UNIVERSITÄT OSNABRÜCK
Geostrategy and Geopolitics
Department 1
49069 Osnabrueck

# Cyber war

# Methods and Practice

26 Sep 2022

**Summary**

Cyberwar (Cyber war, Cyber Warfare) is the military confrontation with the means of information technology. This paper presents the current state and deals with the theoretical and practical problems. In practice, cyberwar is an integral part of military action, but cannot be completely separated from espionage, since the intrusion into and reconnaissance of target systems is essential for further action.
After an overview of attack methods, attackers (Advanced Persistent Threats), spy tools, cyber weapons and cyber defense, a particular focus is on the attribution of cyber-attacks and the Smart Industry (Industry 4.0). Afterwards, the cyberwar strategies of the US, China, Russia and further leading actors will be discussed. Further chapters present Artificial Intelligence, Smart Industry, smart devices and biological applications.

## Table of Contents

# 1. Fundamentals

## *1.1 Introduction*

The cyberspace is meanwhile regarded as separate military dimension[1]. Cyberwar (Cyber war, Cyber Warfare) is the military confrontation with the means of information technology. This paper presents the current state and deals with the theoretical and practical problems. In practice, cyberwar is an integral part of military action, but cannot be completely separated from espionage, since the intrusion into and reconnaissance of target systems is essential for further action.
After an overview of attack methods, attackers (Advanced Persistent Threats), spy tools, cyber weapons and cyber defense, a particular focus is on the attribution of cyber-attacks and the Smart Industry (Industry 4.0). Afterwards, the cyberwar strategies of the US, China, Russia and further leading actors will be discussed. Further chapters present Artificial Intelligence, Smart Industry, smart devices and biological applications.

## *1.2 Background*

The increasing dependence on computers and the increasing relevance of the Internet by the increasing number of 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:

- Exponential growth of vulnerabilities due to rapid increase of digital devices, applications, updates, variants, networks and interfaces
- Computers and devices are no isolated systems, because for technical, commercial and surveillance purposes digital technologies need to remain accessible from outside
- Data protection and privacy is eroded by voluntary, unknown or enforced (e.g., by usage conditions) data release to third parties
- Professional search for gaps and exploits by hackers, hacktivists, cyber criminals, security companies and –researchers, but also by state authorities or state-linked groups.

Technical aspects are in particular:

- 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

[1] USAF 2010a, DoD 2011

communicate with computers and with each other[2]. The **car-to-car-communication** is another planned feature which will 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 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]), see Section 8.8.
- 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)'** and the **'company owned, personally enabled (COPE)'** concepts that describe 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].

[2] The Machine-to-Machine (M2M) communication potentially concerns 50-70 billion 'machines', of which only 1 % were already connected in 2009 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.
[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.
[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

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].

- 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.

Also, there is a significant trend to more aggressive and larger attacks as shown in detail in Section 2.3.1.1.

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 Cyberwar 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 information technology[12].

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[13].

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[14]. However, most authors believe that large-scale cyber-attacks cannot be

[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). In Germany, the Ministry of the Interior BMI has defined 1.700 objects are relevant core which have to be protected, including 110 hospitals which treat at least 30,000 cases per year, Osterloh 2017, p.B795

[11] Megill 2005, DoD 2011

[12] Wilson 2008, p.3ff.

[13] Beidleman 2009, p.9ff. and p.24

[14] also CSS 2010, Libicki 2009, p. XIV

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.

A comparison of cyber war concepts of various NATO states with Russia and China shows different perspectives. In particular, the question is debated whether cyber war is limited to the military conflict dimension or may also include the civil and economic dimension[15]. Nevertheless, the USA has worked on a more precise and pragmatic cyber war definition.

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*"[16].

General Keith Alexander who was the first 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[17]. 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[18]. 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[19] (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[20].

---

[15] IT Law Wiki 2012a, p.1-4
[16] Alexander 2007, p.61
[17] 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."
[18] Alexander 2007, p.60
[19] IT Law Wiki 2012, p.2
[20] See also Beidleman 2009, p.10

The cyber war concepts of US and China agreed from the very beginning that the use of computers in military activities is only part of other military activities. The debate on the question whether a war can be decided by computer attacks alone is only a theoretical one, for the military practice this option was never taken into consideration.

Sometimes it is further debated whether computers could really be a part of a war as computer attacks could not kill people, but in military practice this debate is misleading. Computers are simply technical tools as e.g., *Radar systems*. Radar systems do not kill enemies directly and indeed, they save a lot of lives in civil air traffic, but nobody would doubt that Radar systems are part of military activities as well.

The Russians include the information war in their cyberwar definition, but the dissemination of opinions and information in the internet serves political and social purposes and not military-technical goals, see also Section 2.2.6.

## *1.4 Cyberwar and Espionage*

It is important to take a closer look at the difference between espionage and cyberwar. Hackers try to inject malware into a digital device such as a computer or e.g., to penetrate also smartphones, in order to perform actions for espionage, manipulation, sabotage, theft/extraction and misuse.
Hackers have to go into computers, but they also have to get the information out to the command-and-control server. This bidirectional communication often allows detection of an infection and tracing the attacker.
For damage of a computer or a system it is necessary to access it. There are a lot of espionage activities and little cyberwar, but cyberwar often requires just an extra mouse click.
On the one hand, this explains why security experts consider the danger of cyberwar to be high and demand appropriate measures, while others find the matter exaggerated because one could not yet observe a large-scale cyberwar.
The boundaries between espionage and cyberwar are fluid, since cyberwar requires preparatory espionage, which is also reflected by a sometimes-unprecise reporting of cyber events. According to US media, a CIA-led discussion on the digitization of espionage concluded that digital espionage can only complement conventional espionage, but cannot replace the presence of local agents.

## *1.5 Terminology*

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 **cybercrime** is mostly used for 'normal' crimes like theft of money by abuse of online banking data[21].
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[22]. However, large-scale cyber espionage can lead to significant computer and network problems and is then often assigned to cyber war by literature, too.
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)**[23].

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[24])
- 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[25]. Drones are used for all kinds of operations that are „dull, dirty, dangerous or difficult"[26]. The practical effect of the drones has led to an increased demand[27][28].

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

[21] See also Mehan 2008, CSS 2010
[22] Libicki 2009, p.23
[23] Neuneck/Alwardt 2008
[24] Hürther 2010, p.33-34
[25] Rüb 2010, p.5
[26] Jahn 2011, p.26
[27] FAZ 2010b, p.6
[28] 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.[29] 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[30]
- to mislead the enemy by **military deception MILDEC**, e.g., as the Iraqi air defense systems in the Gulf war[31]
- 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)**[32], **computer network exploitation (CNE)** and the countermeasures as **computer network defense (CND)**[33]
- the conventional **electronic warfare (EW**) where the electronic signals of the enemy are e.g., disturbed by **jamming**.

### *1.6 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[34].

---

[29] Wilson 2007
[30] USAF 2010b, p.5
[31] USAF 2010b, p.32
[32] Wilson 2008
[33] CSS 2010
[34] Nevertheless, plans for fully computerized counterattacks are under discussion, Nakashima 2012b

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[35] and China[36].

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*[37].

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*[38].

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 restrictions[39]. 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); thus, states need to agree on basic measures of self-restraint during peacetime[40].

The UN including Russia, China and US agreed on an updated GGE report in 2021[41].

---

[35] Nakashima 2012a
[36] Spiegel online 2012a
[37] ITU 2012
[38] See also Fayutkin 2012, p.2
[39] UN 2015
[40] Rõigas/Minárik 2015
[41] Mäder 2021b

The document states that the Law of Nations is applicable to cyberspace as well. In particular, the protection of critical infrastructures is crucial[42]. A new aspect is the need to engage non-state actors as well, including the private sector, civil society, academia and the technical community. Also, the regional and sub-regional levels should be taken into consideration. However, it was also clarified that the norms of responsible State behavior are voluntary and non-binding.

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) [43].

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)[44]. According to CCD CoE in February 2016, the development of an updated Tallinn Manual 2.0 was started. The NATO now formally considers cyber space as a potential place of military conflicts[45].

## *1.7 The Geostrategy of Cyberspace*

In the meantime, the structures in cyberspace were solidified and professionalized. More and more specialized cyber units are being set up, both at the intelligence or military level.
As a result, the focus is increasingly on securing the national IT infrastructure, which is accompanied by a growing risk of fragmentation of the Internet.

---

[42] GGE 2021
[43] CCD CoE 2013, Schmitt 2013
[44] 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.
[45] Gebauer 2016

After a long-term dominance of the perspective of the cyberspace as a virtual world, security experts are gaining a more and more physical understanding: who controls the devices and the cables, also controls the data in them.

### 1.7.1 Control of data exchange

#### 1.7.1.1 Physical data control

The long-term strategies are aimed at **securing or regaining physical control of data exchange**, despite global networking.

In fact, the idea of a virtual control of the own population and opponents appeared to be problematic in the long run for three reasons:

- In the past, access to information was often vertical-hierarchical, but networking allows aggressive hackers attacking even presidents and releasing their information. Leaks are becoming more common and more serious.
- Virtual surveillance allows unprecedented control of the own population, but also for attacking adversaries, as shown in the so-called '*OPM-Breach*', where hackers copied the personal files of US citizens with security clearance checks and also, they copied their digitally stored fingerprints.
- Third, virtual control can be used to gain and secure power through technical superiority, but if the technology advantage is disappearing, it is practically impossible to keep away from attackers.

The **physical data control** could be (re)gained by several approaches, namely by

- physical system access
- creation of cyber-islands
- Squeezing foreign companies out of their own security architecture.

Long-term control can ensure **physical system access**, e.g., access to servers, to internet nodes, tapping of deep-sea cables, etc. or redirects the data traffic with strategically positioned internet node servers with the **Border Gateway Protocol hijack**. The re-routing allows undetected copying of the data or even their elimination from traffic and US studies have shown that this already done sometimes even for some weeks.

- Increasingly, states require that servers are set up by international providers in their own country so that the authorities can have direct access to the system.
- Moreover, some states require that certain data are to be stored only nationally and not allowed to be stored outside the country. This may not

really protect against espionage, but it increases the attacking risks and costs of the attacker.
- Earlier attempts to gain physical control, the separation of subsystems from the network, could usually not prevent, but only delay the opponent's access.
- Note that despite the rise of remote hacking, **physical interception and data collection units** closely located to the targets are essential for enduring and successful intelligence operations.

**Formation of cyber islands**
Blocking access to content from foreign providers, in conjunction with blockades of **Virtual Private Network VPN** tunnel[46] allow the creation of cyber-islands.
A 'soft' island forming method is the **offering of national services and platforms**, which increase the attractiveness for the own population and at the same time create linguistic and possibly also technical entrance hurdles for foreigners.
A special case is Russia, whose network developed independently in Soviet times and is now known as *Runet*. The long abstinence of the West resulted in a continued dominance of Russian providers[47]. From the original Soviet Internet system *Relkom* emerged the Russian part of the Internet. Early, the search engine *Yandex (Yet another index)* and the social network *VKontakte* started, which continue to dominate the market.

