitere Methoden zur Erhöhung der Firmensicherheit betreffen die Wahl der Serverstandorte, Datenaufteilung und Verschlüsselung.

Neben der oben genannten APT10 *Cloud Hopper*, der ein Eindringen in eine Cloud den Zugriff auf die Cloudnutzer eröffnet, fand sich im Rahmen der Fuzzing-Forschung die *SpectreNG*-Lücke in Chips, durch die es möglich ist, von dem Segment eines einzelnen Cloud-Nutzers, der sogenannten **virtuellen Maschine**, in die Cloud selbst vorzudringen.

Neben den verschiedenen Sicherheitsaspekten[722] gibt es auch Unsicherheiten über Rechte und Verantwortlichkeiten bei grenzüberschreitenden Problemstellungen[723], 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[724].

Cloud-Services werden auch von den Nachrichtendiensten genutzt. *Amazon Web Services (AWS)* hatte aufgrund eines Vertrages mit der CIA im Wert von 600 Millionen Dollar 2014 eine **Top-Secret Region** eingerichtet, in der entsprechend klassifiziertes Material gespeichert wird. Ende 2017 richtete AWS nun auch eine **Secret Region** ein, bei der Software und Daten mit der jeweiligen Geheimhaltungsstufe cloudbasiert zur Verfügung stehen. Die Cloudservices *AWS* und *Microsoft Azure* wurden von der US-Regierung als geeignet zertifiziert.[725]

[720] vgl. Menn 2010, S.H12-H13
[721] vgl. Postinett 2013b, S.12
[722] vgl. ENISA 2009b
[723] vgl. EU2011
[724] vgl. EU 2012a, S.5
[725] vgl. Beiersmann 2017f, S.1

8 Die führenden Akteure im Cyberspace

8.1 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.

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[726].
Es geht hier aber nicht um eine Neuauflage eines Ostwestkonfliktes. So fühlen sich beispielsweise die Inder von der Entwicklung insgesamt sehr bedroht[727].

8.2 Die Vereinigten Staaten von Amerika

8.2.1 Überblick

Nachrichtendienste:
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, mit seinem als ODNI bezeichneten Büro, davon sind die 8 militärischen Dienste in der Dachorganisation *Defense Intelligence Agency DIA*[728] zusammengefasst.

Innerhalb der *Intelligence Community* stehen im Cyberbereich vor allem 4 Dienste im Vordergrund:

- Die *National Security Agency NSA* als SigInt Agency, die mit dem *US Cyber Command Cybercom* unter gemeinsamer Leitung steht. Die meist

[726] vgl. Wilson 2008, S.12
[727] 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
[728] 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

zitierte NSA-Einheit ist die *Tailored Access Operations (TAO) group,* eine Elite-Hackereinheit, die sich um den Zugang zu gegnerischen Systemen kümmert. Medienberichte vermuten eine Verbindung zur sog. *Equation Group*, was offiziell aber bisher nicht bestätigt wurde, siehe Abschnitt 5.

Nicht militärische Dienste sind

- die *Central Intelligence Agency (CIA)*,
- das *Department of Homeland Security DHS* (Heimatschutzministerium) und das
- *Federal Bureau of Investigation FBI,* die Bundespolizei.

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[729]. Medienberichte vermuten eine Verbindung zur sog. *Longhorn Group*, was offiziell aber bisher nicht bestätigt wurde, siehe Abschnitt 5.

Militärischer Bereich:

Die militärische Cybereinheit ist das *US Cyber Command Cybercom*., das dem strategischen Kommando US STRATCOM unterstellt ist, das übergeordnet für die Planung und Ausführung von Operationen im Cyberspace zuständig ist[730].

Cybercom ist jetzt die Dachorganisation der vorher gegründeten Cybereinheiten der Navy, Army und Air force, die zwischen 1996 and 1998 errichtet wurden. Das US *Cybercom* schützt 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[731]. Die US-CERTs arbeiten mit dem DHS zusammen.

Für militärische Forschungen auch im Cybersektor hat das US-Verteidigungsministerium *US Department of Defense DoD* die Agentur *Advanced Research Projects Agency DARPA.*

Technische Aspekte:

Man kann im militärischen Sektor drei Bereiche abgrenzen, nämlich:

- das mit dem normalen Internet verbundene Non-classified Internet Protocol Router Network NIPRNET
- das mit gewissen Sicherungen für kritische Infrastrukturen und militärnahe Einrichtungen arbeitende Secret Internet Protocol Router Network SIPRNET und

[729] vgl. Die Welt 2015 online, S.1, Tagesschau 07.03.2015
[730] vgl. USAF 2010a, S.21-22
[731] vgl. Porteuos 2010, S.7

- als militärisches Hochsicherheitsnetz das Joint Worldwide Intelligence Communication System JWICS[732].

Sicherheitspartner:
Die Plattform für die Zusammenarbeit zwischen Staat und Privatwirtschaft ist seit 2005 die *Intelligence and National Security Alliance (Insa)*, die früher als *Sasa (Security Affairs Support Association)* bekannt war [733].

Die NSA begann mit der Privatisierung von 1999-2005, die Vertragsfirmen ließen sich nur eine Meile vom Hauptquartier der NSA in einem Gewerbegebiet nieder. Die gesamte interne IT der NSA wurde an die Firma *CSC* ausgelagert[734].

Die US-Geheimdienste haben seit langem Kooperationen mit Firmen, die Dienstleistungen oder Unternehmer zur Unterstützung der staatlichen Organisationen anbieten. Im Jahr 2013 waren die 4 Hauptanbieter[735] *Booz Allen Hamilton BAH, CSC, SAIC/Leidos und L-3 Communications.*
Rüstungsunternehmen mit großen IT-Service-Einheiten sind z.B. *Lookheed Martin, Northrop Grumman, General Dynamics* und *Raytheon*[736].

Neuere Zahlen von 2016 zeigen, dass nur 5 Firmen (*Leidos, BAH; CSRA, SAIC* und *CACI International*) 80% der 45.000 externen US-Nachrichtendienstler beschäftigen, insgesamt haben die Dienste 183.000 Mitarbeiter[737]. Im militärischen Nachrichtendienst *Defense Intelligence Agency (DIA)* sind 35% der Mitarbeiter Externe, in der *National Reconaissance Organization (NRO)* sogar 95%[738].

Die CIA hat die Firma *In-Q-Tel* für die Unterstützung von Firmen im IT-Sektor, 2013 waren es 60 Firmen[739]. Ein bekanntes Beispiel ist das Joint Venture *Recorded Future*.

Wie in den vorherigen Kapiteln gezeigt, haben die US eine starke Cybersicherheitsfirmen-Szene.

---

[732] in Deutschland wäre die Herkules-Plattform ähnlich zum SIPRNET und die JASMIN Datenbank zu JWICS
[733] vgl. Wendt 2014
[734] vgl. Cyrus 2017
[735] vgl. SZ 2013, S.8-9
[736] vgl. SZ 2013, S.8-9. China glaubt, dass die USA und andere westliche Staaten Aufträge zur Entwicklung an Anwendung von Cyberwaffen an Firmen wie Lockheed Martin, Boeing, Northrop Grumman und Raytheon vergeben; vgl. Zhang 2012, S.805
[737] vgl. Cyrus 2017
[738] vgl. Cyrus 2017
[739] vgl. Buchter 2013

8.2.2 Capacity building (Kapazitätenauf- und ausbau)

Die USA haben ihre Cyberwarkapazitäten über zwei Jahrzehnte systematisch aufgebaut und koordiniert[740].

1988 errichtete das US-Verteidigungsministerium (*Department of Defense 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[741].

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[742], 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* unterstellt ist[743], und ist räumlich bei der NSA angesiedelt[744].

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[745]. 2018 übernahm Army General Paul Nakasone das Kommando.

Zur Verbesserung der Effizienz verknüpft die NSA 2016 die defensiv und offensiv ausgerichteten Abteilungen IAD/SID. Das *Information Assurance Directorate (IAD)* versucht, Sicherheitslücken zu finden und zu schließen, während das *Signal Intelligence Directorate (SID)* Sicherheitslücken für Cyberoperationen einsetzt[746].

Auf der militärischen Ebene umfasst der Aufbau 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

---

[740] vgl. Hiltbrand 1999
[741] vgl. Porteuos 2010, S.3
[742] 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
[743] vgl. Hegmann 2010, S.5, The Economist 2010, S.9/22-24, Glenny 2010, S.23
[744] vgl. DoD 2011, S.5
[745] vgl. Winkler 2014b, S.3
[746] vgl. Gierow 2016, S.1-2

elektronische Eindringlinge erkennt, Netzwerke verteidigt und Cyberattacken ausführt[747].
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[748]. 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[749].
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[750].

Ab 2012 begann US-Verteidigungsministerium mit der Einrichtung der *Cyber Mission Force (CMF),* die insgesamt 6200 Militärs, Zivilisten und Vertragsmitarbeiter umfassen sollen[751]. Diese sind dann in 133 Teams organisiert, 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.

8.2.3 Strategien und Konzepte

Das Primärziel aller Akteure ist die Erringung der **elektromagnetischen Dominanz** und insbesondere der **Überlegenheit im Cyberspace**[752], d.h. der Beherrschung des Cyberspace im Konfliktfall. Da die gegnerischen Systeme 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 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

[747] vgl. Barnes 2012
[748] vgl. Schanz 2010, S.50ff., Franz 2011, S.87. Für den gängigen Begriff **cyber warrior** (Cyberkrieger) wurde der förmlichere Begriff **cyber warfare operator** eingeführt.
[749] vgl. Black zitiert bei Schanz 2010, S.52
[750] vgl. Matthews 2013, S.8
[751] vgl. DOD 2015, S.6
[752] vgl. USAF 2010a, S.2

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.

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[753]. 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.[754]
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.[755] Die Arbeiten im defensiven Sektor gehen jedoch unvermindert weiter[756].
Im April 2015 publizierte das *US-Verteidigungsministerium (Department of Defence DoD)* die neue *DOD Cyber Strategy*. Das DoD hat fünf strategische Ziele 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[757]. Die *DOD Cyber Strategy von 2018* bestätigt die bisherige Linie[758].

Angesichts der wachsenden Probleme z.B. durch zunehmende Infiltration von kritischen Infrastrukturen, hat Präsident Obama am 12.02.2013 eine Executive

[753] vgl. White House 2011, insbesondere S.5 und 9
[754] vgl. DoD 2011, S.8-9
[755] 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
[756] 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.
[757] vgl. DoD 2015, S.8
[758] vgl. DoD 2018

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.[759].

Am 11. Mai 2017 unterzeichnete Präsident Trump eine *Executive Order*, um die Cyber-Sicherheit von föderalen Netzwerken und kritischen Infrastrukturen zu stärken, und die die Behörden dazu anhält, mit privaten Unternehmen zur Verteidigung und Risikominderung zusammenzuarbeiten[760].

8.2.4 Cyber-Übungen

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.
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.

Das *US Department of Homeland Security DHS* hat inzwischen einen eigenen Wettbewerb zur Rekrutierung talentierter junger Hacker durchgeführt, die *Virginia Governors Cup Cyber Challenge*[761].

Regelmäßige Übungen sind die *Cyber Storm Exercises,* die unter der Leitung des DHS stattfanden, bei denen ebenfalls Großangriffe auf die 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.[762] Die Codes sollten in der Übung in Kalifornien getestet werden, man nahm aber aus

[759] vgl. White House 2013
[760] vgl. Perloth 2017b
[761] 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.
[762] vgl. Welchering 2011, S. T2

Furcht vor ungeplanten Ausfällen davon Abstand[763]. Solche Werkzeuge zur Internet-Abschaltungen werden auch als "**kill switches**" bezeichnet [764].

8.3 Die Volksrepublik China

8.3.1 Überblick

Sowohl der Zivil- als auch der Militärsektor von China stehen unter der Kontrolle der Kommunistischen Partei Chinas. Chinas Volksbefreiungsarmee PLA wird verdächtigt, große Cybereinheiten an mindestens einem halben Dutzend Standorten zu unterhalten[765].
Der zuständige PLA-Bereich ist das *General Staff Department GSD*, das aus 4 Abteilungen besteht. Dies besteht aus der Abt. Operationen in der 1. Abteilung, Abt. Intelligence in der 2. Abteilung, Signals Intelligence und Netzwerk-Verteidigung in der 3. Abteilung und elektronische Gegenmaßnahmen und offensive Cyber-Operationen in der 4. Abteilung[766].

