Cyber war

Methods and Practice

Version 12.0 – 07 Sep 2016

Summary

Computer and internet security is under discussion due to the increasing relevance of the Internet and of the information and communication technology (ICT). The cyberspace is meanwhile regarded as separate military dimension. This paper gives an overview on the methods and practice of cyber war and presents the cyber war activities since 1998 and the security architecture of the cyberspace. Finally, the cyber war strategies of the United States, China and Russia and the cyber policies of the European and African Union are discussed.

Table of Contents

1. Fundamentals

1.1 Introduction

Computer and internet security is under discussion due to the increasing relevance of the Internet and of the information and communication technology (ICT). The cyberspace is meanwhile regarded as separate military dimension[1]. This paper gives an overview on the methods and practice of cyber war and presents the cyber war activities since 1998 and the security architecture of the cyberspace. Finally, the cyber war strategies of the United States, China and Russia and the cyber policies of the European and African Union are discussed.

1.2 Background

The increasing dependence on computers and the increasing relevance of the Internet by the increasing number at users and available information are well-known. However, the intensive use of network-dependent technologies increased the susceptibility of states for attacks within the last years.

An increased risk for cyber attacks results in particular from:

- The Next or **New Generation Network NGN** where television, internet and phone submit their data packets via the internet protocol IP (**Triple-Play**).
- In the **Internet of Things IoT**, things (machines and goods) get IP-addresses to localize and track them, to receive status reports and so on. Also machines and devices with **Radiofrequency Identification (RFID)**-chips can communicate with computers and with each other[2]. The car-to-car-communication is another planned feature which may lead to a massive expansion of IoT applications[3].
- Remote control and maintenance of industry machines by Industrial Control Systems ICS or **Supervisory Control and Data Acquisition SCADA** allow the communication with machines via internet.
- The combination of machine-to-machine communication, Internet of Things and SCADA systems are key elements of **cyber-physical systems**

[1] USAF 2010a, DoD 2011

[2] The Machine-to-Machine (M2M) communication potentially concerns 50-70 billion 'machines', of which only 1 % are connected today EU 2009a, p.2. In a Swedish company, employees got a chip implanted as identification key for door and devices. The information may however be taken by a handshake of a person with a small sender, Astheimer/Balzter 2015, p.C1. RFIDs are a subtype of **smart cards**.

[3] Quirin 2010, p.2f.

CPS, where production processes are increasingly managed and modified by a network of machines, products and materials[4].

- Further extensions of the net are intelligent household appliances and electric meters (**smart grid**) [5] and the use of external computing centers via the Internet instead of using own capacities (**cloud computing**[6])
- The introduction of mobile phones with internet access (**smartphones**[7]), which integrate the functions of navigation equipment (Global Positioning System GPS location data) and are used as key device in the **'bring your own device (BYOD)'** concept that describes the option for wireless coordination of multiple devices and machine, e.g. within **smart homes**.
- The trend is going forward from **smarter cities** with enhanced infrastructure up to **smart cities** where the entire city has a preplanned IT platform for all relevant urban functions.[8]
- The network based or **network centric warfare** is also a source of new problems such as security and stability of flying computer networks in the air force[9].

These developments and the dependence on information technology massively increase the vulnerability of critical infrastructures (CII)[10]. On the other hand, the execution of an attack is relatively simple[11].

---

[4] Synonyms are Smart factory, Integrated Industry or Industry 4.0 (after mechanization, electricity and standardized mass production).

[5] In early 2013, the European energy supplier organization Entso-e presented plans for remote control of large household devices (like refrigerators) for all citizens of European Union so that energy companies can modify or switch off devices in case of energy shortages; this would also create a new large-scale vulnerability; Schelf 2013, p.1. The German government supports this plan, Neubacher 2013, p.82

[6] Postinett 2008, p.12, Knop 2010, p.14. Risks of cloud computing are e.g. the storage of data on foreign computers that are subject to foreign legislation. Also, this may lead to political influence; refer to FAZ 2010f, p.17. The cloud provider represents an additional entrance gate for attacks, with may be difficult to control by the outsourcing company, Menn 2010, p.H12-H13. In addition, cloud providers may look into the data of their users to scan and analyze them, also they can disconnect accounts under certain circumstances, Postinett 2013b, p.12

[7] For android smartphones, more than one million virus variants resulting from adaptive ('mutating') viruses are known, FAZ 2013b, p.21

[8] Currently, Masdar City in Abu Dhabi and New Songdo in South Korea are under construction. The IT of New Songdo is constructed by Cisco, Frei 2015, p.27

[9] Grant 2010

[10] Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for: electricity generation, transmission and distribution; gas production, transport and distribution; oil and oil products production, transport and distribution; telecommunication; water supply (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices); agriculture, food production and distribution; heating (e.g. natural gas, fuel oil, district heating); public health (hospitals, ambulances); transportation systems (fuel supply, railway network, airports, harbors, inland shipping); financial services (banking, clearing); security services (police, military).

[11] Megill 2005, DoD 2011

- The attacks can be started from a long distance. A certain technical know-how is needed, but attacks can be conducted with less material and logistic efforts than conventional attacks
- This allows asymmetric attacks of small groups against large targets
- The notification of an attack and the identification of the attacking person/group is very difficult if the attack is well prepared (**attribution problem**), which makes deterrence and counterstrikes much more difficult.

In literature, there is no agreement when the first cyber war took place, but the first activities discussed in this context began already in the year 1998 with the operation **Moonlight Maze**.

1.3 Definition

The term **Cyber war** (also cyberwar, cyber warfare, computer warfare, computer network warfare) is a combination of the terms war and cyberspace and designates the military conflict with the means of the information technology. In practice, this is the attack on computers and their data, the computer network and the systems dependent on the computers[12].

War is the conflict between 2 states, so it is sometimes doubted whether there were any cyber wars at all and whether cyber war can be done as an independent conflict[13].
However, most authors believe that large-scale cyber attacks cannot be done without governmental support due to the required resources and the possible political consequences. Therefore, some large-scale cyber attacks are presented in literature as cyber war even when the aggressor could not be clearly identified.

Generally attacks on computers, information, networks and computer-dependent systems are called **cyber attacks**. Cyber attacks can also be of private, commercial or criminal nature, but in all types of attack the same technical methods are used, which makes the identification of the aggressor and the motives very difficult or even impossible.
If the attack has a terrorist background, the attack is called **cyber terrorism**, if the primary aim is illegitimate acquisition of information, it is called **cyber espionage**. Cyber terrorism and espionage are both illegal, however the term cyber crime is mostly used for 'normal' crimes like theft of money by abuse of online banking data[14].
In contrast to cyber war, cyber espionage tries to avoid damage of the attacked system to avoid detection and to ensure information flow after intrusion, i.e. it is a more ‚passive' form of an attack[15]. However, large-scale cyber espionage can lead

[12] Wilson 2008, p.3ff.
[13] also CSS 2010, Libicki 2009, p. XIV
[14] also Mehan 2008, CSS 2010
[15] Libicki 2009, p.23

to significant computer and network problems and is then often assigned to cyber war by literature, too.

In summary, there is an overlap between terms and definitions and the attribution of an incident to a certain kind of attack or aggressor may be very difficult. Without evidence, it should be avoided to accuse other states or governments.

1.4 The general concept of cyber war

1.4.1 Basic principles

The networking of computers in a protected Internet environment with general improvements of encryption tools and pattern recognition as well as the Global Positioning system (GPS) are the technical basis for a multiplicity of technical and strategic innovations, which are summarized in the USA under the term **Revolution in Military Affairs (RMA)**[16].

Applications are in particular

- the **Airborne Early Warning and Control System (AWACS)**, which allows radar surveillance via airplanes,
- the **Network based warfare (NBW**) which focuses the **C4ISR** (Command, Control, Computers, Communications, Information for intelligence, surveillance, and reconnaissance)
- the use of **smart weapons** such as smart bombs
- the use of **drones** (Unmanned Aerial Vehicles UAV) or bomb defusors (PackBots[17])
- and the **integrated warfare**.

Drones are not only used for reconnaissance, but also for active fighting against terrorists as already done e.g. in Afghanistan and Pakistan[18]. Drones are used for all kinds of operations that are „dull, dirty, dangerous or difficult“[19]. The practical effect of the drones has led to an increased demand[2021].

In the **integrated warfare** civil issues and actors are already considered in the planning and execution of war and the war is accompanied by a systematic

[16] Neuneck/Alwardt 2008
[17] Hürther 2010, p.33-34
[18] Rüb 2010, p.5
[19] Jahn 2011, p.26
[20] FAZ 2010b, p.6
[21] The trend is to reduce size, as the drone type Rabe that looks like a toy, refer to Singer 2010; the research is also focusing on range, armament and noise, Jahn 2011, p.26. Meanwhile, private drones are available like the French AR-2.0, which can be controlled via smartphone and can fly 50 meters high, Fuest 2012, p.37.

information policy. The systematic embedding of media in the political and military context of a conflict may help to influence the flow and content of information in a positive manner to achieve the goals of the conflict. This holistic approach is also known as **Effects based operations EBO** and aims to achieve **information dominance** at any time on all actors and stakeholders.

The Department of Defense has described the objectives of **Information Operations IO** in detail.[22] Within IO, 5 core capabilities need to be achieved and maintained

- the **psychological operations PSYOP** to achieve information dominance. Further operation types are **counterintelligence (CI)** operations, counter propaganda and **public affairs (PA)** operations[23]
- to mislead the enemy by **military deception MILDEC**, e.g. as the Iraqi air defense systems in the Gulf war[24]
- protection of operations (**Operation Security OPSEC**), e.g. to prevent internet release of sensitive and military relevant information
- the cyber war as **computer network operations (CNO)**. **CNO** can be divided into three subsets: **computer network attacks (CNA)**[25], **computer network exploitation (CNE)** and the countermeasures as **computer network defense (CND)**[26]
- the conventional **electronic warfare (EW**) where the electronic signals of the enemy are e.g. disturbed by jamming.

1.4.2 Cyber war Definition

There are practical problems to answer the question „What is cyber war?“ In addition, there are political and legal concerns, because if an attack fulfills the criteria of a given definition, this may have massive political and military implications[27].

A comparison of cyber war concepts of various NATO states with Russia and China shows different perspectives. In particular, the question whether cyber war is limited to the military conflict dimension or may also include the civil and economic dimensions, is debated[28]. Nevertheless, the USA has worked on a more precise and pragmatic cyber war definition.

[22] Wilson 2007
[23] USAF 2010b, p.5
[24] USAF 2010b, p.32
[25] Wilson 2008
[26] CSS 2010
[27] Beidleman 2009, p.9ff. and p.24
[28] IT Law Wiki 2012a, p.1-4

In 2007, the US Strategic Command USSTRATCOM defined *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*"[29].

General Keith Alexander who was the previous commander of the US Cyber Command CYBERCOM, outlined his perspective on cyber war and emphasized the need to protect the own systems and to ensure the **freedom of action** for the own and allied forces[30]. Cyber war is an integral and *supportive* activity and not a stand-alone military concept. Also, the concept includes defensive and not only offensive components[31]. As a consequence, cyber war is done as common action of humans and computers (computers do not 'on their own') and is usually a group of activities and not only a single hit even if a surprising action may start the war.

This is reflected by the current definition of cyber war of the US Army[32] (note that CyberOps abbreviates the term 'Cyber Operations' and while Global Information Grid 'GIG' means military network):

„Cyber war is the component of CyberOps that extends cyber power beyond the defensive boundaries of the GIG to detect, deter, deny, and defeat adversaries. Cyber war capabilities target computer and telecommunication networks and embedded processors and controllers in equipment, systems and infrastructure."

The definition clarifies that cyber war is not limited to the internet, but includes all kinds of digital technologies[33]. Also, cyber war is only one part of military cyber activities.

In 2014, the NSA and Cybercom command was taken over by Vice Admiral **Michael Rogers**, who is a cryptology expert from them 10th fleet. Rogers emphasized the increasing role and frequency of cyber attacks and reported an intrusion into unsecured sections of the Navy network in 2013 by hackers for the purpose of cyber espionage[34].

[29] Alexander 2007, p.61
[30] Alexander 2007, p.61: "We are developing concepts to address war fighting in cyberspace in order to assure freedom of action in cyberspace for the United States and our allies while denying adversaries and providing cyberspace enabled effects to support operations in other domains."
[31] Alexander 2007, p.60
[32] IT Law Wiki 2012, p.2
[33] See also Beidleman 2009, p.10
[34] Winkler 2014b, p.3

1.4.3 Cyber warfare and International Law

The term 'adversary' in the above definition is used in literature both for state and non-state actors. A non-state actor or his cyber activities may require a military response, if this cannot be handled by police or intelligence alone. Even if war is legally the conflict between states, a cyber war concept has to consider attacks from non-state actors as well.

This leads to the question when the stage of war is reached. As in conventional conflicts, the question whether an incident is a reason for war is a strategic and political decision that cannot be defined upfront in each case. This is also relevant for any counter-reaction, because an attack could also by answered by political sanctions or conventional measures, automatic reactions are problematic due to the escalation potential[35].

Also the **attribution problem**, i.e. to identify the correct source of an attack is legally important, because it is problematic to attack a certain opponent without clear evidence.

To overcome these uncertainties and to avoid uncontrolled escalation of cyber conflicts, the US government started in spring 2012 an initiative to set up **cyber hotlines** (in analogy to the 'red telephones' of the cold war era) with Russia[36] and China[37].

The United Nations Organization International Telecommunications Union (ITU) was mandated at the World Summits on the Information Society 2003 and 2005 to serve the member states as neutral cyber security organization. The ITU coordinated in 2012 the evaluation of the recently discovered spy software Flame[38].

A debate on global **cyber conventions** is ongoing since several years, but as the cyberspace is the only man-made domain, any convention would not only regulate actions *within* the naturally given domain, but could affect or even determine the *structure of the domain itself*[39].

In July 2015, a kind of **cyber convention** was adopted by the United Nations, the consensus report of the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications (ICT). The report includes recommendations for good cyber practices and

[35] Nevertheless, plans for fully computerized counterattacks are under discussion, Nakashima 2012b
[36] Nakashima 2012a
[37] Spiegel online 2012a
[38] ITU 2012
[39] See also Fayutkin 2012, p.2

restrictions[40]. The states should cooperate to increase stability and security in the use of ICT and prevent harmful practices and for this, they should exchange information with other states on all relevant aspects. On the other hand, they should neither support nor conduct any harmful activities to the ICT of other states, prevent the proliferation of malicious functionalities and respect privacy and human rights in internet.
This document was supported by US cyber diplomacy, as in the view of the US, most cyber incidents occur below the 'use of force' threshold (and thus do not permit responses in self-defense); so states need to agree on basic measures of self-restraint during peacetime[41].

The NATO Cyber Defense Centre of Excellence (CCD CoE) presented in 2013 the **Tallinn Manual** on the International Law applicable to Cyber Warfare. The Manual was compiled by an international group of legal experts and covers both the *jus ad bellum* (law related to use of force) and *ius in bello* (international law regulating the conduct of armed conflicts) [42].

Overall, the suggested rules for cyber war are consistent with the conventional international law and in principle, cyber warfare is handled in the same way as other military operations (use of force, rule 11). Per 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*". The key event is however the **cyber attack** that is defined as "*a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction of objects*" (rule 30). Cyber warfare activities can be responded by other military activities (proportionate responses, rule 5.13). However, the proposed rules do not apply to cyber espionage per se (rule 6.4) and an act must be attributable to a state (rule 6.6). Non-state actors may fall under the rules, if the state has effective control over them, i.e. by giving instructions and directions (rules 6.10, 6.11)[43]. According to CCD CoE in February 2016, the development of an updated Tallinn Manual 2.0 is in progress. The NATO now formally considers cyber space as a potential place of military conflicts[44].

[40] UN 2015
[41] Rõigas/Minárik 2015
[42] CCD CoE 2013, Schmitt 2013
[43] In the Manual, the usage of seemingly harmless, but damaging cyber traps (**cyber bobby**) is not acceptable. However, non-damaging defensive traps could be imagined, e.g. a harmless file, placed into sensitive folders with knowledge of the authorized users, indicates an intrusion to administrators if this file is used, e.g. opened, changed, copied or moved.
[44] Gebauer 2016

1.4.4 Cyber warfare and Drones

A special cyber war issue is the progress of the drone technology. Drones allow observation and/or targeted killing of adversaries[45]. However, the technical progress allows more and more **assistance functions**, i.e. the human decision making is increasingly supported and influenced by computers[46]. Meanwhile, the creation of a legal '**machine liability**' is now under discussion[47]. Any progress to fully automated drones would require enhanced cyber security efforts to avoid that machines are taken over by adversary hackers (Section 3.2.9) [48]. Autonomous drones can avoid detection by communication with control station, so this is part of stealth drone concepts such as the **Lijan** drone tested in 2013 by China[49].
The functioning of autonomous devices is dependent on the underlying programs which can result in ethical and practical dilemmas[50]. If the programmed habit is known, e.g. drones (or cars) could be intentionally misled, captured or destroyed by mimicking certain situations or objects.

The drone technology has various vulnerabilities resulting in losses of relevant number of drones. For US, the loss of 5 Global hawks, 73 Predators and 9 Reaper drones was reported, for Germany, the loss of 52 mostly small drones in the previous decade[51]. Mostly, these losses were caused by handling errors and conventional technical problems. Also, loss of communication can enforce the unplanned landing and require destruction, if there is a relevant danger of takeover by adversaries.
A systematic analysis by the *Washington Post* revealed 418 drone crashes from 2001 to 2014, main causes were limited capabilities of camera and sensors to avoid collision, pilot errors, mechanical defects and unreliable communication links[52].

Tests in New Mexico 2012 have shown that drones are vulnerable for **GPS spoofing**. The same could be shown for Automatic Dependent Surveillance

---

[45] Thiel 2012, p.Z2
[46] However, a possible future with fully automated killing decisions remains speculative. The research on **lethal autonomous robots (LARs)** is in progress, Klüver 2013, p.2. Scientists expect that progress in Artificial Intelligence (AI) will soon allow the use of war robots that autonomously decide about fighting and killing. Based on this, AI and robotic researchers proposed a ban of this kind of autonomous weapons in an open letter on 27 July 2015, Future of Life Institute 2015
[47] In the civil sector, this is discussed in US for self-driving cars (i.e., cars with autopilot functions), California plans a respective regulation until 2015, Burianski 2012, p.21
[48] The largest drones are meanwhile able to replace conventional airplanes, i.e. an intrusion could create major security risks. The European drone project **Neuron** is an unmanned aerial combat vehicle (UACV) with stealth technology which may be able to execute larger air attacks than current drones (Bittner/Ladurner 2012, p.3; Hanke 2012, p.14).
[49] TAZ online 2013
[50] Hevelke/Nida-Rümelin 2015, p.82
[51] Gutscher 2013, p.4, Spiegel 2013a, p.11
52 Whitlock 2014

Broadcast systems (ADS-B) that allow tracking of the flight route every second. Also, it was observed that drones can be inadvertently irritated by signals that are intended for other drones.[53]

The company *Airbus* develops a drone defense system with a detection range of 10 kilometers with radar and infrared cameras[54]. The attacking drone can then be deactivated by electromagnetic jamming to disrupt the connection between pilot and drone.
The drone defense research in Germany is going forward to the use of laser weapons. In May 2015, a small quadrocopter drone could be destroyed after application of 20 Kilowatt over 3.4 seconds[55]. However, for larger objects energy levels up to 200 Kilowatt will be needed, the technology is in development.

The trend is going forward to complex **Anti-UAV defense systems (AUDS).** Computers may detect approaching drones by comparison of acoustic patterns, by optical comparison of movement patterns (to distinguish from birds), signal detection and infrared systems. Advanced AUDS combine all these methods[56]. **Geofencing**, i.e. the electromagnetic blockade of no-fly-areas is currently developed. The Dutch police tried to catch and bring down drones by trained eagles.

However, there is also a risk for cyber attacks which may in the long run be the largest threat (Section 3.2.9).

The selling of a certain drone model to more than one state results in sharing knowledge of the capabilities and vulnerabilities[57]. To protect critical knowledge, the **black box-principle** is used by the US, i.e. technology modules e.g. for the EuroFighter, but also for the EuroHawk drones are provided as completed modules without access to foreigners[58]. The same principle is used for submarines of the French company DNCS for India and Australia which was leaked in August 2016 together with many other data. However, DNCS explained that data for Australian submarines type *Barracuda* were not leaked, but only for Indian *Scorpene* submarines[59].

---

[53] Humphreys/Wesson 2014, p.82
[54] Lindner 2016, p.24, Heller 2016, p.68
[55] Marsiske 2016
[56] Brumbacher 2016, p.5
[57] And conventional espionage is still an issue. In Northern Germany, a man was arrested in 2013 who tried to find out vulnerabilities of drones in a drone research unit and who was suspected to work for Pakistan, Focus 2013, p.16. The security company FireEye reported a large-scale espionage campaign against drone technology providers that was suspected to be linked to a Chinese hacker group, named **Operation Beebus**, Wong 2013, p.1/4. Iran's new surveillance drone **Jassir** has similarities to the ScanEagle drone that was captured by Iran, Welt online 2013
[58] Löwenstein 2013, p.5, Hickmann 2013, p.6
[59] Hein/Schubert 2016, p.22

DNCS assumed that the leakage may have been part of an economic warfare by other competitors from Japan and Germany, but the competitors denied or did not comment[60].

The meanwhile suspended[61] EuroHawk drone combined drone technology derived from the Global Hawk drone provided by Northrop Grumann and a new advanced reconnaissance technology called **ISIS** from the EADS affiliate Cassidian. During a flight to Europe, this drone showed temporary losses of communication for a few minutes. As these times may also be potential windows of opportunity for (cyber) attacks from adversaries, cyber security is an essential issue for future drone technologies.

In the European Union, various research projects are evaluating the use of drones which are not steered by a human operator, but by a server for daily routine operations. Relevant projects are INDECT for the internal EU security since 2009[62] and certain others as part of the European Border Surveillance System (EUROSUR) which took place between 2008 and 2012.

The Eurosur projects were in particular[63]:

- OPARUS (Open Architecture for UAV-based Surveillance Systems) for border surveillance by drones that also intends to ensure integration into civil airspace
- TALOS (Transportable autonomous patrol for land border surveillance) with patrol machines
- WIMAAS (Wide Maritime area airborne surveillance) for use of UAVs for maritime control

The concept to conduct daily routine operations of these devices by a control server (**Unmanned Units Command Center UUCC**) was presented as part of these projects, but from a cyber war perspective this would be the key vulnerability and would need to be maximum secure and resilient. The European Union has enhanced their cyber security activities recently as shown in Section 4.5.

[60] FAZ 2016a, p.29

[61] Buchter/Dausend 2013, p.4, Vitzum 2013, p.6. An issue was a missing sense-and-avoid system; details are disputed between involved parties. However, collision prevention and integration into airspace traffic are general challenges for drone technology.

[62] Welchering 2013a, p.T6. The research for automatic threat detection focuses on scenarios like the following one. If a camera observes abnormal behavior of an individual, the combination of automatically activated observation drones, microphones and automated face recognition may help to identify the individual and its intentions. If necessary, it is planned to utilize data from Facebook, Twitter, Google plus, credit card data etc. to identify and prevent dangerous activities.

[63] Oparus 2010, SEC 2011, p.7, Talos Cooperation 2012.

The above border concept is also known as **virtual border** or **virtual wall** and describes the combination of physical barriers with computed surveillance for long borders that are difficult to control. Similar approaches are currently developed in Saudi-Arabia (by EADS) [64] and in certain sectors of the US border[65].
The planned opening of US civil airspace for private drones may lead to a drone boom and will further increase the need for cyber secure drones[66].

[64] Hildebrand 2010, p.6
[65] Miller 2013, p.12-13
[66] Wysling 2014, p.5

2. Methods

2.1 General issues

In general, there are three main types of attacks; these are the physical damage of computers and communication lines, the destruction of transistors by an electromagnetic pulse and the manipulation of computers and networks by malicious software (**malware**).[67]

2.1.1 Physical damage of computers and communication lines

This can be done by destruction and sabotage of hardware, cables, aerials and satellites. To prevent destruction of command and control structures by nuclear weapons, the decentralized computer network ARPANET was created by the USA, which was the very first step to the Internet. As communication lines can also be destroyed by disasters like fire or flooding, it is usual to protect mainframe computers and to have back-up systems, if possible.

2.1.2 Electromagnetic Pulse EMP

Modern electronic devices can be destroyed by electromagnetic waves as they occur during a so-called **electromagnetic pulse EMP**. An EMP could be caused by nuclear weapons, but may also naturally occur as an effect of strong solar storms[68]. The EMP protection is technically possible, but expensive and can only be done for selected systems.

2.1.3 The attack on and manipulation of computers and networks

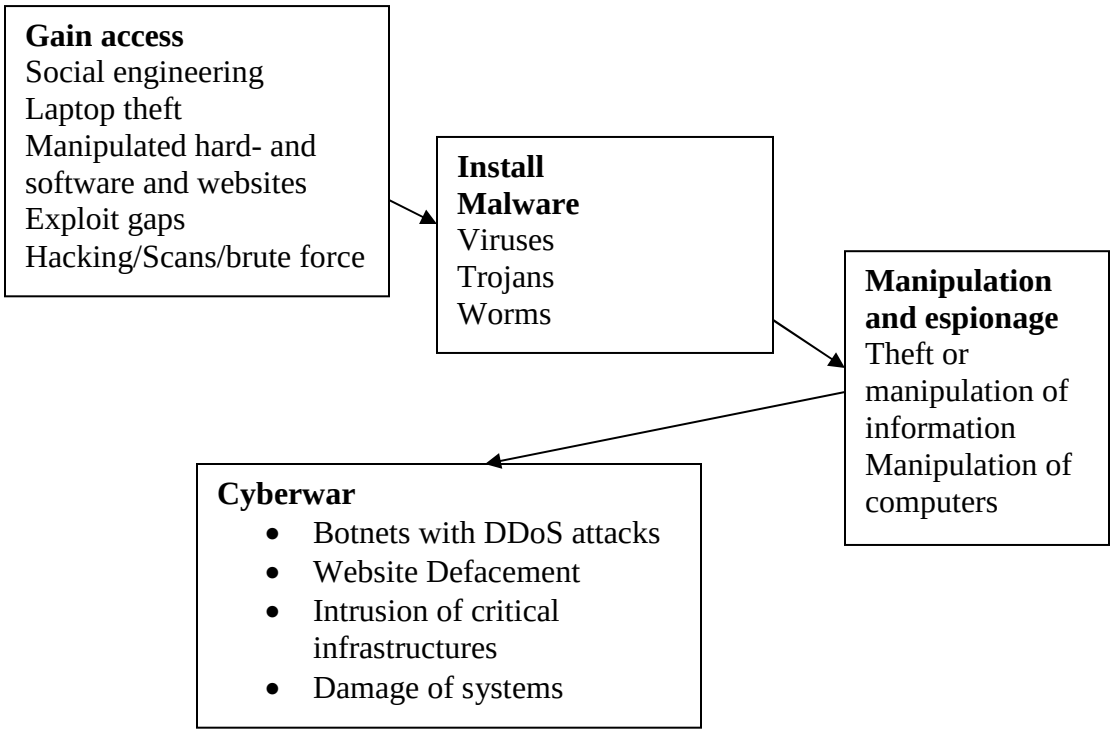
Computers and networks can be attached e.g. by placement of programs (i.e. a set of instructions) on the computer, but also by disturbing communication between computers. Cyber attacks typically use one of these methods or both methods in combination.

2.2 Attack on Computers

2.2.1 Strategy

There is a typical attack strategy: at the beginning, the attacking person or group tries to gain access to the computer and/or the network, then to install malware that can be used to manipulate the computer and/or the data on the computer and/or to steal data. This allows starting further actions which are presented below[69].

[67] Wilson 2008, p.11
[68] Morschhäuser 2014, p. 1-2
[69] Northrop Grumman TASC 2004



2.2.2 Gain access

The following methods are common to gain access:

- the exploitation of security gaps in software programs and operation systems (e.g. Adobe and Windows) that is also known as **exploit problem.** The probing of computers can also be done by port scans[70]. Typically, IT architecture consists of multiple hardware and software components from multiple providers which makes it difficult to keep everything updated. Special programs can scan computers automatically for update status and apply known exploits for intrusion[71].
- **Hacking** of passwords which is increasingly done automatically (**brute force**)
- Intentional misleading of users by **social engineering**, where e.g. wrong 'administrators' ask users for passwords. But insiders, in particular those with IT knowledge can help to breach organizational security, this was discussed in wiper malware attacks, see Section 3.3 below.

[70] A port scanner is a software application that checks a server or host for open ports, i.e. which services a system offers.
[71] Kurz 2013, p.31

- An increasingly used technique is to attack average employees of an organization and then to escalate unprivileged user accounts[72] to administrator rights (**lateral movement**). As a consequence, a more and more systematic collection of personal data by cyber attackers is going on to find people who are relevant and/or vulnerable and/or involved in security matters.[73]
- Also, manipulated emails with malicious attachments and links to malware-containing websites are increasingly used. **Phishing** is a method where users are misled to a malicious website by masquerading as a trustworthy entity to acquire sensitive information such as usernames, passwords and credit card details or to open attachments with malware (tailor-made emails for individual attack are known as **spear-phishing**). **Spoofing** is a situation where a person or program masquerades as another by falsifying data (in particular wrong Internet IP addresses) while **Cross-site-scripting** is a method where computers are infected while being on another website. **Drive-by download** is the unintended download of malware from the Internet during a website visit.
- **Infected data storage media** (such as floppy and hard discs, DVDs and now USB-Sticks) are more 'physical' ways to be infected.
- Also the IT environment can be used for intrusion, such as routers[74], wireless mouses and printers. Increasingly, network and multi-function printers (MFPs) are attack targets, which may allow data capture or reprint of documents[75].
- Another method is **interdiction**, i.e. replacing shipped CD-ROMs and other physical media and replacing them by infected media.
- Also there is a debate on '**backdoors**'[76], i.e. intentionally installed security gaps that allow access for secret services. Microsoft Germany confirmed in January 2007 an official cooperation with the American National Security Agency NSA with regard to the Windows Vista operating system, but

72 Also, one of the largest known cyber crime activities, the theft of 1 Billion Dollars in total from 100 bank institutes worldwide by the **Carbanak** group was done in that way, Bilanz 2015, p.50-57. Also, they took over the video surveillance and could inspect the institutes before proceeding, Kaspersky Lab 2015c, p.1

73 Recent attacks included the **Office of Personnel Management (OPM)** in the United States where in two attack waves approximately 22 million files were stolen, including security checks, medical data, resumes, interviews, and 1.1 million digitalized fingerprints. In 19.7 million cases, dossiers with approximately 100 pages per dossier were copied. Winkler, 2015, p.3. On 23 Sep 2015, the OPM updated the number of stolen fingerprints to 5.6 million. Also, US Dating Portals were intruded, a recent intrusion included registrations from government employees and people from the army, Mayer 2015, p.13. In March 2016, a security gap was reported by a White Hat Hacker which could given him access to all 1.59 billion Facebook accounts. Facebook was notified and closed the gap, SZ online 2016.