The **blocking of internet access** and/or slowing down the network speed are frequent measures by nation states to control political tensions. In 2015, this was done in 75 cases, 2016 already in 106 cases[48].

**Squeezing foreign companies out of their own security architecture**
- States are increasingly making sure that foreign providers cannot buy into their critical infrastructure and thus enter the defense perimeter of the respective state.
- Foreign security companies are increasingly being targeted by investigators.

### 1.7.1.2 Deep Sea Cables

US Technology companies currently control more than 50% of the deep-sea cables which currently transfer 95% of all internet data. Currently, there are 400 cables with 1.3 million km length and until 2025, 45 further cables are planned.
Now, new global players appear, e.g., China with the *Pakistan and East Africa connecting Europe (Peace) Cable* from China via land to Pakistan, then in the sea

[46] China planned a VPN ban in mid-2017. In China, Chinese equivalents for search engines and social media such as *Baidu* and *Wechat* exist since long times and are extensively used.
[47] Limonier 2017, p.1, 18-19
[48] Kormann/Kelen 2020, p.4

to France[49]. From 2016-2019, Chinese companies were involved in around 20% of all deep-sea cable projects[50].
Western states try to avoid involvement of Chinese company *Huawei* while China tries to stop *Google*-owned cables where possible.

While there are concerns about sabotage, currently fishery and anchors are still the most frequent reason for failures[51].

However, there are growing concerns on cable espionage. On the land, China Telecom has ten internet **Points of Presence (PoPs)**, i.e., major connection points where a long-distance telecommunications carrier connects to a local network, across the internet backbone of North America, thereof eight in the US and two in Canada[52], and also further servers in Europe, such as in Frankfurt/Germany. Several temporary events were noted which were by far too long and too large to be technical errors, including a takeover of 15% of the Internet traffic for 18 minutes by China Telecom on 08 Apr 2010 and further redirections of data traffic[53].

According to the *Snowden Leaks*, the US *National Security Agency (NSA)* put a computer virus into the administration center of the sea cable SEA-ME-WE 4, which goes from Marseille to North Africa, the Gulf Region and South East Asia[54].

However, meanwhile detectors were placed globally by the Five-Eyes Intelligence Cooperation (see Section 6.2). However, France started in 2008 its own surveillance program[55].

Russia would at least be technically able to cut deep sea cables, the era of **Seabed Warfare** may come. The Russian ship *Yantar* has two manned deep-sea submarines which can go down to 6,0000 meters and it was seen near Ireland. Until 2024, the British Navy will provide a *Multi Role Ocean Surveillance Ship* with sensors and autonomous remotely controlled unmanned underwater vehicles (UUV). France will update is seabed strategy in 2022, too[56].

A future game changer for the cable-bound data transfer could be *Starlink*[57]. *Starlink* is a satellite-based network with low-orbit satellites which are released by SpaceX since 2019. The aim is to put up to 42,000 satellites into space. The users need a receiver and routing device to get the data which are transported with light. The low-orbit allows a reliable and fast data transfer. This makes senders and users

[49] Rolfs 2021, Gollmer 2022b
[50] Perragin/Renouard 2022
[51] Gollmer 2022b
[52] Demchak/Shavitt 2018
[53] Demchak/Shavitt 2018
[54] Perragin/Renouard 2022
[55] Perragin/Renouard 2022
[56] Gollmer 2022b
[57] DW 2022

independent from the physical internet. This was the reason why the owner Elon Musk provided it to the Ukraine shortly after the Russia attack. The satellites have an expected work time of 5 years which requires permanent replacement. The astronomy is concerned about interference with space observation. The number of satellites makes it impossible to establish a second competitor system, i.e., Starlink will be the only system.

#### 1.7.1.3 Control of Content

A study from 2020 showed an increasing internet censorship in over 100 countries worldwide[58]. The most commonly used censorship methods were internet shutdowns, *domain name server (DNS)* manipulations to block contact to certain servers, blocking of IP addresses by IP/TCP blocks and interference on the http(s)-layer for censored keywords[59].
The censored content strongly varies between countries, but the top 5 global categories were anonymization and circumvention tools, foreign relations and military, pornography, certain search engines and topics from history, arts and literature[60].

### 1.7.2 Control of Critical Elements

#### 1.7.2.1 Rare Metals

China had in 2010 a 97% market share[61] for rare industry metals such as niobium, germanium, indium, palladium, cobalt, and tantalum which cannot yet be recycled in an efficient manner and are irreplaceable in IT industry. China reduced the export volume to satisfy the needs of their domestic industry[62]. 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[63].

The US has identified 35 raw materials as critical, for 14 of these raw materials have no own production. For rare earths, China has 71% market share and 37% of reserves in 2019, while Vietnam and Brazil, each with 18% reserves, could be future alternative support states.[64]

[58] Raman et al. 2020
[59] Raman et al. 2020, p. 50
[60] Raman et al. 2020, p.65
[61] Büschemann/Uhlmann 2010, p.19
[62] 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
[63] FAZ 2010d, p.12, Bierach 2010, p.11, FAZ 2013d, p.24
[64] FAZ 2019b, p.17

### 1.7.2.2 Semiconductor Chips

For computer chips, the market is dominated by Taiwan and South Korea. Taiwan has a global market share of 64%, the *Taiwan Semiconductor Manufacturing Company TSMC* alone already of 50%, for the most advanced chips the market share of Taiwan is even 92%. South Korea is the second largest provider, while China has less than 10% market share[65].

TSMC does not develop chips, but can produce them with a 5-nanometer technology, in the near future 3-nanometer chips are expected. In comparison, China is currently advancing to the 7-nanometer level[66]. As TSMC builds e.g., microchips for US F-35 jets, US pushed TSMC to build a fabrication in Arizona.

### 1.7.2.3 Relation USA - China

Both US and China are major cyber powers: China is the main producer of physical electronics in computers and smartphones, even US firms outsource their production often to China. This is logic as China is the main owner of computer-relevant metals. Also, China produces 75% of the mobile phones and 90% of all PCs, as even US companies outsource this production step to China.

On the other hand, US dominate the infrastructure level of central servers and of deep-sea cables. In the physical world, the internet is finally bound to a physical network with a significant level of centralization. The US-based company *Equinix* controls according to their website with their own IXPs and co-location of client computers in their data centers roughly 90% (!) of the data volume transfer of the internet.

### 1.7.2.4 The Huawei Conflict

The 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. The US authorities instructed *Huawei* to sell their shares of the Cloud computing company *3Leaf* for security reasons[67].

As in previous years, security concerns against the Chinese company *Huawei* were expressed in 2018 by Western countries, as this is meanwhile one of the largest global smartphone producers and also one of the largest infrastructure providers, in particular radio masts for smartphones and other data traffic[68]. In Germany, they

[65] Bost 2022
[66] Ankenbrand/Finsterbusch 2022, Welter 2022
[67] Mayer-Kuckuck/Hauschild 2010, p.28, Wanner 2011, p.8
[68] Giesen/Mascolo/Tanriverdi 2018

provided almost 50% of all radio masts, while *Huawei* components were already forbidden in the German government network despite protests. While the German IT security organization BSI did not find anything in technical analysis so far, the technology is very complex which leaves some uncertainty.

The *Huawei* matter escalated for two reasons: The next Internet communication generation **5G** is coming which will allow the first time a broad implementation of the **Internet of Things** and of smart home and smart city solutions, in particular by much higher data flows, real-time transfer massively reduced latency times (transmission delays) under 1 millisecond and also reduced energy need for transfer per bit. The other point was the capture of the Finance chief of *Huawei* in Canada due to assumed violations of the US sanctions against Iran on 01 Dec 2018[69].

In United Kingdom, Huawei cooperates with the official *Huawei Cyber Security Evaluation Centre (HCSEC)*. While the cooperation between Huawei and HCSEC was overall assessed as positive and transparent, the number of vulnerabilities in their systems has risen to several hundred (point 3.11) and even known vulnerabilities were used again, as a result of a speedy product development and updating. The HCSEC suggested changes of the software up to chips (point 3.16). The problem was the (too) fast product development[70].

The US sanctions against *Huawei* 2019 should stop *Huawei*'s rise, e.g., the US advises other countries not to use *Huawei* products in sensitive areas. *Huawei* is now the world's leading mobile infrastructure provider with more than 30% market share, i.e., higher than *Apple* for smartphones. *Huawei* has 92 suppliers, including 33 from the US, such as Google's *Android* system, *Qualcomm* chips and *Microsoft* applications.[71]
Further restrictions for trade between US and Huawei were implemented in 2020 which targeted Huawei's production ability[72].

### 1.7.2.5 Clean Network versus 3-5-2

Already since years, US and China are using increasingly separated internet environment. While US is dominated by the 'big five' (*Google, Apple, Microsoft, Amazon* and *Facebook*), China has the messenger platform *WeChat* (owned by *Tencent*), the search engine *Baidu*, the Twitter-equivalent *Sina Weibo* and the video applications *Tiktok, Duoyin* (both owned by *Bytedance*) and *Kuaishou*[73].

[69] Giesen/Mascolo/Tanriverdi 2018
[70] HCSEC 2019
[71] Müller 2019, p.9
[72] Ankenbrand/von Petersdorf 2020, p.16
[73] Gollmer 2019, p.7

Now, both states work on the complete separation of their internet infrastructure which bears the risk of a separation of the internet into two different technology worlds.

In the *3-5-2 project* from late 2019, Beijing has ordered all government offices and public institutions to remove foreign computer equipment and software within three years, with 30% in first, 50% in second and 20% in third year, which explains the name 3-5-2[74].

On the other hand, the United States set up the *Clean Network Program* in 2020 which intends to remove Chinese IT components from IT infrastructure with the five areas Clean Carrier, Clean Apps, Clean store Clean Cable and Clean 5G Path[75].

### 1.7.3 The Centralization Trend

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 drives of their computers, but the work is done after log in by computers of large server farms[76].
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[77], of classic espionage and of conventional physical attacks[78].
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 weighed against 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.

---

[74] Financial Times 08 Dec 2019
[75] State Department 2020
[76] ENISA 2009, p.2; see also Dugan 2011, p.8
[77]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.
[78] Also, electricity issues can damage large computers seriously as reported in Oct 2013 for the *Utah Data Center*, Spiegel online 2013b

Typically, states start managing cyber matters with setting up cyber authorities. In a second step, new matters are addressed with setting up further authorities which then leads to overlapping or unclear responsibilities. The final step is then restructuring and centralization.