China hat die formale Informationskriegsstrategie "*Integrated Network Electronic Warfare*" (INEW) für computer network operations (CNO) für Computernetzwerkangriffe (CNA) und Electronic Warfare (EW) in der 4. Abteilung der GSD eingeführt, während die Computer Network Defense (CND) und die SigInt in der dritten Abteilung verbleibt.[767].
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[768]. Chinesische APTs wurden früher in Abschnitt 5 vorgestellt.

Ab 2017 verlangt ein neues Cyber-Sicherheitsgesetz für kritische Infrastruktur-Sektoren, dass Hard- und Software eine Sicherheitsüberprüfung durch den Staat durchlaufen, bevor sie von ausländischen Unternehmen geliefert werden. Dazu ist die Datenspeicherung ab jetzt nur auf chinesischen Servern erlaubt[769].

Unterdessen sind die USA der Ansicht, dass das Ministerium für Staatssicherheit 2015 die Koordination von Cyber-Operationen von der PLA übernommen hat. [770]

---

[763] 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.
[764] von Tiesenhausen 2011, S.11
[765] vgl. Finsterbusch 2013, S.15
[766] vgl. Mandiant 2013, Sharma 2011, S.64
[767] vgl. Sharma 2011, S.64
[768] vgl. Kremp 2011
[769] vgl. Müller 2016, S.3
[770] vgl. Langer 2018b

Im Jahr 2018 stand die APT10 im Verdacht, mit dem Ministerium für Staatssicherheit in Verbindung zu stehen.

8.3.2 Strategische Ziele

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[771]. Natürlich besteht das Risiko, dass der Gegner sein Netz wieder repariert, so dass diese Strategie auf lange Sicht erfolglos sein kann; umso 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.[772]
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[773]. Daraus ergibt sich jedoch, dass sich die zukünftige Forschung nicht mehr nur auf Defensivmaßnahmen konzentrieren kann[774]. Die NSA rüstete sich auch zum offensiveren Umgang mit China[775].

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 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

[771] vgl. Krekel et al. 2009
[772] vgl. Tinner et al. 2002
[773] 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."
[774] 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
[775] vgl. Barnford 2010

die frühzeitige und gezielte Ausschaltung der möglichen Gegenschlagskapazitäten des Gegners geht[776].

Außenpolitisch hat China das Problem, von Staaten umgeben zu sein, die China nicht unbedingt positiv gegenüberstehen bzw. mit den USA verbündet sind[777], 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.

8.4 Russland

8.4.1 Überblick

Die APTs stehen unter Kontrolle der Geheimdienste.
Russland hat vier Dienste als Nachfolger des ehemaligen sowjetischen Geheimdienstes KGB[778]:

- FSO – Föderaler Schutzdienst, auch für den Schutz des Präsidenten im Kreml
- FSB – Inlandsgeheimdienst, aber auch zum Teil im Ausland aktiv
- SWR - Auslandsgeheimdienst, auch für Intelligence Cooperation zuständig[779]
- GRU oder GU - militärischer Nachrichtendienst

Wie bereits erwähnt, werden diesen Diensten vom Westen (und von Russland dementiert) die APT28 und APT 29 sowie drei Einheiten mit Schwerpunkt auf der Industrie, die *Waterbug/Turla-Gruppe*, die *Sandworm/Quedagh-Gruppe* und *Energetic Bear/Dragonfly*[780] zugeordnet. Die Existenz weiterer APTs wird diskutiert.
Die prominenteste Sicherheitsfirma ist *Kaspersky Labs*, die eine gute Arbeitsbeziehung zum russischen Staat hat[781], aber energisch bestreitet, im Hintergrund backdoors für den russischen Staat oder ähnliche Maßnahmen zu installieren.

[776] vgl. Kanwal 2009, S.14
[777] vgl. Rogers 2009
[778] vgl. Ackert 2018a, p.7
[779] vgl. Ackert 2018a, p.7
[780] See e.g. Jennifer 2014
[781] vgl. Russia Today (RT Deutsch) online 27 Jan 2017

Es wird wenig über die **Cyber-Truppen** in der russischen Armee veröffentlicht, die seit 2014 von Medienberichten vermutet werden (und mittlerweile als GRU-Mitglieder gelten). 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[782]. Zudem wurde ein allrussischer Hackerwettbewerb ins Leben gerufen, um begabte junge Cyberspezialisten rekrutieren zu können[783].

Im Jahr 2015 hat die russische Armee **Science Squadrons** (Wissenschaftsschwadronen) gegründet[784]. Jedes Geschwader ist mit 60-70 Soldaten geplant.
Die Besetzung erfolgt von führenden Universitäten wie Moskau, St.Petersburg, Nowosibirsk, Rostow und Fernost. Zu den Tätigkeitsbereichen gehören unter anderem Luftfahrt, Lasertechnik, Softwareforschung und Biotechnologie.
Das *Militärwissenschaftliche Komitee* der Streitkräfte hat die Kontrolle, die dem *National Defense Management Center NDMC* angehört, das auch den fähigsten militärischen Supercomputer beherbergt, der auf Petaflop-Level arbeitet. Die Ergebnisse werden meist klassifiziert, aber es wurde berichtet, dass in der IT-Sicherheit bereits 45 neue Softwareprogramme entwickelt wurden.

Western Analysten glauben auch aus den jüngsten Inhaftierungen verschiedener Russen (*Yahoo Hack, Michailow Vorfall, US-Wahlen*), dass Russland einen deutlichen Vorteil im Cyber-Bereich haben würde, weil es Cyber-Kriminelle als Deckung bei Cyber-Attacken engagieren würde[785]. Nach Angaben des Vereinigten Königreichs und anderer NATO-Nachrichtendienste umfasst das Cyberpotential von Russland eine Million Programmierer und 40 Ringe aus Cyber-Kriminellen[786].

Wie im nächsten Kapitel gezeigt, schließt der Cyber-Krieg aus russischer Perspektive auch den Informationskrieg mit ein, siehe auch Abschnitt 2.2.6 in Bezug auf die angenommene Rolle der **Cyber-Trolle** und der **Social Bots**. Aus russischer Sicht versuchen westliche Staaten, den Informationsfluss zu beherrschen und Russland und andere Akteure zu untergraben.

Russland hat seine Cyber-Sicherheit in diesem Jahrzehnt deutlich gestärkt. Russland nutzt das Überwachungssystem SORM für die Überwachung des Datenverkehrs[787]. Im Jahr 2016 wurde ein neues Sicherheitsgesetz veröffentlicht. Ab Mitte Juli 2018 müssen alle Inhalte von Telefongesprächen, sozialen Netzwerken und Messenger

[782] 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”
[783] vgl. Prawda 2012
[784] vgl. Gerden 2015, SCMagazine 2015
[785] vgl. Johnson 2016
[786] vgl. Johnson 2016
[787] vgl. FAZ 2010h

Services für 6 Monate mit einem legalen Zugang für den internen Geheimdienst FSB von den Anbietern gespeichert werden[788].
Die russischen Behörden (FSB und *Bundesdienst für Technische und Exportkontrolle FSTEC*) fragen Anbieter seit 2014 zunehmend nach dem Quellcode, um sicherzustellen, dass sich keine Backdoors und andere Sicherheits-Lücken in der Software befinden. Cisco, IBM und SAP kooperierten, während *Symantec* die Zusammenarbeit eingestellt hat. Die Überprüfung des Quellcodes erfolgt nur in Räumen, in denen Code nicht kopiert oder verändert werden kann[789].

8.4.2 Das Cyberwarkonzept Russlands

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[790].
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."* [791] Diese Definition passt zu der Doktrin zur Informationssicherheit, die Präsident Putin im Jahr 2000 erließ[792] 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*." [793]

---

[788] vgl. Wechlin 2016, S.6
[789] vgl. Reuters 2017b
[790] vgl. Bazylev et al. 2012, S.10
[791] 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*."
[792] 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*."
[793] 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[794].

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[795]. Die Kontrolle des Informationsflusses und die Beeinflussung seiner Inhalte zur Unterstützung der eigenen Position sind nun Instrumente der soft power in internationalen Beziehungen[796]. Fehlende Kontrolle kann auch zur Destabilisierung und Destruktion führen[797].

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[798].

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[799].

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)[800].

---

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

[795] vgl. Maliukevicius 2006, S.121

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

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

[798] 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).

[799] 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.

[800] 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 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

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.

8.4.3 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[801]. 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")*[802], der Auffassung, dass die verschiedenen Technologien in Wirklichkeit nicht voneinander getrennt werden können und der bereits bestehenden Rolle in Cyberangelegenheiten[803] (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 Kommunikationstechnologie (IKT), d.h. für die gesamte digitale Technologie sein kann[804].
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[805]. Während die öffentliche Berichterstattung auf das Internet fixiert war, sollte laut Vertragstextentwurf dieser Staaten die gesamte IKT erfasst werden[806]. Außerdem

---

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".

[801] vgl. WCIT2012 Präsentation, introductory section

[802] 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")*

[803] 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."

[804] IKT wird in der WCIT2012 Präsentation genannt, section myths and misinformation

[805] vgl. Touré 2012

[806] vgl. WCITleaks 2012. Es handelt sich aber nur um ein 'geleaktes' Dokument ohne offiziellen Status.

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[807]. 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[808] und auf die Innovationskraft auswirken würde, weshalb sich diese Staaten jeder Formulierung, die der ITU Einfluss auf das Internet geben würde, widersetzten[809].
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*"[810].
Außerdem wurden neue ITRs angenommen, aber ein Konsens konnte nicht erreicht werden[811]. Infolgedessen haben die Vereinigten Staaten, die EU-Staaten, Australien und viele weitere Staaten die neue ITRs nicht unterschrieben[812].

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*

[807] vgl. EU 2012b (Position Paper of the EU)
[808] vgl. Kleinwächter 2012, S.31, Lakshmi 2012, S.1
[809] vgl. Touré 2012
[810] 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*"
[811] vgl. WCIT2012 Final Acts
[812] vgl. Betschon 2012, S.4; Lakshmi 2012 schätzte, dass 113 der 193 ITU-Mitgliedsstaaten die neuen ITRs unterschreiben, 80 nicht.

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".* [813]

8.5 Israel

Israel ist einer der führenden Cyber-Akteure. Basierend auf ehemaligen Offizieren der Militär-Cyber-Einheit *Unit 8200* und einer dynamischen akademischen Umgebung wie der Universität Tel Aviv gibt es eine schnell wachsende Szene von Cybersecurity-Firmen wie *Cellebrite* und *NSO-Group*, die z.B. ihre Fähigkeiten bei der Smartphone-Intrusion und Entschlüsselung bereits demonstriert haben.
So dienten z.B. die Gründer der Sicherheitsfirmen *CheckPoint* und *CyberArk* in der Unit 8200.[814]

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[815].
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[816].
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[817].

---

[813] 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
[814] vgl. FAZ 2018e
[815] vgl. Croitoru 2012, S.30
[816] vgl. EPRS 2014, S.5/6
[817] vgl. Rößler 2016, S.6

8.6 Die Bundesrepublik Deutschland

8.6.1 Überblick

Der zivile Sektor besteht aus:
Bundesministerium des Innern BMI mit

- *Bundesamt für Sicherheit in der Informationstechnik (BSI)* zum Schutz der IT-Infrastruktur
- *"Zentrale Stelle für Informationstechnik im Sicherheitsbereich" (ZITIS) für Entschlüsselung* (BSI sind die code maker, Zitis die code breaker)[818]
- Die *Agentur für Innovation in der Cybersicherheit* soll als zivil-militärische Zusammenarbeit zwischen den Ministerien des Innern BMI und des Verteidigungsministeriums BMVg im August 2019 starten.[819]

Militärischer Sektor:

- *Cyberinformationsraumkommando CIR* mit *Kommando Strategische Aufklärung KSA* und dessen Einheiten für die Elektronische Kampfführung (EloKa), *Computer- und Netzwerkoperationen (CNO)* und die Satelliten (mit der *Geoinformation GeoBw*).