74 Handelsblatt 2014 b, p.23

75 Dörfler 2015, p.P4

76 A special variant are **bugdoors**, i.e. programming mistakes (bugs) that can be used as backdoors and which are sometimes intentionally implemented; Kurz 2012, p.33

denied the existence of backdoors[77]. Also, Microsoft has initiated the Government Security Program GSP where governments get insight into 90% of the source code. However, the USA is also afraid of backdoors, in particular in hardware, thus the use of Asian chips is avoided for security-relevant technologies. For the same reason, the US State Department avoids use of Chinese computers within their networks[78]. Nevertheless, military and government cannot produce all hard– and software alone, so the use of commercial off-the-shelf (COTS) technology cannot be avoided and will be a source of vulnerabilities[79]. The global supply chain of such products is also a potential source of vulnerabilities[80]: a study of the US senate from 2012 reported that up to one million falsified chips were installed in US weapons, 70% of these chips came from China, but a significant amount came from UK and Canada also[81]. As each chip has minimal construction differences, these differences can be measured and serve as a kind of unique fingerprint, a **Physically Unclonable Function (PUF)** [82].

- **State Trojans** are Trojans created and/or used by states for surveillance of target computers. But as other backdoor technologies, state Trojans could introduce security gaps in computers which are then at risk to be exploited by third parties.
- As encrypted communication could be used for terrorist activities also, it is essential for intelligence agencies to get access to keys or to the source code of encryption software to have the option to decode encrypted information based on the applicable legal provisions. In Germany, this access is guaranteed by the telecommunication surveillance regulation **Telekommunikations-Überwachungsverordnung (TKÜV)** since 2002. Similar regulations exist worldwide in almost all states, e.g. in the USA, where the **National Security Agency NSA** has access to the source codes of encryption software[83]. The access of national intelligence agencies means that a foreign or international IT platform can be technically accessed by foreign agencies[84].

[77] Die Welt 10 January 2007

[78] USA and India suspected in 2010 the Chinese provider Huawei and its competitor ZTE to have pre-installed espionage software (spyware) in their products. Huawei opened the source code and allowed inspections and this convinced Indian government that Huawei products are secure, Mayer-Kuckuck/Hauschild 2010, p.28. The US authorities instructed Huawei to sell their shares of the Cloud computing company 3Leaf for security reasons; Wanner 2011, p.8

[79] Security issues may exist here as well, e.g. the Software **Carrier IQ**, that was installed on estimated 130 million smartphones and that could track the location and work as keylogger; Postinett 2011, p.32

[80] USAF 2010a, p.5

[81] Fahrion 2012, p.1

[82] Betschon 2016, p.39

[83] Scheidges 2010, p.12-13 Welchering 2013c, p.T2 reported a potential vulnerability of **quantum encryption**. Blinding of photon receivers by light pulses sent by a man in the middle-attack may allow to collect, decrypt and replace photons.

[84] Scheidges 2010, p.12-13

- Meanwhile, it is known that many companies including IT security companies provide information on potential exploits to the intelligence *before* the exploits are published or closed by patches to support intelligence activities[85]. As a practical consequence, user of devices, software or IT security software have to consider the possibility that the intelligence of the manufacturer/provider country *may* have and use access, that by intelligence cooperation[86] an indirect access *may* also exist for further agencies from other countries and that a zero day-exploit *may* not be 'zero' at all. Together with the surveillance of information flow[87] and the above described intelligence access to encryption systems, cyber security *between* computers may also be a problem. Meanwhile, the US government officially confirmed to use exploits. The decision on keeping exploits secret is based on a thorough risk-benefit assessment, i.e. who else could use it, how large is the risk of disclosure and damage to own users and companies[88].
- Another issue is **pre-encryption access**, as providers often decrypt data for internal handling and re-crypt afterwards. By accessing node servers, intruders can bypass encryption. For this reason, some countries asked the Blackberry provider Research in Motion (RIM) in 2010 to put servers into their own countries[89].
- The outsourcing of sensitive IT projects to external providers brings additional risks by creating additional interfaces which may be used for attacks by adversaries[90]. Also, this can lead to loss of internal IT competence.
- A new area of cyber war is **offline-attacks** on computers that are not connected with the internet. Of course, infected USB-sticks can affect every computer, but it was believed than physical distance (air gaps) would ensure a high level of security.

[85] FAZ 2013a, p.1

[86] There is for example the **five eyes-agreement** on intelligence cooperation of the USA, UK, Canada, Australia and New Zealand based on the **UKUSA agreement** from 1946 that was declassified in June 2010. Also, there is e.g. a cooperation between US and German intelligence for surveillance and prevention of terrorist activities, Gujer 2013, p.5. See also Section 2.2.11 for more details.

[87] This includes conventional surveillance of paper-based and analog communication as well as interception of information from optical fibers, Gutschker 2013b, p.7, Welchering 2013b, p.6. Also, in line with respective national law, e.g. the 1994 **Communications Assistance for Law Enforcement Act (CALEA)** and the **Foreign Intelligence Surveillance Act (FISA)** in US, providers may give technical access to data or systems.

[88] Daniel cited in Abendzeitung 2014

[89] Schlüter/Laube 2010, p.8

[90] Some outsourcing examples: Switzerland plans to outsource significant parts of the public IT infrastructure, the German army utilized encryption systems of US providers, Scheidges 2011, p.17, Baumgartner 2013, p.25. The US company CSC helped Germany to implement the public email system De-Mail and the new electronic passport, Fuchs et al. 2013a, p.1 and 2013b, p.8-9.

- After reports about a malware called **BadBios** that was suspected to exchange information via the air in late 2013[91], the New York Times reported a radio pathway into computers and that is used by NSA as part of their active defense (Project **Quantum**). Here, a very small sender covertly placed on the computer or USB sticks is sufficient, the signals with the information can be sent over several miles/kilometers[92]. While the technical details remain unknown, researchers recently showed that a covert acoustical mesh network can be construed in computers via near-field audio communications. The system is based on high-frequency audio signals that can even be used for keylogging over multiple hops[93]. The vulnerabilities are increasing, because computers are increasingly communicating with smartphones, or are e.g. involved in smart home and smart entertainment environments. By this, even the car or the TV[94] can be an entry for an attacker.

2.2.3 Install malware and start manipulation

Cyber espionage may be done for private, commercial, criminal or political reasons and attempts to get sensitive information such as passwords, PIN numbers etc. while cyber war tries to manipulate computer systems actively.
In general, three types of **malware** are most relevant: **viruses** (programs that infect computers), **Trojans** or Trojan horses (programs that report information to other computers) and **worms** (programs that are able to spread actively to other systems). Typically, a malware program consists of two parts, an infection part, that installs the program on a computer and other parts that contain the instructions of the attacker. Meanwhile, it is practice to install a small initial **backdoor program** and to install further parts later that may also allow expanding administrator rights on the infected computer.
Examples for such programs are **keyloggers**, which report any pressed key to another computer which allows to overview all activities and also to register all passwords[95] and **rootkits**, which are tools that allow logins and manipulations by the attacker without knowledge of the legitimate user.

Cyber weapons can be defined as software tools that can attack, intrude, doing espionage and manipulate computers. This type of software is more and more in use and the conventional differentiation between viruses, worms and Trojans is becoming less relevant. The term ‚cyberweapon' does not suggest that this is a

[91] Betschon 2013b, p.34
[92] Winker 2014a, p.3
[93] Hanspach/Goertz 2013, p.758 ff.
[94] Via manipulated video files, Schmundt 2014, p.128
[95] Stark 2009, Schmitt 2009, p.83

military tool, as the technical principles are essentially the same as for software used for cyber crimes.

The most sophisticated cyber weapons are typically used for espionage of high-level targets and with exception of Stuxnet not for destruction. The most advanced show technical similarities (refer also to Section 3.3) which characterize a modern cyber weapon:

Initially, only a small program is loaded which makes intrusion easier. To avoid detection, the malware conducts **self-encryption step**s and creates a **self-deletion** module for the time after completion of espionage. Ideally, this includes the option for **self-deactivation** (going silent). Then, further malware is imported based on the initial information gained. Instead of creating large malware programs, now variable **modules** are uploaded that are tailor-made for the target user and the computing environment. The most advanced malware has a more or less total control of the infected computer and can extract all kind of data. Storage of malware and information is done at uncommon places such as the registry or even in the firmware to avoid detection and removal from the computer. A typical operational step is to escalate unprivileged users to administrator right to gain network control (**lateral movement**). This results in an **Advanced Persistent Threat (APT),** i.e. is the access by unauthorized persons to a network and to stay (persist) there for a longer time. Analysis of malware is impacted by **false flags**, i.e. misleading time stamps and language settings of computer the intruder used for malware creation, in addition, code pieces and terms maybe used that give misleading hints to other attacker groups.
Meanwhile, a new terminology for cyber weapons is emerging; they are sometimes called **digital weapons (d-weapons)**, or **electronic weapons (e-weapons)** or virtual weapons[96].

2.2.4 Cyber war

Distributed Denial of Service (DDoS)-attacks play a key role in cyber war. A DDoS attack is an attempt to make a computer resource unavailable to its intended users by concerted attacks of other computers[97]. The most important tool for a DDoS-attack is a **botnet**.

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

[97] A new form of cyber attack is the **distributed reflected denial of service attack (DRDoS)** where automated requests are sent to a very large number of computers that reply to the requests. Using Internet protocol spoofing, i.e. giving a wrong IP address as the source address all the replies will go to the victim computer (who normally has this address) and overload him. This kind of cyber attack makes attribution (identification of attacker) even more difficult than DDoS.

Computers can be controlled via a distributed software to cooperate with each other to conduct an action that requires large computing capacities[98] (**bot** is derived from robot = worker); the software can operate in the background while the normal programs are running. The coordinated network of bots is the botnet and allows to direct thousands of computers against another systems. Illegal botnets can be even leased today[99].

The dominance of botnets in cyber war is based on the following:

1. botnets are often not located in the country of the attacker which makes localization and attribution of an attack difficult and an immediate counterstrike almost impossible[100]
2. botnets provide large computer capacities needed for a successful attack
3. botnets allow targeted attacks while viruses and worms can spread without control and even affect the own systems/allies
4. the botnet software can theoretically be located in every computer, so it not possible to protect a system by excluding certain groups of computers

Summary: In line with the criteria of Clausewitz for a maneuver botnets can be used for a massive, surprising, efficient and easy manageable attack[101].

Other really used methods are:

- **Website Defacement**, where the look of a website is altered for propaganda reasons
- the infiltration and manipulation of **critical infrastructures** such as radar systems, power grids and power plant control systems
- and the **sabotage** of computer systems, which is often a side effect of massive espionage and subsequent system failures.

New technologies may change the scenario and strategies suddenly and completely so the history of cyber war may not allow to predict the future developments here[102]. However, it can be expected that botnets will be used in future as core tool for large-scale attacks.

---

[98] The first large botnet was intentionally created by volunteers as part of the SETI (Search for Extraterrestrial Intelligence)-Project. The users downloaded a program that allowed to use their computers for analysis of data and to send back the analysis results to SETI.

[99] FAZ 225/2009, In East Asia one can ‚buy' packages of thousand infected computers, to resell them in the Western world for several hundreds of Dollars. It was estimated that the botnet based on Conficker infection consisted of 5 million computers in 122 countries, Wegner 2009.

[100] States may also use informal hacker groups, i.e. specialists who do not work in official positions. In case of a successful attribution, these groups could also serve as 'buffer', i.e. the state can reject the responsibility for an attack, if necessary. Hackers who use their know-how to protect their state, are sometimes called **white hat** or **ethical hackers** in contrast to destructively acting **black hat** hackers.

[101] WhiteWolfSecurity 2007

[102] Gaycken 2009

A subtype of cyber weapon is a **logic bomb**, i.e. a malware that executes actions at a predefined timepoint or after a predefined number of certain computer activities. A recent example of a logic bomb was the data-deleting wiper malware **DarkSeoul** that was activated in March 2013 in all infected computers at the same time[103]. Meanwhile, several destructive attacks with wiper malware were reported, refer to Section 3.3.

A new variant of DDoS is **fake traffic**. In a test, fake traffic software could execute 100,000 clicks on a certain website from one computer, but simulate that each of these clicks came from single different computers, i.e. removing the need for a botnet. Also, it is possible to create large amounts of fake tweets and fake human communication (**socialbots, internet of thingies**)[104].

2.2.5 Attribution

The attribution, i.e. the identification and localization of an attacker to start countermeasures is in important goal, but difficult to achieve.

However, the attribution research is in progress. Instead of immediate shut down of an infected computer, this could be used to find out which information is sent to whom, but often the information flow is going via interim servers („springboard computers“).

Also, hackers create **digital fingerprints**; these are typical program codes or certain access patterns which allow characterizing a certain group of attackers.[105] These patterns can include the use of **malware families** (related sets of malicious codes), use of specific tools or tool combinations, scope of stealing, characteristic encryption algorithms, use of covert communication to control servers (such as mimicking legitimate communications) and language used (incl. typos, styles, preferred terms etc.) [106].

Meanwhile, the **programming styles** of certain programmers are also collected and analyzed, so that any new software programs can be compared with older ones (‘stylometrics’). The NSA e.g. checks for way of setting brackets, use of variable names, empty spaces and programming text structure. Programming pieces are e.g. collected during hacking camps or by collection of informatics students works.

[103] Darnstaedt/Rosenbach/Schmitz 2013, p.76-80
[104] Graff 2014, p.13 Another new trend of bot communication is the creation of automated texts (**bot journalism**), where bots e.g. create weather and sports news without a human journalist involved. Providers of such services are e.g. Narrative Science and Automated Insights, Dörner/Renner 2014, p.18-19
[105] Mayer-Kuckuck/Koenen/Metzger 2012, p.20-21
[106] Mandiant 2013

However, a growing use of **obfuscation software** to replace names and modification of brackets is observed, too[107].

However, this does not allow clarifying whether an attacker worked on behalf of another state or authority.

The attribution business has meanwhile changed. More and more private security firms emerge that collect data and do-long-term analyses to identify certain groups, refer to Section 3.3. In difficult cases, security firms meanwhile tend to cooperate and to combine their analyses. As sophisticated attacks are typically executed by groups that operate over years and not as isolated 'hit and run'-incidents, attribution efforts are increasingly effective, see Section 3.3.

Yomiuri Shimbun has reported that the Japanese Ministry of Defense awarded a three-year research project to the company Fujitsu Ltd. in 2008 for software that should detect attacks and also the source of the attack with all interim servers. This should work as cyber weapon and thus be able to deactivate the source of the attack including springboard computers. The budget was 178.5 million Yen. The tool was successfully tested in prepared networks[108].

The DoD agency **Defense Advanced Research Projects Agency DARPA** has initiated the project ‚**Plan X**' that also included a partially classified workshop on 27 Sep 2012. Due to the essential role of attribution in cyber warfare, a goal within this project is the mapping of the entire cyberspace (computer and other devices) for visualization and planning of cyber actions[109]. The research budget for Plan X is 110 million US-Dollars.

2.2.6 Cyber defense

2.2.6.1 Attack detection and prevention

In addition to standard recommendations on cyber defense such as strong passwords, updated systems, careful behavior in internet, avoiding suspect emails and attachments etc., an increasing effort is made on automated attack detection.

The US Government is currently expanding the use of advanced sensor systems[110]: The **Continuous Diagnostics and Mitigation (CDM)** program provides real-time capacity to sense anomalous behavior and to create reports to administrators on a dashboard.

[107] Welchering 2016, p.T4
[108] Daily Yomiuri online 03 Jan 2012
[109] DARPA 2012, Nakashima 2012b
[110] Gerstein 2015, p.4-5

Einstein 3A is working by installing sensors at Web access points to keep threats out while CDM should identify them when they are inside.

For cyber defense, US researchers have developed pattern recognition algorithms, which allow after attack detection the automated deletion of data packages that are part of the cyber attack. To avoid escalation, retaliation to networks or systems is not automated. China is researching on attack simulation[111].

The German Deutsche Telekom has installed 200 **honey pot** computers that simulate average mobile phones and computers. The honey pot computers are able to document each step of the intruder[112], the analysis environment is also known as **sandbox**. As advanced malware stays silent in virtual machines, advanced sandboxes try to mimic real computers as far as possible. On the other hand, malware may be protected by **code morphing**, an approach used in obfuscating software to protect software applications from reverse engineering, analysis, modifications, and cracking.

Rob Joyce, head of the **NSA Tailored Access Operations (TAO)** group, made a public presentation at a conference in Jan 2016 with security advice. For intrusion, even smallest issues are used, also temporary gaps during remote system maintenance, in particular when done remotely. Other interesting targets are ventilation and heating systems from building infrastructure if connected to computer systems, cloud service connections, hard-coded passwords, log files from system administrators, also smartphones and other devices while zero day exploits are not so relevant in practice[113]. Based on this, the security recommendations included **Whitelisting** (only listed software can be used), strict rights management, use of up-to-date software, segmented networks (separation of important parts), **reputation management** to detect abnormal user behavior and close surveillance of network traffic.

2.2.6.2 Analysis of Leakages

Meanwhile, the WikiLeaks disclosure of confidential data from the secured **Secret Internet Protocol Router Network SIPRNET** for critical infrastructure and government from 28 Nov 2010 showed that too many people also of low ranks had access to SIPRNET[114], as discussed in the debates after the incident[115].

[111] Welchering 2014b, p.T4
[112] Dohmen 2015, p.75
[113] Beuth 2016a, p.1-3
[114] About 2.5 million persons had basic access and 280.000 persons access to higher classified documents; Schneider 2011, p.9
[115] Schaaf 2010, p.9

Possible countermeasures against massive data theft as in the Wikileaks incident or by cyber attacks from outside could be **vertical segmentation** based on ranks and **horizontal segmentation** of access depending on project-related or topic-related involvement, blockade of printing and downloads by **document management** systems and the **tracking** of document usage and changes. Also the transmission of confidential data via secured or physically **separated communication** lines in line with the **need to know-principle** may help to prevent further security incidents[116]. As a first step, the number of people with SIPRNET access was reduced[117].

In 2012, an IT administrator within the secret service of Switzerland, the **Nachrichtendienst des Bundes NDB**, started an unauthorized data collection which was discovered early enough. Security countermeasures here were separation of and restricted access to sensitive data bases and the **four eye-principle** for IT administrators[118].

The public disclosure of the surveillance programs PRISM (NSA) and Tempora (GCHQ) with the involvement of large internet companies as well as of telecommunication providers[119] by Edward Snowden who worked for the security firm Booz Allen Hamilton (and the subsequent reporting in the newspaper *The Guardian*) led to a broad debate on security matters[120].
In fact, 1.5 million people in US have a cyber-relevant security clearance level, thereof 480,000 from private companies[121]. Moreover, the ODNI (office of the Director of National Intelligence who coordinates the US Intelligence Community) was cited that 70% of the intelligence budget is assigned to private firms[122]. On the other hand, it was argued that the cooperation with private firms is already long-standing[123] and would be necessary to utilize expert knowledge in the rapidly growing cyber sector.

---

[116] Sattar et al. 2010, p.3
[117] Schneider 2011, p.9
[118] Gujer 2012a, p.30, Gujer 2012b, p.24, Häfliger 2012a, p.29. The key cyber security structure of Switzerland is the **Melde- und Analysestelle Informationssicherung Melani** (reporting and analysis office for information security), where the Departments of Defense and Finance and the NDB are involved, Gujer 2012a, p.30
[119] Tomik 2013b, p.2.
[120] However, some aspects were already discussed during the European "Echelon debate" in the 1990ies, such as an assumed global surveillance of telecommunication, internet and emails by the NSA. The debate resulted in a preparation of a summary report by the EU 2001, refer to Ulfkotte 1998, p.8, FAZ 2000, p.1, Schröm 1999a/b, Schmid 2001, Schöne 1999, p.32, Schöne 2000, p.39.
[121] Gartmann/Jahn 2013, p.24
[122] Huber 2013, p.18-19
[123] BAH cracked German submarine codes in WWII, Gartmann/Jahn 2013, p.24. Other security firms are e.g. Xe and USIS.

2.2.6.3 Defense against DDoS attacks

General recommendations against DDoS attacks were given by the German IT security authority BSI[124]. The attacked server may prolong responses to attacking computer so this computer needs to wait for the responses for a very long time. This method is also known as **tar pitting.**

Also, the number of connections per IP address can be restricted. If certain source addresses are blocked, this is called **sinkholing**. By blocking of suspect attacker regions (geoblocking) the effectiveness can be increased further, but with the risk of blocking legitimate requests as well. **Blackholing** means to switch off the attacked IP addresses, which may make sense if there is a risk of collateral damage to other systems of the attacked organization.

As a preventive measure, incoming internet traffic may be reduced to the more secure Transport Layer Security (TLS)/Secure Sockets Layer (SSL) ports. Finally, **DDoS mitigation services** may be used, i.e. the internet provider is involved to reduce or block incoming internet traffic.

2.2.6.4 Automated Cyber Defense

The US DoD agency **Defense Advanced Research Projects Agency DARPA** conducted the **Cyber Grand Challenge** on 04 Aug 2016 in Las Vegas, where 7 computers were detecting cyber attacks and creating responses fully automated, i.e. without any human intervention. This procedure went on for 30 rounds over 12 hours. The computers and their programming teams were selected before out of hundred competitors[125].

A machine called *Mayhem* won the Challenge, the success was achieved by being inactive during most of the rounds, while the other computers fought against each other. Another machine detected a vulnerability, but the automatically created patch slowed down the machine, so the machine decided to remove the patch [126]

DARPA was satisfied with the results, it was a first step forward to an automated defense and response system[127]. As the number of vulnerabilities is meanwhile immense[128], automated systems may stop unknown or overseen vulnerabilities.

However, while it may be possible to give routine surveillance to machines, human supervision cannot be removed. Otherwise, a spoofed (misled) machine could decide to attack the own network. Or an attacker may convince the attacked

[124] BSI 2012
[125] DARPA 2016
[126] Atherton 2016
[127] DARPA 2016
[128] A US data base collected 75.000 vulnerabilities in 2015, Betschon 2016; in a test 138 security gaps were found in the Pentagon systems, Die Welt online 2016

computer to get inactive or misconstructed patches may slow down the defense system.

2.2.7 Smartphone security

Eavesdropping of government smartphones[129] is only a part of security problems emerging from smartphones, personal digital assistants (PDAs) and tablet PCs. The smartphone is increasingly replacing the computer in daily routine such as web access and email-work, also the trend is going forward to use smartphones as **virtual master key** for online banking, control of smart homes[130], energy supply by smart grid and later on also for control of cars in the upcoming **e-mobility** projects[131]. The smartphone is increasingly used as primary access point to the internet in particular in Africa where the internet traffic via smartphone is rapidly expanding.[132] The '**bring your own device (BYOD)' concept** describes the option for wireless coordination of multiple devices and machines by a key device. While currently coordination of entertainment devices is increasingly done by Triple play hard disk recorders or e.g. by the X-Box, the trend is going forward to do this via smartphone or tablet. The BYOD philosophy creates a kind of **shadow IT** in companies which is quite difficult to control and to protect[133].

As a result, intruders will not only know all private data, control online banking and locate users by the mobile phone cell systems, but could control the household and the cars.
Relevant intrusion strategies (*in addition* to all standard threats resulting from email and internet access) [134] are simple collection of electromagnetic waves by radio masts (GSM standard is not secure[135]), mimicking radio masts by **IMSI-Catchers**, access to node servers or cables of node servers[136], implanting viruses and Trojans by infected Apps, unauthorized data use by hidden App properties[137], or sending invisible and silent SMS messages (**stealth SMS**) to transfer spyware such as *Flexispy* [138]. In July 2015, a new security gap was found in Android smartphones where **MMS** can import malicious codes and then delete themselves, i.e. the message does not to be opened. The **StageFright** malware allows intruders

[129] Graw 2013,p.4-5. Respective incidents were e.g. reported for Indonesia, Germany, Brazil.
[130] RWE 2013
[131] Heinemann 2013, p.3
132 Langer 2014a, p.7
[133] Müller 2014, p.16
[134] Ruggiero/Foote 2011
[135] FAZ 2013c, p.14
[136] Wysling 2013, p.5
[137] Focus online 2013
[138] Welt 2013, p.3, Opfer 2010

to take over audio and video functions[139]. The later discovered Stagefright 2.0 used MP3 music files instead of MMS files.
Crypto-mobile phones with end to end encryption are the suggested secure solution, but have some disadvantages, as they are cumbersome to handle and both sides need to use the same mobile phone, otherwise encryption is inactive[140].

Researchers from German company Deutsche Telekom have shown that the intrusion of a smartphone including complete data stealing, change of settings and installation of a remote access tool takes only 5 minutes in practice[141]. Meanwhile German ministers are advised to use **one-way mobile phones** that are only used during one travel and then destroyed.[142]

Researchers found weaknesses in the Encryption Algorithm A5/1 of the **Global System for Mobile Communications (GSM)**, but a stronger encryption A5/3 was meanwhile established. Also, the roaming **protocol SS7** was shown to have vulnerabilities that allow to redirect calls and to get location and communicating data by remote attacks[143]. This can be done by approaching or mimicking the **Home-Location-Register (HLR)**, which is a SS7 database. Another attack method is stealing of keys for SIM cards. For matters of easier handling, it is planned to replace conventional SIM cards by **embedded SIM** cards. This concept is based on the GSMA-embedded SIM specification that was originally developed for machine to machine communication and which allows "over the air" access to SIM cards to allow change of operators[144].

A smartphone analysis of the French security firm *Eurecom* loaded 2000 Apps for Android mobile phones on a Samsung smartphone. Then the **background communication**, i.e. internet connections that are not indicated on the screen, was analyzed. The apps sent in the background data to 250,000 websites, the most active App to 2,000 servers. Typically, these servers are used for analysis and marketing purposes.[145]
A problem are also **falsified Apps** which seem to be legitimate, but contain malware, that may e.g. force smartphones to load other websites in the background. The **XCode Ghost** Malware infected iO-Apps from Apple in Sep

[139] Steler 2015
[140] Drissner 2008, p.4, Opfer 2010
141 For this, Deutsche Telekom has installed 200 honeypot computers that simulate average mobile phones and computers. The honeypot computers are able to document each step of the intruder; Dohmen 2015, p.75
[142] Der Spiegel 2015, p.18
143 Der Spiegel online 2014, p.1, Zeit online 2014a
144 Zeit online 2015b, GSMA 2015. As embedded programs can also be infected, this may represent a future key vulnerability of smart phones and also of smart industry, see Section 3.2.12
[145] Spehr 2015, p.T4

2015 via an infected software development kit (SDK) for App programming. More than 250 infected Apps were removed from App stores[146].

QR codes (Quick Response Codes), i.e. matrix or two-dimensional barcodes may redirect smartphones to malicious websites during scanning[147]. The **Near Field Communication** (NFC) is a contactless smartcard technology which is e.g. used for payment by smartphone via short-distance signals. In two hacking contests for mobile devices in 2012 and 2014, security gaps were found, but closed thereafter[148].

In early 2016, the FBI tried to decrypt an iPhone of a suspect which was successful with the help of the company *Cellebrite* from Israel[149].
In August 2016, the sophisticated iPhone malware **Pegasus** was reported by the security firm *Lookout* and the Canadian *Citizen Lab* which was initially found in three iPhones in Mexico, UAE and Kenya[150]. After clicking on a malicious link, this modular software was installed by a drive-by download on the iPhone and able to collect password, photos, E-Mails, contact lists and GPS data[151].
Lookout suspected that this came from the private cyber weapon provider **NSO group** located in Israel. However, the NSO group explained that they sell their products only to government, intelligence and military institutions within the applicable legal framework[152].

2.2.8 Cyber security of complex machines

2.2.8.1 Smart industry

Complex industry machines driven by SCADA and ICS systems, as well as cars and airplanes are a primary matter of concern, as they could be used for tailor-made attacks on infrastructure and/or individuals.
Industry machines/cyber-physical systems are no closed communication environments, but can typically approached via the regular company internet, which allows remote attacks[153].

The cyber attacker group **Dragonfly** (**Energetic Bear/Crouching Yeti/Koala**) intruded providers of ICS software and injected malware, so that all user companies automatically loaded the malware with the next software update[154]. The

[146] T-online 2015
[147] Beuth 2016a, p.1-3
[148] Lemos 2015
[149] FAZ online 2016
[150] Die Welt online 2016
[151] Die Welt online 2016, FAZ online 2016
[152] Jansen/Lindner 2016, p.28
153 For remote control of machines also satellite communication is used, the necessary **Very Small Aperture Terminals VSAT**s are also vulnerable, Reder/van Baal 2014, p.V2
[154] Metzler 2015, p.34

group uses the **Havex/Backdoor Oldrea** malware that infiltrates and modifies ICS and SCADA systems and creates a backdoor. In addition to infection of providers of ICS software, the hackers offered **watering holes**, i.e. the infection of websites frequently visited by the target persons with redirection of visitors to malicious sites and also they used emails with infected PDF files[155]. As second tool, the group used the **Trojan Karagany** which is also available on the underground market. Working times indicate a group located in Eastern Europe (UCT+4) [156].

The Japanese software company *Trend Micro* showed that ICS and SCADA systems are meanwhile routinely checked for vulnerabilities by attackers. A simulated water supply system was set up as honey pot to attract hackers. Over 28 days, 39 cyber attacks with manipulations and malware injections were registered that came from 14 countries. The US ICS Emergency Response Team reported 172 security gaps in systems of 55 different providers[157]. SCADA systems often do not have automatic security updates or virus scans and firewalls can often not be implemented, because this interferes with the liability of the manufacturer of the SCADA-driven machine[158].

In an intrusion test, a White hat hacker was able to intrude and to take over control over the urban water supply in Ettlingen in less than two days[159].
On 18 Dec 2014, the German IT security authority BSI reported that hackers intruded the regular office network of a steel company and were able to access production IT from there resulting in damage of a blast furnace[160].

The US Industrial Control Systems Cyber Emergency Response Team (**ICS-CERT**) recommends[161] to minimize network exposure for all control system devices with protection by firewalls and to avoid internet access. If remote access cannot be avoided, Virtual Private Networks (VPNs) may be used to secure the access. Default system accounts should be removed, renamed or disabled wherever possible.
Shodan is the world's first search engine for Internet-connected devices, webcams and ICS/SCADA systems which may be used by hackers but could also be used by administrators to check the own environment for any internet interfaces. Also, general cyber defense recommendations are applicable as well (strong passwords, Application Whitelisting AWL etc.).

---

[155] Campbell 2015, p.11
[156] Symantec 2014b
[157] Betschon 2013a, p.38
[158] Striebeck 2014
159 Reder/van Baal 2014, p.V2
160 Krohn 2014, p.24
[161] ICS-CERT 2016a

In addition, smart things with IP addresses allow a precise management of production flows, but maybe misused as **thingbots**. The security firm Proofpoint reported between December 2013 and January 2014 waves of malicious email, more of 25% was sent by thingbots, i.e. infected devices such as router, TV and at least one fridgerator. This was possible due to configuration problems, old firmware and default passwords[162]

A key problem of smart home functionality and security is a lack of compatibility of devices in combination with frequent modifications by updates and competing or overlapping standards such as *ZigBee* with substandards, *Thread*, *Home Matic*, *Qivicon* etc. which leads to connectivity issues and a high number of potentially vulnerable interfaces[163].