# 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**).[79]

### 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[80]. The EMP protection is technically possible, but expensive and can only be done for selected systems. However, a study by the *Electric Power Research Institute* on the EMP showed in simulations that the explosion of a 1.4-megaton bomb at a height of 400 kilometers would only result in regional power grid collapses and no scenario would lead to a nationwide collapse[81].

### 2.1.3 The attack on and manipulation of computers and networks

Computers and networks can be attacked 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.

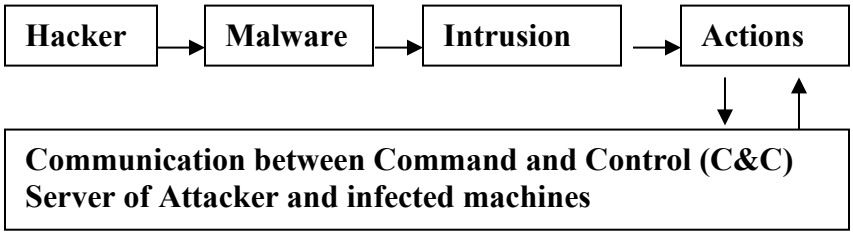
## *2.2 Attack on Computers*

### 2.2.1 Basic principles of cyber attacks

Cyber-attacks require the intrusion of the digital device, i.e., the computer, smartphone or all kinds of digital devices with some kind of malware and the communication with the intruded devices to start actions. Dependent on the type of

[79] Wilson 2008, p.11
[80] Morschhäuser 2014, p.1-2
[81] Rötzer 2018

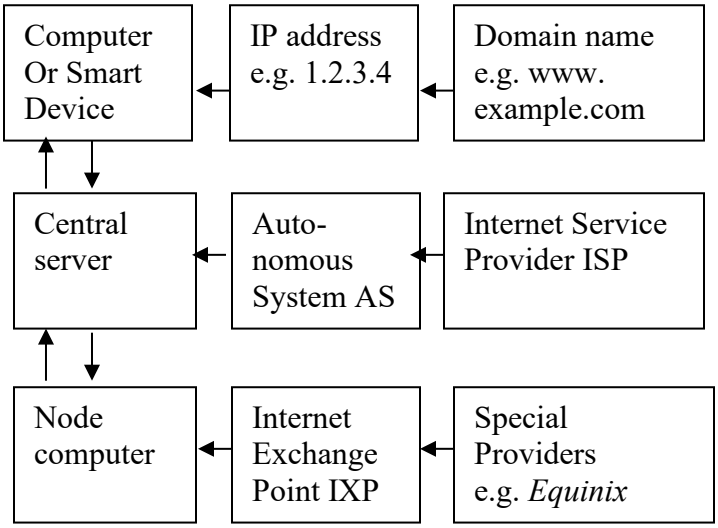
action, the communication will be maintained for a longer time, even for years and complex attacks typically require *bidirectional* communication which gives multiple opportunities for detection and attribution.




### 2.2.2 Communication lines of cyber attacks

Data, i.e., bits and bytes are not fully virtual, but still have physical representations as a defined electromagnetic condition on storage media and device memory systems[82]. Even wireless transfer results in electromagnetic waves and finally these waves end up physically in devices again. This finding is essential for detection and attribution. As the communication is going via networks of computers, it is helpful to keep the general infrastructure of the internet in mind: This structure also forms the hackers' ecosystem.

**Simplified model of Internet communication**




Typically, an internet communication starts at a certain computer and the data are then transferred to the central computer of an **Internet Service Provider (ISP)**. This central computer is formally known as **Autonomous System (AS)** and large providers may have many of those. However, the Internet Services Providers need

[82] This sounds trivial, but this means that deleted data on a device are **not erased**. The device only marks the file as 'deleted' and it does not appear on the screen anymore. In reality, the data are still on the storage medium which allows recovery of "deleted" data by forensic and espionage techniques.

to be connected with each other, this is done via node computers, formally known as **Internet Exchange Point (IXP)**. In reality, these are large computer centers and not only single computers.

Each computer connected to the internet has an **IP (Internet protocol) address**, a number structured after certain rules. The old 4-digit system of the IP version 4 will now be replaced by larger blocks of the IP version 6, but the principle that a domain is related to an IP address number at a certain timepoint remains the same. This has the same function like telephone numbers for phones, i.e., the technical possibility to connect sender and target correctly.

Now, websites have IP addresses as well, but instead of this normally **domain names** are used, e.g., *www.example.com*. At a certain timepoint, domain names refer to certain IP addresses to avoid communication confusion.

As a consequence, the internet may appear decentralized and virtual in daily routine and it seems almost futile to find out where a cyber-attack came from.
In the physical world, the internet is finally bound to a physical network with a significant level of centralization. The US-based company *Equinix* controls with their own IXPs and co-location of client computers in their data centers roughly **90%** (!) of the data volume transfer of the internet[83]. As shown now, this offers opportunities to get insight into the infrastructure of the adversary.

### 2.2.3 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[84].

[83] Müller 2016, p.7
[84] Northrop Grumman TASC 2004

## 2.2.3.1 Introduction

**Expansion of attack targets**

| Past | Today |
|---|---|
| Computer | Equipment: Mouse, Printer, Router, USB-Sticks<br>Smartphones/iPhones<br>Smart home: Internet of Things<br>Infrastructure: Access to national servers, tapping of Internet nodes, redirection and copying of traffic, tapping deep-sea cables, attacks on clouds, 5G towers |
| Software | Hardware (Fuzzing), Firmware, Add-on Chips |
| Hacking/Virus | Interdiction, theft, ‚pre-installed viruses‘ |
| User | Data collection in stock („everything from everybody“) |
| | Higher levels: account holders > bank > interbanking system |
| | Attacks on third vendors, suppliers and maintenance systems, help desks and contract staff |

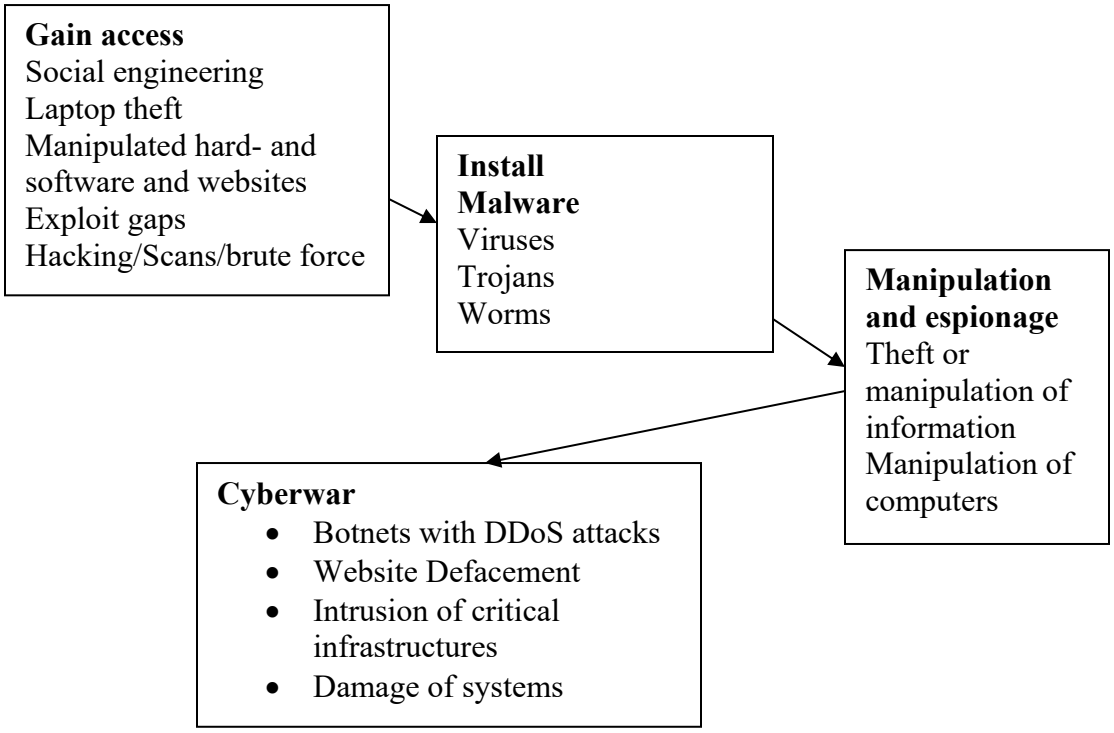
In the period around 2000, computer attacks were often limited to a hacker attacking a computer in order to influence its software (programs) in order to reach a user. The targets have meanwhile massively expanded. Today, in addition to the computer, the equipment is also infected, even the mouse. The trend goes from computers to smart phones as new digital key device (email, smart home, *BYOD, COPE*, smart car, online payments). The weaknesses found in smartphones and iPhones are constantly increasing, malicious apps are a particular problem. In the *Smart Home* everything is attacked from the fridge to the babyphones. New attack targets in addition to the software are now computer chips, the key programs of the so-called firmware, but also the motherboards. For the latter, there were reports of secretly additionally built-in elements as **add-on mini chips**, which were denied by the affected company *Apple*, but at least such an attack seems to be technically possible (for details and literature, see the following sections).
After a long-term dominance of the perspective of the cyberspace as a virtual world, security experts are gaining a more and more physical understanding: who controls the devices and the cables, also controls the data in them. Thus, states may request access to servers, to internet nodes, tapping of deep-sea cables, etc. or redirects the data traffic with strategically positioned internet node servers with the **Border Gateway Protocol hijack**.
The re-routing allows undetected copying of the data or even their elimination from traffic and US studies have shown that this already done sometimes even for some weeks. Large storage computers, the clouds, are already being attacked, and in the future the **resilience**, i.e., the continuation of operability in case of attacks, will be of paramount importance, especially with the upcoming **5G technology**.

It is not necessary to hack, attackers can also intercept postal packets with devices and manipulate them (**Interdiction**) or simply steal computers, CDs and USB sticks,

the *British Ministry of Defense* missed several hundred in recent years[85], some companies deliver the virus already together with their cheap mobile phone. The single user is barely interesting, today it is preferred to collect everything from everyone meanwhile, hacking and data collection for future activities (smartphones, internet of things, hospitals, banking accounts etc.…)[86]

Instead of individual customers, hackers try to rob the bank itself, such as the *Carbanak* group, which captured about 1 billion Euros while other hackers manipulate the exchange between banks, as demonstrated by the North Korean hacker group *Lazarus*, see Section 5.
It is essential for companies that hackers are increasingly targeting suppliers and maintenance systems as well as service providers, so that a company may get the infection together with the third vendor.
Not all methods have changed: automatic contact attempts with search for open communication channels (**port scans**) are still significant. That would be like trying out all the phone numbers and see who's picking up the phone. Password trying is taken by over machines, this method is known as **brute force**.