Nachrichtendienste:

- *Bundesnachrichtendienst BND* als Auslandsgeheimdienst mit der Abteilung T4 für Cyberoperationen[820]
- *Bundesamt für Verfassungsschutz BfV* als Inlandsgeheimdienst
- *Militärischer Abschirmdienst MAD* für den Schutz der Bundeswehr

Sicherheitspartner sind u.a.:

- *Secunet* für die Sichere Netzwerkarchitektur SINA
- *Rohde and Schwarz* für Kryptologie
- *Genua* (gehört der Bundesdruckerei) für VPN und firewalls

Eine staatsnahe Forschungseinrichtung ist das *Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE*.

8.6.2 Hintergrund und Details

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

[818] vgl. Kirchner et al. 2017, S.5
[819] vgl. BMI 2018
[820] vgl. Mascolo/Steinke 2019, S.9

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[821].

Die Aufgaben der Behörde sind unter anderem[822]:

- Mitarbeit im *Arbeitskreis KRITIS* zum Schutz Kritischer Infrastrukturen vor Angriffen[823]
- Schutz der Regierungskommunikation, u.a. durch Kryptohandys für die Regierung, aber auch im *Informationsverbund Bonn-Berlin IVBB* und dem *Informationsverbund Bundesverwaltung IVBV***,** der vom BSI seit 2009 regelmäßig auf Schadsoftware gescannt wird[824]
- 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[825]
- Arbeit an stabilen und resistenten Computertechniken wie der Hochverfügbarkeit[826] 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[827]. Die Arbeit des neuen Cyber-Abwehrzentrums wurde bislang jedoch durch Abstimmungsprobleme zwischen den Mitgliedsbehörden (Regierung, Nachrichtendienste, Polizei usw.) beeinträchtigt[828].

---

[821] 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

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

[823] 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)

[824] vgl. Steinmann 2010, S.10

[825] um Probleme wie das Abfangen von vom Computer abgestrahlten Informationen zu bewältigen, vgl. Schröder 2008

[826] 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.

[827] vgl. FAZ 2010g, S.4, Tiesenhausen 2011, S.11, BMI 2011

[828] vgl. Goetz/Leyendecker 2014, S.5

- Zudem wurde ein *Nationaler Cyber-Sicherheitsrat* ins Leben gerufen, dem u.a. die Staatssekretäre der großen Bundesministerien angehören[829].

Im Jahr 2016 wurde eine neue Entschlüsselungsbehörde, anfangs mit 60, später mit 400 Mitarbeitern unter dem Namen *Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITIS)* etabliert. Diese wird die Bundespolizei, das BKA und den Verfassungsschutz mit Codeknacken unterstützen. Der BND wird nicht beteiligt sein[830].
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 angesiedelt sein werden[831]; auch bekannt als '*Cyberfeuerwehr*'.

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[832] 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.
Sicherheitsleistungen für den Bund werden in der Regel aus Rahmenverträgen des BSI und des Beschaffungsamtes geschöpft, dazu gehörten auch Verträge mit *Symantec*, die nun von *Trend Micro* weiter betreut werden.

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[833]. Das KSA, das seit 2008 den Kern des Militärischen Nachrichtenwesens der Bundeswehr (MilNWBw) bildet, hatte 2010 eine Stärke von ca. 6.000 Mann[834] und ist zuständig für die

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

[829] 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
[830] vgl. Heil/Mascolo 2016, Mascolo/Richter 2016, S.2
[831] vgl. Biermann/Beuth/Steiner 2016
[832] vgl. Rühl 2012, S.10
[833] vgl. Eberbach 2002
[834] vgl. Bischoff 2012

- seit 2007 gehört dem KSA auch die Einheit *Computer- und Netzwerkoperationen CNO*[835] an, die auch für den Cyberwar zuständig ist, d.h. den Kampf im Internet gegen mögliche Angreifer[836] und seit 2012 einsatzbereit ist[837]
- und für die Aufklärungssatelliten des Typus *Synthetic Aperture Radar (SAR-Lupe)* [838] 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 von 6000 auf weniger als 300 reduziert werden konnte; dennoch bleibt die Struktur immer noch komplex[839].

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[840]. Die militärgeheimdienstlichen Fragen werden vom MAD betreut; die Offensivkapazitäten sind im KSA als CNO angesiedelt (siehe oben)[841].

Die Aktivtäten im Cyber- und Informationsraum wurden gebündelt[842] im '*Cyberinformationsraumkommando CIR*'[843].
Das neue Kommando führt nun 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). Dieser Transfer wird dem CIR mehr als 13.700

[835] vgl. Bischoff 2012
[836] 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.
[837] vgl. Steinmann/Borowski 2012, S.1
[838] 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.
[839] vgl. Handelsblatt 2014, S.16
[840] vgl. BmVg 2015a
[841] vgl. BmVg 2015a
[842] vgl. Leithäuser 2015b, S.4
[843] vgl. Köpke/Demmer 2016, S.2

Soldaten zuführen[844]. Die CNO-Kapazitäten werden ausgebaut, um Cyberangriffsübungen ausführen zu können, als sog. **Red teaming**[845].
Die Fähigkeiten zum Hackback sollen ausgebaut werden, geplant ist eine Aufstockung von 100 auf 300 Mitarbeiter. Eine neue Bedrohung laut BMVg sind vor allem Quantencomputer, da alle Akteure Quantenprojekte laufen lassen[846].

Im Jahr 2015 berichtete die Bundeswehr[847] 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.-01.12.2011 die länderübergreifende Übung *Lükex 2011* statt, bei der ein vom *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)* und dem BSI entwickeltes umfassendes Angriffsszenario auf kritische Infrastrukturen getestet wurde[848].

Der *Bundesnachrichtendienst BND* hat 2013 eine Cyberabteilung eingerichtet[849][850]. 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[851]. Zudem ist die aktive Unterstützung der Cyberabwehr geplant, indem die vom Dienst gewonnenen Informationen der Vorbereitung auf Attacken helfen soll. Zudem wird der BND bis 2022 eigene Spionagesatelliten bekommen[852]. Der BND soll bis 2022 zwei Satelliten mit dem System *Geheimes Elektro-Optisches Reconaissance System Germany (Georg)* erhalten. Bisher sind BND und Bundeswehr mit Verbindungsbeamten bei der *National Geospatial Agency (NGA)* vertreten, von der sie zuweilen Luftbilder erhalten.[853]

[844] vgl. BmVg 2016
[845] vgl. BmVg 2016, S.28
[846] vgl. Der Spiegel 2018, S.12
[847] vgl. Köpke/Demmer 2016, S.2
[848] vgl. Spiegel online 2011
[849] vgl. Flade/Nagel 2015, S.4
[850] vgl. Spiegel 2013b, S.22, auch Spiegel 2013c, S.15
[851] vgl. SZ 2014a, S.1
[852] vgl. Lohse 2016, S.4
[853] vgl. Biermann/Stark 2018, p.7

Die *Agentur für Innovation in der Cybersicherheit* soll als zivil-militärische Zusammenarbeit zwischen den Ministerien des Innern BMI und des Verteidigungsministeriums BMVg im August 2019 starten [854] mit einem geplanten Personal von 100 Mitarbeitern und Forschung in diesem Bereich unterstützen. Dabei handelt es sich nicht um eine Behörde, sondern um eine staatliche Agentur, die geminsam vom BMI und BMVg geleitet wird. Der ursprüngliche Name war "disruptive Innovationen", was die Erforschung der Cyberwaffen betont hätte, aber dieser wurde dann nicht verwendet.

8.6.3 Die Doxing-Attacke von 2018/2019

Bei der **Doxing**- oder auch **Doxxing**-Angriffsmethode wird die Privatsphäre von Opfern durch Publikation privater Dokumente gezielt verletzt (abgleitet von docs =documents).

Am Abend des 03.01.2019 wurde bekannt, dass ein da noch unidentifizierter Angreifer, der ein 20 Jahre alter Schüler aus Hessen war, als Twitter-User mit dem Covernamen *G0d* (wohl eine Referenz zu dem Onlinespiel *Minecraft*) alias *Orbit/Troja/Power/Orbiter* mit dem Account @_orbit private Daten von insgesamt 994 deutschen Politikern und Prominenten ins Netz gestellt hatte[855].
Die ersten Aktivitäten begannen schon am 19.07.2017 und am 24. November 2018 gab der User bekannt, dass er einen Adventskalender mit privaten Daten (wie geheime Telefonnummern, Zeugnisse und andere persönliche Daten, aber auch parteiinterne Papiere und Kopien von Pässen und Diplomatenpässen, aus der Zeit von 2011-2018) erstellt hatte[856].
Vom 01.-24. Dezember 2018 wurden dann tatsächlich nach und nach Daten freigegeben, wobei dies u.a. auch Kanzlerin Merkel und Bundespräsident Steinmeier betraf. Die Aktion erregte trotz ca. 17.000 Followern (die evtl. zum Teil aus der Zeit vor der Account-Übernahme durch G0d stammten[857]) zunächst kein öffentliches Aufsehen.
Der User G0d war in der Hackerszene schon seit Jahren bekannt[858], der u.a. YouTube-accounts gehackt hat. Er hackte und übernahm 2015 den Account von Yannick Kromer alias *Dezztroyz*, um die Daten zu verbreiten und hackte dann den Account des bekannten YouTubers Simon Unge, was für verstärkte Publizität sorgte[859].

[854] vgl. BMI 2018
[855] vgl. Bender et al. 2019, Ludwig/Weimer 2019
[856] vgl. Bewarder et al. 2019a und b
[857] vgl.T-online exklusiv 2019
[858] vgl.T-online exklusiv 2019
[859] vgl. Bender et al. 2019, Ludwig/Weimer 2019

Der Doxing-Angriff wurde durch eine Kombination aus gesammelten öffentlich verfügbaren Daten und konventionellem Passwort-Hacken möglich[860].
Um die Daten gegen Löschen zu schützen, wurden sie auf bis zu 7 asiatischen und russischen Servern gelagert[861], zudem wurden die links über verschiedene, wohl auch zum Angreifer gehörende Accounts geschickt (u.a. r00taccess, Nullr0uter, nigzyo usw…).[862]

Ein Abgeordneter bemerkte im Dezember 2018 abnorme Aktivitäten in seiner Kommunikation und informierte die Sicherheitsbehörde BSI, die versuchte, mit dem MIRT-Team Abhilfe zu schaffen, wobei das BSI zu der Zeit noch nicht wußte, dass es sich um einen Teil eines größeren Angriffs handelte.
Nachdem auch der SPD-Politiker Martin Schulz betroffen war[863], wurde schließlich am 04.01.2019 eine Krisensitzung des *Nationalen Cyber-Abwehrzentrums* einberufen. Es wurden intensive Ermittlungen unter Leitung der polizeilichen *Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT)* aufgenommen und angeblich auch Amerika, d.h. die NSA um Hilfe gebeten[864].

Die Behörden fanden keinen Hinweis auf einen Einbruch in das Regierungsnetz und es wurde ein Einzeltäter vermutet[865].
Die Attribution gelang rascher als erwartet. Ein erster Hinweis war ein zu seinem Twitter-Acount gehörendes Photo, das wohl tatsächlich den Angreifer selbst als jungen Teenager zeigte[866].
Der Angreifer nutzte für seine *Telegram*–Botschaften einen Zugang, der mit seiner echten Handy-Telefonnumer von der *Deutschen Telekom* verlinkt war. Zudem zeigte ein Screenshot eines gehackten *Amazon*-Accounts versehentlich auch seine *Windows 10*-Umgebung mit zahlreichen Icons der von ihm genutzten Programme und Erweiterungen (wie *Perfect Privacy, Ghostery* und *ABP*) und die genaue Login-Zeit mit Datum und Uhrzeit, was *Amazon* erlaubt, zu prüfen, welcher Computer (welche IP-Adresse) zu diesem Zeitpunkt mit dem Account kommunizierte[867].