2.2.8.2 Cars and air plane cyber security

Digitalization of cars is rapidly moving forward, e.g. for driving assistance, motor diagnostics, information, navigation and entertainment, security and camera systems[164]. The most important attack target is the **controlled area network (CAN)**, a serial bus system that allows microcontrollers and devices to communicate with each other[165]. Eighty percent of new cars in Germany will have internet access in 2016[166]. From 2018, news cars in the European Union must have the **E-call** system which is an included mobile phone capacity; the car then can automatically do emergency calls in case of accidents. However, the system can systematically track and collect driving data, too[167].

There is also another trend to integrate IT structure with internet connection into cars, e.g. the plans to integrate Google Android into Audi cars. Researchers have found four classes of vulnerabilities, the **Car to X connection** to servers outside the car, the security of infotainment devices within the cars, the immobilizer functions and the internal interfaces of car components. Based on recent tests, it is apparently still (too) easy to intrude the IT infrastructure of cars[168].

There are increasing reports about car hacks. After a successful car hacking by Chinese students (**Tesla** incident), it was emphasized, that such action still requires direct physical access to the systems and could not yet be done remotely[169]. Until now, all these hacks were done in research environments,

[162] Market Wired 2014, p.1-2
[163] Weber 2016, p.T1
164 Hawranek/Rosenbach 2015, p.65
165 Fuest 2015, p.34-35
166 Schneider 2014
167 Fromme 2015, p.17
168 Karabasz 2014, p.14-15
169 Lewicki 2014, p.62

typically by ethical hackers who notified the affected companies to allow early closure of security gaps[170]. However, in mid 2015 the first time a car hack of a Fiat Chrysler Cherokee Jeep model could be done remotely over a distance of 15 kilometers[171].

Smartphone apps will increasingly replace physical keys and will also allow to share the car with others. The **keyless** system enables to open the car and to start the motor via the Bluetooth function of the smartphone[172], but such signals can be easily detected and reproduced by attackers using a **repeater** device[173].

The car model Tesla S was updated in late 2015 with autopilot functions for partial autonomy of the car. More importantly, updates can now be done wireless via WLAN as **firmware over the air (FOTA)** which may increase the risk for hacking[174], but also allows rapid security updates[175]. A Tesla car collided on 07 May 2016 with a white truck that trailer that was not detected by the autopilot sensors in Florida, but apparently also not seen by the driver of the car[176].

Similar problems are occurring in civil air planes where e.g. internal networks are sometimes only separated by firewalls from passenger entertainment systems. Moreover, there is an increasing connection of internal systems which creates the risk of complete takeovers of air planes by hackers. Recently, a US expert was reported to have been able to intrude the passenger entertainment system and in one case into the control systems[177]. On a higher level, also the US National Airspace System for the air traffic control had weaknesses, such as the boundary control of the system as well as between the key operational system and less secure systems and the US Government Accountability Office set up recommendations to overcome these problems.[178]

2.2.8.3 The Black Energy attacks

The US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has identified a malware campaign that since at least 2011 has

170 Meanwhile car manufacturers hire hackers to check the security such as the British telecommunication company BT, FAZ 2015b, p.18

171 Der Standard 2015, p.1. So far, only one real car hack outside research was reported so far, 100 cars were blocked by an employee after he lost his job in 2010.

172 Rees 2016, p.2

173 Heute 2016

174 The FBI and the US National Highway Traffic Safety Administration NHTSA have expressed growing concerns about the risk of cars being hacked in a public statement 2016 and identified remote updates as a relevant vulnerability, BBC 2016

175 Becker 2016, p.78

176 Fromm/Hulverschmidt 2016, p.25

177 Rosenbach/Traufetter 2015, p.72f.

178 GAO 2015, p.1

compromised several ICS systems using a variant of the **BlackEnergy** crimeware on Internet-connected human-machine interfaces (HMIs)[179]. Amongst others, the HMIs *GE Cimplicity*, *Advantech/Broadwin WebAccess*, and *Siemens WinCC* were affected.

Crimeware is malware to support cyber crimes. Commonly used crimeware consists of spyware which may be used for getting online banking data or Trojans to establish botnets for DDoS attacks. An increasingly used crimeware is **ransomware** that encrypts files or hard disks on target computers, thereafter the attacked organization is e.g. requested to submit virtual money (Bitcoins) to foreign accounts to get decryption codes. Current ransomware may also encrypt external hard disks and data stored in clouds, examples of ransomware are **Locky** and **Cryptowall[180]**.

The **Sandworm** or **Quedagh** group (names resulting from references to science fiction world *Dune)* is using the widely used crimeware BlackEnergy for computers of targets.
BlackEnergy is available since 2007 and meanwhile updated to **BlackEnergy3**. BlackEnergy was originally created to establish botnets for DDoS attacks. The Sandworm/Quedagh group made modifications of the conventional BlackEnergy malware and added multiple functionalities such as hijacking of inactive drivers and a large information stealing component[181]. In summer 2014, Black Energy 3 was detected by the security firm *F-Secure Labs* in an attack against Ukrainian targets; before that already the NATO was attacked in December 2013[182]. However, NATO confirmed that the classified operational networks were not affected as they are isolated from internet183.

On 23 Dec 2015, power outages were caused in the Ukraine by cyber intrusions at three regional electric power distribution companies impacting approximately 225,000 customers[184]. Three further companies were intruded, but had no outages. The intruders[185] were able to open multiple breakers remotely resulting in power outage, which happened in a small time window in a coordinated manner[186].

[179] ICS-CERT 2016a
[180] In early 2016, a number of German hospitals was heavily affected by ransomware, for details see also Jüngling 2015, p.67. Meanwhile decryption and encryption detection software is developed to counteract to ransomware, Steier 2016a, p.36. There is a large variety of further criminal activities in internet, e.g. in the DarkNet which is typically accessed by TOR browsers, an overlap to cyber warfare exists e.g. in use of DDoS attacks.
[181] F-Secure Labs 2014, p.2, 10-11
[182] BBC 2014, p.1, F-Secure Labs 2014, p.2
[183] BBC 2014, p.2
[184] ICS-CERT 2016b
[185] Note that the use of BlackEnergy makes it plausible to assume that the Sandworm/Quedagh group may be responsible, but there is no definite evidence for this.
[186] ICS-CERT 2016b

Telephone denial of service attacks (TDoS attacks) were used to flood hotlines with phone calls to prevent customers from reporting the outage by telephone[187].
At the end of the attacks, the wiper malware **KillDisk** was used to damage the systems.
For this Ukraine incident, US ICS-CERT could *not* confirm that the Black Energy 3 variant caused the power outages, the breakers could be opened by intruders without this malware[188].

2.2.9 Professional cyber war

While cyber attacks historically started with spontaneous hacking, there is an ongoing trend to establish professional structures and processes.

On the military level, this includes the systematic training. As an example, US Navy trains 24,000 people per year in their **Information Dominance Center** and the US Air Force has initiated a course (first completers in June 2012) at Nellis Air Force Base in Nevada to train how to detect electronic intruders, defend networks and launch cyber attacks[189].
However, the way is going forward to establish formal cyber officer careers as the US Air Force 17 deltas officer (**17D officer**) since April 2010 as a specialization pathway for communication officers[190]. An undergraduate cyber training (UCT) was also established to provide basic knowledge and how to defend the network, but continue to operate at the same time[191].
The **US Department of Homeland Security DHS** has meanwhile conducted its own young hacker contest to recruit skilled cyber personnel, the Virginia Governors Cup Cyber Challenge[192].
The **Central Intelligence Agency (CIA)** has announced to establish a new Directorate "Digital Innovation". Further reforms aim to create 10 integrated centers that combine analytical and operative capabilities[193]. To enhance effectiveness, NSA is combining defensive and offensive departments IAD/SID in 2016. The **Information Assurance Directorate (IAD)** tries to find and to patch exploits while the **Signals Intelligence Directorate (SID)** is using exploits for cyber operations[194].

---

[187] Zetter 2016
[188] ICS-CERT 2016a
[189] Barnes 2012
[190] Schanz 2010, p.50ff., Franz 2011, p.87. Instead of the widely used term **cyber warrior**, the more formal term **cyber warfare operator** was introduced.
[191] Black cited by Schanz 2010, p.52
[192] Perlroth 2013, p.1. The news agency Reuters reported on 19 Apr 2013 that the NSA and the US Air Force Academy made an inter-agency hacker contest in a three-day cyber war exercise. The NSA has set up a comic series **CryptoKids** for children, Pofalla 2013, p.44.
193 Die Welt 2015 online, p.1, Tagesschau 07 Mar 2015
[194] Gierow 2016, p.1-2

China reported in 2011 to have a group of 30 cyber experts called the **Blue Army** and to have a cyber training center in Guangdong[195].

The Russian Ministry of Defense started in 2012 an information research project including "methods and means of bypassing anti-virus software, firewalls, as well as in security tools of operating systems"[196]. In addition, an All-Russian hacker competition was initiated to recruit skilled young cyber professionals[197].

Media in Israel have reported the creation of a new military category, the 'attacker', who could affect the adversary remotely, e.g. via drones or via cyber operations (while the 'fighter' category includes soldiers who are physically present in a conflict). Also, the training of **cyber defenders** has started and the first course was completed in 2012. As preparation, an intensified cyber education is offered at schools, in addition 'cyber days' for education in ethical (white hat) hacking are conducted by the army and hacker contests[198].
Israel has established a **National Authority for Cyber Defense** to protect civilians against cyber attacks, while a specialized unit already exists in the Intelligence Sector[199].
In Beersheba in Negev desert a **cyber capital** is under construction and private firms as well as military units will be located there, including 35,000 soldiers. This will also include military intelligence and the cyber elite **unit 8200**[200].

Also, the United Kingdom plans to establish the **Joint Cyber Reserve** as a cyber army for defense and counterstrikes in cyber conflicts. The government plans to invest 600 million Euros[201].

The creation or modification of cyber warfare weapons, systems and tools as well as cyber defense require teams that include specialists for certain systems, software, hardware, SCADA applications etc.[202] Moreover, during the cyber operation offensive and defensive roles need to be clearly defined.

Finally, cyber attacks are increasingly based on systematic analysis, pre-tests in simulations and test environments before approaching the real target. This is done

[195] Kremp 2011
[196] Citation in Pravda 2012
[197] Pravda 2012
[198] Croitoru 2012, p.30
[199] EPRS 2014, p.5/6
[200] Rößler 2016, p.6
[201] Spiegel online 2013
[202] Zepelin 2012, p.27, Chiesa 2012, slide 64, Franz 2011, p.88. Bencsath estimated e.g. that the development of the Flame spyware that was discovered in 2012 required up to 40 computer-, software- and network specialists, FAZ2012a, p.16

to reduce risk of discovery and attribution, to prolong the duration of successful attack and to expand the attack volume[203].

Also, the staff recruitment methods by intelligence and military have made significant progress. Studies have shown that the historical distance between hackers and state organizations has changed to a growing acceptance and interest to work for the state under certain circumstances[204].
As a consequence, recruitment methods for cyber security-related positions are now easier[205].

2.2.10 Is Cyber war overhyped?

Intense discussions are going on whether the cyber war debate is a kind of hype or myth which e.g. used by military institutions to justify their expansion in the cyber sector. A key argument presented is that a real cyber war probably did not happen in Estonia 2007, which is one of the most cited cyber war examples. For some authors, the attacks were too uncoordinated and unsophisticated to come from Russian state organizations; instead, they were assumed by these authors to be caused by patriotic **script kiddies**, i.e. attackers using simple standard tools that are available in internet[206].

Another argument presented is that most cases of cyber war as shown in the next section were only cases of cyber espionage, which as conventional espionage is usually not considered as an act of war.
However, there are some significant differences between conventional (physical) espionage and cyber espionage:
It takes a long track of training and covert actions until a conventional agent is placed in a position to gain sensitive information and he is permanently exposed to a high personal risk of discovery and punishment[207]. In cold war, it took years to export thousands of pages of sensitive information.

---

[203] Zepelin 2012, p.27. According to Chiesa 2012, publicly unknown security gaps (zero day-exploits) are also traded, refer to slides 77 to 79. Moreover, standardized malware creation tools are available on the market, refer to Isselhorst 2011, slide 9

[204] Zepelin 2012, p.27. Krasznay 2010 cited by Chiesa 2012, slide 69.

[205] Zepelin 2012, p.27. The following may illustrate the open approach: When searching since 2012 in US for cyber war issues (search words including the term cyber war) on *startpage.com*, a service allowing anonymous search on Google, it could happen that a sponsored link from the NSA appeared (also visible on *ixquick* or *metacrawler*). This offered cyber careers under the link www.nsa.gov/careers saying "National Security Agency has cyber jobs you won't find anywhere else!". In 2016, this is available under intelligencecareers.gov/nsa. The CIA also set up an own search engine ad "CIA Cyber careers – The work of a Nation – cia.gov The Center of Intelligence –Apply today" and opened in June 2014 an official Twitter account.

[206] Luschka 2007, p.1-3

[207] A short and simple introduction into the topic is presented by Melton 2009, p.200ff.

Cyber espionage can be done from home and even in case of discovery, the probability of punishment is low. It takes only seconds to export thousands of pages from an intruded system. As a result, cyber espionage is much more frequent and aggressive than conventional espionage.
But more importantly, the modern cyber weapons allow installing backdoors and to decide on attack escalation and manipulation later. If a critical system is successfully intruded for espionage, the intruder has the option to damage it, i.e. the border between passive espionage and active damage is now diminishing.

And finally, conventional weapons are increasingly based on computers, so cyber activities do affect conventional capabilities as well. As a result, the size of cyber staff in military is increasing, the Cyberspace Operations and Support Staff of the US Air Force included 63,828 persons, thereof 4,095 officers as of May 2012[208].

In summary, not any larger cyber attack may be an act of war and the terminology has to be used cautiously, but the cyber war problem should nevertheless be taken seriously[209].

2.2.11 Intelligence Cooperation

Media reports in 2013 gave the impression, that Intelligence cooperation is focused on computers and Signals Intelligence SigInt. However, intelligence cooperation was created during World War II, and was expanded during Cold War and in response to growing terrorist activities already in the decades before 9/11. As a result, the intelligence cooperation also includes the collection and analysis of information derived from human intelligence (HumInt), imaging intelligence (ImInt) and open source intelligence (OsInt)[210].

The system of intelligence cooperation can be sorted into three levels, the intelligence cooperation within one country (**intelligence community**), the widespread bilateral intelligence cooperation and the multinational intelligence cooperation. Many countries have multiple intelligence organizations that cover inner and external security and civil and military issues. There is a never-ending discussion about the optimum size and number of organizations: a single organization may be too large to be controlled, also the potential damage in case of intrusion could be serious and internal communication maybe too cumbersome with the risk of information loss, late reactions and blind spots in analysis. Smaller

[208] Matthews 2013, p.8
[209] The growing relevance of drones and cyber warfare is reflected by the US plan to create a new medal in 2013 for distinguished warfare for drone pilots and cyber warriors, the first one since 1944. This plan was cancelled after veterans and others said, that these fighters maybe under high stress, but are not directly exposed to hostile fire, NTV 2013.
[210] Best 2009

organizations have specialization advantages and may be more focused on certain topics, but there is a risk of overlapping actions and responsibilities, internal competition and communication issues. The standard solution is to have multiple organizations with a coordinating level[211]. The largest Intelligence Community is in the US (formally established in 1981) where the **Director of National Intelligence DNI** (since 2004 in response to 9/11) coordinates all organizations, 8 of them are forming the military umbrella organization **Defense Intelligence Agency DIA**[212].

The second level is a network of **bilateral intelligence cooperation**, e.g. Germany has relations with more than 100 countries[213]. Depending on quality of political relationship, there may be formal official intelligence representatives and/or as (more or less) accepted alternative, intelligence staff as diplomatic (embassy and consulate) staff. This is necessary to detect, discuss and resolve bilateral intelligence-related incidents and topics.

The highest level is the **multi-lateral cooperation**, because even the largest intelligence organizations have limited human, technologic and budgetary capacities to achieve a global coverage. The information mode is typically as follows[214]:

- **Do ut des** – if you give something, the other one has to give something, too
- **Need to know** – only necessary information is provided, this is also important if the organization is infiltrated or agents are captured by adversaries
- **Third party rule** –an information received from second parties should not be given to third parties without approval
- **Assessed intelligence** – no raw data to protect knowledge on methods and sources[215].

Based on this exchange logic, smaller groups can easier have deep cooperation. US has established already after World War II the declassified **5-eyes** cooperation with UK, Canada, Australia and New Zealand and in response to 9/11 (officially not confirmed, reported in 2013 by *The Guardian* and others in November 2013) a

[211] Carmody 2005
[212] Air Force Intelligence, Surveillance and Reconnaissance Agency (ISR), United States Army Intelligence Corps (G2), Office of Naval Intelligence (ONI), Marine Corps Intelligence Activity (MCIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO) for satellites, National Security Agency (NSA) for SigInt. Non-military organizations are the Central Intelligence Agency (CIA), Office of Intelligence and Counterintelligence (Department of Energy), Bureau of Intelligence and Research (INR) (State Department), Office of Intelligence and Analysis (OIA) (Department of Finance), Office of National Security Intelligence (NN) (Drug Enforcement Administration DEA), Homeland Security DHS and Federal Bureau of Investigation (FBI). DNI Handbook 2006
[213] Daun 2009, p.72
[214] Jäger/Daun 2009, p.223
[215] Wetzling 2007

wider cooperation the **9-eyes** cooperation including Denmark, France, Netherlands and Norway and the **14-eyes** cooperation additionally including Belgium, Italy, Spain, Sweden and Germany[216].

In the European Union, cooperation started with small counter-terrorist working groups in the 1970ies and was stepwise expanded. The Joint Situation Center **SitCen** (which since 2010 is subordinated to the **Standing Committee on operational cooperation on internal security COSI**)[217] is analyzing information provided by member state organizations, counter-terrorist working groups etc. [218] Africa has established the multinational cooperation **Committee of Intelligence and Security Services of Africa CISSA** a part of the African Union (see Section 4.7).

[216] See e.g. Shane 2013, p.4
[217] Note of 22 October 2009 which was followed by a Draft Council Decision: Council Decision on setting up the Standing Committee on operational cooperation on internal security (EU doc no: 16515-09 and EU doc no: 5949-10).
[218] Scheren 2009

3. The Practice of Cyber war

3.1 Introduction

In reality, cyber war is defined in literature as c*yber attack with damaging effects which was presumably conducted or supported by states due to their extent and/or complexit*y.

For analysis, please note a **very important abnormality**: in contrast to conventional conflicts, the information on the incident **is presented by one side only**, mostly by the victim, in exceptional cases by the attacker (Section 3.2.6). This unilateral information makes it extremely difficult to create objective evidence and analyses.

3.2 Cyber war from 1998-today

3.2.0 Cold war: Pipeline explosion in the Soviet Union

The Soviet Union tried to get high-tech control systems for their own pipelines which were not legally accessible due to the restrictions of the cold war. Nevertheless, the USA tolerated the theft, but managed to install a software bug that increased the internal pressure in the Chelyabinsk pipeline above maximum range in 1982[219]. A three kilotons explosion resulted which equaled 20% of the nuclear bomb of Hiroshima[220]. However, Russia contradicted to this presentation of events.

3.2.1 Moonlight Maze 1998-2000

Within nearly two years from 1998 on, **Moonlight Maze** was a series of attacks with probing of computer systems at the Pentagon, NASA, Energy Department and other private actors and tens of thousands of files were stolen. The US Defense Department assumed Russia as origin of attacks, but Russia denied any involvement[221].

3.2.2 Yugoslavian war 1999

Some authors believe that the first cyber war-like action was the blockade of Yugoslavian Telephone networks by the NATO during the Kosovo conflict in 1999[222]. Following the accidental bombing of the Chinese embassy in Belgrade, Chinese hackers attacked US government websites such as the website of the White House[223].

---

[219] Kloiber/Welchering 2011, p.T6
[220] Falliere 2010, Herwig 2010
[221] Vistica 1999
[222] Hegmann 2010
[223] Hunker 2010, p.3. For the NATO, not only cyber war, but all forms of cyber attacks are relevant, Hunker uses the term **cyber power**.

3.2.3 The Hainan- or EP3-incident 2001

After a collision of a US reconnaissance plane of type EP-3 and a Chinese fighter jet, known as the Hainan or EP-3 incident, probably patriotic Chinese hackers released the worms *Code Red* und *Code Red II*, which resulted in nearly $2 billion in damages and infecting over 600,000 computers. This resulted in system downtimes and Website defacements, with the phrase „hacked by Chinese“[224].

3.2.4 Massive attacks on Western government and industry computers 2000-2011

Civil and military networks are main targets, but also arms manufacturers are of interest; US experts believe that a **cold cyber war** with China is already ongoing[225]. China was suspected to take away at least 10-20 terabytes of data from respective US computers in 2007; in the same year 117,000 internet-based attacks on Department of Homeland Security computers were reported. These activities followed a series of attacks which took some years and which was called **Titan Rain** by the US[226]. Also the German Federal Government reported attacks on their computer systems at a similar.

The analysis of Titan Rain revealed an attack pattern similar to the following: a team of 6-30 hackers takes control of computers, copies everything on the hard drive within 30 minutes, and then send that via a botnet to computers in the Chinese province of Guangdong, however, this could not be definitely proven[227].

Also, there are several media reports about Russian and Chinese attempts to intrude the systems of the Pentagon and the White House in the years 2007-2008. ArcSight reported 360 million attempts to break into the Pentagon in 2008[228].

Other large-scale cyber attacks were **GhostNet** and **Operation Aurora** in 2009. According to BBC news, **GhostNet** was a large-scale computer virus attack on the embassies (amongst others) of India, South Korea, Indonesia, Thailand, Taiwan, Germany and Pakistan and the foreign ministries of Iran, Bangladesh, Indonesia, Brunei and Bhutan.

China was suspected to be the origin of the attack as the computer of the Dalai Lama was infected, too, but this could not be definitely proven. The virus was able to activate webcam and microphones to control the room where the infected computer was standing.

Within the **Operation Aurora** presumably Chinese intruders tried to gain access to computer programs and source codes of companies of the IT sector (such as

[224] Fritz 2008 and also Nazario 2009, who gives in his paper an overview on politically motivated relevant DoS attacks.

[225] Hegmann 2010, p.5. ‚Cold', because it was espionage without the intention to damage the systems. This term shows how difficult an exact definition of cyber war is; see also Herwig 2010, p.61

[226] Fischermann/Hamann 2010

[227] Fritz 2008, p.55 and also Stokes 2005

[228] ArcSight 2008, p.2

Google and Adobe) and from high-tech companies of the security and defense sector in 2009[229]. Operation Aurora was meanwhile linked to the **Axiom/Deep Panda Group**, see Section 3.3.5. Two further coordinated large-scale cyber attacks have been conducted in 2009 against global oil, energy, and petrochemical companies (**Operation Night Dragon**) and against 72 global organizations over 5 years from July 2006 on (**Operation Shady RAT**), but China strongly denied involvement[230][231]. 2011 further attacks were reported, that affected in particular Google's mail service Gmail and the armament company Lockheed Martin[232].

3.2.5 The attack on Estonia in 2007

In 2007, the systems of Estonia were massively attacked by a distributed denial of service attack after moving a Russian memorial that represented for Russia the liberation of Estonia from Hitler, but was perceived by Estonia as symbol of repression[233]. Estonia's networks were flooded by data from Russia, however probably not by the state, but by patriotic organizations[234][235]. Some computers had an increase from 1,000 requests *per day* to 2,000 requests *per second* and the attack went on for weeks[236].

3.2.6 The attack on Syria 2007

On 06 September 2007, a suspected nuclear plant in Eastern Syria was destroyed by Israeli air attacks. Such an attack required a long route through the Syrian air space. Israel was technically able to simulate a free heaven to Syrian air defense systems and could thus conduct this attack without disturbance. This is a very good example how cyber war can be used as an additional tool within conventional attacks[237].

3.2.7 The attack on Georgia 2008

Already before the start of conventional war between Georgia and Russia in 2008 Georgia noted massive cyber attacks against its critical infrastructure systems e.g. in the media, banking and transportation sectors[238]. Some weeks before the

[229] Markoff/Barbosa, 18 Feb 2010
[230] Alperovitch 2011, McAfee 2011. RAT stands for remote administration tool.
[231] FAZ 2011b, p.7
[232] Koch 2011, p.20. There is a possible relationship between the attack on Lockheed Martin in May 2011 and on the IT security company RSA in March 2011, where information on the widespread security system **SecurID** was hacked, FAZ 2011a, p.11. RSA has developed the ‚Secure Cloud' concept for Lockheed Martin; Fuest 2011
[233] Busse 2007
[234] Later on the patriotic Youth Organization **Naschi** ('our people') said that they conducted the attack, Frankfurter Allgemeine Zeitung 11 Mar 2009
[235] Koenen/Hottelet 2007, p.2
[236] Wilson 2008, p.7ff.
[237] Herwig 2010, p.60
[238] refer to official statement of government of Georgia 2008

website of the Georgian President was shut down by a distributed denial of service (DDoS)-attack on 20 July 2008. Also, web site defacement was executed and photos of Hitler were put next to photos of the Georgian president. One day before conventional attack, a massive DDoS attack seriously affected the Georgian IT systems.

3.2.8 Intrusion into US electricity net 2003-2009

Also during the power failure of 2003 it was discussed whether this was caused by a computer virus[239]. In August 2003, the worm *Slammer* intruded the nuclear power plant in David-Besse in Ohio, but luckily this was turned off anyway at that time[240]. Since 2006 nuclear power plants were shut down two times after cyber attacks[241]. In April 2009, hackers successfully intruded the US electricity net control[242] and installed programs that allowed manipulation and turn-off. China was suspected, that denied and also Russia.

3.2.9 Intrusion of US drones 2009/2011

Iraqi insurgents were able to use commercially available software to intrude U.S. drones which allowed them to view the videos of these drones[243]. In 2011, the Creech Air Force Base in Nevada that serves as control unit for Predator- and Reaper- drones reported a computer virus infection; but the US Air Force denied any impact on the availability of the drones[244]. Also, Iran was able to capture a US drone (type RQ-170) in 2011[245].
The US Navy decided in 2012 to switch the drone control bases to Linux which will be done by the military company Raytheon, the estimated costs are 28 million dollars[246]. The vulnerability of drones depends also on the drone type with can have different control modes and grades of system autonomy[247].

3.2.10 Local cyber conflicts

An increasing number of local military and/or political conflicts are accompanied by more or less coordinated cyber attacks which may occur over a longer period of time. These attacks can also affect computers of the opponents' security structure, but activities may be accompanied by parallel media campaigns[248]. Important examples, out of many, are the conflicts of India and Israel with actors from

[239] Gaycken 2009 with picture of power failure in Northeast USA 2003
[240] Wilson 2008, p.22
[241] ArcSight 2009
[242] Goetz/Rosenbach 2009, Fischermann 2010, p.26
[243] Ladurner/Pham 2010, p.12
[244] Los Angeles Times 13 October 2011
[245] Bittner/Ladurner 2012, p.3. As intrusion method, the use of a manipulated GPS signal (GPS spoofing) was discussed, but this could not be proven.
[246] Knoke 2012
[247] Heider 2006, p.9.
[248] Saad/Bazan/Varin 2010

neighbor states[249]. During the Crimea crisis in March 2014, cyber attacks were reported between Russia and Ukraine, also the Russian military firm **Rostec** claimed the capture of a US MQ-5B drone over the Crimea peninsula by electromagnetic jamming[250].

3.3 Sophisticated malware and hacker units

Meanwhile, several sophisticated hacker units and malware families were discovered and reported which are presented in the following chapters. Typically, it is assumed that these units are linked to or sponsored by states (government/intelligence/military). Reasons for this assumption are the efforts and complexity of the used tools, the need for specialists to maintain and hide the operations sometimes over several years, to select victims of high political and strategic relevance, to collect and analyze the gathered information and so on. Also, these attacks are typically cases where no immediate profit can be expected, in contrast to cyber criminals who could make money with banking trojans, ransomware etc.

Additionally, each group has its characteristic combination of access vectors, exploits/vulnerabilities, and toolkits which allow differentiation between groups[251]. A widely used term for this combination is **Tactics, Techniques, and Procedures (TTPs)**. As each group has a typical set of attack targets, the logic of target selection is also called **victimology**.

However, assignments to states should be handled with caution. Sometimes, false flags are set, i.e. misleading traces to blame another actor, or malware was utilized which is meanwhile known and available on the underground market. In certain cases, cyber weapons are even commercially available with restrictions.

Also, so far no government or authority has ever officially confirmed a link to a hacker unit. A 'linkage' to a state is a vague term, this does not indicate that a unit is a formal part of a government organization or only contracted or cooperating.

The below groups are the most prominent units in the media, the total number of larger active hacking groups is estimated around hundred groups.

From the US security analyst perspective, Russia has made significant progress with establishing sophisticated units within the last ten years. While **APT28, APT29** and **The Waterbug group** are attributed by many analysts to Russia, the links to Russia are still under debate for groups with focus on ICS/industry systems such as **Energetic Bear/Dragonfly** and **Sandworm/Quedagh**[252].

The **Comment Crew/APT1** and the **Axiom/DeepPanda Group** were discussed to be linked with China, while the **Lazarus Group** was assumed to be linked to

[249] Saad/Bazan/Varin 2010, Valeriano/Maness 2011, Even/Siman-Tov 2012, p.37
[250] FAZ online 2014
[251] See also Jennifer 2014
[252] See e.g. Jennifer 2014

North Korea. The **Equation Group** is typically assumed to be linked to US, with common reference to the so-called *Snowden leaks*. But please note that all respective governments denied and declined to comment.

3.3.1 The Equation group

The first subsection presents the detection history of Stuxnet, Duqu and Flame malware which started with the discovery of Stuxnet in 2010, followed by Flame and Duqu.
Later on, it was shown that Stuxnet already existed at least since 2005.

Researchers of *Kaspersky Labs* discovered the Equation Group in 2015 that was already active since many years, with first traces back to the year 1996. This is presented in the second subsection. Stuxnet, Duqu and Flame together with other malware families could be assigned to the Equation Group. However, as the earliest Stuxnet versions were somewhat different, also with a different attack target (valves instead of centrifuges), the involvement of a second programming group may be possible.

The third subsection presents the **Shadow Brokers** incident from August 2016. The malware presented by them was claimed to be taken from the Equation Group which was linked by media to the NSA, due to similarities to malware presented in the Edward Snowden leaks. However, evaluations could not show that the NSA was hacked; also the malware was from 2013 or older.