[85] vgl. Zeit online 2016b
[86] Such as the *MySpace* hack with 360 million passwords in 2016 and the *Yahoo* hack in 2014 with 500 million user accounts, Hern/Gibbs 2017




### 2.2.3.2 Gain access

The following methods are the most common to gain access:

- **Phishing** in combination with **social engineering**
- **Infected Websites**
- **Backchannels**
- **Exploits**, i.e., use of vulnerabilities, **backdoors** and **bugdoors**
- **Infected storage media and digital devices** such as routers
- **Infected software** for download such as **Apps** and **updates**
- **Hacking of passwords**
- Physical measures such as **interdiction** and **theft** of computers and smartphones
- **Falsified microchips**
- **Firmware infections**
- **Modified motherboards**
- **Fuzzing**
- **Pre-encryption access** to servers
- **Misconfigured internet servers (BGP hijacking)**

- **Phishing** in combination with **social engineering**

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). Intentional misleading of users can be done by **social engineering**, where e.g., wrong 'administrators' ask users for passwords (or e.g., wrong 'CEOs' for money transfers known as '**CEO fraud**'). Social engineering via telephone call is also known as **Vishing (Voice Phishing)**. A former NSA agent found in studies that 14% of phishing attacks are successful, sometimes even more. A trick is to make minimal variations to real website, e.g., one letter large instead of small, a method known as **typosquatting**. In larger attacks, the first email was opened after 2 minutes and the first attachment was opened after 4 minutes.[87]

But **insiders**, in particular those with IT knowledge, can help to breach organizational security as well as discussed later. An increasingly used technique is to attack average employees of an organization and then to escalate unprivileged user accounts 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.[88] The outsourcing of sensitive IT projects to external providers brings additional risks by creating additional interfaces which may be used for attacks by adversaries[89]. Also, this can lead to loss of internal IT competence.

- **Infected Websites**

**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.

---

[87] Schmieder 2017, p.74

[88] 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.

[89] 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.

- **Backchannels**

The *Efail* vulnerability was discovered in 2018 and uses html-based backchannels. A backchannel is here a method for forcing the email client to invoke an external URL, e.g., forcing to download an image. *Open Pretty Good Privacy (PGP)* solely uses *Cipher Feedback Mode (CFB)* and *Encryption Methods Secure/Multipurpose Internet Email Extensions (S/MIME)* and the *Cipher Block Chaining Mode (CBC)* for operation. Malicious CFB/CBC tools can be used for attack. The attacker needs to wrap the encrypted message into plaintext MIME parts containing a html-based backchannel, the decrypted text is then returned via a html-link to the attackers, if html is allowed in the email program[90]. This was possible not for all, but for most tested email clients.

- **Exploits**, i.e., use of vulnerabilities, **backdoors** and **bugdoors**

The exploitation of security gaps in software programs and operation systems (e.g., *Adobe* and *Windows*) is also known as **exploit problem.** The probing of computers can also be done by **port scans**[91]. Typically, an 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[92].
Also, there is a debate on '**backdoors**'[93], 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 denied the existence of backdoors[94]. Also, Microsoft has initiated the *Government Security Program GSP* where governments get insight into 90% of the source code.

The *Crypto AG* from Switzerland was a leading provider of encryption technology for decades. 148 countries ordered encryption technology. However, CIA and the German Intelligence BND had secretly bought the Crypto AG and by this access to the encrypted communication[95]. Also, for the Switzerland *Omnisec AG* which was dissolved in 2017 links to the CIA were discussed[96].

- **Infected storage media and digital devices** such as routers

[90] Siegel 2018a, p.20, Poddebniak et al. 2018
[91] A port scanner is a software application that checks a server or host for open ports, i.e., which services a system offers.
[92] Kurz 2013, p.31
[93] 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
[94] Die Welt 10 January 2007
[95] Skinner/Oesch 2020, Hermann 2020
[96] Skinner/Oesch 2020

**Infected data storage media** (such as floppy and hard discs, DVDs and now USB-Sticks) are more 'physical' ways to be infected. For example, the infections with *agent.btz* and with *Stuxnet* were driven by USB-sticks. Also, the IT environment can be used for intrusion, such as routers[97], wireless mouses and printers. Increasingly, network and *multi-function printers (MFPs)* are attack targets, which may allow data capture or reprint of documents[98]. For example, routers were attacked e.g., during the *Mirai* attack in late 2016.

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.

After reports about a malware called *BadBios* that was suspected to exchange information via the air in late 2013[99], 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[100]. 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[101].

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[102] can be an entry for an attacker.

- **Infected software** for download such as **Apps** and **updates**.

A problem is 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 2015 via an infected *software development kit (SDK)* for App programming. More than 250 infected Apps were removed from App stores[103].

- **Hacking** of passwords which is increasingly done automatically (**brute force**)

- Physical measures such as **interdiction** and **theft** of computers and smartphones

[97] Handelsblatt 2014 b, p.23
[98] Dörfler 2015, p. P4
[99] Betschon 2013b, p.34
[100] Winker 2014a, p.3
[101] Hanspach/Goertz 2013, p.758 ff.
[102] Via manipulated video files, Schmundt 2014, p.128
[103] T-online 2015

Another method is **interdiction**, i.e., replacing shipped CD-ROMs and other physical media and replacing them by infected media.
The *British Ministry of Defense* reported the unexplainable loss of 759 laptops and computers and 32 computers were definitely stolen within 18 months. Also, from May 2015 to October 2016, 328 CDs, DVDs and USB-sticks were lost[104].

- **Falsified microchips**

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. 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[105]. The global supply chain of such products is also a potential source of vulnerabilities[106]: 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[107]. 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)** [108].

- **Firmware infections**

The *LoJack* anti-theft software from the company *Absolute Software* which implements a UEFI/BIOS firmware module to prevent deletion appeared in trojanized versions since at least early 2017. The malicious versions are now known as *LoJax* which is like *LoJack* very deeply embedded into the computer system and also persistent[109].

- **Modified motherboards**

The company *Super Micro* is a provider of server motherboards and during an evaluation of the software company *Elemental Technologies* by *Amazon Web Services (AWS),* a tiny microchip was found, a little bit larger than a grain of rice that was not part of the original design[110]. This was a major issue, because *Elemental Technology*, which is a development partner of CIA's *In-Q-Tel* since 2009, provided servers to the DoD data centers, the CIA's drone operations and to navy warships. Also, thousands of *Apple* servers were compromised.

---

[104] Zeit online 2016b
[105] 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
[106] USAF 2010a, p.5
[107] Fahrion 2012, p.1
[108] Betschon 2016, p.39
[109] ESET 2018
[110] Robertson/Riley 2018

Also, China produces 75% of the mobile phones and 90% of all PCs, as even US companies outsource this production step to China. According to the *Bloomberg* report, subcontractor companies in China may have been put under pressure by the hardware hacking unit of the Chinese army PLA to insert these additional chips which would allow total background control[111]. All actors including *Amazon* and *Super Micro* strongly denied this incident. *Bloomberg* however insisted on the accuracy of the report stating that they were in touch to 17 insiders, including national security officials, *Amazon* and *Apple* insiders. Concrete discussion within White House started in 2014 and Apple silently exchanged more than 7,000 servers (Apple denied this).

- **Fuzzing**

The fuzzing procedure systematically tests possible commands to the software or to the hardware, even without concrete evidence of any vulnerabilities. A significant number of weaknesses, documentation and design flaws was found in the first tests in 2017, in particular for the central processing unit CPUs (computer chips).
The CPU vulnerabilities *Meltdown* und *Spectre*, discovered in 2017 and published in 2018, are only a small part of the problem. The US avoids, as already mentioned, the use of Chinese chips in weapon technology, however, many falsified chips exist which –in contrast to the original chips- may contain more intentional or unintentional vulnerabilities.
**Superbugs** are those vulnerabilities that can affect major parts of the Internet and that can often no longer be completely closed due to the costs.
Known superbugs alongside *Meltdown* and *Spectre* are[112] the 2014 *Heartbleed Open SSL Gap*, which is still active, as well as *Shellshock* of 2014 in the Linux operating system, which is still active on hundreds of millions of devices. Also, the so-called *Krack error* found in October 2017 in the *WPA2 encryption standard* that is important for routers cannot be closed on all devices.

**Software Fuzzing:** With the grammar-based software fuzzing, commands suitable for the programming language are processed in order to detect possible errors or incorrect reactions. Since 2011, the software fuzzing researcher Holler has discovered around 4,000 vulnerabilities[113].

**Hardware Fuzzing:** While *Meltdown* und *Spectre* were discovered on the basis of theoretical considerations and self-hacking experiments by researchers from Graz/Austria, numerous other errors were discovered at the same time. [114]

[111] Robertson/Riley 2018
[112] Fuest 2018
[113] Asendorpf 2017
[114] Schmidt 2017, FAZ 2018a

The hardware fuzzer *Sandsifter* can test 100 million-byte combinations in one day[115].
In a first test, this tool found in three chips (*Intel Core, Advanced Micro Devices AMD Athlon, Via Nano*) numerous undocumented commands and numerous hardware bugs, especially a command "halt and catch fire", which forces the processor to stop its work. Researchers at the *University of Bochum* also showed that it is possible to subsequently infect CPUs from AMD with Trojans and infiltrate them via updates; a discovery is hardly possible even after fuzzing.

**Meltdown/Spectre**
The patch *Kaiser (Kernel Address Isolation)* which served later on as *Meltdown* patch was already developed in May 2017 on the basis of theoretical considerations by the same Graz research team, which later discovered *Meltdown* and *Spectre*. The researchers hacked themselves and could easily access server, cloud systems, passwords, photos etc.[116].

The discovery was initially kept secret in 2017 to give manufacturers the opportunity to close the gap, but experts noticed the speed and number of updates [117].
The *Meltdown* gap, which affects only *Intel* processors, allows e.g., the unprivileged readout of kernel memory, i.e., access to the deepest internal information, and breaking out of virtual machines. The **Page Table Isolation (PTI)** or the patch *Kaiser (Kernel Address Isolation)* improve separation of the individual sections and thus protect the information[118].

The *Spectre* gap affects processors of computers and smartphones from *Intel, Advanced Micro Devices (AMD)* and *ARM Holdings*. In the **speculative execution**, the processors make preliminary calculations in order to have them ready when needed, which significantly increases the computing speed. By a **side channel attack**, e.g., a malignant JavaScript in the browser, the access to the information is possible in the context of the speculative execution, but only in very narrow timeframes (**timing attack**). The protective measures include numerous individual changes that better isolate the processes and complicate the timed attacks on speculative execution[119].
More precisely, *Spectre* consists of two gaps, *Spectre-1* Common Vulnerability Exploit CVE-2017-5753 (bounds check bypass, spectre-v1) and *Spectre-2*, and CVE-2017-5715 (branch target injection, spectre-v2), respectively, which have to

[115] Schmidt 2017
[116] FAZ 2018, RP online 2018
[117] Weber 2018
[118] Weber 2018
[119] Weber 2018

be treated with separate countermeasures. *Spectre-2* also requires changes to the firmware.