Trotz der Vorgänge hat der Angreifer weiterhin e-mails ausgetauscht[868], er teilte u.a. dem YouTuber Jan Schürlein mit einer verschlüsselten Nachricht am 05.01.2019 mit, dass er alle Hardware des Vorganges zerstört hätte[869]. Am 06.01.2019 wurde Jan Schürlein, der im Kontakt zu dem Hacker stand, in Heilbronn polizeilich

[860] vgl. Decker/Köpke 2019, S.2
[861] vgl. Bewarder et al. 2019b/Bender et al. 2019
[862] vgl. Bewarder et al. 2019b/Bender et al. 2019
[863] vgl. Schubert 2019
[864] vgl. Schmiechen 2019, Ludwig/Weimer 2019
[865] Vgl. Bild 2019
[866] vgl. Bender et al. 2019
[867] vgl. Denker et al. 2019
[868] vgl. T-online exklusiv 2019
[869] vgl. Van Lijnden 2019

vernommen[870]. Am selben Tag noch konnte der Angreifer verhaftet werden, der dann am 07.01.2019 ein volles Geständnis ablegte. Es ergaben sich keine Hinweise auf ausländische Akteure, der Angreifer gab an, über einige Personen verärgert gewesen zu sein[871].

Die Bundesregierung hat umgehend eine Stärkung des BSI durch eine Aufstockung von 800 auf 1.300 Mitarbeiter und des *Nationalen Cyber-Abwehrzentrums* durch Koordinationsbefugnisse und eigene Auswertekapazitäten beschlossen[872].

8.7 Großbritannien

Das Vereinigte Königreich hat massive Investitionen im Rahmen der Cyberstrategien unternommen, die aktuelle *National Cyber Security Strategy 2016* sagt, dass bis 2021 1,9 Milliarden £ investiert werden[873].

Aktuelle Struktur:

- *National Cyber Security Centre (NCSC)* als Behörde für die Cybersicherheit, die Weitergabe von Informationen, Bekämpfung systemischer Schwachstellen und Führung bei zentralen Angelegenheiten der nationalen Cybersicherheit. Das militärische *Cyber Security Operations Centre* wird eng mit dem NCSC zusammenarbeiten.
- Die *National Cybercrime Agency NCA* ist für die Bekämpfung der Cyberkriminalität zuständig.
- Die *Defence Intelligence (DI)* als Teil des Verteidigungsministeriums *Ministry of Defence (MOD)* hat militärnachrichtendienstliche Funktionen und wird der Ort der neuen Cyberwareinheit sein. Die DI ist nicht Teil der anderen Geheimdienste (MI6*, Government Communication Headquarters GCHQ* und MI5); wobei das GCHQ für Cyber Intelligence zuständig ist[874].

8.8 Frankreich

Ausgangspunkt war die Überprüfung der *Strategie für Verteidigung und nationale Sicherheit* im Jahr 2017.
Zivile und militärische Einrichtungen werden klar getrennt.
Die *Nationale Agentur für Cybersicherheit ANSSI* koordiniert die Cybersicherheit des Staates.

[870] vgl. Van Lijnden 2019
[871] vgl. Decker/Köpke 2019, S.2
[872] vgl. FAZ 2019a, S.1
[873] vgl. National Cyber Security Strategy 2016
[874] vgl. National Cyber Security Strategy 2016, Ross 2016

Frankreich errichtete 2017 seine erste Cyberwar-Einheit, diese begann ihre Arbeit im Januar 2017[875]. Das neue *Commandement de Cyberdefense* (*Comcyber* oder *Cocyber*) umfasst mehr als 3.200 Soldaten der Armee, Marine und Luftwaffe, nachdem es schon Cyberdefenseabteilungen seit 2011 gab.
Comcyber ist für Cyber-Operationen, Aufklärung und Verteidigung zuständig mit Ausnahme des DGSE, d.h. dem Auslandsnachrichtendienst, der weiterhin autonom ist und Berichten zufolge bei Bedarf offensiv gegen Cyberangriffe vorgeht[876].

Die russische APT Turla griff 12 Beamte an, um die Ölversorgungskette der Marine in den Jahren 2017 und 2018 zu enthüllen, die Franzosen bevorzugen jedoch die diskrete Klärung von Vorfällen statt öffentlicher Anklagen[877].

8.9 Weitere Akteure

Iran ist ebenfalls ein aktiver Akteur. Ein aktuelles Beispiel ist die Errichtung des *Hohen Cyberrats (Shoray-e Aali-e Fazaye Majazi)*, der nun die Aktivitäten aller im Cyberspace tätigen Einrichtungen koordiniert[878]. Zuvor wurde 2010 als Reaktion auf die Stuxnet-Attacke das *Cyber Defense Command* zum Schutz kritischer Infrastrukturen errichtet.
Die Cyberaktivitäten des Iran finden sich im Abschnitt 5.

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[879].

8.10 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.

[875] vgl. AFP 2016
[876] vgl. Lawfareblog 2019
[877] vgl. Lawfareblog 2019
[878] vgl. Nligf 2012, wo auch die Existenz einer informellen ‘cyber army’ erwähnt wird.
[879] vgl. Chhabra 2014, S.66-67

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* hatte aber immer noch nur 12 Mitglieder (Finnland, Frankreich, Deutschland[880], Niederlande, Norwegen, Ungarn, Spanien, Schweden, England, Schweiz, Österreich, Dänemark, Großbritannien mit 2 CERTs)[881][882]. Ab 2012 wurde ein CERT-EU-Team für die Sicherheit der IT-Infrastruktur dauerhaft eingerichtet [883]
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.“[884]

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[885].
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[886].
Die ENISA wird 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)

[880] Zur deutschen Gruppe CERT-Bund siehe Website des BSI
[881] vgl. IT Law Wiki 2012b, S.1
[882] 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 Intruder*).
[883] vgl. EU2013b, S.5
[884] 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
[885] vgl. EU-ISS 2007
[886] vgl. ENISA 2007

stärken[887], u.a. durch die Förderung und Ausweitung bestehender Kooperationsmechanismen wie der ECG-Gruppe

- Die ENISA hat 2009 eine vergleichende Analyse der EU- und EFTA-Staaten veröffentlicht, in der u.a. die sehr unterschiedlich geregelten Zuständigkeiten im Bereich der Netzwerksicherheit, der unzureichende Aufbau von CERTs und deren mangelnde Kooperation sowie unzureichende Prozeduren bei der Berichterstattung sicherheitsrelevanter Ereignisse (*incident reporting*) festgestellt wurden. Es wurden Empfehlungen für verbesserte Prozesse und zu einer verstärkten Kooperation unter Federführung der ENISA gegeben[888].
- Im Einklang mit dem Plan zum Schutz kritischer Infrastrukturen von 2009[889] 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[890]. Jedoch zeigten sich auch bei dieser Übung die uneinheitlich geregelten Zuständigkeiten innerhalb der EU und die mangelnden Strukturen kleinerer Staaten[891]. 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[892].
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 [893].

[887] vgl. EU 2007, EU 2009b
[888] vgl. ENISA 2009a
[889] vgl. EU 2009b
[890] vgl. ENISA 2010a, ENISA2010b
[891] 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."
[892] vgl. EU2009b, auch EU 2010b
[893] vgl. EU2013a

Das neu gegründete *European Cybercrime Centre E3C* wird mit der ENISA und der *europäischen Verteidigungsagentur (European Defense Agency EDA)* verstärkt in NIS-Fragen zusammenarbeiten[894].
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.

Die EU plant seit 2017, die ENISA zu einer umfassenden Cyber- und Datensicherheitsbehörde auszubauen, die auch für Zertifizierungen und Übungen zuständig sein wird.[895] Die EU plant eine Cybersicherheitszertifikat für Geräte, die im Internet der Dinge eingesetzt werden sollen. [896]

8.11 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[897] und bildet im Rahmen des 2002 verabschiedeten NATO Cyber Defense Programms die vorderste Verteidigungslinie der NATO zum Schutz ihrer eigenen IT-Infrastruktur[898].
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 (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[899] enthält 3 Elemente der Cyberabwehr, dies sind

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

[894] vgl. EU2013b, S.18
[895] vgl. Kirchner et al. 2017, S.5
[896] vgl. Siegel 2018b, S.18
[897] vgl. Schuller 2010, S.6
[898] vgl. NCSA 2009a-c
[899] vgl. NATO 2015

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[900], das in den ersten Jahren von Estland, Litauen, Lettland, Italien, Spanien, der Slowakei und Deutschland unterstützt wurde und zunächst 30 Mitarbeiter umfasste.[901], 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. Das CCD CoE ist seit Januar 2018 verantwortlich für die Planung und Koordination von Aus- und Weiterbildungslösungen in der Cybersicherheit für das gesamte Bündnis.
Bisher fanden als NATO Cyber Defence Übungen *Digital Storm* und *Cyber Coalition* statt, wobei das CCD CoE diese Übungen gemeinsam mit dem NCIRC und anderen NATO-Einrichtungen organisierte[902]. Die *Cyber Coalition (CC)*-Übung findet nun regelmäßig statt. *Locked Shields* ist eine jährliche Echtzeit-Cyberübung, die seit 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“*)[903].

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

[900] Faktisch hat das CCD CoE nach einer 2004 von Estland ausgehenden Initiative schon seit 2006 existiert, vgl. CCDCoE 2010a
[901] Die NATO will sich im Falle eines Cyberangriffs im ersten Schritt lediglich auf Konsultationen stützen, vgl. von Kittlitz 2010, S.33
[902] vgl. Wildstacke 2009, S.28/29, CCDCoE 2010b
[903] 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.

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[904]. Im Ergebnis muss die Sicherheitspolitik mit einem besonderen Augenmerk auf die Resilienz der eigenen Systeme intensiv durchdacht werden[905]. 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[906].

Analysten des BND gehen davon aus, dass Cyberaktivitäten in bewaffneten Konflikten vor allem am Anfang des Konfliktes eine wichtige Rolle spielen[907]. 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[908]. Die Vorbereitung des Schlachtfeldes (*Preparing the battlefield*) gilt als wesentlich für erfolgreiche Strategien, in der Praxis werden vorsorglich Sender (**beacons**) oder Implantate in ausländischen Computernetzwerken platziert, das ist Computercode, mit dessen Hilfe die Arbeitsweise des Netzwerks untersucht werden kann[909].

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[910]. 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

[904] vgl. NATO 2014, BMVg 2015b
[905] vgl. BMVg 2015b
[906] vgl. Jones 2014, S.1
[907] vgl. Leithäuser 2015, S.8
[908] vgl. Leithäuser 2015b, S.4
[909] vgl. Sanger 2015, S.5
[910] vgl. Leithäuser 2016, S.8

gesichert werden[911]. Ein Eurofighter-Kampfjet hat mehr als 80 Computer und 100 Kilometer Verkabelung[912].

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).

8.12 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[913].
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*)[914].

2009 vereinbarten die Mitgliedsstaaten der Afrikanischen Union (AU) die Entwicklung einer Konvention zur Cyber-Gesetzgebung im Rahmen der AISI-Initiative, von der ein erster Entwurf im Jahr 2011 vorgelegt wurde[915]. Die Konvention befasst sich mit dem elektronischen Handel, Datenschutz und –verarbeitung und Cyberkriminalität im Allgemeinen, enthält aber keine speziellen Regelungen zum Cyberwar[916].

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[917] diskutiert.

---

[911] vgl. Mahaffey 2016, S.V6
[912] vgl. Köpke/Demmer 2016, S.2
[913] vgl. ECA 2012, S.1
[914] 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
[915] vgl. ECA 2012, S.3, AU 2011
[916] vgl. AU 2011
[917] vgl. ECA 2012, S.4

Ein wichtiger Aspekt in vielen Dokumenten ist die Forderung nach verstärkter inner-afrikanischer Kooperation und einem verbesserten Sicherheits-bewusstsein[918].
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[919]. Ein vorrangiges Ziel war die Koordination aller mit Cybersicherheit befassten Stellen[920].

In Afrika wächst die Bedeutung von Smartphones rapide, weil dies die Überbrückung von Lücken in der digitalen Infrastruktur ermöglicht, was Afrika für die oben gezeigten Sicherheitslücken besonders anfällig macht[921].