3.3.1.1 Detection history - The ‚digital first strike'

A series of sophisticated spyware programs and Trojans was deployed to computers mainly in Iran from end of 2006 on. A very large computer program called **Flame** served as technology platform for development and application of further programs such as **DuQu** and later on **Stuxnet** that affected uranium centrifuge control in Iranian nuclear facilities. In 2011 and 2012, US newspapers have reported that these activities were part of an US-Israeli plan called '**Olympic Games**' to stop Iran's nuclear plants, but this was officially not confirmed. The following section presents the events by order of discovery.

Industrial Control Systems ICS such as Supervisory Control and Data Acquisition SCADA[253]) allow remote control of and communication with machines.
Stuxnet is a malware that was used for the first large-scale attack on SCADA systems, here on Siemens systems in particular[254].

[253] Shea 2003
[254] Welt online 2010b. Consequently, Siemens expands its cyber war research capacities, Werner 2010, p.7

Stuxnet is a **worm,** i.e. a program that is able to spread actively to other systems[255]. The infection was started via an infected USB-stick and Stuxnet exploits security gaps in Windows LNK-files to intrude systems[256]. Falsified security certifications (digital signatures) of Realtek and Semiconductor, which were not aware of this, helped Stuxnet to install itself in the operating system Windows 7 Enterprise Edition[257].
The Simatic S7-system of Siemens is running under a Windows environment, also the WinCC software for parameter control and visualization[258]. Stuxnet executes a systematic search for WinCC and the Step 7-software in Simatic S7 to detect and to infect the versions S7-300 und S7-400, but only if a CP 342/5 network interface is used thus demonstrating a high selectivity of Stuxnet[259]. In case of success, Stuxnet starts to send information to external servers, thereof two servers in Malaysia and Denmark. Stuxnet also contains rootkits, i.e. tools for control of computers[260].
Stuxnet is also searching for other applicable systems by exploiting the *autorun*-function of Windows. After a certain number of successful infections, Stuxnet deactivates itself[261]. It was assumed that uranium gas centrifuges needed for construction of nuclear bombs were damaged in Iran, as the number of centrifuges declined in 2009 and the International Atomic Energy Agency (IAEA) reported downtime also in 2010[262], which was confirmed by Iran[263][264].
These issues, the use of several unknown security gaps (**zero-day-exploits**) and the estimated development costs of about 1 Million US-Dollars[265] resulted in the theory of a new weapon constructed by secret services to damage the Iranian nuclear program[266].

The above Stuxnet properties are applicable for Stuxnet Version 1.0 or higher. Symantec reported in 2013 that earlier versions existed that can be distinguished

[255] As Stuxnet has dozens of functions and tools, it sometimes also described as Trojan horse or virus, FAZ2010a.
[256] On 13 Oct 2010 Microsoft released 16 Updates to cover 49 security gaps, Handelsblatt 2010, p.27
[257] Rieger 2010, p.33, who invented the term ‚digitaler Erstschlag' (‚digital first strike').
[258] Krüger/Martin-Jung/Richter 2010, p.9
[259] Schultz 2010, p.2
[260] Kaspersky 2010
[261] Falliere 2010
[262] FAZ2010c, p.6
[263] refer to FAZ2010d, p.5, where it was also reported that on 29 Nov 2010 the leading cyber expert and coordinator of a Stuxnet task force, Madschid Schariari, was killed.
[264] The Institute for Science and International Security (ISIS) assumed due to respective findings in the Stuxnet code and the temporary reduction of available uranium gas centrifuges in Iran, that possibly 1000 Type IR-1 centrifuges were affected by Stuxnet. According to this analysis, Stuxnet could change the rotation frequency from the nominal value of 1064 Hertz to 1410 Hertz or to 2 Hertz leading to an unusual amount of centrifuge breakage (such breakage however also can occur during normal usage); ISIS 2010. Stuxnet also secretly recorded normal functions and simulated normal function to plant controllers during its actions, Broad/Markoff/Sanger 2011, p.3.
[265] Schultz 2010, p.2
[266] Ladurner/Pham 2010, p.12

via different exploits used for intrusion. Stuxnet version 0.5 was developed from November 2005 on and used from November 2007 on. The infection was done via Step 7 Systems only and led to a random close of valves which could damage the uranium gas centrifuges. Infections with version 0.5 stopped in April 2009[267].

The New York Times reported on 15 Jan 2011 that the Department of Homeland Security and the Idaho national laboratories as part of the US Energy department checked Siemens systems for vulnerabilities in 2008[268]. In the same article, it was speculated that findings from these tests were then possibly used by an Israeli-US-intelligence cooperation to develop Stuxnet after they were able to build models of the uranium gas centrifuges for test purposes.

On 01 June 2012, the New York Times reported that Stuxnet was part of a cyber attack program called **Olympic Games** that was initiated in 2006 by the former US president George W. Bush[269]. The reports of the NY Times were *not* officially confirmed, but elements of the 2012 article were regarded by US Government officials and politicians as unauthorized disclosure of confidential information (but it was not said *which* elements) [270].

Erroneously, Stuxnet infected the computer of an engineer and then spread over the internet to other countries[271]. This would explain why other states were also affected, in particular Indonesia, India, Azerbaijan and Pakistan, and also many other states such as the USA and Great Britain[272]. Moreover, Stuxnet was not perfect even from the perspective of the attacker: Stuxnet was programmed to act within a certain time window, but as some internal computer clocks are altered to bypass license agreements, this did not work. Thus, Stuxnet was probably highly selective with regard to the system, but not with regard to time and location of attack[273].

Stuxnet may have unintended effects. The designers of Stuxnet have shown their sophisticated understanding of cyber war, but now this knowledge is disclosed to the public[274].
The German media reports on Stuxnet showed a strange ‚reporting gap' of 2 months. Newspapers started articles around mid of September 2010, while Stuxnet was already discovered in June 2010 by a Belorussian company. A commercially

[267] McDonald et al. 2013, p.1-2
[268] Broad/Markoff/Sanger 2011, p.4
[269] Sanger 2012, p.3
[270] NZZ 2012, p.1, FAZ 2012b, p.7
[271] Sanger 2012, p.6
[272]Handelsblatt 2010, p.27, Symantec 2010, p.5-7
[273] Gaycken 2010, p.31 explained that the time window of Stuxnet was repeatedly changed by the attackers, acc. to Symantec (2010, p.14) to 24 Jun 2012
[274] Rosenbach/Schmitz/Schmundt 2010, p.163; Rieger 2011, p.27

available protection software was already released since 22 July 2010, refer also to the report of *Bloomberg Businessweek* on 23 July 2010. The Iran confirmed the Stuxnet attack already on 26 July 2010 in *Iran Daily*[275]. Siemens confirmed that 15 clients were affected, thereof 60% in the Iran. Possible explanations for this gap may be the upcoming assumption of intelligence involvement, a presumed infection of the nuclear plant in Buschehr and the debate of the new NATO strategy[276].

The Stuxnet attack was accompanied by other activities. Significant portions of the source code of industry spyware **W32.DuQu** that was detected in September 2011 were identical to Stuxnet[277]. DuQu used a stolen security certificate from a Taiwanese company for intrusion and was e.g. able to make screenshots, keylogging and to extract information and like Stuxnet it had an expiry date with self-destruction[278]. It was speculated that DuQu may have been created to gain information from the target systems for creation of Stuxnet[279].
After Iranian oil terminals were affected by a data destruction virus called **Wiper** in April 2012, the security company Kaspersky Labs discovered another multifunctional 'virus'[280] in May 2012 named **Flame** that gives very detailed system information about the infected systems and that again had some technical overlaps with Stuxnet[281]. *Washington Post* reported that Flame was already developed in 2007 and also part of the cyber activities against Iran[282]. The program part that allowed the distribution of Flame via USB-sticks was first used in Flame and then in Stuxnet[283].
Later in 2012, further malware technically related to Flame was reported: the Trojan **Gauss** collected information on financial transactions, e.g. from banks in Lebanon and a small Flame variant called **Mini-Flame**[284].

3.3.1.2 Equation group cyber tools

In early 2015, the security company *Kaspersky Labs* reported the existence of a new malware family called the **Equation group**. It is noteworthy that the malware

[275] Iran Daily 26 July 2010
[276] Knop/Schmidt 2010, p.20
[277] Goebbels 2011, p.8. The name came from the DQ-prefix used in the program files.
[278] Goebbels 2011, p.8
[279] Welchering 2012, p.T1
[280] Flame was much larger than normal viruses with 20 MB and functions included key logging, screenshots, control of audio functions, data flow and it had access to Bluetooth applications, Spiegel 2012, p.123. Like Stuxnet, it had also a self-destruction function. The name came from the word flame used in the program files. Flame is an example, why the conventional differentiation between viruses, worms and Trojans becomes less relevant.
[281] Welchering 2012, p.T1, Graf 2012, p.8, Gostev 2012, p.1
[282] Graf 2012, p.9
[283] Nakashima/Miller/Tate 2012, p.1-4
[284] Focus 2012, Symantec 2012, Mertins 2012, p.10

could be tracked back to 2001, perhaps even to 1996. Due to technical overlaps, there are some things that may indicate that Stuxnet is part of a larger group of malware.[285]

Originally, two groups of malware programs were set up on the Equation Group platform, one called **EquationLaser** used around 2001-2004 which was then followed by the malwares **EquationDrug** and **Grayfish** presumably developed between 2008 and 2013, the other one was **Fanny** created in 2008 which used two zero-day exploits that were later on used for Stuxnet, and computers infected with Fanny were partially upgraded later on to the malwares **Double Fantasy** and **TripleFantasy**. The two malware groups were used together, a typical infection way was infecting computers by web exploit, then DoubleFantasy is installed to check whether the infected computer is an interesting target and if so, EquationDrug or Grayfish are loaded[286].

Grayfish injects malicious code into the boot record of the operating system and takes over total control of the computer, i.e. it runs the whole computer[287]. It collects data and puts them as **encrypted Virtual File System** into the Registry section of the computer, and it is not visible to antivirus products[288]. Fanny is a worm that infects computers not connected to the internet by USB-Sticks and then sends all information as soon as the stick is put into an internet-linked computer. [289]

The Equation group malware is also spread by **interdiction**, i.e. replacing shipped CD-ROMs and other physical media and replacing them by infected media. Also, EquationDrug and Grayfish are able to infect firmware, i.e. the hardware-embedded essential programs of a computer[290]. This makes the malware resistant against reinstallation of operating systems and allows deeply hidden data storage. However, these complex infection methods were used only against high-level targets, i.e. a few hundred computers.

Important links between the equation malware family and the Stuxnet-related malware family are the following[291]: In one infection step, Grayfish uses a hash code self-encryption step that shows similarities to the Gauss malware. Fanny, Stuxnet, Flame and Gauss use the same LNK exploit while Fanny, Stuxnet,

285 Kaspersky Lab 2015, p.3
286 Kaspersky Lab 2015, p.5, 8
287 Kaspersky Lab 2015, p. 10. Already the EquationDrug malware was able to get full control over the operating system, see p.8
288 Kaspersky Lab 2015, p. 10-12
289 Kaspersky Lab 2015, p. 13
290 Kaspersky Lab 2015, p. 15-16
291 Kaspersky Lab 2015, p. 5

Double Fantasy and Flame use a certain escalation of a privilege account. Finally, DoubleFantasy, Gauss and Flame use a certain way of USB infection.

In mid 2015, *Kaspersky Labs* reported that they were infected by **DuQu 2.0**, a malware with similarities to DuQu[292]. Also, other high-level targets were approached, in particular computers of participants of the P5+1 events, i.e. the talks about the Iran nuclear program. The malware used an exploit that allowed lateral movement, i.e. that an unprivileged domain user could elevate credentials to a domain administrator account[293]. The programmers set a series of **false flags** to mislead researchers, these are strings used in other already known malware from other attackers[294]. Also time stamps were manipulated.

Regin is a multi-staged, modular threat, i.e., it can upload further features for a tailor-made attack on a specific computer and was discovered in late 2014, but may have been created already in 2008 or earlier. While there no evidence for a relation to Stuxnet was reported, Symantec found a similar level of sophistication with the modular approach that has been seen in Flame and Weevil (Careto/The Mask), while the multi-stage loading architecture was similar to that seen in the Duqu/Stuxnet family of threats[295].
Also, similar to Equation group, encrypted virtual file system containers and RC5 encryption is used[296]. Regin has multiple properties, such as monitoring traffic, stealing information and collecting data[297]. As in the malware described above, only a few selected high-level targets were attacked[298].

In February 2014, another cyber attack was reported by *Kaspersky Labs*[299]. The malware **Weevil (Careto/The Mask)** was able -amongst other many functions- to record Skype VoIP talks. As in various other sophisticated cyber attacks, only a few computers were infected, but the profile of the targets is quite typical: research units, providers of critical infrastructures, diplomats, embassies and political activists. Despite the sophisticated modular approach, a clear link to Equation Group was not yet shown, the origin remains unclear.

3.3.1.3 The Shadow Brokers incident

In August 2016, a previously unknown group called **Shadow Brokers** claimed to have cyber weapons from the Equation Group. To provide evidence, they released

[292] Kaspersky Lab 2015b, p. 3
[293] Kaspersky Lab 2015b, p. 4
[294] Kaspersky Lab 2015b, p. 43
[295] Symantec 2014a, p.3
[296] Symantec 2014a, p.3
[297] Symantec 2014a, p.11
[298] Martin-Jung 2014, p. 17
[299] Kaspersky 2014

a public file with material and offered a second file for 1 million Bitcoins (500 million Euros at that time) in an auction[300]. However, the auction was quickly taken offline, the last offer was 0.12 Bitcoins (60 Euro). [301] Media speculate that this was a symbolic warning by Russia that was accused for the **DNC hack** (see next section) by media, i.e. to show that they are also able to trace and unveil espionage from others as needed[302].

The analysis of the public file showed that it was software from 2013, the assumption of security experts was that this material was copied from a command and control server used by the Equation Group, i.e. no 'NSA hack' or similar.
In a later statement on *Pastebin* and *Tumblr* –claimed to come from the hackers- they explained that a contractor from the company *RedSeal* took away copies after a security exercise. *RedSeal* is an *In-Q-Tel* portfolio company[303]. In-Q-Tel was founded by the CIA as Venture Capital firm in 1999 for strategic investments in start-ups etc. The statement maybe correct, but it is uncommon that hackers disclose their access strategy, so theoretically it may be a communication to obfuscate other vulnerabilities or an attempt to involve the CIA into this affair.

The material seemed to be real and some file names were identical to names presented by Edward Snowden as NSA tools, such as *Epicbanana, Buzzdirection, Egregiousblunder, Bananaglee, Jetplow and Extrabacon*[304]. The IT technology firms *Cisco* and *Fortinet* confirmed that there were real security gaps, one of the Cisco gaps was not closed at time of report, while Fortinet gaps affected only older versions[305].

3.3.2 APT28 and APT29

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

APT 28 (aka Sofacy, Pawn Strom, Csar Team, Sednit, Fancy Bear) is a group focusing on targets of political relevance for Russia. The malware compilation times correspond with Moscow time zone, Russian language is used, and typically tools for continued long-term use are used. Backdoors use http protocol and the mail server of the target computer[306]. APT 28 uses a variety of malware droppers (**Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer and DownRange**) and also malware for smartphones[307].

[300] Jones 2016
[301] Beuth 2016b, Spiegel online 2016
[302] Jones 2016
[303] Ragan 2016
[304] Steier 2016b, Spiegel online 2016, Solon 2016
[305] Steier 2016b
[306] Weedon 2015, p.71-72
[307] Alperovitch 2016

APT28 was under discussion for attacks on TV5Monde and German Parliament (Bundestag) network attack as well.
In 2015, the French Television **TV5Monde** was temporarily taken offline by apparently jihadist hackers, but later on traces to APT28 were found[308]. The server for the satellite signals was attacked and as the maintenance of this server was done by another vendor, a longer signal downtime was achieved[309].

In the same time, the German Intelligence BfV was informed by a foreign source that a cyber attack with data traffic from two Bundestag computers to an Eastern European server was going on[310]. Investigations confirmed intrusion of several computers by infected emails[311], including takeover of administrator rights[312]. As it was not possible to detect the complete extent of infection, the Federal Office for Information Security BSI recommended exchanging the whole network. The Bundestag IT infrastructure was not part of the secure IVBB government network[313]. Interestingly, the attack showed similarities to the cyber attack on TV5Monde[314].
One of the servers used for the Bundestag attack was identical with those used for the attack on the DNC in 2016 and also one falsified security certificate[315].

3.3.2.2 APT29 (aka Cozy Duke/Cozy Bear)

In Feb 2013, a new malware called **MiniDuke** was discovered by *Kaspersky Lab*. This consisted of 20 KB in the old computer language Assembler and was placed into PDF-files that sent with spear-fishing the emails. By this, 59 computers in 23 states were infected. The malware worked as beachhead to allow installation of further malware. MiniDuke was able to check whether it was in a **virtual machine** (simulated computers) and used Twitter for communication with attack servers. Also, information was hidden into small pictures, a method known as **steganography**. Such virtual machines can be part of cloud systems, but are also used as analysis tool for malware and in such machines, the program was inactive then to prevent analysis[316].

---

[308] FAZ online 2015, p.1
[309] Wehner 2016, p.6
310 Baumgärtner/Röbel/Schindler 2015, p. 28. After initial analysis, the **Russian Foreign Intelligence SWR** was suspected as attacker, Baumgärtner/Müller/Röbel/Schindler 2015, p.34.
311 Mertins 2015, p.4
312 Hoppe/Osman 2015, p.1
313 Erk et al. 2015, p.2
314 FAZ online 2015, see also Wehner 2015, p.1
315 Baumgärtner/Neef/Stark 2016, p.90-91
[316] Raiu/Baumgartner/Kamluk 2013

The Dukes are a malware family with a growing number of toolsets known as **MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke** and **GeminiDuke** which are used by a group known as **The Dukes** or also as **APT29**[317]. The attacks show a two-step pattern with initial breach and rapid data collection, then in case of a relevant target changing to long-term observation tools[318]. For this action, multi-step loading and backdoors are available. Remote Access Tools (RATs) include **AdobeARM, ATI-Agent,** and **MiniDionis**[319]. To avoid detection, the malware checks the security measures of the infected computer in detail. The profile of infected computers (of relevance for Russian federation from a security policy perspective), the time zones used for programming (matching Moscow), the use of highly-targeted spear phishing emails and a Russian-language error note in PinchDuke samples were the reasons to assume that the Dukes are programmed and used by an advanced Russian cyber espionage group.

3.3.2.3 The DNC hack

The Democratic National Committee (DNC), the formal governing body for the US Democratic Party alerted the security firm *Crowd Strike* due to an attack on their systems[320].

The APT29 intrusion was going back to summer of 2015, while APT28 intruded the network independently in April 2016. This second intrusion interfered with the first one and led to discovery. separately breached the network in April 2016. APT29 used the **SeaDaddy** implant, which finally allowed launching malicious code automatically as needed while APT28 operated with its **X-Agent** malware to do remote command execution, file transmission and keylogging[321]. The US evaluators are convinced that this was caused by Russia, while Russian government denied this[322]. One of the servers used for the DNC attack was identical with those used for the attack on the German Bundestag in 2015 and also one falsified security certificate[323].

Later on, a Romanian hacker named **Guccifer 2.0** claimed to be the attacker, but he was not able to respond properly in Romanian language to questions and used a Russian-based communication channel[324]. As a result, Guccifer 2.0, if existing, was also suspected by US to be a member of Russian intelligence who later on released contact data of leading members of the Democratic Party[325].

---

[317] Weedon 2015, p.70-71
[318] F-Secure Labs 2015
[319] Alperovitch 2016
[320] Alperovitch 2016, Nakashima 2016a
[321] Alperovitch 2016
[322] Nakashima 2016a
323 FAZ online 2015, see also Wehner 2015, p.1
[324] Baumgärtner/Neef/Stark 2016, p.90-91
[325] Lichtblau/Weiland 2016

End of August 2016, it was detected that online voting ystems were intruded in Illinois and Arizona, in Illinois data of 200,000 voters were copied[326]. Media speculated that this was part of a Russian campaign, but definite evidence was not yet found.[327]

3.3.3 The Waterbug group (Turla malware family)

Waterbug is the name for the actors who used the malware **Wipbot/Tavdig/Epic Turla**, **Uroburos/Turla/Snake/Carbon** and **agent.btz/Minit**.

In 2008, it was reported that 1,500 pentagon systems were shut down after the U.S. Defense Secretary's e-mail was breached. A successful intrusion in the Pentagon system resulted from an infected USB stick that was inserted into a computer linked to the Pentagon by a naive soldier in the Near East region[328]. The infection by a worm called **agent.btz/Trojan Minit** led to a set of security measures called **Operation Buckshot Yankee** which also included the creation of the US Cyber Command[329].

The multi-functional malware named **Uroburos/Turla/Snake/Carbon** is a rootkit that is able to connect computers within intranets as peer to peer-network and has multiple technical links to **agent.btz/Trojan Minit**[330]. Within this network, Uroburos is then searching for a computer that has internet access to conduct data exchange. It is noteworthy that Uroburos remains inactive in computers that are already infected by the malware agent.btz indicating the same source[331]. Attackers used Snake/Uroburos/Turla against Ukrainian computers in 2013/2014. Together with agent.btz from 2008 it seems to form a malware family that could be backdated to 2005. The group is utilizing satellite-based internet links for action[332].

Wipbot/Tavdig/Epic Turla was found in the systems of the Swiss armament company RUAG after first hints in Sep 2014; the Waterbug group stopped the activities in May 2016, when they noted from media reports that RUAG was aware of the intrusion[333].

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

3.3.4 APT1 (Comment Crew)

Chinas People Liberation Army PLA is suspected to have specialized cyber units in approximately 6 main locations[334]. The US agency NSA was reported to track about 20 Chinese units in 2014, over half of them PLA cyber units[335].

The Third Department of the PLA is responsible for Signal Intelligence SigInt operations and is divided into twelve offices (bureaus). The 2nd Bureau is also known as **Unit 61398** which assumed to have a focus on English language organizations while the 12th Bureau, **Unit 61486** is assumed to have a focus on satellite/aerospace industries. Unit 61486 was named **Putten Panda** by security firms and attack activity from Unit 61486 has been linked to Unit 61398 based on shared infrastructure[336].

In 2013, the Cyber security company **Mandiant** presented an in-depth analysis of Chinese cyber activities[337]. The cyber war unit 61398 in the Datong Road in Pudong near Shanghai conducted 141 major cyber attacks on government institutions, companies and energy suppliers in the previous years and Mandiant stated that the hacker group APT1 may be identical with a state-backed cyber unit 61398 which was strongly denied by China. The standard cyber tactic was to send spear-phishing mails containing malware that installed small backdoor programs to allow further actions.

Later on, 5 Chinese senior military persons were officially accused by US, including a person assumed to be the hacker with the cover name '**UglyGorilla**'. China rejected the accusation, but US media speculated in 2016 that this may have caused the decrease on cyber attacks suspected to come from China in the last two years[338].

3.3.5 Axiom Group (Deep Panda)

The Axiom Group is also known under many other names, such as **DeepPanda, Shell_Crew, Group 72, Black Vine, HiddenLynx, KungFu Kittens** etc.
The group was observed to do highly sophisticated spear-phishing attack by **piggybacking** (settling) on ongoing real conversations to motivate the victim to click on compromised links[339].
Within the **Operation Aurora** the intruders tried to gain access to computer programs and source codes of companies of the IT sector (such as Google and

[334] Finsterbusch 2013, p.15
[335] Perlroth 2014
[336] Novetta 2015, p.15, Perlroth 2014
[337] Mandiant 2013
[338] Mandiant 2013, Jones 2016, p.5, Nakashima 2016b
[339] Alperovitch 2014. The company *Crowd Strike* used a kernel sensor (*Falcon host*) deployed on Windows and Mac servers, desktops, and laptops that detected attcks and compared them to a threat intelligence repository for attribution.

Adobe) and from high-tech companies of the security and defense sector in 2009[340]. Other operations included the Elderwood platform attack from 2011-2014, the VOHO Campaign wateringhole attacks on nearly 1000 organizations in 2012 an attack on Japanese targets 2013, and attacks on US think tanks in 2014. Various zero-day exploits and specific malware families were used such as **Zox, Hikit, Gh0st RAT, PoisonIvy, Hydraq** and **Derusbi**[341]. Note that Zox and Hikit were only seen in Axiom activities, while the other malware was also used by other organizations[342]. Attack targets included a wide range of government organizations, companies from technology sector and academic institutions.

3.3.6 The Lazarus group

Over several years, intrusion and wiper attacks were observed primarily in South Korea (in particular Operation Troy in 2009, Darkseoul/Destover in 2013) and US, but also in other countries.
At the end of 2014, a cyber attack on **Sony Pictures Entertainment (SPE)** was under discussion as this affected the release of a cinema movie called *The Interview* that was about North Korea. An important aspect was the use of wiper malware that deleted data and files from the infected computers. However, this attack seemed to be only an overlap of different long-term series cyber attacks. Sony was frequently attacked in the recent years, while South Korea was affected by a long-term cyber espionage campaign. Further, this was the third large wiper malware attack in the last years. So each possible dimension of the attack needs to be analyzed separately. Also, this shows the practical challenges of attribution and digital forensic efforts.

In 2016, a joint effort of IT security firms like *Symantec*, *Kaspersky*, *Alien Vault* etc. led by *Novetta* called **Operation Blockbuster** was made[343]. The joint analysis showed strong evidence that at least two of the three large wiper attacks and the Sony/SPE hack were conducted by the same group called **Lazarus group**[344]. While many traces led to the conclusion that the Lazarus group is somehow linked to North Korea, definite evidence is still missing. The group permanently expands its malware, such as the Trojans **Hangman/Volgmer** in 2014 and **Wild Positron/Duuzer**[345] in 2015.
In summer 2016, the Lazarus Group was discussed to be behind the attacks on the SWIFT interbanking system, see Section 3.3.6.4.

[340] Markoff/Barbosa, 18 Feb 2010
[341] Novetta 2015, p.12-13
[342] Novetta 2015, p.20
[343] Novetta 2016
[344] Novetta 2016
[345] Guerrero-Saade/Raiu 2016, p.2

Novetta identified 45 malware families with multiple examples of code reusage and programming overlaps. This included special issues like similar **Suicide Scripts** to remove executable malware programs after completion and a typical **space-dot-encoding**, where terms that could be detected by security software are spread by dots and normally unnecessary symbols between the letters[346]. Also the programs included specific typos such a 'Mozillar' instead of ‚Mozilla' across several malware families, a use of BAT files across various Hangman/Volgmer variants to delete components of the malware after infection and also there was a reuse of a shared password across malware droppers for different malware variants[347]. The time stamps of the program indicate that the attackers are probably located on a time zone of GMT+8 or GMT+9 which would match Korea[348].

3.3.6.1 Wiper Malware Attacks

On 15 August 2012, the Saudi-Arabian Oil company ARAMCO was attacked the **Shamoon/Disttrack** malware; on 20 March 2013 South Korean banks and broadcasters were affected by a malware called **DarkSeoul/Jokra** while Sony was attacked by the **Destover** malware on 24 November 2014. There were certain similarities:

After intrusion, the wiper malware was placed on the infected computers[349]. The commercially available software **EldoS RawDisk**[350] was used to access Windows drives. In all cases, the malware was used as a **logic bomb**, i.e. a malware that executes actions at a predefined timepoint[351].

In all three cases, data were deleted from computers and file-server hard drives and re-booting was blocked. In the Aramco case, oil supply was temporarily affected[352] (32,000 computers damaged), in Seoul business of affected companies was temporarily interrupted (30,000 computers damaged), for Sony Pictures this ended amongst other damages and data leaks with the initially cancelled and later on limited release of the movie *The Interview*.

Moreover, in all cases the attack was claimed by 'hacktivist' (hackers and activists) groups, but various authors assume that they may have been created to

346 Novetta 2016
347 Guerrero-Saade/Raiu 2016
348 Guerrero-Saade/Raiu 2016, p.6
349 This was done stepwise. For Darkseoul, a remote access trojan as backdoor was compiled on 26 January 2013, the wiper already on 31 January 2013 while a dropper trojan for attack start was compiled at the day of attack on 20 March 2013, McAfee 2013, p.4
350 Baumgartner 2014, p.2, 4
351 Darnstaedt/Rosenbach/Schmitz 2013, p.76-80
352 As already mentioned earlier, Iranian oil terminals were already attacked with Wiper Malware in April 2012

cover state-driven activities or as proxies for states[353], these were *Cutting Sword of Justice* (Aramco), *Whois/NewRomanic Cyber Army Team* (for Darkseoul hack[354]) and the *Guardians of Peace* (Sony Pictures). From Operation Blockbuster, it is now apparent that *Whois/NewRomanic Cyber Army Team* and the *Guardians of Peace* were cover names for members of the Lazarus group[355].
All attacks were accompanied by warnings with graphical illustrations (such as skeletons, skulls) and/or vague statements which did not allow identifying a clear political position[356]. The English used in the messages indicated non-native speakers as authors.

Operation Blockbuster provided many findings supporting a relationship between the Darkseoul attack and the SPE hack. However, no clear relationship to the wiper attack on Aramco and the Shamoon malware could be found. Novetta assumed that the Lazarus group and the Aramco hackers had contact via a technology exchange treaty between Iran and North Korea[357]. However, it needs to be clarified further why the Lazarus group would have been in need for help from outside as they showed their attack capability already years before, also Iran itself suffered from a wiper attack in the same year.

3.3.6.2 Cyber espionage in South Korea

The IT security firm McAfee identified a long-term cyber espionage from at least 2009 to 2013, where a "Troy" family of Trojans (named after the Trojan **HTTP Troy**) with many similarities was used to attach military targets as well as other firms. For example, the attacks on military targets used a shared complex encryption password which was also used for the **TDrop** malware that was part of the DarkSeoul attack[358]. Furthermore, there were similarities with respect to source code and use of certain dll.files. This is also an indicator that the attacks were more than **cyber vandalism**, i.e. attacks with the only intent to damage intruded systems.

The IT security firm Symantec was also able to link several non-military attacks against banks and broadcasters to the DarkSeoul attackers who in addition to the attack on 20 March 2013 (Symantec calls the malware **Trojan.Jokra**) used the Trojans **Dozer** and **Koredos** as part of DDoS and wiper malware attacks in 2009

353 McAfee 2013
354 Sherstobitoff/Liba/Walter 2013, p.3. The IT security firm CrowdStrike thinks that the attackers are the same as the group they called Silent Chollima, which has been active since 2006 already, see Robertson/Lawrence/Strohm 2014.
355 Novetta 2016
356 See e.g. Baumgartner 2014, p.4-6
357 Novetta 2016, p.15
358 McAfee 2013, p.28

and 2011[359]. On the 63th anniversary of the Korean war, the Trojans **Castov** and **Castdos** were used to initiate DDoS attacks against the South Korean government. In late 2014 and in parallel to the Sony Hack, the only South Korean nuclear plant provider **Korea Hydro and Nuclear Power Co (KHNP)** was repeatedly attacked and a series of technical and personal data was leaked[360].