The previously closed gaps for *Meltdown/Spectre* carry the risk of a reduced system performance[120].

US CERT reported in March 2018 new variants of *Meltdown* (is a bug that melts down enforced security borders in hardware) while *Spectre* is a flaw that can force a CPU to present its information. *SpectrePrime* and *MeltdownPrime* are not really new gaps, but some chips allow automated attacks using *Meltdown* and *Spectre*, for *Spectre* this was already successfully tested[121].
In 2018, further gaps were discovered with a separate **CVE (Common Vulnerability Enumerator)** number, and by August 2018 there were a total of ten gaps, including *Spectre Next Generation (Spectre NG)* which affect Intel. One of the gaps allows to advance from the virtual machine to the cloud, or to directly attack other virtual machines, known as *Spectre NG*[122].
*Speculative bypass* is a new variant where an attacker can read older memory values in a CPU stack or another location. The *Foreshadow gap (L1 Terminal Fault)* allows to extract data from the Intel Level 1 cache which coordinates calculation processes[123].
Hackers were able to get access to the logic analyzing system of *Intel* chips called *Visualization of Internet Signals Architecture (Visa)*[124], which allows in-depth analysis of the chip.
Further vulnerabilities were found in 2019/2020, such as the SWAPGSA-Attack vulnerability, but security patches were also provided.

- **Pre-encryption access** to servers

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[125].

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[126]. As a practical consequence, user of devices, software or IT security software have to consider the

[120] Leyden/Williams 2018
[121] Scherschel 2018
[122] CT2018
[123] Betschon 2018b, p.37
[124] Grüner 2019
[125] Schlüter/Laube 2010, p.8
[126] FAZ 2013a, p.1

possibility that the intelligence of the manufacturer/provider country *may* have and use access, that by intelligence cooperation[127] 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[128] 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[129]. In 2015, the NSA disclosed 91% of the detected vulnerabilities of that year[130].

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, German: 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[131]. The access of national intelligence agencies means that a foreign or international IT platform can be technically accessed by foreign agencies[132].
In line with respective national law, e.g., the *Communications Assistance for Law Enforcement Act (CALEA)* which came into effect with the opening of the internet for the public in 1994 and the *Foreign Intelligence Surveillance Act (FISA)* in US, providers may give technical access to data or systems. The *US Patriot Act* contains further provisions for internet providers.
**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 may be exploited by third parties.

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,

[127] 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.
[128] 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.
[129] Daniel cited in Abendzeitung 2014
[130] Perloth/Sanger 2017
[131] 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.
[132] Scheidges 2010, p.12-13

hardware, SCADA applications etc.[133] 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 to reduce risk of discovery and attribution, to prolong the duration of successful attack and to expand the attack volume[134].

- **Misconfigured internet servers (BGP hijacking)**

As shown in Section 2.2.2 above, **Autonomous Systems (AS)** play a key role as these are the central servers of **Internet Service Providers (ISPs)** and each AS controls a set of IP addresses assigned in blocks of consecutive numbers. Each router checks the destination IP address in a transferred data packet and forwards it to the closest AS based on forwarding tables which show the best (next) AS server for a given data packet. These forwarding tables are built by the AS administrators with the **Border Gateway Protocol (BGP)** and show whether their server may be an appropriate destination or transit node.

If an AS announces through its BGP that it owns an IP block that is in reality owned by another AS, a portion of the data will be routed to and through the wrong AS. This may happen by error or maliciously which is then called **BGP hijack**[135]. The re-routing allows undetected copying of the data or even their elimination from traffic. The redirection and copying may cause only minimal and probably undetected delays in data connections.

China Telecom has ten internet **Points of Presence (PoPs)**, i.e., major connection points where a long-distance telecommunications carrier connects to a local network, across the internet backbone of North America, thereof eight in the US and two in Canada[136], and also further servers in Europe, such as in Frankfurt/Germany.

Several temporary events were noted which were by far too long and too large to be technical errors, including a takeover of 15% of the Internet traffic for 18 minutes by China Telecom on 08 Apr 2010 and further redirections of data traffic via China for traffic from Canada to Korea and US to Italy in 2016, Scandinavia to Japan and Italy to Thailand in 2017 as classic cases of **man-in-the-middle (MITM)** attacks[137].

[133] 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
[134] 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
[135] Demchak/Shavitt 2018
[136] Demchak/Shavitt 2018
[137] Demchak/Shavitt 2018

However, a planned redirection between national servers would be a possibility to disconnect the national internet from the global internet for defensive purposes, Russia planned a test in 2019[138].

### 2.2.3.3 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. Typical aims are:

- Malware installation for all kinds of **cyber espionage** (military, politics, industry, finance sector, researchers, international organizations etc.). Sometimes, this is combined with the use of **cyber weapons** such as logic bombs and wiper malware
- creation of **botnets**, i.e., groups of infected and controlled machines which are misused to send automated and senseless requests a target computer or system which then collapses (distributed denial of service attacks, short **DDoS attacks**). This can be done for political reasons, but also to blackmail the victim as part of cybercrime activities
- Installation of crimeware such as **ransomware** which encrypts the device and the victim is asked for money to get decryption code and banking trojans to gain access to online banking accounts.

In general, three types of **malwares** 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). **Cyber weapons** can be defined as software tools that can attack, intrude, doing espionage and manipulate computers. The term ‚cyberweapon' does not suggest that this is a military tool, as the technical principles are essentially the same as for software used for cybercrimes.

### 2.2.3.4 Cyber espionage tools

Sophisticated espionage malware is increasingly used and the conventional differentiation between viruses, worms and Trojans is becoming less relevant.
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

[138] Ma 2019

passwords[139] and **rootkits**, which are tools that allow logins and manipulations by the attacker without knowledge of the legitimate user.
To avoid detection, the malware conducts **self-encryption steps** 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.

### 2.2.3.5 Offensive Cyber Weapons

**Overview**

| What? | Used for… |
|---|---|
| Misleading signals | GPS Spoofing: Misleading of drones, ships etc. |
| | Dummies for misdirection of autonomous systems, new form of camouflage painting with large low-contrast pixels |
| | >20 kHz-commands: Ultrasound commands for remote manipulation of home assistant systems |
| Botnets | Flooding with inquiries and data can paralyze computers or networks |
| Logic bombs | Malicious programs, which become active only after a certain time or specific action |
| Text bombs | Difficult-to-interpret symbols overloading the chip and causing a crash |
| Wiper Malware | Deletion programs that delete files from the infected computer |
| Bricking | Programs that overwrite important control files with zeros on smart devices, rendering the device unusable |
| Ransomware | Lock screens for which ransom money has to be paid to get an unlock code: increasing use of destructive ransomware, i.e., the screen cannot be unlocked anymore |
| Fuzzing | Random commands to chips, which cause via design gaps a data access/release or even turn off the chips permanently (halt and catch fire) => digital ‘rescue shot’ is technically possible, potential danger of 'shutdown' by opponents in combat |

Offensive Cyber Weapons with destructive potential are:

- **Spoofing**: misleading of *Global Positioning System (GPS)* controlled systems by sending a false GPS signal which overrides the right signal, e.g., against drones or ships
- **Home assistants** have been vulnerable to commands in the inaudible 20 kilohertz range, decoys such as stickers or images lend themselves to the

[139] Stark 2009, Schmitt 2009, p.83

confusion of autonomous vehicles. Small tapes on the street were sufficient to drive the autopilot of a *Tesla* vehicle on the opposite lane[140]. Suitable dummies would certainly be able to mislead even autonomous combat drones to be able to turn them off in peace. Meanwhile, there are pixel-style camouflage paintings on modern Chinese military vehicles, but also on Russian helicopters.[141]

- **Distributed Denial of Service (DDoS)-Attacks** with **botnets**, i.e., manipulated computers, smartphones and other smart devices to flood a target computer or network with senseless requests.
- **Logic bombs**: malware that is dormant until a pre-defined timepoint is reached, which allows simultaneous attacks on a large number of targets
- **Text bombs:** sending messages or symbols which are difficult-to-interpret and lead to computer crashes. An example is the *Black Dot-bug* where Black Dot within brackets leads to crash of the iOS11 news app. A similar bug was already observed for *Android*[142]. A special message can cause a crash of the *Play Station4* system[143]. Another technical option are **zip-bombs** with extremely high data compression. Decompression could lead to extreme data volumes up to terabytes.
- **Wiper Malware**: destroys data by deletion, can damage the target system if essential data and functions are affected
- **Bricking**: attacks smart devices, gives instructions to alter settings and or overwrites the firmware which leads to factual destruction of the device
- **Ransomware**: malware that encrypts files. Victims are typically asked to pay ransom for decryption, but in early 2017, this was used in Pakistan in an attack for encryption only, i.e., to make the computer useless
- **Combined weapons**: in smart grid attacks, combinations of beachheads, manipulation software and wipers were used by *Black Energy* and *Industroyer/CrashOverride*
- **Fuzzing:** Perhaps the strongest cyber weapon is fuzzing, the sending of random codes to chips, which has far-reaching military consequences: the US stopped the use of Chinese chips in the weapons systems around 2007 in fear to be shut down during combat. Earlier, it was already shown that many chips are susceptible to interference by fuzzing. The chip makers are trying to fill in the gaps, but new ones are constantly being discovered. Thus, chips should be tested intensively in the existing military technology so that the lights do not suddenly go out when they come too close to the enemy. One of these random commands has the name "*halt and catch fire*" which irreparably shuts off the computer chip. Although this command could only

[140] FAS 2019, p.21
[141] Marquina 2019
[142] Becker 2018
[143] Welch 2018

be executed on certain chips and details were understandably kept secret, it shows that a **'digital rescue shot'** is at least technically possible.[144]

The Linux kernel of a computer can be crashed if a special buffer for sending data packets (*TCP function Selective Acknowledgment*) is overloaded, this attack is known as **Ping of Death** due to the ability to crash the target computer over the network, but the computer is not permanently damaged as in fuzzing attacks.[145]

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[146].

### 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 or devices[147]. The most important tool for a DDoS-attack is a **botnet**.

Computers can be controlled via a distributed software to cooperate with each other to conduct an action that requires large computing capacities[148] (**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[149].

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

---

[144] It should be noted, however, that in Fuzzing research already earlier commands were found that disturbed that affected the chip functions, which was initially more seen as Marquita an annoying test obstacle.
[145] Böck 2019
[146] Schmundt 2015, p.120-121, Langer 2014b, p.1
[147] 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.
[148] 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.
[149] 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.