Im Hauptquartier der Afrikanischen Union, das mit Hilfe Chinas in Addis Abeba gebaut wurde, wurden regelmäßige Hackerangriffe festgestellt, die von 2012 bis 2017 aus Shanghai gekommen sein sollen. China dementierte dies energisch, dennoch wurden die chinesischen IT-Techniker ersetzt[922].

[918] 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.
[919] South Africa 2012
[920] South Africa 2010, S.6
[921] vgl. Puhl 2013, S.118f.
[922] vgl. FAZ 2018b

9 Cyberwar und biologische Systeme

9.1 Intelligente Implantate

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[923]. Aus diesem Grunde ist die Forschung zum Signalschutz und anderen Strategien bereits im Gange[924].

Als Reaktion auf die Bedrohungen im digital health-Sektor hat die amerikanische *Food and Drug Administration FDA* eine ‚*safety communication on health-related cyber security*' herausgegeben[925]. 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.[926]. Die Herausforderung besteht darin, Sicherheit und Privatheit mit der medizinischen Sicherheit und Nutzbarkeit in Einklang zu bringen[927].

Die Cybertech-Firma *Xtrap* in Kalifornien fand bei einem Check, dass alle 60 von 60 Krankenhäusern bereits mit Malware infiziert waren.[928] Die FDA veröffentlichte im Jahr 2015 eine Warnung für eine Internet-verbundene Insulin-Pumpe von *Hospira* wegen des potenziellen Risikos des Hackens; im Jahr 2016 warnte *Johnson und Johnson* 11.400 Patienten wegen ihrer vernetzten Insulinpumpe ebenfalls [929].

Die drei Grundprinzipien der FDA sind die Begrenzung des Zugangs auf autorisierte Nutzer, die Beschränkung auf autorisierte und sichere Inhalte und die

[923] vgl. Gupta 2012, S.13
[924] vgl. Xu et al 2011, Gollakota et al. 2011
[925] vgl. FDA 2013a
[926] vgl. FDA 2013b, S.2
[927] vgl. Gupta 2012, S.26
[928] vgl. Lindner 2017
[929] vgl. Jonas 2016, S.22, Lindner 2017

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 Malwareschutz und Sicherheit des Datentransfers des Gerätes, wobei auch anerkannte Verschlüsselungsmethoden genutzt werden sollte[930].

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[931]. 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[932]. 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[933].
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[934]. Mittlerweile wurden Herzschrittmacher entwickelt, die die Bewegung der Organe als Energiequellen nutzen können[935]
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.[936]. Der Chip benötigt jedoch noch eine externe Energieversorgung.

[930] vgl. FDA 2013b
[931] vgl. Young 2013, S.1, Medtronic 2013
[932] LFP Signale kodieren dynamische Komponenten des Verhaltens, Hintergrundaktivitäten des Gehirns und evtl. noch andere Aspekte, vgl. Stamoulis/Richardson 2010, S.8
[933] vgl. ClinicalTrials.gov 2013
[934] vgl. Jürisch 2013, S.10
[935] vgl. Welt online 20.01.2014
[936] vgl. Stingl et al 2013

Das Hacken solcher Implantate birgt nicht nur Manipulationsgefahren, sondern auch das Risiko schwerer körperlicher Schäden[937], so dass der Gesetzgeber sicherstellen muss, dass das Hacken von Implantaten nicht nur als virtuelle Straftat verfolgt werden kann.

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[938]. Angreifer könnten mit Hilfe dieser Computerbrillen nicht nur den User, sondern auch andere beobachten[939]. Andere Konzepte sind smarte Perücken oder Helme (**smart wigs** oder **smart helmets**), mit denen gelähmte oder blinde Menschen unterstützt werden können und intelligente Pflaster, die den Gesundheitszustand der Nutzer aufzeichnen[940].

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.

9.2 Beziehungen zwischen Cyber- und biologischen Systemen

9.2.1 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.

[937] Wie das Setzen von Elektroschocks, vgl. Gollakota et al 2011, S.1
[938] vgl. Postinett 2013a, S.30
[939] Dazu werden RFID-Chips mittlerweile als Diebstahlschutz in wertvolle Pferde und als Kidnappingschutz zuweilen auch Kindern eingepflanzt.
[940] Die Untersuchung des Befindens kann auch mit Kameras erfolgen wie bei der Microsoft X-Box, vgl. Mähler 2013, S.38.

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 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[941]. 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[942]. Die exzessive Zytokinfreisetzung, auch als Zytokinsturm oder **cytokine release syndrome** bekannt, kann in potentiell tödlichen schockartigen Reaktionen (Kreislaufzusammenbruch, Organversagen, Blutgerinnungsstörungen usw.)[943] 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[944]. Der Virophage Sputnik richtet sich gegen das Mimivirus, das auch menschliche Pneumonie verursachen kann[945] inzwischen wurde der verwandte *Zamilon-V*irophage entdeckt[946]. 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[947], in Deutschland kam es 1990 zu einigen tödlichen Pockenfällen, als

[941] vgl. Haller 2009, S.57
[942] vgl. Kash et al 2011, Stegemann-Koniczewski 2012
[943] 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
[944] vgl. Zhou et al 2012
[945] vgl. Zhanga et al. 2012
[946] vgl. Krupovic et al. 2016
[947] vgl. Shah 2014, S.27

Kuhpockenviren, die die Artenbarriere zu Katzen überwunden hatten, vorwiegend immunsupprimierte Menschen befiel[948].
Die Anzahl der Virophagen wächst ständig, so dass mehrere Virophagen-Genomsequenzen, die teilweise oder vollständig aus metagenomischen Datensätzen zusammengesetzt sind, z.B. in zwei antarktischen Seen und dem Yellowstone Lake entdeckt wurden[949].

9.2.2 Bakterien

Bakterien sind einzellige Organismen, die andere Organismen infizieren können, so auch den Menschen[950]. Einige Bakterien, die bedeutsame Infektionen beim Menschen auslösen, können flüssige Plattformen, die sogenannten **Biofilme**[951] 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[952].

Die Biotechnologie ermöglicht die Veränderung von Genen oder die Einführung neuer Gene in Organismen, so dass Bedenken bestehen, dass gefährliche Organismen absichtlich[953] oder versehentlich erschaffen werden. Im vergangenen Jahrzehnt wurde das neue Phänomen des **bio-hacking** beobachtet[954]. 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[955]. 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

[948] vgl. Scheubeck 2014, S.7
[949] vgl. Krupovic et al. 2016
[950] 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.).
[951] vgl. Bakaletz 2012, S.2
[952] vgl. Gebhardt 2013, S.38.
[953] 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).
[954] vgl. Kunze 2013, S.19-20
[955] 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.

Glykoproteinoberflächen, die dann als eine Art Fingerdruck eine Zuordnung zu einer Produktionsstätte erlauben helfen[956].

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[957]. 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[958]. Trotz der Erwartung einer kommenden post-antibiotischen Ära wird im Westen nur wenig geforscht und es gibt auch keine hinreichenden rechtlichen Regelungen[959]. Bakteriophagenenzyme sind jedoch militärisch bedeutsam, denn eines davon ist gegen die Standardbiowaffe Bazillus *anthracis* wirksam, besser als Milzbrand bekannt[960].

9.2.3 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

[956] 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 Bedingungen. Larven der Großen Wachsmotte (*Galleria melonella*) verzehren Polyurethan weitaus schneller als *Ideonella*, vgl. Neuroth 2017.
Für 2019 ist ein hierzu passender Artikel zur biologischen Kriegsführung in Arbeit, der Abstract befindet sich unter Biological Warfare - The Reference Module in Biomedical Sciences 2019. Elsevier ScienceDirect. https://doi.org/10.1016/B978-0-12-801238-3.62160-8
[957] vgl. Yang et al. 2013, S.46ff
[958] vgl. Mandal 2014
[959] vgl. WHO 2014, Verbeken et al. 2014
[960] vgl. Zucca/Savoia 2010, S.83

menschliches Verhalten und die Entscheidungsfindung zu kontrollieren[961]. Jedoch sind diesem Cyborg-Szenario[962] 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 Freßfeinden zu begünstigen[963]. 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[964].

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.)[965], was durch Ergebnisse von mehreren psychologischen Standardfragebögen belegt werden konnte. Der Einfluss auf das Verhalten geht mit veränderten Dopamin- und Testosteronwerten einher[966], 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[967]. Außerdem ist noch unklar, inwieweit die Veränderungen beim Menschen wirklich Manipulationen oder nur Nebenwirkungen der chronischen Infektion darstellen.[968].

---

[961] vgl. Juengling 2014, S.63

[962] 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.

[963] 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

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

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

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

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

[968] vgl. Flegr 2013, S.127

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.[969]. Die Wirkung erfolgt durch elektrische Stimulation von spezialisierten Nervenzellknoten, den Nuklei, an denen die Sonden platziert werden und die sich tief im Gehirn befinden[970]. 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 Implantat ansetzt, in das emotional-hormonale System des Menschen mit einbezogen sind[971] 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[972]. 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*[973]. 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[974]. Elektrische Signale an den Fühlern bewirken dann eine Richtungsänderung der Schabe, wobei die Signale über Smartphone und Bluetooth versendet werden[975]. 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.

---

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

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

[971] 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

[972] vgl. Hummel 2014b

[973] vgl. Hummel 2014a, S.1

[974] vgl. Hummel 2014a, S.2

[975] Der Chip wird benötigt, um die Befehle des Smartphones 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

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[976]. 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.

9.3 Zusammenfassung und Implikationen für den Cyberwar

Wenngleich Kommunikation und Netzwerke eine wichtige Rolle auch in biologischen Systemen spielen, ist die Vergleichbarkeit zu Computersystem 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[977]. 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.

[976] vgl. Park et al. 2016
[977] Sogar der Fernseher kann unbemerkt Daten verschicken, wenn er als Internet-TV (IPTV) designed wurde, vgl. SZ online 2013

10 Literaturquellen

Abdollah, T. (2019): US launched retaliatory strike against Iranian military computers, as cyber war escalates. The Sydney Morning Herald 23 Jun 2019

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

Ackert, M. (2018a): Russlands Geheimdienst fürs Grobe. Neue Zürcher Zeitung, 26.09.2018, S.7

Ackert, M. (2018b): Russlands Militärgeheimdienst wird bloßgestellt. Neue Zürcher Zeitung, 08.10.2018, S.3

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

AFP (2016): France launches first cyber-warfare unit to take on hackers. 13.12.2016

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

Akamai (2017): akamai's [state of the internet] / security Q1 2017 report 26 Seiten

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.

Alvarez, S., Jansen, F. (2016): Hackerangriff auf die Telekom. Der Tagesspiegel online 28.11.2016

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

Ammann, B. (2016): Genug Daten für eine Doktorarbeit. Neue Zürcher Zeitung 24 Okt 2016, S.3

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

Asendorpf, D. (2017): Error. Die Zeit 27 Juli 2017, S.33

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.

Atzei, N., Bartoletti, M. Cimoli, T. (2016): A survey of attacks on Ethereum smart contracts. Universita degli Study di Cagliari; Cagliari Italy, Working Paper 2016, 24 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.