3.3.6.3 The 'Sony Hack´ (aka SPE hack)

The term Sony Hack was used for the attack of the **Guardians of Peace (GoP)** group in media. However, Sony as media provider was also attacked by others, e.g. in April 2011 a massive attack including taking data of 77 million Playstation user accounts by unknown attackers was reported[361] and in December 2014, Sony was hacked by the Group **Lizard Squad**[362][363].

On 21 November 2014, intruders calling themselves Guardians of Peace notified Sony of having 100 Terabytes of data and asked for money to prevent publication[364]. On 24 November 2014, the release of data started, as indicated in the warning by the GoP. On 01 December 2014, large portions of Sony data including employee data were leaked from the St Regis Hotel in Bangkok/Thailand and other locations. Further data were leaked in the following days [365]
On 16 December 2014, the GoP explicitly mentioned the movie *The Interview* and exposed terror threats with reference to 9/11; the planned release of the movie on 25 Dec 2014 was cancelled a few days before[366].

As a consequence, President Obama considered this as an act of **cyber vandalism** and asked China for support against North Korean cyber attacks, as the only Internet provider in North Korea is China Unicom[367]. A subsequent internet collapse on 22 Dec 2014 in North Korea caused speculations that this may have been some kind of retaliation, but on the other hand the North Korea had sometimes technical issues already before.[368] At Christmas 2014, the movie *The Interview* was then published in a limited number of cinemas. Furthermore,

359 Symantec 2013, p.1-2
360 Leyden 2014, p.1-3. KHNP confirmed that no critical data were leaked and initiated cyber exercises to enhance security.
361 Lambrecht/Radszuhn 2011, p.25, Betschon 2014, p.34
362 In 2015, the Hacking platform **Darkode** was closed by Europol and FBI after successful use of under-cover agents, Finsterbusch 2015, p.26. Lizard Squad used this platform.
363 Handelszeitung online 2014, p.1
364 Fuest 2014b, p.31
365 Betschon 2014, p.34
366 Steinitz 2014, p.11
367 FAZ 2014a, p.21. FAZ 2014b, p.1. The North Korean internet has a few thousand IP addresses, as there is a national intranet called Kwangmyong (Brightness) with some thousand websites, SZ2014a, p.1
368 SZ2014b, NZZ 2014

sanctions against some North Korean individuals were imposed in early 2015, but these were not related to the Sony hack, but to military technology matters[369].

The origin of the attack was intensely discussed. The key arguments for North Korea as attack origin were the following:
The FBI found that attackers used some IP addresses exclusively used by North Korea for the Sony Hack and their Facebook accounts, probably inadvertently[370]. Also, there are the similarities described in wiper malware attack section above. The system settings of the computer used for malware compilation were Korean, the malware also contained some Korean terms[371]. Also, The Sony Hack and other attacks on South Korea used a common command and control server located in Bolivia[372]

Moreover, North Korea's primary intelligence agency, the **Reconnaissance General Bureau** was reported to have certain cyber capabilities, in particular two units called **Unit 121** and **No. 91 office**. There are a few reports that due to the limited internet structure persons of these units may work outside North Korea[373]. Also it was argued that North Korea had a reasonable political motive[374], but North Korea strongly denied any involvement in the attack[375].

Alternative theories were discussed, because initially intruders asked for money[376] and later on, after media speculated about a link to the movie *The Interview* switched to political statements asking to cancel the publication of the movie. The Norwegian IT security firm Norse suspected 6 Persons from US, Canada, Singapore and Thailand to be the Guardians of Peace, one of them was a former Sony employee with knowledge of the company IT network[377]. In particular, the employee had documented communications with other persons, one them could be directly related to a server where the first version of the malware was compiled in July 2014[378]. IP addresses used in the attack were also used by other hacking groups and elements of the malware would have been available on the black market[379][380].

369 Zoll 2015, p.1
370 FBI Director James Comey cited in Schmidt/Perlroth/Goldstein 2015, p.1f.; the exclusive use by the North Koreans was mentioned in a tweet of KajaWhitehouse who also cited Comey.
371 Fuest 2014b, p.31
372 Robertson/Lawrence/Strohm 2014, p.1
373 Robertson/Lawrence/Strohm 2014, p.2
374 Fuest 2014b, p.31
375 NZZ 2014
376 Fuest 2014b, p.31
377 See SZ 2014c, Bernau 2014, p.1
378 The Security Ledger online 2014, p.1
379 See e.g. Bernau 2014, p.1

US authorities confirmed their assessment and argued that they cannot present all details of evidence, otherwise hackers would get too much insight into the investigation methods[381]. Thus, the FBI kept its conclusions on the attack origin[382]. In addition, the *New York Times* reported that the NSA would have been able to intrude North Korean network via Malaysia and South Korea which enabled them to observe and track North Korean hacking activities, but this report was not officially confirmed[383].

3.3.6.4 The SWIFT Attacks

In summer 2016, the Lazarus group was assumed by security experts of BAE systems to be behind the intrusion of the global financial network Society for Worldwide Interbank Financial Telecommunication **SWIFT**, which allowed transferring 81 Million Dollars from the central bank of Bangla Desh to other accounts on 04 Feb 2016[384]. The original plan was to transfer 951 million Dollars, but a typo in the word 'foundation' alerted the bankers and further transfers were stopped. The vulnerability probably resulted from computers that were not up to date; the transfer time which was outside working hours in Bangla Desh to avoid that someone could be informed or asked there before the transfer[385]. Meanwhile, more cyber attacks on SWIFT were reported for banks in Ecuador, Russia, Ukraine and Vietnam[386]. The wiping code used to hide the bank hacks was the same used in the SPE attack[387].

3.3.7 Other groups

In Section 2.2.8, two sophisticated hacker groups with focus on industry are presented, the group **Dragonfly** (**Energetic Bear/Crouching Yeti/Koala**) and the **Sandworm/Quedagh** group that uses the **BlackEnergy** malware.

Another complex malware of unknown origin leading to a high-level infection of diplomatic and government institutions from 2007 to 2013 was **Red October**. By spear-phishing, a Trojan was placed on the victim computers to extract files also

---

[380] Fuest 2014b, p.31. Theoretically, the initial leaks and the terror threats could also have been done by different actors as there was some inconsistent communication via the GdP mail address (see also Fuest 2014b, p.31 reporting a North Korean Hacking Army, but with Korean language errors).
[381] Zoll 2015, p.1
[382] SZ 2014c
383 FAZ 2015a, p.5. The question came up why the Hack was not detected earlier. However, in the Shamoon wiper malware attack there was some evidence that an insider with high-level access helped to intrude the systems, but Aramco declined to comment on this, Finkle 2012, p.1
[384] Brächer 2016, p. 26-27
[385] Storn 2016, p. 29
[386] FAZ 2016b, p.23, Storm 2016
[387] Storm 2016

from machines using the classified software *acid cryptofiler* [388]. In December 2014, a similar malware for smartphones reappeared as **Cloud Atlas/Inception**[389].

3.4 Cyber warfare against Islamic State ('IS')

The **Islamic State IS** (also known as ISIS, ISIL and Daesh) is a major jihadist actor in the ongoing conflicts in Syria and Iraq and controls relevant territories of both countries since the takeover of Raqqa in Syria and Mosul in Iraq in 2014.
US officially announced in 2016 that the US Cyber Command is active against IS to interrupt communication by affecting their networks, in particular to overload them to stop functioning, in order to counter recruiting, planning and moving resources[390]. The activities are embedded in the overall military activities. While the IS is no state actor from a legal perspective (as not recognized by foreign countries as such[391]) it is equal to a state from a military perspective (size, power, people, territory, control).

After the terrorist attacks in Paris in November 2015, the hacking activist (hacktivist) group **Anonymous** declared a cyber war on IS which was then intensely discussed in media. This declaration was unexpected, because Anonymous already declared in August 2014 the „full-scale cyberwar" against the Islamic State[392]. but the second declaration may have been a reinforcement. In the week after the Paris attacks, Anonymous was able to shut down 5,500 ISIS Twitter accounts[393]. In 2015, cyber war declarations from Anonymous were also released against Israel and Turkey. Meanwhile, Twitter has enhanced its own activities and has closed 360,000 accounts that were supporting terror attacks within one year from mid 2015 on[394].

To bypass the surveillance of emails, messenger services with encryption are increasingly used[395]. A document which was related to the Islamic State (IS) from January 2015 listed 33 messenger services and divided them into 5 security categories. In fact, the secure messenger service *Telegram* was utilized by IS activists, because it allows to communicate and to send files without digital traces. Telegram closed more than 660 IS accounts since November 2015[396].
Initially, it was assumed that the attackers from Paris in November 2015 used the communication channels of *Playstation 4 (PS 4),* but evidence could not be found.

[388] Kaspersky Labs 2013
[389] Dilger 2014
[390] Paletta/Schwartz 2016, p.1-2
[391] Kurz 2016, p.14
[392] Anonhq 2014
[393] Chip.de 2015
[394] DW online 2016
[395] Langer 2015b, p.5
[396] Dörner/Nagel 2016, p.37

In Jan 2016, the IS released a cyber war magazine with the title *Kybernetiq* with cyber war information[397]. On 08 Mar 2016, the TV broadcasting company *Sky News* received the personal files of 22.000 IS fighters showing personal data and contact details in particular about foreign fighters[398]. The files were reported to be extracted from IS security department by an internal leakage.

In April 2016, US officially confirmed to drop **cyber bombs** on the IS systems, but details of these tools remained confidential[399]. However, it was said that US was able to intrude IS systems giving the option to inject false messages, to affect financial payments and to contain social network communication[400].
However, Pentagon wanted to enhance activities, as the IS continued to operate, e.g. via the news agency *Amaq* or the release of the periodical magazine *Dabiq*. So the head of Cybercom, Rogers, created the Unit "**Joint Task Forces Ares**" with 100 members[401].
In May 2016, General Lieutenant Cardon was instructed by Cybercom to ensure cooperation of **Ares** with the Central Command for Middle East and Asia and to develop or to gain digital weapons[402]. The IS has been shown to use all kinds of communication channels and encryption and may not be so dependent from a centralized server architecture like large-scale adversaries, i.e. is difficult to attack.[403] As an example, the NSA successfully supported Germany in cracking the encrypted communication of IS instructors for the terror attackers in Wuerzburg und Ansbach in July 2016. The communication seemed to come from Saudi Arabia, but the embassy of Saudi-Arabia stated that for the instructor of one attacker the use of a Saudi-Arabian telephone number could be confirmed, but the individual itself was located in the IS-controlled areas [404].

In order to increase the cyber war capabilities of the United States, President Obama now plans to upgrade *Cybercom* to a separate military command and with a focus on military aspects of the cyberspace. The link to the NSA would end and the NSA is planned to be led by a civilian in future[405].

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

4 The security architecture of the cyberspace

4.1 Basic principles

In general, the security sector is divided into three sectors; the civil sector which is usually responsible for the protection of critical infrastructures, the Intelligence sector which is responsible for analysis of communication and data flow (**Signals Intelligence SigInt**) and the military sector. Often the offensive cyber war capacity is assigned to the military sector, at least the official and unclassified capacities.

4.2 The Federal Republic of Germany

In the civil sector, the key organizations are the **Federal Ministry of the Interior (Bundesministerium des Innern BMI)** and the subordinated **Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik BSI)**.

The **Federal Office for Information Security BSI** is the government agency in charge of managing computer and communication security for the German government since 1991. The predecessor of the BSI was the cryptographic department of Germany's foreign intelligence agency (BND). With the rise of the Internet and the end of cold war there was a need for an agency for the new technical challenges. Within Germany's foreign intelligence agency, the central service for information security was created in 1989 (Zentralstelle ZSI), and then the new BSI in 1991. The new amendment of the BSI-Act BSIG von 2009 has significantly strengthened the central role of the BSI for information security matters in Germany, in section 5 of the amendment also for the government communication[406].

Important responsibilities and projects are e.g.[407]:

- member of the German Critical Infrastructure working group (AK KRITIS)[408]
- communication security for the German government, e.g. by recommending encrypted mobile phones, but also by maintaining the **Berlin-Bonn Information Network (IVBB)** and the **Federal Administration Information Network (IVBV)** that is regularly scanned by the BSI for malware since 2009[409]
- document protection within **Government** procedures

[406] Act to Strengthen the Security of Federal Information Technology dated 14 August 2009
[407] Refer to Annual reports of the BSI 2005, 2006-2007 and 2008-2009 and 2010
[408] As part of the National Plan for Information Infrastructure Protection (NPSI) BMI and BSI were asked in 2005 to prepare an implementation plan for critical infrastructures (German Umsetzungsplan KRITIS)
[409] Steinmann 2010, p.10

- Protection of NATO communication via encryption technology, in particular **Elcrodat 6.2**
- BSI provides the Secure Inter-Network Architecture (SINA) to allow very secure communication via the ordinary internet
- BSI works on communication security (**Comsec**) projects such as shielding of buildings[410]
- Work on **computer resilience**[411] and on the **micro kernel's architecture** is based on firewalls within the computer sealing off the program segments from each other
- As part of the National Cyber Security Strategy (Nationale Cyber-Sicherheitsstrategie für Deutschland) published on 23 Feb 2011, a **National Cyber Defense Center** with a staff of 10 people became operational at the BSI[412]. The efficacy of the cyber defense center was so far affected by coordination issues between member authorities (Government, Intelligence, Police etc.)[413].
- Also, a **National Cyber Security Council** that consists of the State Secretaries of all large federal ministries was established[414].

From 2016 on, a new decryption office will be established, starting with 60 employees (later on up to 400), this office is called **"Zentrale Stelle für Informationstechnik im Sicherheitsbereich" (ZITIS)**, i.e. **Central Service for IT in the security sector**. This will support the federal police (Bundespolizei/BKA) and the interior intelligence service BfV with code cracking. The external intelligence service BND will not participate[415].
In addition, the new **National Cyber Security Strategy (Nationale Cyber-Sicherheitsstrategie für Deutschland) from 2016** foresees the creation of a national CERT with **Quick Reaction Forces** located at the federal police BKA, the BSI and the BfV[416].

Within the Intelligence Sector, the Federal Office for the Protection of the Constitution (German: **Bundesamt für Verfassungsschutz BfV** and

[410] To control problems such as the computer radiation which allows to detect the information that is shown on the computer screen, Schröder 2008
[411] Resilience means permanent availability. Not only cyber attacks, but physical damages by an **electromagnetic pulse** are relevant issues here.
[412] FAZ 2010g, p.4, Tiesenhausen 2011, p.11, BMI 2011
[413] Goetz/Leyendecker 2014, p.5
[414] A cooperation in the economic sector, the **International Security Forum ISF** with currently 326 member companies was established. In 2012, the German IT association BITKOM and the BSI founded the **Allianz für Cybersicherheit** (Cyber Security Alliance) with 68 member companies and 22 member organizations who cooperate in cyber defense matters based on confidentiality agreements, Karabasz 2013, p.14-15
[415] Heil/Mascolo 2016, Mascolo/Richter 2016, p.2
[416] Biermann/Beuth/Steiner 2016

Landesämter für Verfassungsschutz LfV on federal state-level) is the Federal Republic of Germany's domestic intelligence agency, while the Military Counterintelligence Agency **(Militärischer Abschirmdienst MAD)** is responsible for the protection of the German army including cyber security and cyber defense[417]. The Germany's foreign intelligence agency **Bundesnachrichtendienst BND** is responsible for all foreign issues. The BSI is allowed to support intelligence agencies technically under certain circumstances.

In the military sector, the **Zentrum für Nachrichtenwesen in der Bundeswehr ZnBW** served several years as Intelligence Center of the armed forces, but was then divided between the Germany's foreign intelligence agency BND and the new **German Army Secret Service for Exterior Affairs** (**Kommando Strategische Aufklärung KSA**) that was founded in 2002[418] and which has key functions in military intelligence since 2008. In 2010 it had a workforce of 6,000 people[419] and is responsible for

- the electronic warfare (Elektronische Kampfführung EloKa),
- since 2007, the KSA has a c**omputer- and network operation (CNO) unit**[420] which is also responsible for cyber war issues[421] and since 2012 ready for operations[422]
- the new military satellites Synthetic Aperture Radar (SAR-Lupe)[423] and the communication satellites COMSATBW1 and 2.

In the IT sector the German Army is working on a modern and secure IT platform (**Herkules**), which is built by a joint venture of Siemens and IBM called **BWI IT**. The Herkules project led to simplification of IT infrastructure, the amount of used software programs was reduced from 6,000 to less than 300; however the structure is still complex[424]. So, the current cyber structure of the Bundeswehr is as follows:

The 60 specialists of the **Computer Emergency Response Team der Bundeswehr (CERTBw)** are responsible for supervision of the IT infrastructure with 200,000 computers in 2015. Their recommendations are then checked and implemented by 50 specialists of the Operating IT center **Betriebszentrum IT -**

[417] Rühl 2012, p.10
[418] Eberbach 2002
[419] Bischoff 2012
[420] Bischoff 2012
[421] Goetz 2009, p.34f., von Kittlitz 2010, p.33. On 01 July 2010, the information operations unit (Gruppe Informationsoperationen InfoOp), was relocated from the KSA to the Centre for Operative Information which is also part of the Joint Support Service Branch of German Army (Streitkräftebasis SKB) (Uhlmann 2010). This allows providing a centrally coordinated information policy for media and citizens.
[422] Steinmann/Borowski 2012, p.1
[423] Bischoff 2012. Acc. to Bischoff, SAR Lupe is also part of the German-French cooperation in satellite reconnaissance. Together with the French satellite Helios II it forms the basis of the European satellite reconnaissance cooperation ESGA. For 2017, a successor system of SAR-Lupe is planned, SARah.
[424] Handelsblatt 2014, p.16

Systeme der Bundeswehr (BITS)[425]. The military cyber intelligence is handled by the MAD; the offensive capabilities are located in the KSA as CNO[426].

The German Ministry of Defense BMVg announced in September 2015 to coordinate the activities in the cyber and information space[427], which is planned to be organized in a central Cyber and Information Space Command ('**Cyberinformationsraumkommando**'[428]). Currently, 320 persons are active in the cyber sector.
The new command will be established in 2017 and will now be leading the **German Army Secret Service for Exterior Affairs** (**Kommando Strategische Aufklärung KSA**) with the above mentioned sublevels for electronic warfare, cyber network operations (CNO) and the satellites (with the whole Geoinformation GeoBw). This transfer will expand the CIR sector to more than 13,700 soldiers in total[429]. The CNO capacities will be expanded to allow **Red teaming**, i.e. to train cyber attacks[430].

In 2015, the German military reported[431] 71 million unauthorized and/or malicious attempts to access, thereof 8.5 million high danger attacks. During military operations outside Germany, 150,000 attacks, thereof 98,000 high danger attacks were observed. In total, 7,200 malware programs could be detected and removed. On average, 1.1 million emails were sent daily within the troops.

In Germany, the federal states conducted the common exercise **Lükex 2011** from 30 Nov to 01 Dec 3011 using an attack scenario on critical infrastructures developed by the Federal Office of Civil Protection and Disaster Assistance (BBK) and the BSI[432].

The BND has established a cyber intelligence department in 2013[433][434]. From BND perspective, important attack sources are China and also Russia where (in contrast to China) state hackers would be organized as private firms. The BND also plans to develop counter-strike capacities to switch off servers of cyber attackers. The BND has set up the **Strategische Initiative Technik** (Strategic Initiative Technology SIT) to enhance real-time surveillance capabilities of metadata and other measures[435]. Also, it is planned to give more support to cyber

[425] BmVg 2015a
[426] BmVg 2015a
[427] Leithäuser 2015b, p.4
[428] Köpke/Demmer 2016, p.2
[429] BmVg 2016
[430] BmVg 2016, p.28
[431] Köpke/Demmer 2016, p.2
[432] Spiegel online 2011
[433] Flade/Nagel 2015, p.4
[434] Spiegel 2013b, p. 22, also Spiegel 2013c, p.15
[435] SZ 2014a, p.1

defense, i.e. the information gained should help to prepare for cyber-attacks. However, the necessary funding of 300 million Euros until 2020 was not yet approved[436].

The German parliament (Bundestag) is a primary attack target since years[437].

4.3 The cyber war strategies of the USA and of China

Presumably more than 100 countries try to establish cyber war capacities and US experts say that approximately 140 foreign intelligence agencies try to get access computers of US government and companies[438].
The USA and China are the most discussed actors with regard to cyber war. However, it this is no new 'East-West-conflict', e.g. India is concerned about of the cyber war in general[439].

4.3.1 Strategic goals

The primary aim of actors is to achieve and maintain **electromagnetic dominance** and **cyberspace superiority**[440] in particular, that is to control the cyberspace during a conflict. As the system of the adversary can be restored after some time, the practical goal is to achieve the **freedom of action** for the own forces and to limit the others at the same time. The cyber activities are combined with conventional operations.

The Chinese cyber strategy is to hit the enemy network first and to check the resulting ‚operational blindness' with conventional weapons and to continue attack, if possible[441]. Of course, the enemy may be able to repair the network and the strategy may not be successful, thus it is necessary to get electromagnetic dominance as early as possible and to maintain this as long as possible. Also the enemy may not be hit as expected and is still able to react. US studies indicated that such a war can only be conducted for a limited time.[442]

---

[436] Spiegel 2014, p.18
437 However, other government units as well, e.g. the German foreign department and embassies, Lohse/Sattar/Wehner 2015, p.3
[438] Wilson 2008, p.12
[439] Kanwal 2009. At the end of 2010, the French Department of Commerce experienced a massive cyber espionage that presumably aimed to gain information on the strategy for the G20 Economic Forum in 2011, Meier 2011, p.9
[440] USAF 2010a, p.2
[441] Krekel et al. 2009
[442] Tinner et al. 2002

In April 2015, the US Department of Defense released the **DOD Cyber Strategy**[443]. The DoD has defined five strategic goals for its cyberspace missions, including capacity building, defense of and risk mitigation for own systems, focus on US homeland and US vital interests, to have cyber options to control and shape conflict and building of international alliances and partnerships[444].

4.3.2 Cyber war capacities

The USA emphasizes the defensive character of their cyber war strategy with the **cyber triad** *resilience*, *attribution* and *deterrence*. Meanwhile, the **Comprehensive National Cyber security Initiative (CNCI)** was started to strengthen cyber security by enhancing cooperation between all actors and by increasing awareness and education of citizens. The defensive elements are emphasized in the **National Strategy to Secure Cyberspace** while the **National Military Strategy for Cyberspace Operations (NMS-CO)** is more focused on operational issues to achieve cyberspace superiority.

The USA has systematically developed their cyber war capacities in the last 2 decades[445].
In 1988, the Department of Defence DoD established a Computer Emergency Response Team CERT at the Carnegie-Mellon University[446].
In 1992, the Defensive Information Warfare Program was established that was accompanied by a Management Plan in 1995.
According to Hiltbrand, the Air Force established the Air Force Information Warfare Center (I.W.C.) in 1996. That same year, the Navy established the Fleet Information Warfare Center (F.I.W.C.) and the Army established the Land Information Warfare Activity (L.I.W.A.). In 1998, the Pentagon established the Joint Task Force for Computer Network Defense.
Thereafter, Cyber Commands were established within the military branches[447] and consequently, a central **Cyber Command** (US CYBERCOM) was established in May 2010 with an estimated staff of 1,000 people and which is led by the director of the National Security Agency NSA, General Keith Alexander[448]. Also, it is co-located with the NSA[449]. US CYBERCOM is subordinated to the Strategic Command US STRATCOM that plans and executes Cyberspace Operations[450].

443 DoD 2015
444 DoD 2015, p.8
445 Hiltbrand 1999
446 Porteuos 2010, p.3
447 USAF: 24th Air Force, Army Forces Cyber Command (ARFORCYBER), Fleet Cyber Command (10th fleet/FLTCYBERCOM) and Marine Forces Cyber Command (MARFORCYBER), refer also to Dorsett 2010
448 Hegmann 2010, p.5, The Economist 2010, p.9/22-24, Glenny 2010, p.23
449 DoD 2011, p. 5
450 USAF 2010, p.21-22

The CYBERCOM is responsible for the protection of the domain ‚.mil' that is exclusively used by the US military, while the Department of Homeland Security DHS is responsible for the civil US government domain 'gov'[451].

A first large cyber exercise was the so-called **electronic Pearl Harbour** of the US Navy in 2002, where a massive attack on critical infrastructures was simulated. Since that time, the term ‚electronic Pearl Harbour' is often used as figure of speech for the consequences of cyber attacks.
Regular exercises are the **Cyber Storm** exercises; Cyber Storm I-IV were organized in the years 2006, 2008, 2010 and 2012 by the Department of Homeland Security (DHS) and again, the capability to defend against massive attacks was tested. For the DHS exercise in 2010, a new defensive tool was developed, an internet shut down by codes that alter the Border Gateway Protocol BGP that is needed to transport information between two providers[452]. It was planned to test these codes in California, but not done to avoid unintended internet breakdowns[453]. Such internet shutdown tools also known as "**kill switches**" [454].
In March 2007, the Idaho National Laboratories (INL) conducted the **Aurora Generator test** that demonstrated that it is possible to damage a generator by manipulation of control programs.

The question of whether a more offensive alignment is necessary, was discussed in the context of the strategy papers published in 2011, which were more defensively oriented.
The White House emphasized in its *International Cyberspace Strategy* from May 2011 that it will promote compliance with international norms and standards on the Internet to ensure the functionality and freedom of information[455].
The DoD released a Defense Strategy for Operating in Cyberspace in July 2011 which emphasizes the need for interagency cooperation as well as for an intensified public-private partnership to protect the Defense Industrial Base DIB.[456]
To strengthen cyber security considering the growing problems, e.g. by increasing intrusions of critical infrastructure, President Obama released an Executive Order on 12 Feb 2013 to establish a Cyber-security framework that involves the agencies involved in protection of critical infrastructures and is intended to identify, control, communicate and mitigate cyber risks for critical infrastructures[457].

---

[451] Porteuos 2010, p.7
[452] Welchering 2011, p.T2
[453] Welchering 2011, p.T2 who also reported, that Egypt used these codes for an internet shut down on 27 Jan 2011 to restrict protests against government. The same method was reported for an internet breakdown in Syria end of November 2012, Spiegel online 2012b.
[454] von Tiesenhausen 2011, p.11
[455] White House 2011, in particular p.5 and 9
[456] DoD 2011, p.8-9
[457] White House 2013

In 2012, DoD started to build the **Cyber Mission Force (CMF)**, which is planned to include 6,200 military, civilian and contractor employees[458].
They will then be organized in 133 teams in three groups. **Cyber Protection Forces** will be responsible for defensive measures, **National Mission Forces** will defend the US against significant cyber attacks, and **Combat Mission Forces** will support Combatant Command operations with cyber operations. Cyber Protection Forces and Combat Mission Forces will be integrated into Combatant Commands while the National Missions Force will be commanded by US CYBERCOM.
The US Department of Defense noted that DoD's own network would still consist of thousands of networks across the globe.[459]

An analysis of the DoD agency **Defense Advanced Research Projects Agency DARPA** has shown that information security software needs up to 10 million lines of program code while malware only needs an average of 125 lines of code[460]. From this perspective, it is necessary to rethink the research focus on defensive tools[461]. The NSA plans to handle Chinese cyber war issues in a more offensive way[462].
It was reported that the Presidential Policy Directive PPD 20 from October 2012 now defines the conditions under which cyber-attacks against foreign servers are allowed[463]. However, the activities for cyber defense are still going on[464].

Also the Chinese government is working on cyber war issues and is building cyber war capacities like many other states, too.
Compared to conventional war, cyber war is relatively cheap and allows to get to close the gap to other states much quicker than with massive expenses for conventional weapons („leapfrog strategy"). Cyber war cannot replace conventional capabilities, but helps to expand the own options quickly and also

458 DOD 2015, p.6
459 DoD 2015, p.7
460 Dugan 2011, p.16/17: "Over the last 20 years, using lines of code as a proxy and relative measure, the effort and cost of information security software has grown exponentially—from software packages with thousands of lines of code to packages with nearly 10 million lines of code. By contrast, over that same period, and across roughly 9,000 examples of malware—viruses, worms, exploits and bots—our analysis revealed a nearly constant, average 125 lines of code for malware. This is a striking illustration of why it is easier to play offense than defense in cyber, but importantly, it also causes us to rethink our approach."
461 As part of DARPA's Plan X research, one research area "focuses on building hardened "battle units" that can perform cyber warfare functions such as battle damage monitoring, communication relay, weapon deployment, and adaptive defense." DARPA 2012, p.2
462 Barnford 2010
463 Biermann 2012, p.1. However, in other countries a legal framework for activities against foreign computers is discussed as well, e.g. in Switzerland, Häfliger 2012b, p.23
464 According to Clauss 2012, the NSA is building the Utah Data Center which is planned to be able to store and analyze digital communication permanently from 2013 on, computerized analysis should be ready in 2018; Clauss 2012, p.60. However, defensive decryption and re-encryption of encrypted messages e.g. by secure socket layer (SSL)-interception is already now commercially available, Creditreform 2012, p.48.

fits well with the concept of ‚**active defense**', where the early and quick elimination of possible retaliation of the enemy is an essential aim[465].
Also China is surrounded by states which have critical relations with China or are even allies of the USA[466], such as Japan, Taiwan and South Korea, so that China may currently not be able to apply major physical damage to the USA in case of serious conflict (e.g. in an escalating Taiwan conflict scenario). The cyber war can be done without distance problems, it allows making an asymmetric war and the cyber war training brings a lot of useful information, because intrusion can be used for cyber espionage also.

Analysis of Chinese cyber war-strategy by Northrop Grumman showed the critical points. There are three security levels, the normal civil net, the secured **Secret Internet Protocol Router Network SIPRNET** for critical infrastructure and government and close-to-military institutions and the third maximum security level for military operations[467]. The cyber war would be mainly directed against level 2 and would affect networked based warfare operations significantly[468][469].
However, other issues may be even more relevant for the future of computer and internet industry. China has 97% market share[470] for rare industry metals which cannot yet be recycled in an efficient manner and China is reducing the export volume to satisfy the needs of their domestic industry[471]. The extremely high market share resulted from low prices of Chinese metals which led to resignation of most competitors; however the search for and exploitation of such metals was restarted resulting in decreased prices[472].

4.3.3 Centralized or decentralized architecture?

For security architecture, there is a trend towards centralization to improve the coordination, but also to reduce options for attacks and interface issues caused by too many and too small small-scale or too complex network architectures.