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[150]
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[151].

DDoS attacks are meanwhile in 2017 frequent events, mega-attacks topping 100 Gigabit per second (Gbps) occur every quarter, but half of all attacks are between 250 Mbps and 1.25 Gbps in size. [152]
On the afternoon of 28 Feb 2018, the platform *Github* was attacked with a DDoS attack with a maximum of 1.35 terabit per second, using the *Memcached* tool to multiply data[153]. *GitHub* redirected the data traffic to *Akamai*; a few days later another provider was attacked using the same method and 1.7 terabits per second[154].

**Other really used methods are:**

- **Website Defacement**, where the look of a website is altered for propaganda reasons. A recent example are dozens of website defacements by the Islamic State supporters *System DZ team*.
- 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[155]. However, it can be expected that botnets will be used in future as core tool for large-scale attacks.

[150] 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.
[151] WhiteWolfSecurity 2007
[152] Akamai 2017
[153] Beiersmann 2018b
[154] Beiersmann 2018c
[155] Gaycken 2009

### 2.2.5 Insider Threats

Meanwhile, **insider threats** are rare, but by far the most dangerous method to damage an actor:

The most important incidents are:

- *WikiLeaks* disclosure of confidential data from the secured *Secret Internet Protocol Router Network SIPRNET* from 28 Nov 2010 by Bradley/Chelsea Manning.
- In 2012, an IT administrator within the secret service of Switzerland, the *Nachrichtendienst des Bundes NDB*, started an unauthorized data collection of 500 Gigabyte data volume from the secure internal network SI-LAN 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[156].
- Snowden leaks: 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[157] 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[158].
- *Harold T. Martin/Shadow Brokers leak*: details are presented in Section 5. An unauthorized data collection comprised cyber weapons from the NSA and other files which were leaked since 2016
- *Vault 7* leak: as shown in Section 5, more than 8600 CIA documents were presumably leaked by former contractors to the *Wikileaks* platform in 2017
- *Michailow incident*: a shown in Section 6.2.3, several persons related to a Russian intelligence officer named *Michailow* were detained, some cyber operations and also hundred IP addresses of the Ministry of Defense were disclosed.

The 2010 disclosure showed that too many people also of low ranks had access to SIPRNET[159], as discussed in the debates after the incident[160].

---

[156] Gujer 2012a, p.30, Gujer 2012b, p.24, Häfliger 2012a, p.29, Gyr 2016, 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

[157] Tomik 2013b, p.2.

[158] 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.

[159] About 2.5 million persons had basic access and 280.000 persons access to higher classified documents; Schneider 2011, p.9

[160] Schaaf 2010, p.9

In fact, 1.5 million people in US have a cyber-relevant security clearance level, thereof 480,000 from private companies[161]. 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[162]. On the other hand, it was argued that the cooperation with private firms is already long-standing[163] and would be necessary to utilize expert knowledge in the rapidly growing cyber sector.
The *US Department of Defense DoD* noted that DoD's own network would still consist of thousands of networks across the globe.[164]

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[165]. As a first step, the number of people with SIPRNET access was reduced[166]. Also, the regular review of access rights is necessary. Finally, no cyber defense will help if the humans before the screen are not sufficiently supervised.

### 2.2.6 Information warfare

The concept of information war is well established, e.g., in psychological warfare, targeted information or propaganda was released to adversaries to influence their behavior.
The modern information warfare is a bit different, as this is the *combined manipulation of digital technologies and information* to influence adversaries.

A new attack variant 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. Also, it is possible to create large amounts of fake tweets and fake human communication (**social bots, internet of thingies**)[167].

[161] Gartmann/Jahn 2013, p.24
[162] Huber 2013, p.18-19
[163] BAH cracked German submarine codes in WWII, Gartmann/Jahn 2013, p.24. Other security firms are e.g., Xe and USIS.
[164] DoD 2015, p.7
[165] Sattar et al. 2010, p.3
[166] Schneider 2011, p.9
[167] 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[168].

Fake communication and fake traffic are tools that can be used for influencing political adversaries, but is meanwhile also widespread in marketing, e.g., **fake followers** on *Twitter*, **fake likes** on *Facebook*, manipulated comments to products and services etc. etc. A recent example from 2017 is the *Star Wars* botnet (as terms from Star Wars are used in the fake communications) with 350.000 fake *Twitt*er user accounts, probably controlled by a single user[169].

Social media are also used to initiate contact via **fake profiles**. Suspected Chinese agents are offering money via *LinkedIn* for information against money and, if successful, subsequent invitations to congresses in China. This procedure was observed in Switzerland, Germany, but also in other countries[170].

The NATO and the EU are concerned that Russia could influence political process in European countries by fake communication. In particular, a group of so-called **cyber trolls** located in St. Petersburg was suspected to influence Western discussion. Since 2014, in Riga the *NATO Strategic Communication Center of Excellence*, shortly known as *StratCom*, analyses Russian activities and collects evidence for targeted release of fake news and cyber trolls[171].
The EU has established a task force which should detect fake news, to correct them and also should support a positive perception of the EU in Eastern States[172].

Information can be used as political weapon. In the past, this was called (referring to Russian term) **Kompromat**, which included real and/or fabricated facts about political adversaries to weaken them. AI is enabling increasingly realistic photo, audio, and video fabrications, or "**deep fakes**"[173]

There was a discussion whether fake news influenced the outcome of the presidential elections in 2016 in the US. Researchers from the Universities of Stanford and New York conducted a detailed analysis of fake news during US elections 2016. The impact of fake news -which were often not believed to be true by the readers- was limited. Most voters still prefer television as primary information source while internet is only preferred by a small proportion of

[168] Providers of such services are e.g., Narrative Science and Automated Insights, Dörner/Renner 2014, p.18-19
[169] Wolfangel 2017, p.27-29
[170] Häuptli 2018
[171] Wüllenkemper 2017, p.15
[172] Stabenow 2017, p.3
[173] Hoadley/Sayler 2019, p.11-12

voters[174]. Overall, 14 percent of Americans called social media their most important information source. The average American saw and remembered 0.92 pro-Trump fake stories and 0.23 pro-Clinton fake stories[175].

In summer 2017, a study about **computational propaganda** was published by the University of Oxford. A team of 12 researchers evaluated the situation in 9 countries[176]. The authors define computational propaganda *„as the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks"*. Currently, *Facebook* and *Twitter* are the main platforms for those activities. During the US election of 2016, the number of bots supporting Trump was three times higher than pro-Clinton bots, which is in line with the above-described fake news study.

In particular, *Twitter* is increasingly populated by social bots, which together with the finding in Section 4 below, that tweets are also a new form of covert communication of control servers with hacked computers, indicates that *Twitter* is now a main platform of bot communication in general.

Another concern is whether the above-described methods may also be misused to undermine electronic voting.
The only officially confirmed manipulation of voting so far was the *„Second referendum petition"* that asked after the *Brexit* vote for a repeat of the referendum in June 2016[177]. The *UK Petition committee* officially removed 77,000 fake signatures from the petition on 27 Jun 2016. However, the number of fake signatures was much larger at the end, as e.g., from Vatican State who has ca. 1,000 inhabitants 42,000 signatories were reported. Later on, Hackers from *4chan* claimed responsibility and said this was a prank (practical joke).

The hacks during US election campaign on voting systems and the *DNC hack* are discussed later in Section 5 in detail.

## *2.3 Electronic Warfare*

### 2.3.1 Introduction

A military topic related to cyberwar is the **electronic warfare (EW)** which is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. During Cold War, electronic warfare was an important military activity; a typical attack method was jamming

[174] NZZ 2017a, p.32
[175] Hunt/Gentzkow 2017, p.1
[176] Woolley/Howard 2017
[177] Heighton 2016

(disturbance) of communication frequencies and radar signals. After cold war, the focus shifted to network-centric and cyber warfare and drove attention away from traditional EW.
Meanwhile, the development of directed energy (laser and high-powered microwave) weapons has made substantial progress. In particular, the US and Chinese Navy have advanced prototypes of military laser weapons and first reports of real-world attacks exist. In the United States, electronic warfare and cyber warfare are now integrated in the concept of **cyber electromagnetic activities (CEMA)**. Moreover, satellites and their communication lines are increasingly important, but they are vulnerable for CEMA. The concept of space resilience was developed as a technical backbone of space defense.

### 2.3.2 Electronic Warfare Operations

In the United States, Electronic warfare (EW) is defined as *"any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy"*[178]. Electronic warfare consists of the three divisions electronic attack, electronic protection, and electronic warfare support[179].

**Signals intelligence (SigInt)** is intelligence information derived from signals and includes communication intelligence (COMINT), electronic intelligence (ELINT) and foreign instrumentation signals intelligence (FSINT). Signals intelligence systems primarily collect spectrum emissions passively, i.e., they do not emit their own signal. The SigInt is covered by the *National Security Agency (NSA)*. The difference between SigInt and EW support is that the EW support is tactical, i.e., only limited to the needs for a certain situation at a certain timepoint, but EW support and signals intelligence missions use the same resources[180]. Signals intelligence above the tactical level is under the operational control of the NSA.

The **Spectrum Operations** include the

- **signature management** where weapons systems reduce their electromagnetic signature to reduce the probability of detection, interception and destruction;
- **Navigation Warfare (NAVWAR)** as *"deliberate offensive and defensive actions to assure friendly use and prevent adversary use of positioning, navigation, and timing information through coordinated employment of space, cyberspace, and electronic warfare capabilities. NAVWAR is further enabled by supporting activities such as* ***Intelligence, Surveillance, and***

[178] Field Manual 3-36, Section 1
[179] Field Manual 3-36, Section 1-17
[180] Field Manual 3-36, Section 1-17

***Reconnaissance (ISR)*** *and* ***electromagnetic spectrum (EMS) management"***[181].

- Also, Command and Control (C2) systems are supported.

Jamming of communication signals was already done to a limited extent in 1904 in the Russia-Japanese war and in World War 1. In World War 2, radar systems and radar jamming emerged as new phenomenon. Further advances in tactics and technology occurred during the Vietnam War in air tactics[182].
During Operation *Enduring Freedom* in Afghanistan and Operation *Iraqi Freedom* in Iraq, the U.S. Army used new electronic attack (EA) capabilities to jam radio-activated triggers and defend friendly forces against radio-controlled improvised explosive devices [183].

After the end of Cold War, the dominance of the US enabled the uninterrupted use of the *Global Positioning System (GPS)* with unhindered communications. As a result, concepts such as radio discipline, electromagnetic signature control, and frequency hopping became less important[184]. Also, the cyber warfare emerged and drove attention away from traditional EW. But meanwhile, Russia and China have significantly upgraded their EW capabilities. In Eastern Ukraine, Russian-backed forces used sophisticated jamming and interception tactics to undermine communications and surveillance drones[185]. The development of directed energy weapons and the expansion of EW capacities to outer space by satellites are further reasons for the rapid re-emergence of electronic warfare.