Baches, Z. (2016): Wie Hacker eine Notenbank knacken. Neue Zürcher Zeitung, 10.10.2016, S.7

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

BBC (2019): Ex-CIA agent Jerry Chun Shing Lee admits spying for China. BBC online 02 May 2019

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

Becker, L. (2018): "Black Dot Bug" in iOS11: Zeichenfolge legt Nachrichten-App auf iPhone lahm. Mac & I news 04.05.2018

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

Beiersmann, S. (2017a): Wikileaks macht Tool zur Erkennung von CIA-Malware öffentlich. ZDNet 03 April 2017

Beiersmann, S. (2017b): Brutal Kangoroo: Wikileaks enthüllt weiteres Hacking Tool der CIA. ZDNet 26 Juni 2017

Beiersmann, S. (2017c): Sicherheitsforscher: Petya 2017 soll Daten zerstören und nicht verschlüsseln. ZDNet 29 Juni 2017

Beiersmann, S. (2017d): HighRise: CIA-Malware für Android fängt SMS-Nachrichten ab. ZDNet 17.07.2017

Beiersmann, S. (2017e): NSA verliert erneut wichtige Daten. ZDNet. 06.10.2017

Beiersmann, S. (2017f): Amazon kündigt AWS Secret Region für Geheimdienste an. ZDNet 21.11.2017

Beiersmann, S. (2018a): EternalBlue: Botnetz nutzt NSA-Exploit für Kryptomining. ZDNet 03.02.2018

Beiersmann, S. (2018b): GitHub trifft weltweit größter DDoS-Angriff. ZDNet 02.03.2018

Beiersmann, S. (2018c): GitHub Hacker steigern DDos-Rekord auf 1,7 Terabit/s. ZDNet 07.03.2018

Bender, J. et al. (2019): Erst Flop, dann Staatsaffäre. Frankfurter Allgemeine Zeitung 05.01.2019, S.3

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

Betschon, S. (2017): Raub von Rechenleistung. Neue Zürcher Zeitung 18.10.2018, S.37

Betschon, S. (2018a): Saisonschlussverkauf der iPhoneHacker. Neue Zürcher Zeitung 19.03.2018, S.7

Betschon, S. (2018b): Intel-Prozessoren veruntreuen Daten. Neue Zürcher Zeitung 22.08.2018, S.37

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.

Beuth, P. et al. (2017): Merkel und der schicke Bär. Die Zeit Nr.20 11 Mai 2017, S.13-15

Bewarder, M. et al. (2019a): Hackerangriff erschüttert das politische Berlin. Die Welt 05.01.2019, S.1

Bewarder, M. et al. (2019b): Gods Werk und Twitters Beitrag. Die Welt 05.01.2019, S.4

BfV (2017): Cyberbrief 01/2017, 6 Seiten

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.

Biermann, K, Stark, H. (2018): Merkel sieht alles. – Der BND bekommt eigenen Satelliten. Die Zeit Nr. 8/2018, S.7

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

Bild (2017): Russen-Hacker führen deutschen Diplomaten vor. Bild 20 Nov 2017, S.1 und 3

Bild (2019): Wer steckt hinter den Angriffen? Bild 05.01.2019, S.2

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

BMI (2018): Bundesministerium des Innern (Federal Ministry of the Interior): Agentur für Innovation in der Cybersicherheit. 29.08.2018

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

Bodkin, H, Henderson, B. (2017): NHS cyber attack spreads worldwide. The Telegraph online 12 Mai 2017

Böck, H. (2017): Hacker sabotieren das Internet der unsicheren Dinge. Die Zeit online 07 April 2017

Böck, H. (2019): Linux-Rechner übers Netz abschießen. Golem.de 18 Jun 2019

Boey, D. (2017): North Korean Hacker Group linked to Taiwan Bank Cyberheist Bloomberg Technology online Oktober 2017

Borchers, D. (2017): Wikileaks: CIA tarnt Spionage-Software mit gefälschten Kaspersky-Zertifikaten. Heise online 11/2017

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

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.

Brühl, J., Tanriverdi, H. (2018): Einbruch per email. Süddeutsche Zeitung Nr. 51 vom 02.03.2018, S.2

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

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

Buchter, H. (2013): Die Profiteure. Die Zeit Nr. 33/2013, S.21

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

Büschemann, K.-H., Uhlmann, S. (2010): Deutschland braucht eine Rohstoffstrategie. Süddeutsche Zeitung vom 15.10.2010, S.19

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

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

Cherepanov, A. (2018): GreyEnergy - A successor to BlackEnergy. ESET White Paper, Oktober 2018, 31 Seiten.

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

Check Point Research (2017): Mid-Year Report Cyber Attack Trends 2017, 19 S.

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

Chiesa, R. (2015): Lectio Magistralis Hacking Cybercrime e underground economy (con u po di cyber espionage) Arcetiri, Firenze, INFN 5 Novembre 2015

Chiesa, R. (2017): IoT & IoX Cybersecurity: are you ready for the very first Hackmageddon? Presentation in Milan, 17 Mai 2017

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

Cimpanu, C. (2018): How US authorities tracked down the North Korean Hacker behind Wannacry. ZDNet 06.09.2018

Cimpanu, C. (2019): NASA hacked because of unauthorized Rapsberry Pi connected to its network. ZDNet 21 June 2019

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

CrowdStrike (2016): Danger close Blog Nov 2016

CT (2018): Super-Gau für Intel: Weitere Spectre-Lücken im Anflug. CT online 03.05.2018

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

Cyrus, O. (2017): Geheimdienste auslagern - ein Spiel mit dem Feuer, Neue Zürcher Zeitung 13.10.2017, S.16

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.

Decker, M., Köpke, J. (2019): Ein Schüler hackt das Land. Neue Westfälische 09.01.2019, S.2

Demchak, C.C., Shavitt, Y. (2018): China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking. Military Cyber Affairs: Vol. 3: Iss. 1, Article 7. 9 Seiten

Denker, H., Roodsari, A.V., Wienand, L., Kartheuser, B. (2019): Wie konnte ein 20-Jähriger den Riesenhack schaffen? T-Online Nachrichten 08.01.2019

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

Derespins, C. (2017): Wikileaks releases entire hacking capacity of the CIA. FOX News US 07 März 2017

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

Der Spiegel (2018): Gerüstete Cyberkrieger. Der Spiegel Nr. 25/2018, S.12

Deutsche Welle (2017): Hackerangriff auf OSZE Deutsche Welle online 25 Dez 2016

Deutschlandfunk (2017): CIA verdächtigt ehemaliges Vertragsunternehmen Deutschlandfunk online 13 März 2017

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

Diehl, J. et al. (2018): Teherans Papierdiebe. Der Spiegel Nr. 17/2018, S.58-59

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.

Die ZEIT online (2017): Mutmaßlicher russischer Hacker in Spanien festgenommen. 10 April 2017

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

DoD (2018): Summary of the 2018 DoD Cyber Strategy, 10 pages. Published by US Department of Defense (DoD)

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

DoJ (2018): Indictment United States of America versus Zhu Hua and Zhang Shilong. United States District Court - Southern District of New York. Unsealed on 20 Dec 2018.

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

Dragos Inc. (2017): CRASHOVERRIDE. Analyzing the Threat to Electric Grid Operations. 35 Seiten

Dragos (2017): TRISIS malware. Dragos version 1.2017213, 19 S.

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

DW (2017): Yahoo-Datenklau viel größer als gedacht. Deutsche Welle online

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.

Eckstein, P., Strozyk, J.L. (2018): Hacker erbeuten Pläne von Atomanlagen. Tagesschau online 01.11.2018

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

ESET (2016): En Route with Sednit Part 1: Approaching the Target. Version 1.0 October 2016, 40 Seiten ESET

ESET (2018): LOJAX - First UEFI rootkit found in the wild, courtesy of the Sednit group. ESET Research Whitepapers, September 2018, 24 Seiten

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 (2016): Commission Services Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace. Brussels, 2 December 2016 15072/16

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

EUROPOL (2016): ‘Avalanche’ Network dismantled in International Cyber Operation. Press Release 01 December 2016

Europol (2017): Massive blow to criminal dark web activities after globally coordinated operation. 20.07.2017

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

FAS (2018): Lernende Spione. Frankfurter Allgemeine Sonntagszeitung Nr. 9/2018, S.7

FAS (2019): Sicherheitsexperten manipulieren Teslas Autopiloten. Frankfurter Allgemeine Sonntagszeitung Nr. 9, 03 April 2019, S.21

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.

FAZ (2017a): Geheimdienstler verhaftet. Frankfurter Allgemeine Zeitung, 28.01.2017, S.5

FAZ (2017b): Russische Spione wegen Cyberangriffs auf Yahoo angeklagt. Frankfurter Allgemeine Zeitung 16 März 2017, S.23

FAZ (2017c): Schlag gegen Darknet-Handel. Frankfurter Allgemeine Zeitung 13 Juni 2017, S.4

FAZ (2017d): Amerika: Hinter Wannacry steckt Nordkorea. Frankfurter Allgemeine Zeitung 20.12.2017, S.6

FAZ (2018a): Die gefährlichste Sicherheitslücke aller Zeiten und ihre Entdecker. Frankfurter Allgemeine Zeitung 08.01.2018, S.22

FAZ (2018b): Hat Peking spioniert? Frankfurter Allgemeine Zeitung 31 Jan 2018, S.18

FAZ (2018c): Wie die Schlange vor dem Kaninchen, Frankfurter Allgemeine Zeitung Nr. 52/2018, S.2, 02.03. 2018

FAZ (2018d): Der Flughafen Saarbrücken wird bald ferngesteuert. Frankfurter Allgemeine Zeitung Nr. 91/2018 vom 19 April 2018, S.21

FAZ (2018e): Wie sich Hacker in der Telegram-App zusammentun. Frankfurter Allgemeine Zeitung Nro. 107/2018 vom 09 May 2018, S.22

FAZ (2018f): Bitcoin-Kurs verliert nach Hackerangriff 13 Prozent. Frankfurter Allgemeine Zeitung 20.06.2018 online

FAZ (2018g): Mit Sicherheit aus Israel. Frankfurter Allgemeine Zeitung 26.11.2018, S.20

FAZ (2019a): Bundesregierung will nach Datendiebstahl Cyberabwehr verbessern. Frankfurter Allgemeine Zeitung 08.01.2019, S.1

FAZ (2019b): Amerika will mehr seltene Erden fördern. Frankfurter Allgemeine Zeitung, Nr.130, S.17

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

FireEye (2014): APT28: A window into Russia‘s cyber espionage operations? Fire Eye Special Report 45 Seiten

FireEye (2015): APT30 and the mechanisms of a long-running cyber espionage operation. 12 April 2015

FireEye (2017): APT overview in www.fireeye.com/current-threats/apt-groups.html

FireEye (2018a): APT overview in www.fireeye.com/current-threats/apt-groups.html

Fireeye (2018b): Triton Attribution: Russian Government-owned Lab most likely built tools. FireEye-Intelligence online 23 Oct 2018

FireEye (2019): APT39: An Iranian Cyber Espionage Group Focused on Personal Information. 29 Jan 2019

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.

Fox News (2017): John Kasich: OhioGovernor‘s webiste hacked with pro-ISIS propaganda 25 Juni 17

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

Freidel, M. (2018): Pjöngjangs digitale Raubzüge. Frankfurter Allgemeine Zeitung 05 Feb 2018, S.3

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

Fuest, B. (2018): Leben mit einem Geist. Welt am Sonntag 07 Jan 2018, S.42

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

Gartmann, F., Jahn, T. (2013): Die Geheim-Dienstleister. Handelsblatt 26.06.2013, S.24

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.

Gebauer, M. et al. (2016): Kühler Krieg. Der Spiegel 39/2016, S.14-20

Gebauer, M., Wolfangel, E. (2017): Wer war das? Die Zeit 01 Juni 2017, S.31-32

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

Gerden, E. (2015): Russia to ramp up spending on military science. Chemistry World online 02 Sep 2015

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.

Giesen, C., Mascolo, G. and Tanriverdi, H. (2018): Hört, hört. Süddeutsche Zeitung 14.12.2018, S.3

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

Goetz, J., Steinke, R. (2017): Geheimnisse aus Tresor Nummer 7. Süddeutsche Zeitung Nr. 58/2017, S.7

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.

Goodin, D. (2017): Advanced CIA firmware has infected Wi-Fi routers for years. Ars Technica 16 Juni 2017

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

Gräfe, D., Link, C. und Schulzki-Haddouti, C. (2018): Das ist über den Hackerangriff bekannt. Stuttgarter Nachrichten online 01.03.2018

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

GReAT (2018): OlympicDestroyer is here to trick the industry. 08 March 2018

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

Gruber, A., Reinhold, F. (2017): Was die Whistleblowerin Reality Winner enthüllte. Spiegel online 06 Juni 2017

Grüner, S. (2019): ME-Hacker finden Logikanalysator in Intel-CPUs. Golem.de 01 April 2019

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

Gyr, M. (2016): Geheime Daten aus dem Innersten des Nachrichtendiensts entwendet. Neue Zürcher Zeitung 11 Nov 2016, S.29

Hacquebord, F. (2017): Zwei Jahre Pawn Storm. Analyse einer mehr in den Mittelpunkt rückenden Bedrohung. Forward-Looking Threat Research (FTR) Team, TrendLabs Forschungspapier 2017, 37 Seiten

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

Harris, S., McMillan, R. (2017): Authorities Question CIA Contractors in Connection with Wikileaks Dump. Wall Street Journal 11 März 2017

Häuptli, L. (2018): Chinesen spionieren in der Schweiz. Neue Zürcher Zeitung 08.01.2018, S.1

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

HCSEC (2019): Official Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. Annual Report 2019. A report to the National Security Adviser of the United Kingdom March 2019

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.