A simplified network structure and centralization would be possible through the use of **cloud computing**, where data and programs are no longer on the hard

[465] Kanwal 2009, p.14
[466] Rogers 2009
[467] In the USA, these are the Non-classified Internet Protocol Router Network NIPRNET, the Secret Internet Protocol Router Network SIPRNET and the Joint Worldwide Intelligence Communication System JWICS; in Germany the Herkules platform is similar to SIPRNET and the JASMIN database to JWICS.
[468] Krekel et al. 2009
[469] The Internet worm **Conficker** damaged in 2008 German army and French Marine, also military jets could not start for 2 days, Leppegrad 2009.
[470] Büschemann/Uhlmann 2010, p.19
[471] Mayer–Kuckuck 2010, p.34-35, refer also to Mildner/Perthes 2010, p.12-13, Bardt 2010, p.12 and Schäder/Fend 2010, p.3
[472] FAZ 2010d, p.12, Bierach 2010, p.11, FAZ 2013d, p.24

drives of their computers, but the work is done after log in by computers of large server farms[473].
This would reduce the complexity of the networks and the number of possible attack points considerably. However, these centralized data centers can also be targets of cyber attacks[474], of classic espionage and of conventional physical attacks[475].
There seems to be a change in security architecture, because the Internet and its predecessor ARPANET were installed to reduce the probability of success of a physical attack by decentralization. Thus, there is a strategic optimization problem where the benefits of decentralization (protection against physical attacks) must be compared with the benefits of centralization (protection against virtual attacks).

However, while technical centralization may be an optimization problem, it is widely agreed that countries have a need for administrative centralization and coordination of the cyber activities. A recent example is the establishment of a **High Council of Cyberspace** (Shoray-e Aali-e Fazaye Majazi) in Iran which now gives directions to all other authorities involved in cyberspace[476]. Before that, already a Cyber Defense Command was established in 2010 for protection of critical infrastructures after the Stuxnet events.

Centralization debate is also ongoing in India. Indian ministries handled cyber security matters by creation of cyber agencies, finally resulting in almost 30 cyber agencies with overlapping or not precisely defined responsibilities and various other organizations in addition. As a result, a recent analysis by the Indian Navy strongly recommended realignments and improved communications under new central cyber agencies[477].

Large server farms can also be used for analysis of large data volumes, also known as **big data**. As shown in Section 2.2.2, the main problem is not to gain information, but to store[478] and analyze them in a useful manner.
The storage of metadata (e.g. who spoke when and how long to whom) is also done to identify contact networks of individuals under suspicion. As an example,

[473] ENISA 2009, p.2; See also Dugan 2011, p.8
[474]Cloud computing can also be vulnerable. The attacks on several US banks in late 2012 have shown novel features such as conscripting computers in cloud computing centers to use them for data traffic, The Economist 2013, p.59. The cloud computing service Evernote was affected by stealing all passwords, FAZ 2013b, p.21.
[475] Also, electricity issues can damage large computers seriously as reported in Oct 2013 for the Utah Data Center, Spiegel online 2013b
[476] Nligf 2012, where also the existence of an informal 'cyber army' was noted.
[477] Chhabra 2014, p.66-67
[478] The storage volume discussed for the NSA data center in media is in Yottabytes, this is 10^{24} bytes, Juengling 2013, p.52.

the terrorist network involved in the Madrid 2004 attack could be represented by analysis of connection data[479].
To reduce the data volume, e.g. the British GCHQ (Government Communication Headquarters) does a **massive volume reduction (MVR)** procedure by removing large files such as music files[480].
Then, search terms (selectors) help to identify relevant data. As an example, the German Intelligence Service BND has analyzed e-mail traffic, SMS and connections by more than 15,000 search words, but only 290 of 2.9 million initial checks in 2011 led to relevant findings[481]. More than 90% of the BND search terms are formal terms such as telephone numbers, email- or IP-addresses of users or companies under suspicion[482].

A more targeted approach is the collection and analysis of **user profiles**. In March 2012, Google announced that profiles of users can be compiled by combining data from search engine usage, YouTube, Google plus and gmail[483]. Similar procedures are also known from social network companies, but Google and other companies were affected in 2013 by a presumably Chinese hacking by which profiles of Chinese users were checked and exported[484].

4.4 The cyber war concept of Russia

4.4.1 Definitions and background

Definitions

In 2012, an article presenting the official Russian position was released based on a preceding presentation at a security conference in Berlin in Nov 2011[485].
The definition of cyber war is based on the agreements of the **Shanghai Cooperation Organization (SCO)** from 2008 which provides a wide definition as follows: "*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*." [486] This definition is consistent with the

[479] Hayes 2007. The network identification is also known as **community detection.**
[480] Tomik 2013a, p.6.
[481] Amann 2013, p.17
[482] Schulz 2013, p.6.
[483] Spiegel 2013d, p.111
[484] Süddeutsche Online 2013
[485] Bazylev et al. 2012, p.10.
[486] Annex I to the Agreement between the Governments of the Member Countries of the Shanghai Cooperation Organization on Cooperation in International Information Security in Yekaterinburg in 2008, cited by Bazylev et al. 2012, p.11.

information security doctrine given by President Putin in the year 2000[487] and integrates aspects of cyber warfare in a strict sense, information warfare and psychological warfare. Thus, this definition is much broader than e.g. the US definition which is focused on the military aspects. Consequently, the Russian definition of cyber weapons is also a broad one: "*Cyber weapons are information technologies, capabilities, and methods used in cyberspace warfare operations*." [488]

Russia emphasizes the defensive attempt of this doctrine and the need for a cyber convention of the United Nations and suggests an international cooperation to stop proliferation of cyber weapons[489].

Background

The definition is influenced both by theoretical considerations and historical experience.

Cyberspace warfare in the above defined way is a tool of modern geopolitical strategies[490]. The control of the information flow and the influence on the content to support the own position are now relevant tools of soft power in international relations[491]. Also, lack of control may lead to de-stabilization and destruction[492].

Moreover, this perspective could also be influenced by historical experience. Various authors argue that the collapse of the Soviet Union and the socialist state system was also influenced by information influx from the Western alliance[493].

Strategic implications

Based on the above concept, it is essential to control the information flow within the own territory. This requires a legal framework with the nation state as key actor and technical measures[494] to control the information flow.

Consistent with the above concepts and definitions, the SCO members Russia, China, Tajikistan and Uzbekistan submitted a letter to the United Nations on 12

[487] Annex I to the Agreement between the Governments of the Member Countries of the Shanghai Cooperation Organization on Cooperation in International Information Security in Yekaterinburg in 2008, cited by Bazylev et al. 2012, p.11.

[488] Annex I, cited by Bazylev et al. 2012, p.11

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

[490] Maliukevicius 2006, p.121

[491] Maliukevicius 2006, p.125ff.

[492] Bazylev et al. 2012, p.12

[493] As an example, leading intelligence officers from the former Communist German Democratic Republic analyzed the collapse and concluded that the measures of part III in the Organization for Security and Co-operation in Europe OSCE treaty of 1975 such as travel, personal contacts, information and opinion exchange contributed to the erosion (German: Aushöhlung) of the socialist Warsaw Treaty states (Grimmer et al. 2003, I/101, also I/189-I/190).

[494] Russia uses the surveillance system SORM for supervision of data traffic, FAZ 2010h. A new security law was released in 2016. From mid of July 2018 on, all content of phone calls, social networks and messenger services has to be stored for 6 months with a legal access for the interior intelligence service FSB to the providers, Wechlin 2016, p.6.

Sep 2011 with a suggestion for an international code of conduct for information security which emphasizes the rights and the role of the sovereign Nation State (Preamble/Section d) with the right to control information by law (Section f) [495].
Technically, it is possible to block certain websites and/or to redirect users to national substitutes for search engines, Twitter and other services. For larger countries, such an 'island solution' may be challenging and difficult to control[496].

4.4.2 The WCIT 2012

In 1988, International Telecommunication Regulations (ITR) of the International Telecommunication Union (ITU) were agreed which replaced separate regulations for telegraph, telephone and radio[497]. Based on the rapid technological changes since 1988, the World Conference on International Telecommunications (WCIT) was held in Dubai from 03 to 14 Dec 2012 to discuss new ITRs.
Based on the telecommunication definition in the ITU Constitution *("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"*)[498], the opinion that the various technologies cannot be separated in practice[499] and some involvement in cyber issues (such as Flame), the ITU hold the opinion that this organization could be the responsible body for regulation of Internet *and* Information and Communication Technology (ICT), i.e. for all digital technology[500].

---

[495] UN letter 2011, p.1-5. The role of the nation state is emphasized. The preamble states that "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." and in Section (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 information and communications technologies or to threaten the political, economic and social security of other countries". Section (f) states "To fully respect rights and freedom information space, including rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulation".

[496] In 2012, another technology was under discussion. At the World Telecommunication Standardization Assembly (WTSA-12) in Dubai from 20 to 29 Nov 2012 a technical recommendation defining the requirements for **Deep Packet Inspection (DPI)** in next generation networks was submitted by a Chinese expert (Y.2770 2012). This recommendation Y.2770 describes the use of DPI e.g. for the detection of encrypted data and classification of data types such as VoIP, video streams, MP3 music files, BitTorrent traffic, Business cards (vCards) etc. The approval by ITU members on 20 Nov 2012 via Traditional Approval Procedure TAP, i.e. unopposed agreement of Member States present at the respective meeting of this draft may be a step forward to a standardized targeted content analysis; but, the ITU emphasized that this recommendation does not open the door to private user information.

[497] WCIT2012 presentation, introductory section

[498] WCIT2012 presentation, section myths and misinformation

[499] Touré 2012. Touré, the Secretary General of the ITU said *"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*"

[500] ICT is mentioned in the WCIT2012 presentation, section myths and misinformation

A group of states led by Russia, China, some Arabian and other states called to discuss whether the ITU should be the responsible body for the Internet Regulation[501]. While media reports focused much on the internet issue, the draft document suggested by these states also used the term ICT[502]. Also it was argued that the Internet affects all people on the globe and should thus be regulated by a UN body, the ITU.
The United States, the European Union, Australia and other states argued that the current multi-stakeholder model of Internet Governance with organizations like the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Society (ISOC), the Internet Engineering Task Force (IETF) and others should be kept, because it has proven to be fair, flexible and innovative. This model was able to manage the rapid expansion of the Internet around the globe[503]. Also, it was emphasized that except the ICANN that is linked via a Memorandum of Understanding to the US Department of Commerce, the US government does not control these organizations. Also, these states expressed concerns that a control by states may affect freedom of information[504] and could hamper innovation and for these reasons this group of states resisted against any formulation that could open the door for ITU influence on the Internet[505].
Finally, a legally non-binding annex was adopted by a disputed voting procedure stating that the "*Secretary General [of the ITU] is instructed to continue the necessary steps for ITU to play an active and constructive role in the development of broadband and the multi-stakeholder model of the Internet as expressed in paragraph 35 of the Tunis Agenda*"[506]. Also, new ITRs were adopted, but a consensus could not be reached[507]. As a consequence, the United States, the states of the European Union, Australia and many other states did not sign the new ITRs[508]. The hard dispute between two large groups of states gave to some observers the impression of a **digital cold war**.

In addition to the issues discussed above, the Internet Governance also influences the cyber capabilities. Recently, the US Air Force analyzed this as follows:[509]: "*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*

[501] Touré 2012
[502] WCITleaks 2012. Please note that this was a 'leaked' draft only and not an official presentation
[503] EU 2012b (Position Paper of the EU)
[504] Kleinwächter 2012, p.31, Lakshmi 2012, p.1
[505] Touré 2012
[506] WCIT 2012 Resolution Plen/3
[507] WCIT 2012 Final Acts
[508] Betschon 2012, p.4, Lakshmi 2012 estimated that 113 of 193 member states will sign, 80 not.
[509] Yannakogeorgos 2012, p.119-120

through its position of developer and core provider of Internet Services made possible by the ICANN and the top-level Domain Name System."

4.5 The cyber policy of the European Union

In contrast to USA and China the European Union consists of 28 nation states. Security gaps (exploits) in national networks are highly sensitive information. Disclosure of such information may lead to intrusion by other states. In real life, distrust is still dominating between nation states.
This is caused by a security paradox: IT and cyber attacks are global matters, but IT security structure paradoxically promotes national solutions.

In most states so-called **Computer Emergency Response Teams (CERTs)** or Computer Security Incident Response Teams (CSIRTs) are established for detection and reporting of security incidents and for countermeasures. However, the **European Government CERT Group EGC** still has only 12 member states (Finland, France, Germany[510], Netherlands, Norway, Hungary, Spain, Sweden, United Kingdom with 2 CERTs, Switzerland, Austria and Denmark)[511] [512].
Meanwhile, a CERT-EU team for the security of EU IT infrastructure was permanently established in 2012 [513]

Cyber attacks are a global problem and nation states would profit from an information exchange, the EU summarized the central problem of European cyber policy as follows (in German, English translation follows): „Die Wirkung einer besseren Zusammenarbeit wäre sofort spürbar, doch sind zunächst kontinuierliche Bewusstseinsbildung *und Vertrauensaufbau* erforderlich (the effects of an improved cooperation could be seen immediately, but as a first step we need to enhance awareness *and to build trust*.)"[514]

The focus is now on the **ENISA (European Network and Information Security Agency**), that was founded in 2004 with regulation 460/2004 with a budget of 33 Mio. Euros and 50 employees. ENISA became operational in 2005 and is located in Heraklion/Iraklion, the capital of Crete, at the Southern EU border, which is perceived as a suboptimal solution[515].

---

[510] The German group CERT-Bund is presented on the BSI Website
[511] IT Law Wiki 2012b, p.1.
[512] ECG 2008, Website der ECG Nov 2010. Weitere CERT-Foren, an denen die deutsche CERT-Bund beteiligt ist, sind FIRST (Forum of Incident Response and Security Teams) und TI (Trusted Introducer).
[513] EU2013b, p.5
[514] EU 2010b. The European Council released already in 2006 a cooperation plan for Critical Information Infrastructure Protection, it took some time after attack on Estonia 2007 before further steps were implemented. Taking these facts into consideration, the discussed development of an international **cyber war convention** seems to be unlikely, Dunlap 2011, p.83
[515] EU-ISS 2007

The ENISA works on network security studies, encryption tools, etc. Cryptography is also part of the current EU research program[516]. In 2008, the mandate of the ENISA was prolonged until 2012, already in 2011 then until 2013 and 2013 the mandate is planned to be prolonged until 2020 with expanded responsibilities.
The director of the ENISA, Dr. Udo Helmbrecht, was the former president of the German BSI and was appointed in 2009. Since that year, the following actions were started to strengthen the key role of ENISA in European cyber policy:

- the ENISA should strengthen the cooperation between National/Governmental CERTs, also by leveraging and expanding existing cooperation mechanisms like the EGC[517],
- the ENISA has released a comparative study in 2009 of the states of the European Economic Area EEA that showed major differences between member states with regard to regulatory settings, the insufficient capacity building of CERT groups, a lack of cooperation and poor procedures for *incident reporting*. Consequently, the ENISA gave recommendations how processes and cooperation could be improved under the leadership of ENISA[518].
- In line with the European Commission Communication on Critical Information Infrastructure Protection 2009,[519] the ENISA conducted the first Pan-European Exercise **Cyber Europe 2010** with 70 organizations from 22 countries (and 8 observer countries) with a total of 320 stress tests[520]. However, the exercise showed the uneven and uncoordinated national approaches and insufficient preparedness of smaller member states[521]. After analysis and lessons learned sessions, the next exercise will also include private actors.
- Meanwhile, a common exercise of the EU and the USA took place, **Cyber Atlantic 2011**.

The European Commission plans to establish a **European Public Private Partnership for Resilience (EP3R)** and a European Information Sharing and Alert System (EISAS), which is also accessible for citizens and small and medium-size enterprises (SMEs). Moreover, it is planned to develop in cooperation with Member States and all relevant stakeholders the criteria for identifying European critical infrastructures for the information and communication technology (ICT) sector [522].

[516] ENISA 2007
[517] EU 2007, EU 2009b
[518] ENISA 2009a
[519] EU 2009b
[520] ENISA 2010a, ENISA2010b
[521] Mertins 2010, ENISA 2010a: „There is a lack of pan-European preparedness measures to test. This reflects the fact that many Member States are still refining their national approaches."
[522] EU2009b, also EU 2010b

A legal framework to enhance network and information security (NIS) was proposed in early 2013. It was stated that there still is no effective mechanism at EU level for effective cooperation and collaboration for trusted information sharing on NIS incidents and risks among the member states. Therefore, each member state should establish a competent authority (CA) for NIS and establish a communication network with the other CAs, and provide early warnings and relevant information. Also, the cooperation with private stakeholders should be enhanced [523].
In 2013, an evaluation of CSIRTs within the EU is planned and an anti-botnet initiative.[524] The recently launched **European Cybercrime Centre E3C** will cooperate with ENISA and the **European Defense Agency EDA** to enhance cooperation for NIS matters[525]. For 2014, ENISA and EU Commission will organize a cyber security championship for students.
The United Kingdom and France agreed upon a general military cooperation in November 2010, which also should include cyber war issues[526].
The **EDA** found in a study from 2013 that there is a need to develop military cyber defense at the European level.[527]
On 03 Sep 2014, it was officially announced that a new **Joint Cybercrime Task Force J-CAT** will be established at the Europol as a joint effort of Europol, the European Cybercrime Taskforce, the FBI and the British National Crime Agency NCA.

A new area of concern is the rapid growth of cloud computing where data may be stored on external computers under a foreign jurisdiction. In addition to the various security issues[528] uncertainties about rights and responsibilities on cross-border situations[529] are relevant so an update of the European legal framework for to address cloud computing is under discussion.
In the new **Cloud Computing Strategy** the EU has identified three primary problems, the fragmented market, problems of contracts and the "jungle of standards"[530].

[523] EU2013a
[524] EU2013b
[525] EU2013b, p.18
[526] Thibaut/Alich 2010, p.15
[527] EPRS 2014, p.8
[528] ENISA 2009b
[529] EU2011
[530] EU 2012a, p.5

4.6 The cyber capabilities of the NATO

While the focus of the CCD CoE is on research, the **NATO Communication and Information Systems Services Agency** in Mons near Brussels is responsible for operative issues[531].

The primary purpose of the NCSA is to install, operate, maintain and support the communication and information systems of the NATO. In line with the NATO Cyber Defense Program of 2002, the NCSA is the first line of defense for the NATO IT-infrastructure[532].
The NATO Information Security Technical Centre (NITC) is NCSA's authority for operational information security and operates both the NATO Information Security Operations Centre and the NATO Computer Incident Response Capability Technical Centre (NCIRC).
The Information Security Operations Centre provides centralized management of integrated communication and cyber defense capabilities while the NCIRC is responsible for incident detection, response and recovery.

Cyber defense matters are handled by the **Cyber Defense Committee** (name used since April 2014).
The **Smart Defense Initiative[533]** includes 3 cyber defense elements, these are

- Malware Information Sharing Platform MISP
- Multinational Cyber Defense Capability Development MNCD2 and
- Multinational Cyber Defense Education and Training MNCDET

The **NATO Communications and Information Systems School NCISS** will move to Portugal. Cyber defense is also supported by the NATO School in Oberammergau/Germany, while the NATO defense college in Rome supports strategic thinking. Cyber defense trainings also include smart phone security and forensics.

A collection of National Cyber Security Strategy Documents for many NATO and non-NATO countries with links is available under ccdcoe.org/strategies-policies.html

The attack against Estonia in 2007 alerted the NATO that now works on protection of member states against cyber attacks. In May 2008, the **Cooperative Cyber Defense Centre of Excellence (CCD CoE)** was initiated in Tallinn[534], Estonia with a staff of 30 people, which was in the first years supported by

[531] Schuller 2010, p.6
[532] NCSA 2009a-c
[533] NATO 2015
[534] In reality, the CCD CoE became operational already in 2006 after an Estonian initiative in 2004; CCDCoE 2010a

Estonia, Lithuania, Latvia, Italy, Spain, Slovakia and Germany[535]. Further countries joined later: Hungary 2010, Poland and USA in 2011, Czech Republic, United Kingdom and France in 2014, Turkey, Greece and Finland in 2015.

NATO Cyber Defense exercises were **Digital Storm** and **Cyber Coalition** 2008, 2009 and 2010 and were managed by the CCD CoE together with the NCIRC and other NATO bodies[536]. The exercise Cyber Coalition (CC) is now done annually. Together with Sweden, the CCDCoE conducted the **Baltic Cyber Shield** exercise in May 2010. **Locked Shields** is an annual real-time exercise organized by CCDCoE since 2012, following the first exercise Baltic Cyber Shield in 2010.

At the Lisbon summit in November 2010 the NATO presented a new strategy with the aim to intensify and coordinate cyber war defense *(„bringing all NATO bodies under centralized cyber protection"*)[537].

The NATO and also the German Ministry of Defense (Bundesministerium der Verteidigung BMVg) are discussing the **hybrid warfare** as new challenge. Here, physical power by special and proxy forces is combined with full range of cyberspace activities, i.e. including information and psychological warfare via internet and social media on one hand and cyber attacks on the other hand[538]. As a result, there is need for intense review of security policy with a particular focus on cyber resilience[539]. In November 2014, the NATO held a very large cyber exercise in Tartu, Estonia with more than 670 soldiers and civilians from 80 organizations from 28 countries[540].
Analysts of the German Foreign Intelligence BND concluded that in armed conflicts cyber activities are particularly important in the early stage of the conflict[541]. While this conclusion which is supported by the previous experience with large cyber attacks, the vulnerabilities and malware have rapidly expanded. So it may have to be taken into consideration that in longer conflicts cyber exploits may not be used as 'single-shot' for initial surprise, but when one gap in a certain system is closed, the adversary will activate the next exploit and so on. In the era of stay-behind forces and USB sticks, internet blocks and kill switches may not prevent attacks sufficiently.

[535] The NATO plans to rely on consultations after a cyber attack; von Kittlitz 2010, p.33
[536] Wildstacke 2009, p.28/29, CCDCoE 2010b
[537] NATO 2010. For the NATO, not only cyber war, but all kinds of cyber attacks are relevant, Hunker used 2010 the term **cyber power**.
[538] NATO 2014, BMVg 2015b
[539] BMVg 2015b
[540] Jones 2014, p.1
[541] Leithäuser 2015a, p.8

The German government reported for the first half of 2015 4,500 infections with malware and on average it took seven months to detect the infection and a further month to remove the infection[542].
Preparing the battlefield is essential for successful strategies, in practice this means to place **beacons** or **implants** into foreign computer networks, this is code to monitor how these networks work[543].

A NATO country decomposed a jet to secure all components against cyber attacks and re-assembled everything thereafter, but due to the costs it was suggested that component security should be requested from component providers instead[544]. However, this would mean to rely on the security efforts of multiple vendors, i.e. it is difficult to delegate the IT security. Similar checks were done in car hacking and the **walled garden concept** that believes that a system of multiple components can be secured externally as a whole did not stand intrusion tests, i.e. each component needs to be secured individually[545]. A Eurofighter Jet has more than 80 computers and 100 kilometers wires[546].

However, preventive activities could e.g. include spot checks of "normally" working computers/smart devices with in-depth diagnostics and worst-case exercises, i.e. to check how far communication and operations could be maintained in case of a complete computer system failure (EMP scenario).

4.7 The cyber policy of the African Union

In May 1996, the United Nations Economic Commission for Africa (ECA) started the African Information Society Initiative (AISI) which included an initiative to develop and implement National Information Communication (NICI) policies and plans[547].
Since that time, the IT infrastructure of Africa was massively expanded, e.g. by new broadband deep sea cables as well as by intense competition between European and Chinese telecommunication providers (in particular Huawei and ZTE)[548].
In 2009 the African Union (AU) agreed to develop a convention for cyber legislation within the AISI framework which was released as draft version in

[542] Leithäuser 2015b, p.4
[543] Sanger 2015, p.5
[544] Leithäuser 2016, p.8
[545] Mahaffey 2016, p.V6
[546] Köpke/Demmer 2016, p.2
[547] ECA 2012, p.1
[548] Martin-Jung 2008, EMB 2010, Schönbohm 2012 who stated that 8.400 kilometers deep sea cable were provided 2010 at the East African coast to enhance high-speed internet. Also, on the West Coast new cables were provided at the same year which allowed e.g. expansion of Nigeria's internet, Adelaja 2011, p.7

2011[549]. The convention is dealing with electronic commerce, data protection and processing and cyber crime in general, but does not contain specific provisions on cyber war[550].

In addition, cooperation on cyber legislation is discussed within the African Regional Economic Communities (RECs) such as the East African Community EAC, the South African Development Community SADC and the Economic Community of West African States ECOWAS[551].
A main topic in many documents is the need for intensified Inter-African Cooperation and to enhance cyber security awareness[552].
South Africa already started the development of a National Cyber security Policy Framework in 2010 which was approved by the cabinet in March 2012[553]. One of the primary aims of this policy was the coordination of various national authorities dealing with cyber security[554].

In Africa, the role of smartphones is rapidly growing, as this helps to abridge digital infrastructure gaps, but this exposes Africa more than other regions to the vulnerabilities shown in Section 2.2.7[555].

[549] ECA 2012, p.3, AU 2011
[550] AU 2011
[551] ECA 2012, p.4
[552] For general intelligence and security cooperation in Africa, the **Committee of Intelligence and Security Services of Africa CISSA** was founded in 2004 in Nigeria which organizes regular meetings of the member institutions, Africa 2010, p.72f.. Meanwhile, 50 Intelligence and Security Services have signed the CISSA Constitutive Memorandum of Understanding, CISSA 2012.
[553] South Africa 2012
[554] South Africa 2010, p.6
[555] Puhl 2013, p.118f.

5 Cyber war and biologic systems

5.1 Implantable devices

There are a growing number of wireless **implantable medical devices (IMDs) s**uch as cardiac pacemakers/defibrillators, deep brain neurostimulators, implants for ear and eye (cochlear and ocular) and others. It was shown that insulin pumps can be hacked and modified remotely[556]. As physicians need to have easy access in case of emergencies, protection is difficult and communication may be affected by adversaries. For this reason, the research for signal jamming and other strategies is in progress[557].

In response to the threats for the digital health sector, the US Food and Drug Administration FDA released a safety communication on health-related cyber security[558]. This includes recommendations to protect hospital networks to prevent identification of potential targets, i.e. patients with devices and the respective device specifications. As hospitals may have data exchange with devices to supervise patients remotely, hospitals are a potential entry for cyber attackers to certain patients. In addition, draft guidance was released to ensure cyber security of medical devices by requiring manufacturers to develop a set of security controls to assure medical device cyber security to maintain information confidentiality, integrity, and availability[559]. The challenge is to balance security/privacy with medical safety/usability[560].

The three key principles of both FDA documents are to limit access to trusted users only, to ensure trusted content use and to provide fail safe and recovery features. The security recommendations included a large variety of measures such as authentication of users, a layered authorization model, avoiding “hardcoded” passwords (which are the same for each device, difficult to change, and vulnerable to public disclosure), appropriate controls before permitting software or firmware updates, including those affecting the operating system, applications and anti-malware and to ensure secure data transfer to and from the device, and when appropriate, use accepted methods for encryption[561].

Meanwhile, deep brain neurostimulators were developed that can measure the brain activity, emit signals out of the brain (‘brain radio’) and influence the brain

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

by giving electric stimulation[562]. The evaluation of the emitted signals allows to modify the stimulation pattern by sending wireless instructions into the stimulation device, which could help e.g. to influence neuromuscular disorders or severe cases of depression. The brain radio analyses so-called **latent field potentials** (LFPs), which can be displayed as complex curves which reflect a specific activity pattern of the brain[563]. The collection and analysis of LFP (as a kind of brain signal decryption) is expected to be complex and the first analysis is expected to take some years and the study to take almost a decade until late 2023[564].

The recent progress motivated the DARPA on 12 Nov 2013 to suggest new devices that help to analyze and treat severe brain injuries.
A current limitation is the need for battery exchange or reload, for this reason, the research is targeting on using the human body as energy source by glucose (blood sugar) utilization[565]. Recently, cardiac pacemakers were developed that could utilize organ movements to win energy[566]
Retinal implants are already in use as sub retinal implants, i.e. chips that are positioned behind the retina (the natural optical detection layer of the eye) and contains 1500 pixels (independent micro-photodiode-amplifier-electrode elements) on a 3 mm*3 mm; an amplified electrical signal is sent by the electrode to the bipolar cells, i.e. the cells that process the optical input further[567]. The chips however still need an external energy supply.
Hacking of implantable devices does not only include the risk of manipulation, but also of serious injuries[568], so legislators need to ensure that device hacking is not only judged as virtual crime.

Another topic are **wearable technologies** such as *Google Glass*, i.e. glasses with integrated computing and competitor products which are expected to be marketed during 2014[569]. Intruders could not only track the individual user, but also use the glasses to observe others[570]. Other concepts are **smart wigs** or **smart helmets** that may support paralyzed or blind people, and device patches that monitor the health status of the user[571].

[562] Young 2013, p.1, Medtronic 2013
[563] LFP signals were found to encode dynamic aspects of behaviour, unrelated background dynamics with distinct state fluctuations, and possibly other aspects, refer to Stamoulis/Richardson 2010, p.8
[564] ClinicalTrials.gov 2013
[565] Jürisch 2013, p.10
[566] Welt online 20 Jan 2014
[567] Stingl et al 2013
[568] Such as delivery of electric shocks, see Gollakota et al 2011, p.1
[569] Postinett 2013a, p.30
[570] Also, RFID chips are meanwhile implanted e.g. in expensive horses to prevent stealing and in some children to prevent kidnapping.
[571] The analysis of user condition could also be done by cameras, such as in the new Microsoft X-Box, Mähler 2013, p.38.

From a cyber war perspective, wireless wearable technologies that can be attributed to individuals as well as the possibility to give IPv6 addresses to weapons as part of the Internet of Things may allow tailor-made attacks on certain groups of individuals and/or objects. While the cyber war was initially believed to be a large-scale conflict between computers and is meanwhile seen as embedded part of military operations, the trend may go forward to highly selective attacks.

5.2 Relations between cyber and biological systems

5.2.1 Viruses

Nucleic acids are the code within cells, genes are sequences of nucleic acids. Each gene is used for production of a specific protein, which can be used for formation of structures (like muscles) or that conduct metabolism as enzymes. So genes are the biologic equivalents to computer programs.
Historically, the term computer virus was derived from it biological counterpart. Biological viruses are small coated particles that contain a defined set of genes, i.e. are the biologic counterpart of malware. They use cells of an infected organism to copy (replicate) themselves and the copies leave the cells to infect other cells.

In former times, it was believed that the damage resulting from viral infections in humans was only caused by using infected cells and their subsequent destruction. However, meanwhile it is clear that many viruses also have 'Trojan-like' properties and can disturb the network of immune cells, where different types of immune cell communicate via release and receipt of molecules called **cytokines**.
Many viruses find ways to reduce Interferon gamma levels which is the key cytokine for anti-virus actions[572]. Some viruses, e.g. from the group of influenza ('flu') viruses, can even confuse the immune system communication, resulting in imbalanced and/or excessive release of cytokines and/or enhance secondary infection with bacteria[573]. The excessive release of cytokines, known as **cytokine release syndrome** or 'cytokine storm' can result in potential fatal shock-like conditions (circulation failure, organ failure, blood clotting etc.)[574].

An unconventional matter is viruses against viruses, so called **virophages**. From a cyber-perspective, it could be interesting to develop codes that could be inserted into existing malware to modify or re-direct it (malware infecting other malware), however this remains hypothetical.