### 2.3.3 Cyber Electromagnetic Activities (CEMA)

In 2014, the United States integrated cyber warfare and electronic warfare into the new concept of **cyber electromagnetic activities (CEMA)**. The *US Army Field Manual 3-38* defines: *"Cyber electromagnetic activities are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system"*[186].

While cyber capabilities area used to achieve objectives in and through cyberspace, electromagnetic and directed energy are used to control the electromagnetic spectrum or to attack the enemy[187]. Obviously, electromagnetism plays an important

[181] DoD cited by Hoehn/Sayler/Gallagher 2021
[182] von Spreckelsen 2018, p.42
[183] APT 3-12.3 2019, Section 1-3
[184] von Spreckelsen 2018, p.42
[185] von Spreckelsen 2018, p.42
[186] Field Manual 3-38, Section 1-1
[187] Field Manual 3-36, Table E-1

role for the cyberspace as well. There is the power supply by electric energy, while bits (0 and 1) are certain magnetic conditions on storage media. The electronic warfare targets the electromagnetism, i.e., the physical component of the cyberspace.

In summary, CEMA are implemented via the integration and synchronization of cyberspace operations, electronic warfare (EW), and the active management of the electromagnetic spectrum, the **spectrum management operations (SMO)** [188].

## *2.4 Emission Security EMSEC*

Computers and other digital devices work with electromagnetism and emit electromagnetic waves to their environment. This means that computers can be interpreted as senders and then, receivers can collect these signals. A receiver that is close enough to a computer can collect the radiofrequency signals and display what is currently shown on the computer screen (texts, pictures etc.) even if there are some several rooms and standard walls between the sender and receiver room.

For this reason, computers and devices that work with classified data should meet security standards that avoid inadvertent radiation, these criteria are internationally known as TEMPEST criteria (Tempest is a code word, not an acronym). In Germany, the *Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik BSI*) is the *National Tempest Authority (NTA)*[189].

For buildings where classified data are processed, e.g., computing centers in ministries, *Zoning Models of Emission Security* are developed which show the distance needed to detection of computer emissions. According to the BSI standards, a particularly high-risk situation exists if a controlled area around the installation site of a CI processing device does not include at least a sphere radius of 8 m[190].
If a zoning model cannot be conducted, e.g., because an authority is located centrally within a city, then specially protected devices have to be used for confidential data. Commercially available devices are typically not protected which allows **remote snooping**, e.g., from electronic car keys or banking automats.

As a real-world example, the Snowden leaks revealed that the smartphone of the German Chancellor Angela Merkel would have been intercepted. In 2013, this sparked speculations that certain constructions on top of the British and US embassy buildings in Berlin which are located closely to the Germany Parliament building

[188] Field Manual 3-38, Introduction
[189] BSI 2022
[190] BSI 2022

*Reichstag* (which has a glass dome) and the Chancellery would be interception devices[191]. UK and US did not confirm or comment, but removed the constructions.

[191] Campbell et al. 2013, SZ online 2013b

# 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 complexity*.

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[192]. A three kilotons explosion resulted which equaled 20% of the nuclear bomb of Hiroshima[193]. 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[194].

### 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[195]. Following the accidental bombing of the Chinese embassy in Belgrade, Chinese hackers attacked US government websites such as the website of the White House[196].

---

[192] Kloiber/Welchering 2011, p. T6
[193] Falliere 2010, Herwig 2010
[194] Vistica 1999
[195] Hegmann 2010
[196] 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“[197].

### 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[198].
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[199]. Also, the German Federal Government reported attacks on their computer systems at a similar time.
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[200].
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[201].

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 Google

[197] Fritz 2008 and also Nazario 2009, who gives in his paper an overview on politically motivated relevant DoS attacks.
[198] 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
[199] Fischermann/Hamann 2010
[200] Fritz 2008, p.55 and also Stokes 2005
[201] ArcSight 2008, p.2

and Adobe) and from high-tech companies of the security and defense sector in 2009[202]. *Operation Aurora* was meanwhile linked to the *Axiom/APT17 Group*, see Section 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[203][204]. 2011 further attacks were reported, that affected in particular Google's mail service *Gmai*l and the armament company *Lockheed Martin*[205].

### 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[206]. Estonia's networks were flooded by data from Russia, however probably not by the state, but by patriotic organizations[207][208]. Some computers had an increase from 1,000 requests *per day* to 2,000 requests *per second* and the attack went on for weeks[209].

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[210].

### 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.

---

[202] Markoff/Barbosa, 18 Feb 2010
[203] Alperovitch 2011, McAfee 2011. RAT stands for remote administration tool.
[204]FAZ 2011b, p.7
[205] 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
[206] Busse 2007
[207] Later on, the patriotic Youth Organization **Naschi** ('our people') said that they conducted the attack, Frankfurter Allgemeine Zeitung 11 Mar 2009
[208] Koenen/Hottelet 2007, p.2
[209] Wilson 2008, p.7ff.
[210] Luschka 2007, p.1-3

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[211].

### 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[212]. Some weeks before the 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. Meanwhile, the attack was suspected to come from *APT28/Fancy Bear/Sofacy*[213].

### 3.2.8 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[214]. 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[215]. Also, Iran was able to capture a US drone (type RQ-170) in 2011[216].
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 were 28 million dollars[217]. The vulnerability of drones depends also on the drone type with can have different control modes and grades of system autonomy[218].

### 3.2.9 North Korea

The *New York Times* reported that the NSA would have been able to intrude the 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[219].

---

[211] Herwig 2010, p.60
[212] refer to official statement of government of Georgia 2008
[213] Beuth 2017, p.14
[214] Ladurner/Pham 2010, p.12
[215] Los Angeles Times 13 October 2011
[216] 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.
[217] Knoke 2012
[218] Heider 2006, p.9
[219] FAZ 2015, p.5

During the so-called *Sony hack* (see chapter *Lazarus group* in *Section 5*), a network failure in North Korea took place which led to speculations that this was a **cyber retaliation** by the US for the pressure exposed on *Sony* and the movie *The Interview*. In 2014, US President Obama ordered to step up cyber and electronic strikes against the North Korean missile program. While there is a high failure rate in testing, the program nevertheless made progress. The current discussion assumes that the North Korean program may be more resilient than expected[220].

### 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[221]. Important examples, out of many, are the conflicts of India and Israel with actors from neighbor states[222].

After presumably hackers from Pakistan successfully hacked the India National Security Guard webpage, computers of the Islamabad, Multan and Karachi airports were attacked from Indian hackers with **retaliatory ransomware** on 02 Jan 2017, which impacted the airport traffic. In contrast to earlier attacks, no code against ransom was offered, instead the ransomware was used to damage the computers only. In contrast to other cyberwars, little efforts were done to hide the origin of the attack or to deny anything, instead this is seen as a kind of shooting over the virtual border[223].

In 2019, amongst other military activities (air defense systems, helicopters etc.), a number of Russian cyber soldiers was deployed to Venezuela. While this is no evidence that US had caused the large power failures in Venezuela in the weeks before (US said the power plant was damaged by a natural wildfire), it may have been a warning by Russia not to try anything in that direction[224].

### 3.2.11 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.

---

[220] Sanger/Broad 2017
[221] Saad/Bazan/Varin 2010
[222] Saad/Bazan/Varin 2010, Valeriano/Maness 2011, Even/Siman-Tov 2012, p.37
[223] Shekhar 2017
[224] Spetalnick 2019

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[225]. The activities were embedded in the overall military activities. While the IS was no state actor from a legal perspective (as not recognized by foreign countries as such[226]) it was 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[227]. 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[228]. 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[229].

To bypass the surveillance of emails, messenger services with encryption are increasingly used[230]. 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[231].
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.

In Jan 2016, the IS released a cyber war magazine with the title *Kybernetiq* with cyber war information[232]. 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[233]. The files were reported to be extracted from IS security department by an internal leakage.

[225] Paletta/Schwartz 2016, p.1-2
[226] Kurz 2016, p.14
[227] Anonhq 2014
[228] Chip.de 2015
[229] DW online 2016
[230] Langer 2015b, p.5
[231] Dörner/Nagel 2016, p.37
[232] Cyberwarzone 2016
[233] DW 2016

In April 2016, US officially confirmed to drop **cyber bombs** on the IS systems, but details of these tools remained confidential[234]. 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[235].
However, the 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[236].
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[237]. 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.[238] 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 [239].

The *US Department of Defense DoD* found that in the fight against IS the NSA and the Intelligence Community prioritized the gathering of information from the IS networks instead of fighting, i.e., a conflict of covert intelligence work and offensive military needs[240]. In the future, cyber soldiers will work together with the infantry directly at the front, a tactic that has already been tested in the fight against the IS[241].

In order to increase the cyber war capabilities of the United States, President Obama planned in 2016 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 was planned to be led by a civilian in future[242]. President Trump carried out the upgrading in 2017 by subordinating *Cybercom* directly to the DoD.[243]

[234] Strobel 2016, p.2
[235] Lange 2016, p.5
[236] Strobel 2016, p.2
[237] Strobel 2016, p.2, Rötzer 2016, p.2
[238] Rötzer 2016, p.2
[239] FOCUS Online 2016
[240] The Australian 2017
[241] Sokolov 2017
[242] Strobel 2016
[243] Sokolov 2017

A 20-year-old hacker from Kosovo provided in 2015 the addresses of 1,300 US military members and posted them online. In Sep 2016, he pleaded guilty and was sentenced to 20 years into prison[244].

Another activity are dozens of website defacements by the Islamic State supporters *System DZ team*. In the last three years since Oct 2014, the IP-addresses point to a location in Algiers. In June 2017, Ohio Governor John Kasich's website was defaced with a pro-ISIS message coming from the *System DZ team*[245].

Europol und US Police authorities were able to shut down IS platforms in a two-day action in April 2018. This affected the news agency *Amaq*, Radio *Al-Bayan* und the news pages *Halumu* and *Nashir*. However, *Nashir* continued to release *Amaq* news via the messenger service *Telegram*[246].

### 3.2.12 Cyber conflicts in Near East/Gulf Region 2019/2020

In early May 2019, *Hamas* combined its missile attacks from the Gaza Strip with cyber-attacks, after which Israel bombarded the building of the hacker unit, so this is the first time that hackers were killed during a conflict.[247]

In June 2019, it was reported that since at least 2012, US has put reconnaissance probes into control systems of Russian electric grid. In addition to *Wolf Creek*, attempts were made to infiltrate Nebraska Public Power District's *Cooper Nuclear Station* where they reached communication networks, but not the reactor system[248].