Heighton, L. (2016): Second referendum petition: Inquire removes at least 77,000 fake signatures, as hacker claim responsibility for ‚prank'. The Telegraph 27 Juni 2016 online

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

Hern, A., Gibbs, S. (2017): What is WanaCryptOR 2.0 ransomware and why it is attacking the NHS? The Guardian 12 Mai 2017

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

Holland, M. (2018): Fitnesstracker: Strava-Aktivitätenkarte legt Militärbasen und Soldateninfos in aller Welt offen. Heise online 29 Jan 2018

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

Hunt, A. Gentzkow, M. (2017): Social Media and Fake News in the 2016 election Paper of Stanford and New York University 40 Seiten

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

Insikt group (2018): Chinese Threat Actor TEMP.Periscope targets UK-based engineering company using Russian APT techniques. Recorded Future Blog 13 November 2018

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

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

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. (2016): Der Feind in meinem Herzschrittmacher. Frankfurter Allgemeine Zeitung 09 Okt 2016, S.22

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

Jansen, J. (2017): Hunderte Millionen Smartphones ausspioniert. Frankfurter Allgemeine Zeitung 28.08.2017, S.22

JAR (2016): Grizzly Steppe –Russian Malicious Cyber Activity. JAR-16-20296, December 29, 2016, 13 S.

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

Johnson, A. et al. (2013): Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. US Naval Research Laboratory.

Johnson, RF (2016): Experts: The US has fallen dangerously behind Russia in cyber warfare capabilities The Washington Free Beacon 27 Jul 2016

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

Jung, M., Jansen, J. (2017): Telekom-Hacker bereut seineTat vor Gericht. Frankfurter Allgemeine Zeitung 22.07.2017, S.24

Kant, A. (2018): Nordkoreanische Hacker nutzen Zero-Day-Lücke aus. Netzwelt 05 Feb 2018

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 (2013): “Winnti” Just more than a game. April 2013, 80 S. und Appendix

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

Kaspersky (2016): The Project Sauron APT August 2016, 14 S.

Kaspersky (2017a): Securelist BlueNoroff/Lazarus watering hole attack was detected in Poland on 03 Feb 2017

Kaspersky (2017b): Securelist blog on 27 Juni 2017

Kaspersky (2018a): The Slingshot APT Version 1.0 06 March 2018

Kaspersky (2018b): An overview of the Lamberts. Securelist.com

Kaspersky Lab (2017): Investigation Report for the September 2014 Equation malware detection incident in the US. 16 Nov 2017

Kim, C. (2017): North Korea hacking increasingly focused on making money more than espionage: South Korea study. Reuters 28 Jul 2017

Kirchner, T., Mühlauer, A. und Steinke, R. (2017): Hacken und doch nicht gehackt werden. Süddeutsche Zeitung Nr. 213, 15.09.2017, S.5

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

Kling, B. (2017a): NSA Exploits: Eternal Rocks nutzt mehr Schwachstellen als WannaCry. 23 Mai 2017 ZDNet

Kling, B. (2017b): Malware Amnesia bildet IoT/Linux Botnet. ZDNet 07 Apr 2017

Kling, B. (2017c): NSA-Leak: Kaspersky veröffentlicht Untersuchungsergebnis. ZDNet 16 Nov 2017

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

Kolokhytas, P: (2017): CIA Malware Athena kann alle Windows-PCs ausspionieren. PCWelt 22 Mai 2017

Kramer, A. (2016): How Russia Recruited Elite Hackers for Cyberwar. New York Times 29.12.2016

Kramer, A. (2017): Hacker-Gruppe Shadow Brokers veröffentlicht NSA-Tools. Heise online 09 April 2017

KrebsonSecurity (2016): Carbanak Gang Tied to Russian Security Firm? Official Security Blog of Brian Krebs 2016

KrebsonSecurity (2017): Who is Anna Sempai, the Mirai Worm author? Official Security Blog of Brian Krebs 20.02.2017

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

Krupovic, M et al. (2016): A classification system for virophages and satellite viruses. Arch Virol (2016) 161:233–247

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

Kurz, C. (2017): Jetzt ist es an der Zeit, die Lücken zu schließen. Frankfurter Allgemeine Zeitung No. 31, 06.02.2017, S.13

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

Langer, M.A. (2018a): Schwerer Hackerangriff auf Marriot Hotel Gruppe Neue Zürcher Zeitung 03.12.2018, S.11

Langer, M.A. (2018b): Pekings Hacker unter Verdacht. Neue Zürcher Zeitung 14 Dec 2018, S.3

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

Lawfare (2019): France's New Offensive Cyber Doctrine – Lawfare lawfareblog.com 26 Feb 2019

Lee, M. et al. (2017): Wanna Cry? TALOS Intelligence Blog Mai 2017

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

Leyden, J., Williams, C. (2018): Kernel memory-leaking Intel processor design flaw forces Linux, Windows redesign. The Register 02 Jan 2018

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

Limonier, K. (2017): Silicon Moskau, Le Monde Diplomatique Deutsche Ausgabe August 2017, S.1 und 18-19

Lindner, M. (2017): Wenn der Hacker mitbehandelt. Neue Zürcher Zeitung 24 Mai 2017

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

Lohse, E. (2016): Krieg der Sterne. Frankfurter Allgemeine Zeitung 206/2016, S.4

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

Lubold, G., Harris, S. (2017): Russian Hackers stole NSA data on US Cyber Defense. The Wall Street Journal online 05 Oct 2017

Ludwig, J. Weimer, S. (2019): Aufruhr um Datendiebstahl. Neue Westfälische 07.01.2019, S.2

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

Ma, A. (2019): Russia plans to disconnect the entire country from the internet to simulate an all-out cyberwar . Business Insider online Feb 2019

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.

Marimov, AE (2017): Ex-NSA contractor pleaded not guilty to spying charges in federal court. Washington Post 14 Feb 2017

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.

Mascolo, G., Steinke, R. (2019): Lizenz zum Löschen. Süddeutsche Zeitung Nr. 109, 11/12 Mai 2019, S.9

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

Mazzetti, M. et al. (2017): Killing CIA Informants, China crippled US spying operations. New York Times 20 Mai 2017

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

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

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

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

Menn, J. (2018): China-based campaign breached satellite, defense companies: Symantec. Reuters online 19 June 2018

Merkur (2019): Hackerangriff auf deutsche Politiker LiveBlog. Merkur.de online 04.01.2019

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

Mikelionis, L. (2018): Ex-NSA contractor to plead guilty to breathtaking heist of top-secret data. Fox News 04 Jan 2018

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

Miller, G. et al. (2017): Obama‘s secret struggle to punish Russia for Putins election assault. The Washington Post online 23 June 2017

Miller, S. et al. (2019): Triton Actor TTP Profile, Custom Attack Tools, Detections and Attack mapping. Fireye 10 April 2019

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

Mueller, R.S. (2018): Indictment in the United States District Court for The District of Columbia. Received 13 July 2018

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

Müller, G.V. (2016): Der Verpächter des Internets. Neue Zürcher Zeitung, 01.11.2016, S.7

Müller, M. (2016): Die chinesische Datenkrake wächst. Neue Zürcher Zeitung 09 Nov 2016, S.3

Müller, G. (2019): Firmen gehen beim Cloud-Computing unkalkulierbare Risiken ein. Neue Zürcher Zeitung, 18 Mai 2019, S.14

Müller, M. (2019): Die Sanktionen der USA gefährden den weiteren Aufstieg Huaweis. Neue Zürcher Zeitung 22 Mai 2019, S.9

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.

Nakashima, E. et al. (2017): NSA officials worried about the day its potent hacking tool would get loose. Then it did. Washington Post 16 Mai 2017

Nakashima, E. (2018): National Security - Russian military was behind ‘NotPetya’ cyberattack in Ukraine, CIA concludes. Washington Post online, 12 Jan 2018

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

Neuroth, O. (2017): Appetit auf Plastiktüten. Tagesschau online 24 Apr 2017

Niewald, L.V. (2018): Alexa, wie gefährlich bist Du? Neue Westfälische 26 Oct 2018

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

NZZ (2016): Malware knackt Android Handys. Neue Zürcher Zeitung 03 Dez 2016, S.20

NZZ (2017a): Überschätzte Fake-News. Neue Zürcher Zeitung 24 Januar 2017, S.32

NZZ (2017b): Die USA klagen chinesische Hacker an. NZZ 30.11.2017, S.3

Orcutt, M. (2019): Once hailed as unhackable, blockchains are now getting hacked. MIT Technology Review online 19 Feb 2019

ODNI (2017): Intelligence Community Assessement Assessing Russian Activities in Recent US Elections, 14 pages

O’Leary, J. et al. (2017): Insights into Iranian Cyber espionage: APT 33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware. FireEye Blog 20.09.2017

O’Neill, PH and Bing, C. (2017): WannaCry ransomware shares code with North Korean malware. Cyberscoop 15 Mai 2017

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

Osterloh, F. (2017): Schützenswerter Kernbereich festgelegt. Deutsches Ärzteblatt Nr.24 16 Juni 2017, S.B795

Paganini, P. (2018a): The Dutch Intelligence AIVD ‚hacked' Russian Cozy Bears for years. Securityaffairs.co from 26 Jan 2018 Securelist.com

Paganini, P. (2018b): Experts from Kaspersky highlighted a shift focus in the Sofacy's APT group's interest, from NATO member countries and Ukraine to towards the Middle East and Central Asia. Securityaffairs.co from 21 Feb 2018 Securelist.com

Paletta, D.Ä, Schwartz, F. (2016): Pentagon deploys cyberweapons against Islamic State. Wall Street Journal online 29.02.2016, article 1456768428, 4 S.

PandaSecurity (2017): Adylkuzz, the malware that steals virtual money from thousands of computers. 22 Mai 2017

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

Park, J., Pearson J. (2017): Exclusive: North Koreas Unit 180, the cyber warfare cell that worries the West. Reuters 21 Mai 2017

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

Perloth, N. (2017a): Russian hackers who targeted Clinton appear to attack France's Macron. New York Times 24 Apr 2017

Perloth, N. (2017b): Hackers are targeting Nculear Facilities, Homeland Security Dept and FBI say. New York Times 06 Jul 2017

Perloth, N. Sanger, D. (2017): In Computer Attacks, Clues Point to a Frequent Culprit: North Korea New York Times 15 Mai 2017

Perloth, N., Shane, S. (2017): How Israel caught Russian hackers scouring the world for US Secrets New York Times online, 10 Oct 2017

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

Pinkert, H., Tanriverdi, H., Von Bullion, C. (2018): Schläfer im Datennetz. Süddeutsche Zeitung 03/04.03.2018, S.8

Plan, F. et al. (2019): APT 40: Examining a China-Nexus Espionage Actor FireEye 04 Mar 2019

Poddebniak, D. et al. (2018): Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels (draft 0.9.0) Universities of Bochum/Muenster/Leuven 17 May 2018

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.

PwC/BAE Systems (2017): Operation Cloud Hopper PWC in collaboration with BAE Systems Report 25 Seiten April 2017

Quirin, I. (2010): Vorfahrt fürs Netz. FTD Dossier Intelligente Netze 15.10.2010, S.2-7.

RadioFreeEurope (2016): Hacking Group from Russia, China Claims Credit for a Massive Cyberattack. 13.10.2016

Radsan, A.J. (2007): The Unresolved Equation of Espionage and International Law. Michigan Journal of International Law Volume 28, Issue 3, pp.596-623

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

Reuters (2017a): German parliament foiled cyber attack by hackers via Isreali website 29 März 2017

Reuters (2017b): Under pressure, Western tech firms bow to Russian demands to share cyber secrets. 23 Juni 2017

Reuters (2017c): Russian firm provides new internet connection to North Korea. 03.10.2017

Reuters World News (2017): China's economic cyber espionage plummets in US: cyber experts.