---

[572] Haller 2009, p.57
[573] Kash et al 2011, Stegemann-Koniczewski 2012
[574] For such viruses, corrective actions on immune system communication (such as cut-off of cytokine excess) by cortisone and other substances could be a new option to mitigate infections in addition to the established approaches of prevention by vaccines and antiviral medications. See also Li et al. 2012/ Li, C., Yang P., Zhang Y., Sun Y., Wang W. et al 2012

From a biological perspective, nine virophages were found until 2012, all of them directed against a special subclass of viruses, the giant double-stranded DNA viruses[575]. The Sputnik virophage is directed against the Mimivirus that can cause human pneumonia[576]. Interestingly, the pox virus (variola) is also a large double-stranded DNA virus, so maybe modified virophages can open new treatment options. There are increasing reports of pox-like infections with monkey pox[577], in Germany some fatal pox infections were reported already in 1990 mainly in immunosuppressed patients where the cow pox virus was able to pass species barrier to cats[578].

5.2.2 Bacteria

Bacteria are single-cell microorganisms that can infect other organisms such as humans[579]. Some of those who cause relevant infections in humans can form liquid platforms called **biofilms**[580] where they can exchange information via pheromones and can share materials for nutrition, this mode of action is also known as **quorum sensing** (meaning that this platform is established when a critical mass of bacteria is reached). New research is targeted on disrupting these platforms and shutdown of bacterial communication which would make it much easier for immune cells to attack and destroy the bacteria[581].

Biotechnology allows to change genes or to introduce new genes into organisms, which raised concerns that new dangerous organisms maybe created intentionally[582] or inadvertently. In the last decade, a new phenomenon called **bio-hacking** was observed[583]. The typical biohacker works outside established research units or companies and tries as a kind of ethical hacking to modify genes to invent something useful, but due to biosecurity reasons the biohacking scene is closely observed by government authorities[584]. However, there are high structural, functional and energetic hurdles for achieving stable modifications of genes or

[575] Zhou et al. 2012
[576] Zhanga et al. 2012
[577] Shah 2014, p.27
[578] Scheubeck 2014, p.7
[579] Just for matter of completeness, biological worms are multi-cell organisms that can actively move and infect other organisms, while viruses are passively spread (e.g. by cough, diarrhea, rhinitis, blood etc.).
[580] Bakaletz 2012, p.2
[581] Gebhardt 2013, p.38.
[582] This is not only intended by bio-terrorists, but sometimes also in research. Recently, the virus researcher Fouchier enhanced infectious properties of avian flu ('bird flu') virus to get a better understanding of the virus, Guterl 2013, p46f. Both US and China expressed serious concerns, see Guterl 2013, Zeng Guang 2013. Practical recommendations for defense against biological weapons were released by the European Medicines Agency EMA, refer to EMEA 2002 (updated 2007).
[583] Kunze 2013, p.19-20
[584] In US, the responsible authority for biosecurity is the **National Science Advisory Board for Biosecurity** NSABB, but the biohacker scene is also observed by the FBI, the CIA is also interested in this matter, Hofmann 2012, p.14.

organisms. Genetic modifications of bacteria typically result in microscopic variations of surface glycoproteins which could be used for production plant attribution like a fingerprint[585].

A special topic is **bacteriophages**; these are viruses against bacteria which use bacteria for their replication. From a cyber-perspective, tailor-made genetically engineered bacteriophages can specifically bind a large variety of ions and be used for formation of highly effective electrodes in lithium-ion batteries, photovoltaic cells and nanomaterials by self-assembly[586]. However, as phages are dependent from a bacterial carrier system, there is no risk that bacteriophages could damage digital devices by ion-binding, i.e. they are no anti-material weapons.

From the biologic perspective, there is growing bacterial resistance against existing antibiotics which is typically caused by inappropriate use. Bacteriophages were already used as anti-bacteria viruses in the Soviet Union and today Russia and Georgia for severe infections[587]. Despite concerns of a coming post-antibiotic era, the research activity is still low and a legal framework is still missing in the Western states[588]. Bacteriophage enzymes may have also military relevance, as one bacteriophage product was effective against the standard bioweapon *Bacillus anthracis*, more commonly known as Anthrax[589].

5.2.3 Control by cyber implants

Based on progress of device and biologic research, discussions are ongoing whether cyber implants (biochips) could be used to control human behaviour and decision making[590]. However, there are some limitations of potential cyborg[591] scenarios:

---

[585] In the past, there were some discussions whether there is a risk that genetically modified bacteria could infect machines with degradation and depolymerization. However, no such infection was ever reported in practice, so this remains theoretical. But in 2016, a novel bacterium, *Ideonella sakaiensis 201-F6*, was discovered that is able to utilize Polyethylene terephthalate (PET) that is extensively used worldwide in plastic products as its major energy and carbon source, Yoshida et al. 2016. Two fungal species were already identified in 2011, Russell. et al. 2011, p.6076ff.: Two *Pestalotiopsis microspora* isolates were able to grow on Polyurethane PUR as sole carbon source both under aerobic and anaerobic conditions.

[586] Yang et al. 2013, p.46ff

[587] Mandal 2014

[588] WHO 2014, Verbeken et al. 2014

[589] Zucca/Savoia 2010, p.83

[590] Jüngling 2014, p.63

[591] There is some confusion about the definition of cyborgs. A wider definition interprets this as any man-machine system; this could also include wearable technologies. A stricter approach defines cyborgs as physically integrated man-machine systems. Retinal and cochlear implants as well as pacemakers fulfill this definition already. From a cyber war perspective, it is noteworthy that based on analysis of brain implants besides the sensitivity for interfering electromagnetic signals the need for external programming

Certain insects that serve as hosts can e.g. be forced by parasites to execute specific actions that protect the parasites (bodyguard manipulation) and promote their replication by avoiding predators[592]. On the other hand, the endoparasites of insects typically cause only certain actions but do not urge the infected insect to "do whatever they want". However, parasites can modify levels of neuronal transmitters dopamine and serotonin (5-HT) levels which are involved e.g. in the emotional (limbic) system, i.e. a similar way of action as many modern psychiatric medications[593].

In humans, the parasite *Toxoplasma gondii* has been shown to influence human behaviour (such as affects, novelty seeking, schizophrenia risk, dominant attitude of infected males etc.) significantly by infecting the brain[594] as evaluated by several standard psychological questionnaires. The behavioural influence is based on changing dopamine and testosterone levels[595], but does not mean mind control or specific changes of decision making. Human beings are no target host for *Toxoplasma gondii*, they are inadvertently infected and a kind of dead end-host. In the natural rodent intermediate host, the parasite-induced behavioural changes facilitate enhance transmission to the feline definitive host[596]. Also, it is not yet clear which effects in humans are really targeted manipulations or just side effects of the chronic infection[597].

Implantable brain devices (deep brain stimulation DBS and Vagus nerve stimulation VNS) are already tested or used to treat a larger variety of neuropsychiatric disorders, such as depression, anxiety, schizophrenia, obsessive-compulsive disorder, Tourette syndrome, tics, epilepsy, Parkinson disease and so on[598]. The DBS works by sending electric signals to groups of specialised nerve cells, so-called nuclei, which are located deeply in the brain and where the probe is located[599]. The implant electrodes not reach in the grey substance of the neocortex (the functional layer on the brain surface that is responsible for the intellectual functions), so implants do not control the intellect; instead they have an indirect

---

and modification is the key vulnerability of any potential cyborg system, e.g. the handhelds devices needed to modify brain implant settings or the smartphones needed to control biobots.

[592] For example, the spider host *Plesiometa argyt* builds under influence of the parasite wasp *Hymenoepimecis sp.* a unique cocoon web as a durable support for the wasp larva's cocoon to protect this. Manipulated caterpillar *Thyrinteina leucocerae* hosts stay close to parasitoid pupae of parasitic wasp *Glyptapanteles sp* and knock off predators with violent head thrashing leading to higher survival rates or parasite pupae. Eberhard 2000/2001 and Grosman et al., 2008 cited by Maure et al. 2013, p.38

[593] Perrot-Minnot and Cézilly 2013, p136-137

[594] Adamo and Webster 2013, p.1, Flegr 2013, p.127f.

[595] Increased synthesis of dopamine takes place in infected host brains in tissue cysts of Toxoplasma. Disturbed dopamine levels are involved in various severe psychiatric disorders such as schizophrenia.

[596] Adamo and Webster 2013, p.2, Flegr 2013, p.128

[597] Flegr 2013, p.127

[598] Refer to ClinicalTrials.gov - A service of the U.S. National Institutes of Health Search of: deep brain stimulation - List Results Retrieved in June 2014

[599] VNS stimulates the tenth brain nerve, the vagus nerve, the stimulation is done beyond the brain.

influence by as the nuclei below the cortex are involved in the emotional and hormonal system[600] and also in some motoric coordination.
The DARPA initiated in 2006 HI-Mems projects (hybrid insect micro electromechanical systems) to develop biological robots (biorobots, biobots), i.e. cyber-biological systems of insects with integrated electronics. One of the aims was to develop insect drones for espionage and other military duties[601]. Recently, a chip became commercially available which after connection allows control cockroach movements by smartphones, here as **RoboRoach** from the firm Backyard Brains. The cockroach species is *Blaberus Discoidalis*[602]. The cockroach chip is *not* implanted into the head or brain of the cockroach, but only put on the back and then connected with small cables to the antennae[603]. Electric signals to the antennae induce a movement change of the cockroach by remote control via smartphone and Bluetooth[604]. Typically, the control is diminishing after some days, but it is disputed whether this is an adaptation or simply a damage of the chip-antenna connection.
In parallel to cyborgs, the research on **biohybrids** is going on, i.e. combinations of biological and synthetic materials.
In 2016, a swimming robot that mimics a ray fish was constructed with a microfabricated gold skeleton and a rubber body powered by 200,000 rat heart muscle cells[605]. The cells were genetically modified so that speed and direction of the ray was controlled by modulating light. However, the biohybrid was still dependent from the presence of a physiologic salt solution.

5.3 Conclusions and implications for cyber war

Overall, while there are networks and communication also within biological systems, there is only a limited comparability and any reference to biological systems should be made very cautiously.
But the above sections have shown the crucial role of communication. The practical focus of cyber security is currently on prevention of infections, i.e. on *incoming* communication. Much less attention is paid to the *outgoing* communication (which is also needed to expand infections by beachhead Trojans). The average private or business user has neither control nor any overview which

[600] Target areas for deep brain stimulation in severe neuropsychiatric diseases amongst others are: Thalamus; subthalamic nucleus; nucleus accumbens; Cg25, subgenual area of cingulum, Kuhn et al. 2010, p.106. In the military sector, a study to treat post-traumatic stress disorder in soldiers was planned in 2012, but was not conducted, Department of Veterans Affairs 2013
[601] Hummel 2014b
[602] Hummel 2014a, p.1
[603] Hummel 2014a, p.2
[604] The chip is needed to transfer smartphone command into electric signals; the control of the cockroach is limited to give electric stimulation to its antennae. These signals do not contain any specifically coded information; they only irritate the insect to change the direction. For technical details, refer to Latif/Bozkurt 2012. This does not match the common understanding of robots, so it is still a long way to animal-robot hybrids, see Hummel 2014, p.42
[605] Park et al. 2016

data are leaving the computer (or the smartphone) in the background, also not why, to whom and to which extent[606]. The reports from Kaspersky, Symantec, McAfee, Mandiant and others typically show that even massive illegal data export is realized *after* the infection was detected, i.e. by far too late. One reason for this is the widespread "what is not forbidden, is allowed"-approach, i.e. except a list of unsafe or forbidden websites, standard computers settings factually allow sending data to almost everywhere. It may make sense to think about more rigid approaches for sensitive environments (e.g. reverse protocols where only explicitly allowed servers/IP addresses can be approached) and improved tools that facilitate overview about data export and authorization.

[606] Even the television may record and export all user data without knowledge if designed as Internet-TV (IPTV), SZ online 2013

6 Literature references

Abendzeitung (2014): USA halten einige Lücken in Computersystemen geheim. Abendzeitung online 29 Apr 2014

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

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

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

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

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

Alperovitch, D. (2014): Deep in Thought: Chinese Targeting of National Security Think Tanks 07 Jul 2014, 8 pages

Alperovitch, D. (2016): Bears in the Midst: Intrusion into the Democratic National Committee. From The Front Line, update 15 Jun 2016, 3 pages

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

Anonhq (2014): ‚Anonymous' Hacker Group goes after ISIS. One page.

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

Astheimer, S, Balzter, S. (2015): Arbeit geht unter die Haut. Frankfurter Allgemeine Zeitung 21/22 Feb 2015, p.C1

Atherton, K.D. (2016): DARPA's Cyber Grand Challenge Ends In Triumph. Popular Science 06 Aug 2016, 2 pages

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

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 July 2012

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

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

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

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

Baumgartner, K. (2014): Sony/Destover: Mystery North Korean Actor's Destructive and Past Network Activity. Released on 04 Dec 2014, 11 pages. 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 no. 2, 2012, p.10-15

BBC News (2009): Major cyber spy network uncovered. 29 March 2009

BBC (2014): Russian hackers used Windows bug to target NATO. BBC news online 14 October 2014, 3 pages.

BBC (2016): FBI warns on risks of car hacking. Article 35841571. 18 Mar 2016

Becker, J. (2016): Die Flut kommt. Süddeutsche Zeitung No.42/2016, p.78

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

Bernau, P. (2014): Kamen die Hacker doch nicht aus Nordkorea? Frankfurter Allgemeine Zeitung online 31 Dec 2014, p.1

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

Betschon, S. (2012): Konferenz in Dubai gescheitert. Neue Zürcher Zeitung, 17 Dec 2012, p.4

Betschon, S. (2013a): Hacker im Honigtopf. Neue Zürcher Zeitung No. 73, p.38

Betschon, S. (2013b): Wenn Viren Luftsprünge lernen. Neue Zürcher Zeitung 07 Nov 2013, p.34

Betschon, S. (2014): High Noon in Hollywood. Neue Zürcher Zeitung 18 Dec 2014, p.34

Betschon, S. (2016): Die Crux mit gefälschten Chips. Neue Zürcher Zeitung 31 Aug 2016, p.39

Beuth, P. (2016a): Sechs Tipps vom NSA-Hackerchef. Die Zeit online 29 Jan 2016, 3 pages

Beuth, P. (2016b): Unbekannte versteigern angebliche Waffen von Elitehackern. Die Zeit online 16 Aug 2016, 1 page

Bierach, B. (2010): Australien will Seltenerdmetalle fördern. Neue Zürcher Zeitung 18 Dec 2010, p.11

Biermann, K. (2012): Obama erlaubt Angriff auf fremde Netze. Die Zeit online 15 Nov 2012, 2 pages

Biermann, K, Beuth, P. Steiner, F. (2016): Innenministerium plant drei neue Internet-Eingreiftruppen. Die Zeit online, 07 Jul 2016, 6 pages

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

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

Bittner, J., Ladurner, U. (2012): Die Waffe der Überflieger. Die Zeit No.50/2012, p.2-3

BMI (2011): Bundesministerium des Innern (Federal Ministry of the Interior): Cybersicherheitsstrategie für Deutschland. 23 Feb 2011

BMVg (2015a): Überblick: Cyber-Abwehr der Bundeswehr Online article Berlin, 11 May 2015

BMVg (2015b): Auf der Suche nach der Bundeswehr der Zukunft. Online article Berlin, 20 Jul 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/unclassified, 53 pages

Brächer, M. (2016): Das fragile Netzwerk. Handelsblatt No. 155/2016, p.26-27

Brumbacher, B. (2016): Drohnen vom Himmel holen. Neue Zürcher Zeitung 12 Apr 2016, p.5

Broad, W.J., Markoff, J., Sanger, D.E. (2011): Israel Tests on Worm Called Crucial in Iran Nuclear Delay. New York Times. 15 Jan 2011, 9 p.

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

BSI (2012): Abwehr von DDoS-Angriffen. Dokument BSI-E-CS-002 Version 1.0 03 Feb 2012, 2 pages

Buchter, H., Dausend P. (2013): In die Luft geflogen. Die Zeit 29 May 2013, p.4

Burianski, M. (2012): Maschinen können nicht haften. Frankfurter Allgemeine Zeitung No. 272/2012, p.21.

Büschemann, K.-H., Uhlmann, S. (2010): Deutschland braucht eine Rohstoffstrategie. Süddeutsche Zeitung 15 Oct 2010, p.19

Busse, N. (2007): Krieg im Cyberspace. Frankfurter Allgemeine Zeitung 22 Nov 07, p.10.

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

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

CCD CoE (2010a): History and way ahead. Website of the Cooperative Cyber Defence Centre of Excellence. http://www.ccdcoe.org/12.html

CCD CoE (2010b): CCD COE Supports NATO's "Cyber Coalition 2010". http://www.ccdcoe.org/212.html

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

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

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

Chip.de (2015): Anonymous gegen ISIS: Hacker enttarnen Terroristen. 18 Nov 2015, one page

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

Clauss, U. (2012): Sie speichern alles. Welt am Sonntag 13 May 2012, p.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, p. 48

Croitoru, J. (2012): Schule der Hacker. Frankfurter Allgemeine Zeitung No. 248/2012, p.30

Cyberwarzone (2016): Daesh (ISIS) has released a cyberwar magazine titled Kybernetiq. 09 Jan2016, one page

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. and Schmitz, G.P. (2013): Cyberwar - Ausweitung der Kampfzone, Der Spiegel 14/2013, p.76-80.

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

DARPA (2016): Cyber Grand Challenge https://www.cybergrandchallenge.com 05 Aug 2016

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

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

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

Der Spiegel online (2014): Im Zweifel einfach das Telefon wegschmeißen 27 Dec 2014, 2 pages

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

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

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. Article 1381616569, p.1

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

Die Welt online (2016b): Mächtige Spionage-Software für iPhones entdeckt. 26 Aug 2016, 1 page

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 pages

Dörfler, M. (2015): Sicherheitsrisiko Drucker. Frankfurter Allgemeine Zeitung Verlagsspezial IT-Sicherheit, 06 October 2015, page P4

Dörner, A., Renner, K.-H. (2014): Roboter mit spitzer Feder. –Handelsblatt from 07 July 2014, p.18-19

Dörner, S., Nagel, L.M. (2016): Russlands Zuckerberg. Welt am Sonntag 14 Feb 2016, p. 37

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

Dorsett, J. (2010): Information Dominance and the U.S. Navy's Cyber Warfare Vision. Presentation of VADM Jack Dorsett, DCNO for Information Dominance 14 April 2010

Drissner, G. (2008): Hört nichts. Financial Times Deutschland 11 July 2008, p.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 pages

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

DW (2016): IS-Datenleck wird größer und größer. Deutsche Welle.com 10 Mar 2016, one page

DW online (2016): Twitter sperrt 360.000 Konten mit Terror-Botschaften. 19 Aug 2016, 1 page

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 pages

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, p.1-5

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

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

ENISA (2010a): Interim findings of CYBER EUROPE 2010, the First Pan-European Cyber Security Exercise; a successful ’cyber stress test’ for Europe. Press release 10 Nov 2010

ENISA (2010b): Q&As on the first, pan-European Cyber Security Exercise ‘CYBER EUROPE 2010’.

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

Erk, D. et al. (2015): Außer Kontrolle. Die Zeit No. 25/2015, p.2

EU (2007): Communication from the Commission to the European Parliament On the evaluation of the European Network and Information Security Agency (ENISA). COM(2007) 285 final

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 December 2011, 7 p.

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 Sep 2012, 16 pages

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 pages

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 pages

EU-ISS (2007): Chaillot Paper No. 76 of the European Institute for Security Studies EU-ISS

Even, S. and Siman-Tov, D. (2012): Cyber Warfare: Concepts and Strategic Trends. Memorandum No. 117 of The Institute for National Security Studies INSS, May 2012, 95 pages

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

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

Fahrion, G. (2012): Pfusch am Gewehr. Financial Times Deutschland, 23 May 2012, p.1

Falliere, N. (2010): Stuxnet Introduces the First Known Rootkit for Industrial Control Systems. Reported by Symantec 06Aug 2010, http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices

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

FAZ (2000): Amerikaner hören angeblich Datenleitungen in Europa ab. FAZ 24 Jan 2000, p.1

FAZ (2010a): Rätselhaftes Schadprogramm Stuxnet. Frankfurter Allgemeine Zeitung No. 224/2010, p.17

FAZ (2010b): Amerika gehen die Drohnen aus. Frankfurter Allgemeine Zeitung No. 230/2010, p.6

FAZ (2010c): Iran erfolgreich sabotiert? Frankfurter Allgemeine Zeitung No. 275/2010, p.6

FAZ (2010d): Australien sichert Japan seltene Erden zu. Frankfurter Allgemeine Zeitung No. 275/2010, p.12

FAZ (2010e): Getöteter Iraner mit Stuxnet befasst. Frankfurter Allgemeine Zeitung No. 280/2010, p.5

FAZ (2010f): Amazons Wikileaks-Rauswurf nährt die Zweifel an der Cloud. Frankfurter Allgemeine Zeitung No. 283/2010, p.17

FAZ (2010g): Bundesregierung plant „Cyber-Abwehr-Zentrum“. Frankfurter Allgemeine Zeitung No. 302/2010, p.14

FAZ (2010h): Unternehmen und Staaten im Cyberkrieg. Frankfurter Allgemeine Zeitung online 12 Oct 2010

FAZ (2011a): Hacker greifen Rüstungskonzern Lockheed an. Frankfurter Allgemeine Zeitung No. 125/2011, p.11

FAZ (2011b): Unverantwortliche Vorwürfe. Frankfurter Allgemeine Zeitung No. 181/2011, p.7

FAZ (2012a): Eine neue Waffe im Cyberkrieg. Frankfurter Allgemeine Zeitung 30 May 2012, p.16

FAZ (2012b): Unmut über „Lecks“. Frankfurter Allgemeine Zeitung 09 Jun 2012, p.7

FAZ (2013a): Tausende Unternehmen informieren Geheimdienste. FAZ No. 136, 15 Jun 2013, p.1

FAZ (2013b): Auf dem Handy lauern Gefahren. FAZ No. 53, 04 Mar 2013, p.21

FAZ (2013c): Das Smartphone ist gefährdeter als der Schlüsselbund. Frankfurter Allgemeine Zeitung No. 249, p.14

FAZ (2013d): Seltene Erden sind günstig wie lange nicht. Frankfurter Allgemeine Zeitung No. 249, p.24

FAZ (2014a): Wenn sinnlose Anfragen das Internet zusammenbrechen lassen. Frankfurter Allgemeine Zeitung, 24. Dec 2014, p.21

FAZ (2014b): Amerika bittet China um Hilfe gegen Hacker. Frankfurter Allgemeine Zeitung, 22. Dec 2014, p.1

FAZ online (2014): Flugkörper UAV MQ-5B abgefangen. Online report from 14 March 2014

FAZ (2015a): “NSA hat Computer in Nord Korea schon vor 4 Jahren infiltriert”. Frankfurter Allgemeine Zeitung, 20 Jan 2015, p.5

FAZ (2015b): Ein Konzern als Hacker. Frankfurter Allgemeine Zeitung, 22 April 2015, p.18

FAZ online (2015): Cyber-Angriff auf TV5 Monde. Ermittler verfolgen Spur nach Russland. FAZ online 09 Jun 2015

FAZ (2016a): Australien fordert mehr Datenschutz im U-Boot-Bau. Frankfurter Allgemeine Zeitung 27 Aug 2016, p.29

FAZ (2016b): Immer mehr Banken werden von Hackern bestohlen. Frankfurter Allgemeine Zeitung 01 Sep 2016, p.23

FAZ online (2016): So kam die Spionage-Software aufs iPhone. 26 Aug 2016, 2 pages

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 Sep 2012, p.1-4

Finsterbusch, S. (2013): Big Data steht unter Beschuss. In: Frankfurter Allgemeine Zeitung No. 31, 06 Feb 2013, p.15

Finsterbusch, S. (2015): Behörden räuchern Hacker-Nest aus. Frankfurter Allgemeine Zeitung No. 163/2015, p.26

Fischermann, T. (2010): Attacke im Sicherungskasten. Die Zeit No.38/2010, p.26

Flade, F., Nagel, L-M. (2015): Manöver mit der Maus. Welt am Sonntag No.24, 14 June 2015, p.4

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 July 2014, p.27

Focus online (2012): Staatlicher Cyberangriff: Gauss-Trojaner späht Bankkunden aus. Focus online 09 Aug 2012

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

Focus online (2013): Millionenfach installierte Android-App schnüffelte Nutzer aus. 06 Dec 2013

Focus Online (2016): NSA knackte verschlüsselte Befehle für Anschläge in Bayern 13 Aug 2016, 1 page

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

Frei, H. (2015): Effizient – aber überhaupt nicht städtisch. Neue Zürcher Zeitung No. 158 from 11 July 2015, p.27

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

Fromm, T., Hulverschmidt, C. (2016): Totalschaden. Süddeutsche Zeitung No. 151/2016, p.25

Fromme, H. (2015): Der Spion kommt ins Auto. Süddeutsche Zeitung No. 150, 3 July 2015, page 17

Fuchs, C., Goetz, C., Obermaier, P and Obermayer, B. (2013a): Deutsche Aufträge für US-Spionagefirmen. Süddeutsche Zeitung No.265, 16/17 Nov 2013, p.1

Fuchs, C., Goetz, C., Obermaier, P and Obermayer, B. (2013b): Berlin, vertrauensselig. Süddeutsche Zeitung No.265, 16/17 Nov 2013, p.8

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

Fuest, B. (2012): Drohnen für alle. Welt am Sonntag No.51/2012, p.37

Fuest, B. (2014a): Uroburos –Russisches Supervirus greift die Welt an. Welt am Sonntag online 10 March 2014, 3 pages

Fuest, B. (2014b): Der übliche Verdächtige. Welt Am Sonntag No.52/2014

Fuest, B. (2015): Fremdgesteuert. Welt Am Sonntag No.26 from 28 June 2015, p.34-35

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

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

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

Gaycken, S. (2010): Wer wars? Und wozu? In: Die Zeit No.48/2010, p.31

Gebauer, M. (2016): Nato erklärt Cyberraum zum Kriegsschauplatz. Der Spiegel online 14 Jun 2016, 2 pages

Gebhardt, U. (2013): Bakterielle Waffen zum Schweigen bringen. Neue Zürcher Zeitung No.264, p.38

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

Georgia (2008): Russian Invasion of Georgia – Russian Cyberwar on Georgia. Statement of the government of Georgia from 10 November 2008. http://georgiaupdate.gov.ge

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

Gierow, H. (2016): NSA legt Angriff und Abwehr zusammen. Zeit online 05 Feb 2016, 2 pages.

Glenny, M. (2010): Die neuen Cyberkrieger. Financial Times Deutschland, 12Oct 2010, p.23/26

Goebbels, T. (2011): Wurmfortsatz von Stuxnet entdeckt. Financial Times Deutschland, 20 Oct 2011, p.8

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

Goetz, J. Leyendecker, J. (2014): Das Problem mit der Wirklichkeit. Süddeutsche Zeitung No 130, 7-9 Jun 2014, p.5

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

Gostev, A. (2012): Interview in: Der Feind hört mit: Wie IT-Experten die Spionage-Software entdeckten. Welt online, 30 May 2012

Graf, J. (2012): Stuxnet und Flame haben die gleichen Väter. Financial Times Deutschland, 12 Jun 2012, p.9

Graff, B. (2014): Sie sind da. Süddeutsche Zeitung No. 107, 10/11 May 2014, p.13

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

Graw, A. (2013): Freundschaft war gestern. Welt am Sonntag No.43, 27 Oct 2013, p.4-5

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

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

Gujer, E. (2012a): Würmer und andere Computer-Parasiten. Neue Zürcher Zeitung, 01 Sep 2012, p.30

Gujer, E. (2012b): Medizinische Gutachten zum Datendieb. Neue Zürcher Zeitung, 05 Oct 2012, p.24

Gujer, E. (2013): Verfeindete Freunde. Neue Zürcher Zeitung, 03 Jul 2013, p.5

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

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

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

Gutscher, Th. (2013a): Sensibler Sensenmann. Frankfurter Allgemeine Sonntagszeitung No.22 02 Jun 2013, p.4

Gutscher, Th. (2013b): Menschenrechte hochhalten, nach Daten tauchen. Frankfurter Allgemeine Sonntagszeitung No.26 30 Jun 2013, p.7

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

Hafliger, M. (2012b): Staatsschutz will private Computer ausspionieren. Neue Zürcher Zeitung, 05 Nov 2012, p.23

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

Handelsblatt (2010): Update macht Programme von Microsoft sicherer. Handelsblatt 14 Oct 2010, p.27

Handelsblatt (2014a): Das Ende von Herkules. Handelsblatt from 09 May 2014, p.13, 16-17

Handelsblatt (2014b): Viele Wege führen in die Fritzbox. Handelsblatt from 19 Feb 2014, p.23

Handelszeitung online (2014): Finnischer Teenager prahlt mit Sony Hack. 29 Dec 2014, p.1

Hanke, T. (2012): Erfolgreicher Probeflug der europäischen Kampfdrohne. Handelsblatt 03 Dec 2012, p.14-15

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

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

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

Hegmann, G. (2010): Rüstungsindustrie verteidigt Internet. Financial Times Deutschland, 02 Jun 2010, p.5

Heider, D. (2006): Drohnen im zivilen und militärischen Einsatz. University of Münster 01 Feb 2006, 10 pages

Heil, G., Mascolo, G. (2016): Eine Behörde gegen das "going dark". Tagesschau online, 22 Jun 2016, 2 pages

Hein, C., Schubert, C. (2016): Datenleck setzt französische Staatswerft unter Druck. Frankfurter Allgemeine Zeitung 25Aug 2016, p.22

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

Heller, P. (2016): Kanonen gegen Drohnen. Frankfurter Allgemeine Sonntagszeitung vom 24 Apr 2016, p.68

Herwig, M. (2010): Die @-Bombe. Welt Am Sonntag No.39, 29 Jun 2010. p.60-61

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

Heute (2016): Mit Funksender: Autoklub knackt 25 Autos Heute.at online 17 Mar 2016

Hickmann, C. (2013): Kopien nicht erlaubt. Süddeutsche Zeitung No.124, 01/02 Jun 2013, p.6

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

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

Hofmann, N. (2012): Herumstochern im Genom. In: Süddeutsche Zeitung No. 179/2012 from 04/05 Aug 2012, p.14

Hoppe, T., Osman, Y. (2015): Cybersturm auf Berlin, Handelsblatt No.110/2015 from 12 to 14 Jun 2015, page 1

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

Hürther, T. (2010): Das automatisierte Töten. Die Zeit No. 29, p.21

Hummel, P. (2014a): RoboRoach: Smartphone steuert Schabe. 13 March 2014 Zeit online, p.1-3

Hummel, P (2014b) Die Ankunft der Bioroboter Neue Zürcher Zeitung No. 59 from 12 Mar 2014, p.42

Humphreys, T./Wesson, K. (2014): Drohnen auf Abwegen. Spektrum der Wissenschaft (German Edition of Scientific American) March 2014, p.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

ICS-CERT (2016a): ICS-ALERT-14-281-01E: Ongoing Sophisticated Malware Campaign Compromising ICS (Update E). Original release date: 10 Dec 2014, last revised 02 Mar 2016

ICS-CERT (2016b): Alert (IR-ALERT-H-16-056-01). Cyber-Attack Against Ukrainian Critical Infrastructure. Original release date: 25 Feb 2016

Iran Daily (2010): Stuxnet hits Computers. 26 July 2010, p.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 pages

Isselhorst, H. (2011): Cybersicherheit in Deutschland. Presentation by Dr. Hartmut Isselhorst, BSI Department Head from 16 June 2011, 27 pages

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

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

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

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

Jahn, T. (2011): Das Milliardengeschäft mit den Drohnen. Handelsblatt 25 Nov 2011, p.26

Jansen, J., Lindner, R. (2016): Der Spion in meinem iPhone. Frankfurter Allgemeine Zeitung 27 Aug 2016, p.28

Jennifer (2014): Breaking the Code on Russian Malware. The Recorded Future Blog Posted in Cyber Threat Intelligence 20 Nov 2014

Jones, S. (2014): NATO holds largest cyber war games. Financial Times FT.com 29 November 2014, 3 pages.

Jones, S. (2016): Cyber espionage: A new cold war? 19 Aug 2016 Financial Times online, 7 pages

Jüngling, T. (2013): Big Data! Die nächste Revolution Welt am Sonntag 03 March 2013, p.52

Jüngling, T. (2014): Unter die Haut. Welt am Sonntag No. 23 08 June 2014, p.62-63

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

Jürgensen, N. (2016): Mehr als 20 Gigabyte Daten entwendet. Neue Zürcher Zeitung 25 May 2016, p.28

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

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

Karabasz, I. (2013): Gemeinsame Spionageabwehr im Netz. Handelsblatt 29 May 2013, No. 101, p.14-15

Karabasz, I. (2014): Angst vor dem Kontrollverlust. Handelsblatt 06 Jan 2014, No. 3, p.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 19 July 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 Jan 2013, p.1-3

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

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

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

Kaspersky Lab (2015c): Der große Bankraub: Cybergang “Carbanak” stiehlt eine Milliarde US-Dollar von 100 Finanzinstituten weltweit, Moskau/Ingolstadt, 15 February 2015, 3 pages

Kittlitz, A. von (2010): Stuxnet und der Krieg, der kommt. Frankfurter Allgemeine Zeitung No. 283/2010, p.33

Kleinwächter, W. (2012): Sollen Staaten künftig das Internet kontrollieren? Frankfurter Allgemeine Zeitung No.255/2012, p.31

Kloiber, M., Welchering, P. (2011): Militärs suchen Strategien gegen Cyberattacken. Frankfurter Allgemeine Zeitung No.38/2011, p.T6

Klüver, R. (2013): Automaten des Todes. Süddeutsche Zeitung No 187/2013, p.2

Knocke, F. (2012): Indien rüstet zum Cyberwar. Spiegel online 11 June 2012

Knop, C. (2010): Jetzt kommt die Cloud. Frankfurter Allgemeine Zeitung No.229/2010, p.14

Knop, C., Schmidt, H. (2010): Unternehmen und Staaten im Cyberkrieg. Frankfurter Allgemeine Zeitung No.237/2010, p.20

Koch, M. (2011): Die Spur führt nach China. Süddeutsche Zeitung 03 Jun 2011, p.20

Könen, J., Hottelet, U. (2007): Tagesgeschäft Spionage. Handelsblatt No. 171/2007, p.2

Köpke, J., Demmer, U. (2016): Bundeswehr im Visier von Hackern. Neue Westfälische 16 Mar 2016, p.2

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

Kremp, M. (2011): Elite-Hacker führen Cyberwar für China. Spiegel online 26 May 2011

Krohn, P. (2014): Der Schaden durch Hackerangriffe wird immer größer. Frankfurter Allgemeine Zeitung 20 Dec 2014, p.24

Krüger, P.A., Martin-Jung, H., Richter, N. (2010): Der Wurm und der Luftballon. Süddeutsche Zeitung 02/03Oct 2010, p.9

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

Kunze, A. (2013): Die Stunde der Bio-Punks. Die Zeit No. 19/2013, p.19-20

Kurz, C. (2012): Die ganz normale Unterwanderung des Netzes. Frankfurter Allgemeine Zeitung No. 286/2012, p.33

Kurz, C. (2013): Die Angriffsindustrie. Frankfurter Allgemeine Zeitung No. 254/2013, p.31

Kurz, C. (2016): Wir erklären den Cyberwar für eröffnet. Frankfurter Allgemeine Zeitung 07 Mar 2016, p.14

Ladurner, U., Pham, K. (2010): Iran im Krieg 2.0. Die Zeit No.40, p.12

Lakshmi, B. (2012): India signs the new ITR at WCIT: 80 countries including U.S. refuse to sign. Article on 14 Dec 2012 on Mediauama.com

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

Lange, A.M. (2016): Mit Cyberbomben gegen den IS. Neue Zürcher Zeitung 28 Apr 2016, p.5

Langer, M.A. (2014a): Das Netz als Entwicklungshelfer. Neue Zürcher Zeitung No.271, p.7

Langer, M.A. (2014b): Geheimes Wettrüsten. Neue Zürcher Zeitung No.290, p.1

Langer, M.A. (2015a): Spionage für jedermann. Neue Zürcher Zeitung No.6, p.6

Langer, M.A. (2015b): Hinter dem Rücken der Geheimdienste. Neue Zürcher Zeitung, 08 Dec 2015, p.5

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

Leithäuser, J. (2015a): Der virtuelle Krieg. Frankfurter Allgemeine Zeitung from 28 July 2015, p.8

Leithäuser, J. (2015b): Aufrüstung für den Krieg der Zukunft. Frankfurter Allgemeine Zeitung No.217/2015, p.4

Leithäuser, J. (2016): Fortgeschrittene ständige Bedrohung. Frankfurter Allgemeine Zeitung No.48/2016, p.8

Lemos, R. (2015): NFC security. 3 ways to avoid being hacked. PC World online 26 Jun 2015

Leppegrad, L. (2009): Ihr Rechner ist besetzt! Die Zeit No.10/2009, p.34

Lewicki, M. (2014): Hacker am Steuer. Welt am Sonntag 14 Sep 2014, p.62

Leyden, J. (2014): Nuke Hack fears prompt S Korea cyber-war exercise Reactor blueprints leaked on social media. The Register 22 Dec 2014, p.1-3

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

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

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

Lichtblau, E., Weiland, N. (2016): Hacker releases more Democratic Party Documents. New York Times online, 12 Aug 2016

Lindner, R. (2016): Drohnen – und wie sie unschädlich gemacht werden. Frankfurter Allgemeine Zeitung No.7/2016, p.24

Löwenstein, S. (2013): Geheimdienste sind geheim – auch in Österreich. Frankfurter Allgemeine Zeitung No.169/2010, p.5

Lohse, E., Sattar, M., Wehner, M (2015): Russischer Wissensdurst. Frankfurter Allgemeine No. 24/2015, p.3

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

Luschka, K. (2007): Estland schwächt Vorwürfe gegen Russland ab. Spiegel online 18 May 2007, p.1-3

Mähler, M. (2013): TV Total. Süddeutsche Zeitung No. 253/2013, p.38

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

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

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

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

Market Wired (2014): Proofpoint uncovers Internet of Things (IoT) Cyberattack. Market Wired 16 Jan 2014, p.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 Feb 2016, 2 pages

Martin-Jung, H. (2008): Die Schlagadern des Internets. Süddeutsche Zeitung No. 34, p.22

Martin-Jung, H. (2014): Digitale Super-Wanze. Süddeutsche Zeitung Nr. 271, 25 Nov 2014, p. 17

Mascolo, G., Richter, N. (2016): Bundesbehörde soll Verschlüsselungen knacken. Süddeutsche Zeitung online, 23 Jun 2016, 3 pages

Matthews, E. (2013): Cyberspace Operations: HAF Cyber Matrix and Force Development, HAF/A3C/A6C 27 June 2012, p. 8

Mayer, M. (2015): Wir wissen, wen Du triffst. Frankfurter Allgemeine Zeitung from 23 Jul 2015, p.13

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

Mayer-Kuckuck, F. (2010): China verknappt exotische Rohstoffe. Handelsblatt 10/11 Sep 2010, p.34-35

Mayer-Kuckuck, F., Hauschild, H. (2010): Chinesischer Huawei-Konzern wehrt sich gegen Generalverdacht. Handelsblatt 26 Aug 2010, p.28

Mayer-Kuckuck, F., Koenen, J., Metzger, S. (2012): Hacker werden immer dreister. Handelsblatt 15 Feb 2012, p.20-21

McAfee (2011): Global Energy Cyberattacks: "Night Dragon". McAfee White Paper 10 Feb 2011, 19 pages

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 pages

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

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

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

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

Meier, L. (2011): Super-Sarko im Cyberkrieg. Financial Times Deutschland 08 Mar 2011, p.9

Melton, K.H. (2009): Der perfekte Spion (German edition of The ultimate spy). Coventgarden, updated edition from 2009

Mertins, S. (2010): Manöver gegen Web War II. Financial Times Deutschland 11 Nov 2010

Mertins, S. (2012): Cyberkrieg zwischen Iran und USA eskaliert. Financial Times Deutschland 17 Oct 2012, p.10

Mertins, S. (2015): Feindliche Übernahme. NZZ am Sonntag 14 Juni 2015, p.5

Metzler, M. (2015): Hacker legen deutschen Hochofen lahm. NZZ am Sonntag 11 January 2015, p.34

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

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

Morschhäuser, T. (2014): Heftiger Sonnensturm verfehlt Erde nur knapp. Frankfurter Rundschau online version 25 July 2014, p.1-2

Müller, G.V. (2014): Die Schatten-IT wird zum Problem. Neue Zürcher Zeitung 11 April 2014, p.16

Nakashima, E. (2012a): In U.S.-Russia deal, nuclear communication system may be used for cyber security. The Washington Post 26 April 2012

Nakashima, E. (2012b): With Plan X, Pentagon seeks to spread U.S. military might to cyberspace. The Washington Post 30 May 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 June 2012, p.1-4

Nakashima, E. (2016a): Russian government hackers penetrated DNC, stole opposition research on Trump. Washington Post online, 14 Jun 2016, 6 pages

Nakashima, E. (2016b): Russian hackers targeted Arizona election system. Washington Post online, 29 Aug 2016, 4 pages

NATO (2010): "Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation", 11 pages 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, p.82.

Neuneck, G., Alwardt, C. (2008): The Revolution in Military Affairs, its Driving Forces, Elements and Complexity. Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg/Working Paper 13/2008

Nligf (2012): Structure of Iran's Cyber Warfare (Source: the BBC Persian). PDF-file on nligf.nl 7 pages

Northrop Grumman TASC (2004): Cyber Warrior Hacker Methodology. Presentation, 44 pages

Novetta (2015): Operation-SMN-Report June 2015, 31 pages

Novetta (2016): Operation-Blockbuster-Report February 2016, 59 pages

NTV online (2013): USA schaffen neue Kriegsmedaille. 14 Feb 2013

NZZ (2012): Wirbel in den USA um Indiskretionen. Neue Zürcher Zeitung, 07 Jun 2012, p.1

NZZ (2014): Virtueller Gegenangriff auf Nordkorea? Neue Zürcher Zeitung No.300, p.3

Oparus (2010): Oparus Overview and Objectives. Website of the OPARUS project, 3 pages, 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 (18 March 2010)

Paletta, D.Ä, Schwartz, F. (2016): Pentagon deploys cyberweapons against Islamic State. Wall Street Journal online 29 Feb 2016, article 1456768428, 4 pages

Park, S.J. et al. (2016): Phototactic guidance of a tissue-engineered soft-robotic ray. Science 08 Jul 2016: Vol. 353, Issue 6295, pp. 158-162

Perlroth, N. (2013): U.S. seeks young hackers. New York Times international Weekly 28 Mar 2013, p.1 and p.4

Perlroth, N. (2014): 2nd China Army Unit Implicated in Online Spying. New York Times online 10 Jun 2014

Perrot-Minnot, MJ. and Cézilly, F. (2013): Investigating candidate neuromodulatory systems underlying parasitic manipulation: concepts, limitations and prospects The Journal of Experimental Biology 216, 134-141 doi:10.1242/jeb.074146

Pofalla, B. (2013): Datenfüchse von morgen. Frankfurter Allgemeine Sonntagzeitung 11 Aug 2013, p.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 pages

Postinett, A. (2008): Wolken-Reich. Handelsblatt No.245/2008, p.12

Postinett, A. (2011): Lauschangriff in Amerika. Handelsblatt No.234/2011, p.32

Postinett, A. (2013a): Auf die kleine Art. Handelsblatt No. 248/2013, p.30

Postinett, A. (2013b): Aus allen Wolken gefallen. Handelsblatt No. 249/2013, p.12-13

Pravda (2012): USA starts anti-Russian drills, Russia hires nation’s best hackers. Pravda English online 18 Oct 2012, 2 pages

Puhl, J. (2013): Im Silicon Savannah. Der Spiegel 48/2013, p.118-122.

Quirin, I. (2010): Vorfahrt fürs Netz. FTD Dossier Intelligente Netze 15 Oct 2010, p.2-7

Ragan, S. (2016): Salted Hash – Top Security News. Hackers say leaked NSA tools came from a contractor at Red Seal. CSO online article 3109936, 6 pages

Raiu, C., Baumgartner, K., Kamluk, V. (2013): The MiniDuke Mystery. PDF 0-day Government Spy Assembler 0x29A MicroBackdoor, 20 pages

Reder, B., van Baal A. (2014): Wenn Hacker den Strom abstellen. Frankfurter Allgemeine Zeitung Verlagsspezial IT-Sicherheit 7 October 2014, p.V2

Rees, J. (2016): Volvo schafft den Zündschlüssel ab. Handelsblatt online 20 Feb 2016, p.1-4

Rieger, F. (2010): Du kannst Dich nicht mehr verstecken. Frankfurter Allgemeine Zeitung No. 43/2010, p.5

Rieger, F. (2011): Angriff ist besser als Verteidigung. Frankfurter Allgemeine Zeitung No. 14/2011, p.27

Robertson, J., Lawrence, D., Strohm (2014): Sony's breach stretched from Thai Hotel to Hollywood. 07 Dec 2014, www.bloomberg.com

Rößler, C. (2016): Ab in den Süden. Frankfurter Allgemeine Zeitung 02 March 2016, p.6

Rötzer, F. (2016): Der vom Pentagon angekündigte Cyberwar gegen den IS dümpelt vor sich hin. Telipolis 19 Jul 2016, 2 pages

Rogers, J. (2009): From Suez to Shanghai: the European Union and Eurasian maritime security. Occasional Paper - n°77, March 2009

Rõigas, H., Minárik, T. (2015): 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law. Incyder news, 31 August 2015

Rosenbach, M., Schmitz, G.P., Schmundt, H. (2010): Mord ohne Leiche. Spiegel 39/2010, p.163

Rosenbach, M, Traufetter, G. (2015): Der Computerabsturz. Der Spiegel 22/2015, p.72-73

Rüb, M. (2010): Jenseits der Partnerschaftsrhetorik. Frankfurter Allgemeine Zeitung No. 129/2010, p.5

Rühl, L. (2012): Was nur Soldaten leisten können. Frankfurter Allgemeine Zeitung No. 248/2012, p.10

Ruggiero, P., Foote, J. (2011): Cyber Threats to Mobile Phones. Carnegie-Mellon University, 6 pages

Russell, J.R. et al. (2011): Biodegradation of Polyester Polyurethane by Endophytic Fungi. Applied and Environmental Microbiology, Sep 2011, pp.6076-6084

RWE (2013): Wohnen in der Zukunft, p.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 pages

Sanger, D.E. (2012): Obama order sped up wave of cyber attacks against Iran. New York Times online. 01 Jun 2012, 9 p.

Sanger, D.E., Shanker Th. (2014): NSA devises radio pathway into computers. NYTimes 14 Jan 2014

Sanger, D.E. (2015): US and China seek arms deal for cyberspace. New York Times online 20 Sep 2015, 5 pages

Sattar, M., Löwenstein, M., Carstens, P. (2010): Vertrauliches, Geheimes und streng Geheimes. Frankfurter Allgemeine Zeitung No.279/2010, p.3

Schaaf, S. (2010): Wikileaks verstreut massenhaft schmutzige Wäsche. Financial Times Deutschland 29 Nov 2010, p.9

Schäder, B., Fend, R. (2010): Peking macht seltene Erden noch rarer. Financial Times Deutschland 30 Dec 2010, p.3

Schanz, M.V. (2010): Building better cyber warriors. Air Force Magazine September 2010, p.50-54.

Scheidges, R. (2010): Bundesamt misstraut US-Firmen. Handelsblatt 02 Dec 2010, p.12-13

Scheidges, R. (2011): Schlechte Noten für deutsche Kryptographen. Handelsblatt 18 Jul 2011, p.17

Schelf, S. (2013): Stromlobby will im Notfall Kühlschränke abschalten. Neue Westfälische 23/24 Feb 2013, p.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, p.168-181.

Scheubeck, Th. (2014): Über Prioritäten nachdenken. Spektrum der Wissenschaft (German Edition of Scientific American) June 2014, p.7

Schlüter, N., Laube, H. (2010): Der RIM-Code. Financial Times Deutschland 03 Aug 2010, p.8

Schmid, G. (2001): Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 INI)

Schmidt, M.S., Perlroth, N., Goldstein, M. (2015): FBI says little doubt that North Korea hit Sony, New York Times online 08 Jan 2015

Schmitt, J. (2009): Virtuelle Spürhunde. Der Spiegel 10/2009, p.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, p.128

Schmundt, H. (2015): Tödlich wie eine Granate. Interview with Luciano Floridi. Der Spiegel 8/2015, p. 120-121

Schneider, W. (2011): Das Unheimliche am Internet. Neue Zürcher Zeitung NZZ Folio January 2011, p.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 an. Bild online 24 June 2012

Schöne, B. (1999): Der „große Lauschangriff“ im Internet. Die Welt 22 Jun 1999, p.32

Schöne, B. (2000): Ein Netz aus 120 lauschenden Satelliten. Die Welt 17 May 2000, p.39

Schröder, T. (2008): Was Du siehst, sehe ich auch. Frankfurter Allgemeine Sonntagszeitung No.3, p.58

Schröm, O. (1999a): Verrat unter Freunden. Die Zeit Nr. 40, p.13-14

Schröm, O. (1999b): Traditionell tabu. Die Zeit Nr. 40, p.15

Schuller, K. (2010): Der Spion, der aus dem Cyberspace kam. In: Frankfurter Allgemeine Sonntagszeitung Nr.51 vom 26 Dec 2010, p.6.

Schultz, S. (2010): Virenjäger sezieren Sabotage-Software. Spiegel online 01Oct 2010, http://www.spiegel.de/netzwelt/netzpolitik/0,1518,720681-2,00.html

Schulz, T. (2013): Frust beim Filtern. Süddeutsche Zeitung 6/7 Apr 2013, p.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 pages

Shah, S. (2014): Die Rückkehr der Pocken. Spektrum der Wissenschaft (German edition of Scientific American) February 2014, p.24-29

Shane, S. (2013): No morsel too small for a US spy agency. New York Times International 8 Dec 2013, p.1/4

Singer, P.W. (2010): Der ferngesteuerte Krieg. Spektrum der Wissenschaft December 2010, p.70-79

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 pages

South Africa (2012): Statement on the approval by Cabinet of the Cyber Security Policy Framework for South Africa 11 March 2012

Spehr, M. (2015): Ausgespäht mit Android. Frankfurter Allgemeine Zeitung 04 August 2015, No. 187/2015, p.T4

Spiegel online (2011): Deutschland probt den Cyber-Ernstfall http://www.spiegel.de/netzwelt/netzpolitik/0,1518,801114,00.html

Spiegel (2012): Badrnejad, K., Dworschak, M., von Mittelstaedt, J., Schnepp, M., Schmundt, H.: Ansteckende Neugier. Der Spiegel 23/2012, pp.121-124

Spiegel online (2012a): Internet-Sicherheit USA und China wollen Cyberkrieg verhindern. Release from 08 May 2012

Spiegel online (2012b): Wie Syrien das Internet verlor. Release from 30 November 2012

Spiegel online (2013a): Briten gründen riesige Cyberarmee. Release from 27 Sep 2013

Spiegel online (2013b): Stromschwankungen bringen NSA-Technik zum Schmelzen. Release from 08 Oct 2013

Spiegel (2013a): Neues Drohnenprojekt. Der Spiegel 25/2013, p.11

Spiegel (2013b): Das chinesische Problem. Der Spiegel 9/2013, p.22

Spiegel (2013c): Abwehrschlacht gegen Cyberspionage, Der Spiegel 13/2013, p.15

Spiegel (2013d): Verdacht statt Vertrauen, Der Spiegel 26/2013, p.111

Spiegel (2014): BND ausgebremst. Der Spiegel 24/2014, p.18

Spiegel online (2016): Gruppe "Shadow Brokers" Hacker erbeuteten offenbar NSA-Software. 17 Aug 2016, 1 page

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 July 2015, 2 pages

Stark, H. (2009): Digitale Spionage. Der Spiegel 11/2009, p.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 Aug 2016, p.36

Steier, H. (2016b): Riskantes Horten von Sicherheitslücken. Neue Zürcher Zeitung online, 18 Aug 2016, 2 pages

Steinitz, D. (2014): Großes Drama. Süddeutsche Zeitung No. 296 from 19 Dec 2014, p.11

Steinmann, T. (2010): Deutschland im Visier der Cyberkrieger. Financial Times Deutschland 29 Dec 2010, p.10

Steinmann, T., Borowski, M. (2012): Deutschland wird im Netz verteidigt. Financial Times Deutschland 05 Jun 2012, p.1

Steler, H. (2015): Google Geräte als Wanzen. Neue Zürcher Zeitung online from 28 July 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 February 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 Aug 2016

Storn, A. (2016): Plötzlich sind 81 Millionen Dollar weg, Die Zeit No.20, 04 May 2016, p.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 Aug 2016, 3 pages

Süddeutsche Online (2013): Hacker aus China klauen Google Datensätze. 21 May 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 pages

Symantec (2011): W32.Duqu The precursor to the next Stuxnet, Dossier, 14 pages

Symantec (2012): W32.Gauss Technical Details, Dossier, 13 pages

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 pages

Symantec (2014b): Emerging Threat: Dragonfly/Energetic Bear – APT Group. 30 Jun 2014, 5 pages

Symantec (2016): The Waterbug attack group. Security Response Version 1.02 Symantec, 14 Jan 2016, 44 pages

SZ (2014a): Der BND will soziale Netzwerke ausforschen. Süddeutsche Zeitung No 130, 31 May/01 Jun 2014, p.1

SZ (2014b): Nordkorea vom Internet abgeschnitten. Süddeutsche Zeitung No. 296 from 24-26 Dec 2014, p.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. Report on 21 Nov 2013

SZ online (2016): Lücke bei Facebook. Zugriff auf die Welt. Article 1.2901048 10 March 2016

T-online (2015): Apple löscht über 250 Spionage-Apps aus App-Store, 2 pages. Artikel id_75824954

Tagesschau (2015): Umbaupläne vorgestellt: Bei der CIA soll vieles anders werden. Tagesschau.de 07 Mar 2015, 1 page.

Talos Cooperation (2012): Transportable Autonomous Patrol for Land Border Surveillance D.10.3 4th Workshop 25 May 2012

TAZ online (2013): China testet das “scharfe Schwert”. 23 Nov 2013, 4 pages

The Economist (2013): War on terabytes. The Economist 02 February 2013, p.59

The SecurityLedger online (2014): New Clues in Sony Hack point to insiders, away from DPRK, page 1 18 Dec 2014

Thibaut, M., Alich, H. (2010): Paris und London besiegeln Militärkooperation. Handelsblatt No.213/2010, p.15

Thiel, T. (2012): Auf der sicheren Seite. Frankfurter Allgemeine Zeitung No. 281/2012, p.Z1-Z2

Tiesenhausen, F. von (2011): Zehn Beamte gegen den Internetkrieg. Financial Times Deutschland 24 Feb 2011, p.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, p.228-233

Tomik, S. (2013a): Pufferspeicher, Volumenreduktion und Community Detection. Frankfurter Allgemeine Zeitung No. 156/2013, p.6

Tomik, S. (2013b): Enthüllungen am laufenden Band. Frankfurter Allgemeine Zeitung No. 148/2013, p.2

Touré, H.I. (2012): Statement from Dr. Hamadoun I. Touré Secretary General of the ITU. Dubai, 13 December 2012

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 pages including a 3 page annex with the code of conduct

Uhlmann, P. (2010): Informationsprofis arbeiten enger zusammen. Truppe für Operative Information - Übergabe InfoOp. Date: 01 Jul 2010 http://www.opinfo.bundeswehr.de/portal/a/opinfo/unsere_l/zopinfo/infoop/uebergabe

Ulfkotte, U. (1998): Im Visier der Datenjäger. Frankfurter Allgemeine Zeitung No.125, p.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 pages

USAF (2010a): US Air Force Doctrine Document (AFDD) 3-12, Cyberspace Operations 15 July 2010, 55 p.

USAF (2010b): US Air Force Doctrine Document (AFDD) 3-13, Information Operations 17 September 2010, 54 p.

Valeriano, B., Maness, R. (2011): Cyberwar and Rivalry: The Dynamics of Cyber Conflict between Antagonists 2001-2011, 25 pages

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 Sep 1999

Vitzum, Th. (2013): unbekanntes Flugobjekt. Welt Am Sonntag No. 22, 02 Jun 2013, p.6

Wanner, C. (2011): Das Phantom von Shenzen. Financial Times Deutschland 28 Feb 2011, p.8

WCIT (2012): Official Powerpoint Presentation of the ITU

WCIT Final Acts (2012): Final Acts of World Conference on International Telecommunications, 23 pages

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, p.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 mode

Weber, M., Weber, L. (2016): Die smarte Kapitulation. Frankfurter Allgemeine Zeitung No.3/2016, p.T1

Wechlin, D. (2016): Auf Orwells Spuren. Neue Zürcher Zeitung 27 Jun 2016, p.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, p.67-77

Wehner, M. (2015): Cyber-Krieg im Bundestag. Frankfurter Allgemeine SonntagsZeitung. Nr.24 from 14 June 2015, p.1

Wehner, M. (2016): Cyberkrieg. Frankfurter Allgemeine Sonntagszeitung from 07 Aug 2016, p.6

Welchering, P. (2011): Wie Ägypten das Internet gezielt abschaltete. Frankfurter Allgemeine Zeitung No. 32/2011, p.T2

Welchering, P. (2012): Wege in den digitalen Abgrund. Frankfurter Allgemeine Zeitung No. 134/2012, p.T1

Welchering, P. (2013a): Digitale Überwachungsaugen an jeder Ecke. Frankfurter Allgemeine Zeitung No. 110/2013, p.T6

Welchering, P. (2013b): Mit Vierkantschlüssel und Biege-Koppler. Frankfurter Allgemeine Zeitung No. 156/2013, p.6

Welchering, P. (2013c): Geheimdienste lesen auch bei verschlüsselten Daten mit. Frankfurter Allgemeine Zeitung No. 216/2013, p.T2

Welchering, P. (2014a): Das Stromnetz verrät nicht nur Kriminelle. Frankfurter Allgemeine Zeitung from 01 July 2014, p.T4

Welchering, P. (2014b): Arbeiten am Trojaner-Abwehrschirm. Frankfurter Allgemeine Zeitung from 09 September 2014, p.T4

Welchering, P. (2016): So fahndet der Geheimdienst NSA nach Programmierern. Frankfurter Allgemeine Zeitung No. 136/2016, p.T4

Welt (2013): Und alle hören mit. Welt am Sonntag No.43, 27 Oct 2013, p.3

Welt online (2013): Teheran führt Aufklärungsdrohnen vor. Welt am Sonntag No.43, 28 Sep 2013

Welt online (2014): Forscher entwickeln Herzschrittmacher ohne Batterie. Welt online 20 Jan 2014

Werner, K. (2010): Siemens zieht in den Cyberkrieg. Financial Times Deutschland 21 Dec 2010, p.7

White House (2011): International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World, 25 pages

White House (2013): The White House (2013): Executive Order – Improving Critical Infrastructure Cybersecurity 12 Feb 2013, 6 pages

White Wolf Security (2007): Estonia and Cyberwar – Lessons Learned and Preparing for the Future By White Wolf Security, 3 pages, 6 April 2007

Whitlock, C. (2014): When drone fall from the sky. Washington Post online from 20 June 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 Feb 2009 Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr. Presentation 31 pages

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

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

Winkler, P. (2013): Die Affäre Edward Snowden schreckt Washington auf. Neue Zürcher Zeitung International No.133, 12 Jun 2013, p.3

Winkler, P. (2014a): Die NSA kann Computer auch offline ausspähen. Neue Zürcher Zeitung 17 Jan 2014, p.3

Winkler, P. (2014b): Designierter NSA-Chef will mehr Transparenz. Neue Zürcher Zeitung 14 March 2014, p.3

Winkler, P. (2015): Die Mutter aller Datendiebstähle. Neue Zürcher Zeitung, No 139, p.3

Winkler, P. (2016): Russische Hacker in Amerikas Wahlregistern. Neue Zürcher Zeitung, 01 Sep 2016, p.4

Wong, E. (2013): Espionage Suspected in China`s drone bid. New York Times international Weekly 27 Sep 2013, p.1 and p.4

Wysling, A. (2013): Spione im Mobilfunknetz. Neue Zürcher Zeitung 07 Dec 2013, p.5

Wysling, A. (2014): Luftraum frei für Drohnen. Neue Zürcher Zeitung 04 Jan 2014, p.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 pages

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 pages

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, p.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 August 2013

Zeit online (2015a): Sieben Wege, ein Handy abzuhören. 20 February 2015, 2 pages

Zeit online (2015b): Apple and Samsung arbeiten am Ende der SIM-Karte. 17 July 2015, 2 pages

Zeng Guang (2013): Gefährliche Experimente mit Vogelgrippe-Viren. RP online 16. August 2013, 2 pages.

Zepelin, J. (2012): Länder lahmlegen. Financial Times Deutschland 06 Jul 2012, p.27

Zetter, K. (2016): Everything we know about Ukraines power plant hack www.wired.com 20 Jan 2016

Zhanga, X. (2012): Structure of Sputnik, a virophage, at 3.5-Å resolution. PNAS, 06 Nov 2012 vol. 109, no. 45, S.18431–18436

Zhou, J. et al. (2012): Diversity of Virophages in Metagenomic Data Sets. J. Virol. 2013, 87(8):4225. DOI: 10.1128/JVI.03398-12. Journal of Virology p.4225–4236

Zoll, P. (2015): Donnerwetter aus Nordkorea. Neue Zürcher Zeitung from 05 Jan 2015, p.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, p.77-86