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

Robertson, J., Riley, M. (2018): How China used a tiny chip to infiltrate America's top companies. Bloomberg Businessweek 04 Oct 2018

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.

Rötzer, F. (2018): Wer wird zuerst eine EMP-Waffe einsetzen? Heise online 01 Jan 2018

Rogers, J. (2009): From Suez to Shanghai: the European Union and Eurasian maritime security. Occasional Paper - n°77, March 2009

Rohde, D. (2016): Is the CIA ready for the age of Cyberwar? The Atlantic online 02 Nov 2016

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

Rosenbach, M. (2016): Hacker aus dem Staatsdienst. Der Spiegel 40/2016, S.78-79

Rosenbach, M. (2019): Zugriff aus Fernost. Der Spiegel 21/2019, S.74-76

Ross, M. (2016): Global Government Forum - UK Defence Intelligence to establish new cyber warfare unit. 24 Feb 2016

RP online (2018): Forscher hacken sich selbst und entdecken Meltdown. 05 Jan 2018

Rüb, M. (2010): Jenseits der Partnerschaftsrhetorik. Frankfurter Allgemeine Zeitung Nr. 129/2010, S.5

Rüesch, A. (2018): Die Jagd nach Putins Agenten. Neue Zürcher Zeitung, 19.10.2018, S.4-5

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

Russia Today (RT Deutsch) online (2017): Russland: FSB und Kaspersky Lab in Erklärungsnot – Landesverrat im Bereich Cybersicherheit vermutet. 27.01.2017

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.

Sanger, D.E. and Broad, W.J. (2017): Trump inherits a Secret Cyberwar Against North Korean Missiles. NY Times 04 März 2017 online

Sanger, D.E., Perlroth, N. (2019): U.S. escalates online attacks on Russia's power grid. New York Times 15 Jun 2019

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.

Scherschel, F. (2017a): Industroyer: Fortgeschrittene Malware soll Energieversorgung in der Ukraine gekappt haben. Heise 12 Juni 2017

Scherschel, F. (2017b): Alles, was wir bisher über den Petya/NotPetya-Ausbruch wissen. 28 Juni 2017

Scherschel, F. (2018): MeltdownPrime and SpectrePrime: Neue Software automatisiert CPU-Angriffe. Heise Security 15.02.2018

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

Schmiechen, F. (2019): Deutschland ist ein leichtes Opfer Bild 05.01.2019, S.2

Schmieder, J. (2017): Bizarro und die Cyberattacken. Süddeutsche Zeitung 29 März 2017, S.74

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

Scholl-Trautmann, A. (2017): Kaspersky Lab identifiziert 8 auf Ransomware spezialisierte Gruppen, u.a. PetrWrap, Mamba und sechs weitere Gruppen ZDNet

SC Magazine (2015): Research Squadrons to raise IT capability of Russian army. 09 Dec 2015

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

Schmidt, J. (2017): Hardware Fuzzing: Hintertüren und Fehler in CPUs aufspüren. Heise online 23.08.2017

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

Schubert, K. (2019): Als Martin Schulz Nachrichten von Fremden bekommt. Heute.de 04.01.2019

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.

Securelist (2019): OperationShadowhammer 25 March 2019

SecurityWeek online (2017): Poland Banks attack part of a bigger campaign targeting over 100 organizations.

Seliger, M. (2018): Datenstaubsauger mit Anleitung. Frankfurter Allgemeine Zeitung, 20.06.2018, S.4

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

Shane, S., Mazetti, M., Rosenberg, M. (2017): Wikileaks releases trove of alleged CIA Documents Washington Post 07 März 2017

Shane, S., Perloth, N., Sanger, D.E. (2017): Security Breach and Spilled Secrets have shaken the NSA to its core. New York Times online 12 Nov 2017

Shalal, A. (2016): IAEA chief: Nuclear power plant was disrupted by cyber attack. Reuters 10 Okt 2016

Sharma, D. (2011): China's Cyber Warfare Capability and India's Concerns. Journal of Defence Studies 2011, S.62-76

Shekhar, S. (2017): The India-Pakistan cyber war intensifies as retaliatory ransomware attack crippled websites of Islamabad, Multan and Karachi airports. Mail online India 02 Januar 2017

Shields, N.P. (2018): Criminal Complaint United States vs. Park Jun Hyok at the United States District Court for The District of Columbia. Received 08 Jun 2018, 179 pages

Shuster, S. (2016): Hacker Kremlin Emails could signal a turn in the U.S.-Russia Cyberwar. Time Magazine online 07.11.2016

Siegel, J. (2018a): Verschlüsselte emails nicht mehr sicher. Neue Zürcher Zeitung 16.05.2018, S.20

Siegel, J. (2018b): Mehr Sicherheit für das Internet der Dinge. Neue Zürcher Zeitung, 29.10.2018, S.18

Singer, P.W. (2010): Der ferngesteuerte Krieg. Spektrum der Wissenschaft Dezember 2010, S.70-79

Sokolov, D. (2017): USA - Cybersoldaten an die Front. Heise online 14 Dec 17

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

Spehr, M. (2015): Ausgespäht mit Android. Frankfurter Allgemeine Zeitung 04.08.2015, Nr. 187/2015, S.T4

Spehr, M. (2017): Jeder Schritt zählt. Frankfurter Allgemeine Zeitung 25 Okt 2016, S. T1

Spetalnick, M. (2019): Russian deployment in Venezuela includes 'cybersecurity personnel', U.S. official Reuters.com 26 Mar 2019

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 online (2016): Hackergruppe Shadow Brokers: NSA soll Uniserver für Angriffe genutzt haben. 01 Nov 2016

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.

Spiegel (2018): Chinesische Hacker stehlen geheime US-Pläne für U-Boot-Waffensystem. Spiegel online 09.06.2018

Stabenow, M. (2017): Warnung in roten Lettern. Frankfurter Allgemeine Zeitung 25 Januar 2017, S.3

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

Steier, H. (2017): Cyber-Angriff verursacht Chaos. Neue Zürcher Zeitung 15 Mai 2017, S.1

Steinitz, D. (2014): Großes Drama. Süddeutsche Zeitung Nr. 296 vom 19.12.2014, S.11

Steinke, R. (2017): Die dunkle Seite des Netzes. Süddeutsche Zeitung Nr. 155/2017, S.6

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 (2016a): The Waterbug attack group. Security Response Version 1.02 Symantec, 14.01.2016, 44 Seiten

Symantec (2016b): Strider: Cyberespionage group turns eye of Sauron on targets, Symantec Official Blog, 07.08.2016

Symantec (2016c): Odinaff: New Trojan used in high level financial attacks, Symantec Official Blog, 11.10.2016

Symantec (2017): Longhorn: Tools used by cyberespionage group linked to Vault 7. 10 Apr 2017

SZ (2013):Wie CIA und Co. heikle Aufträge zivilen Firmen überlassen. Süddeutsche Zeitung Nr. 265, 16/17 Nov 2013, S.8-9

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

SZ online (2017): Verunglückter Tesla-Fahrer ignorierte Hinweise des Autopiloten. 20 June 2017

T-online (2015): Apple löscht über 250 Spionage-Apps aus App-Store, 2 S. Artikel id_75824954

T-online exklusiv (2019): So begründet der Hacker seine Aktion. T-online Exklusivinterview mit Tomasz Niemiec. 04 Jan 2019, 14 Uhr

T-online (2019): Medien: Polizei durchsucht Wohnung in Heilbronn. 07 Jan 2019

Tanriverdi, H. (2017): Hackerangriff auf den Bundestag. Süddeutsche Zeitung, 29. März 2017, S.5

Tagesschau (2015): Umbaupläne vorgestellt: Bei der CIA soll vieles anders werden. Tagesschau.de 07.03.2015, 1 Seite.

Tagesschau (2018): Microsoft wehrt Hackerangriff ab. Tagesschau online 21.08.2018

Tagesschau online (2019): Spionage im Steakhaus? Tagesschau online 09.02.2019

Talos Cooperation (2012): Transportable Autonomous Patrol for Land Border Surveillance D.10.3 4th Workshop 25.05.2012

Talos (2018): VPN Filter. Talos Threat Intelligence Blog 23 May 2018

TAZ online (2013): China testet das “scharfe Schwert”. 23.11.2013, 4 Seiten

Technology review (2018): Russian hackers are accused of infecting three Eastern European companies with malware. Technology review.com 18 Oct 2018

Tellenbach, B. (2017): Darknet macht keine neuen Kriminellen. Neue Zürcher Zeitung 17.02.2017, S.31

The Australian (2017): US move to boost cyber war capacity. 17 July 2017

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

The Telegraph (2017): The Football Association disappointed as Fancy Bears leak anti-doping records 22 August 2017

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

Threat Connect (2016): ThreatConnect discovers Chinese APT activity in Europe 17 Okt 2016

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

UK Government (2016): National Cyber Security Strategy 2016

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.

Van Lijnden, C. (2019): Ein fast perfektes Spiel Frankfurter Allgemeine Zeitung 07.01.2019, S.2

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

WADA (2016): WADA statement regarding additional data leak via Russian hacker Fancy Bear 09/2016

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

Weber, S. et al. (2018): Meltdown & Spectre: Details und Benchmarks zu den Sicherheitslücken in CPUs. Computerbase online 04 Jan 18

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

Wehner, M. (2016): Häck auf Beck. Frankfurter Allgemeine Sonntagszeitung Dez 2016, S.9

Weidemann, A. (2017a): Spion sieht Spion sieht Spion. Frankfurter Allgemeine Zeitung 02 11.2017, S.15

Weidemann, A. (2017b): Greift Iran jetzt an? Frankfurter Allgemeine Zeitung 20.12.2017, S.15

Welch, C. (2018): Play Station4 reportedly crashing due to malicious message. The Verge online, 13.10.2018

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

Welchering, P. (2017): Cyberwar in der Luft - Hacker warnen vor Angriffen. Heute online Mai 2017

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

Welt online (2019): USA führen Cyberangriffe gegen den Iran aus. 22 Jun 2019

Welter, P. (2018): Hackerangriff trifft japanische Krypto-Börse. Neue Zürcher Zeitung 30 Jan 2018, S.8

Wendt, J. (2014): Geheimdienste - Das Cyber-Konglomerat. Die Zeit online 01 Aug 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

WinFuture (2017): Immer mehr: Geleakte NSA-Hackersoftware infiziert Windows-PCs 24 April 2017

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

Winkler, P. (2018): Spionageaffäre verblüfft die USA. Neue Zürcher Zeitung 19 Jan 2018, S.3

Wired (2019): What Israel's Strike on Hamas Hackers means for Cyberwar. Wired online May 2019.

Wittmann, J. (2017): Gesucht: Bond. Jane Bond. Neue Westfälische 11.02.2017

Wolfangel, E. (2017): Social Bots Eine Armee virtueller Schläferagenten. Spektrum der Wissenschaft 7/17, S.27-29

Woolley, SC, Howard, PN. (2017): Computational Propaganda –worldwide– Executive Summary. Working Paper Nr. 2017.11 University of Oxford, Project on Computational Propaganda 2017, 15 Seiten

Wong, E. (2013): Espionage Suspected in China`s drone bid. New York Times international Weekly 27 Sep 2013, S.1 and S.4

Wüllenkemper, C. (2017): Wir haben es mit medialem Krieg zu tun. Frankfurter Allgemeine Zeitung 27 Januar 2017, S.15

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

Zeit online (2016a): Mögliche CyberAttacke soll Russland bloßstellen. Oktober 2016, 2 S.

Zeit online (2016b): Atemberaubender Computerschwund in britischem Verteidigungsministerium 22 Dec 2016

Zeit online (2017): Ermittler decken riesiges Netzwerk für Phishing und Betrug auf. 04.12.2017

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

Zhang, L. (2012): A Chinese perspective on cyber war. International Review of the Red CrossVolume 94 Number 886 Summer 2012 p.801-807

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