According to own statements, the United States attacked Iranian missile surveillance systems of the *Iranian Revolution Guards* on 18 June 2019 and a spy network.[249] This was also a response to an increase in Iranian cyber-attacks on US government agencies, the business and financial sectors, and oil and gas companies, with attacks typically done by spear-phishing.[250]
Another attack was launched by *US Cyber Command*. It targeted and reportedly wiped out a key database used by Iran's paramilitary forces *The Revolutionary Guards* in August 2019.[251]

The Israeli attack on the *Shahid Rajaee port* in May 2020 caused traffic jam of delivery trucks and delays in shipments as a retaliation for an incident from 24 April

[244] Rohde 2016
[245] Fox News 2017
[246] Tagesschau 27 Apr 2018
[247] Wired 2019
[248] Sanger/Perloth 2019
[249] Welt online 2019
[250] Abdollah 2019
[251] Technology Review 2019

2020, when a pump at a municipal water system in the Sharon region in Central Israel stopped working. This interruption was short, but perceived as significant disruption. The malware apparently came from the cyber units of the *Revolutionary Guards*[252].

### 3.2.13 Impact of Corona Crisis

The Corona crisis in 2020 led to two different kinds of cyber-attacks: cyber criminals misused the Corona reporting as attack opportunity while nation states were looking for know-how on *Coronavirus* research.

Over 50 unique malware pieces were distributed via *Covid-19* themed campaigns by cybercriminals[253].
Amongst other high-tech companies, the Chinese-backed hackers Li and Dong targeted COVID-19 vaccine firm *Moderna* leading to an indictment against Li and Dong[254].
Two Chinese citizens, intelligence officers of the Guangdong branch of the MSS; known as GSSD, intruded with the assistance of Guangdong another MSS officer high-tech firms by exploiting known vulnerabilities, but also using a web shell tool called *Chinese Chopper*. The activities ranged from laser technology, projects for the FBI up to the Covid-19 vaccine development by the US company *Moderna*. They also tried to change last modified dates of files; a technique known as **timestomping**[255].

Hackers tried to break into the World Health Organization in March 2020 by password stealing, which were suspected to come from the group known as *DarkHotel*, which has been conducting cyber-espionage operations since at least 2007[256].

The British *National Cyber Security Centre (NCSC)* reported that the Russian APT29 targeted various organizations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom[257]. APT29 conducted basic vulnerability scanning against specific external IP addresses, used the *WellMess* malware for shell commands and file handling and the *TWellMail* tool for commands or scripts with data transmission to a hardcoded Command and Control

[252] New York Times online 19 May 2020
[253] Whitmore et al. 2020
[254] Bing/Taylor 2020
[255] Hyslop et al. 2020
[256] Satter et a. 2020
[257] NCSC 2020

server[258]. Also, samples of the *SoreFang* malware were found which specifically targets *SangFor* devices, but this malware was also used by the APT *Dark Hotel*.

### 3.2.14 Attacks in the Ukraine

#### 3.2.14.1 Time before 2022

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[259].

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[260]. Three further companies were intruded, but had no outages. The intruders[261] were able to open multiple breakers remotely resulting in power outage, which happened in a small time-window in a coordinated manner[262]. **Telephone denial of service attacks (TDoS attacks)** were used to flood hotlines with phone calls to prevent customers from reporting the outage by telephone[263].
At the end of the attacks, the wiper malware *KillDisk* was used to damage the systems. The *Sandworm/Quedagh* group was suspected as attacker, but their malware *Black Energy* seemed not to have caused the power outages, refer to Section 7.

On 17 Dec 2016, the malware *Industroyer/CrashOverride* caused a blackout in Kiev which was attributed to a new APT called *Electrum* which was linked to the *Sandworm/Quedagh* group. This will be discussed in detail in Section 8 in the Smart Grid chapter.

The IT security firm *CrowdStrike* detected in late 2016 an attack on Ukrainian artillery guns of the *Howitzer* type.
The *APT 28/Fancy Bear/Sofacy* malware *X-Agent* was covertly implanted in an Android package which was developed by a Ukrainian officer named Sherstuk and had 9,000 users. This app supports D-30 122 mm *Howitzer* artillery weapons to process targeting data in a very short time. *CrowdStrike* assumed that this may have contributed to a loss of 80% of the *Howitzer* weapons compared to an average weapon loss 50% in the last two years, but this analysis remained disputed[264].

---

[258] NCSC 2020
[259] FAZ online 2014
[260] ICS-CERT 2016b
[261] Note that the use of *BlackEnergy* makes it plausible to assume that the *Sandworm/Quedagh* group may be responsible.
[262] ICS-CERT 2016b
[263] Zetter 2016
[264] CrowdStrike 2016

### 3.2.14.2 Attacks in 2022

The cyber-attacks that accompanied the Russian attack on Ukraine since 24 Feb 2022 started already months before.

- The Russian *APT29/Cozy Bear* attacked the NATO in 2021, likely to gain information relevant to Ukraine[265].
- Already in December 2021 and January 2022, the United States and United Kingdom sent cyber experts to Ukraine for preparation[266].
- On 14 January 2022, multiple ministry websites were defaced and the message meaning "Be afraid! Expect the worst!" were put there[267].
- On 15 January 2022, the *Microsoft Threat Intelligence Center (MSTIC)* disclosed that the destructive malware, *WhisperGate*, was used against organizations in Ukraine[268]. *Microsoft* established already in January 2022 a special communication channel to Ukrainian authorities[269].
- On 15 February 2022, GRU hackers tried to block internet pages of Ukraine ministry of defense, the army, the broadcast and of two large banks by denial-of-service attacks[270].
- On 23 February 2022, i.e., one day before attack, the *HermeticWiper* malware was being used against organizations in Ukraine to manipulate the master boot record, which results in subsequent boot failure. It looks like a ransomware, but also has a Wiper component to delete data in the background[271].
- In the early morning of 24 Feb 2022, modems of the KA-SAT satellite of the US telecommunication firm *ViaSat* were blocked to stop communication which affected Ukraine military and police units[272], but also thousands of German wind energy systems that used the satellite as well. The attack showed similarities to some activities of the *Sandworm* APT, the GRU unit 74455[273]. *Starlink* is a satellite-based network with low-orbit satellites. The users need a receiver and routing device to get the data which are transported with light. The low-orbit allows a reliable and fast data transfer. This makes senders and users independent from the physical internet. This was the reason

[265] Mäder 2022c
[266] Mäder 2022a
[267] Mäder 2022a
[268] CSA 2022
[269] Mäder 2022c
[270] Benrath/Finsterbusch/Heeg 2022, Mäder 2022e
[271] CSA 2022/Benrath/Finsterbusch/Heeg 2022
[272] Reuters exclusive 11 March 2022
[273] Mäder 2022b

why the owner Elon Musk provided it to the Ukraine shortly after the Russian attack[274].

- In 2016, the attack with the malware *Industroyer*-Attack allowed to give wrong IEC-104 protocol orders to a single infiltrated transmission substation which led to a power outage in Kiev. A similar attack with a slightly modified *Industroyer 2.0* malware in 2022 was ineffective[275]. The attack itself was able to switch the power off, but it could simply be switched on thereafter[276].
- Also, the computing center of the Ukraine government was attacked, but they evaded into a computing cloud[277].
- On 28 Feb and 01 Mar 2022, the IT infrastructure of Ukrainian media enterprises was attacked[278].
- In March 2022, a *deep fake* of Ukraine's president Zelensky was produced where he announced the surrender of the Ukraine in a manipulated video[279].
- After a call from the Ukrainian government in Feb 2022, a voluntary Ukrainian IT Army was formed which communicates via a *Telegram* channel. Initially, the channel had 300,000 followers. The most interesting profiles of volunteers were taken over by the Ukrainian security forces. The main activities of the IT army are defacements and DDoS-attacks on Russian websites[280].
- The IT-activists from *Anonymous* declared cyber war on Russia in March 2022. Their activities included DDoS attacks to block the website of the Russian defense ministry, leaks and doxing of relevant documents[281].
- The chief of the *US Cyber Command* and the NSA, General *Nakasone*, stated that the US would actively support the Ukraine. He did not go into detail, but this is likely "hunting forward", this is to detect coming potential attacks and threats and to take preventive measures[282].
- Until June 2022, the Ukrainian cyber security authority SSSCIP counted 731 relevant attacks[283].
- The Ukraine uses the face recognition search engine *Pim Eyes* to identify dead Russian soldiers and to inform their families[284].

[274] DW 2022
[275] Mäder 2022c, Muth 2022
[276] Muth 2022
[277] Kirschbaum 2022
[278] Mäder 2022c
[279] Mäder 2022e
[280] Mäder 2022d
[281] Herwig 2022
[282] Muth 2022
[283] Muth 2022
[284] Rogers/Oesch 2022

# 4. Attribution

## *4.1 Introduction*

Attribution is the allocation of a cyber-attack to a certain attacker or a group of attackers in a first step and to unveil the real-world identity of the attacker in a second step. While the methods of attacker allocation have made significant progress in the recent years, digital technologies often still do not provide definite evidence for the real-world identity of an attacker.
The situation is different if **attribution** is handled **as a cyber-physical** process, i.e., as combination of digital forensics with evidence from the physical world. Bits and bytes are not really virtual, but still bound to a physical infrastructure which opens different ways to detect adversaries. Gaps can also be filled by human intelligence.

## *4.2 Cyber-attack attribution*

Theoretically, a hacker can start a single attack from 'anywhere' and it may be impossible to track this back. On the other hand, the success rate of this approach is quite low.
Attackers who want to achieve significant success are typically attacking on a larger scale, i.e., as groups, with sophisticated malware and act sometimes for years. The longer and the more intense the attack is, the higher the risk for detection and attribution.
Data are incoming and leaving computers via so-called **ports**. A supervisor (IT administrator) can check the ports and the data traffic with commercially available tools. These tools also tell to which IP address the data are or were going.

Now, there are specialized search engines which automatically check what is behind an IP address. An example for such engines is *Robtex.com*. The providers of this service explain on their website that this tool is "*not only"* used by the *National Security Agency NSA*, which indicates that such services also serve as intelligence tools.
By entering the IP address in the search mask, *Robtex* shows data flows with other IP addresses as well as the way to the autonomous system AS or the Internet Service Provider ISP. It combines IP addresses and domains as well as any-existing subdomains. Also, it shows mail-servers related to the domain name.

This is important for following reasons:

- Attackers often maintain a certain attack structure, because like any construct an attack environment has both construction costs and exit costs. As a consequence, mail-addresses, domain names, servers and IP addresses are at least partially recycled from one attack to the next. These overlaps allow establishing relations between attacks.

- Attackers need computers as distribution hubs for their malware which results in the use of multiple domain names. Any known domain name may give the way back to the IP address and at the same time forward to the owner of the computer as shown below.

Note that AS computers are numbered along the IANA system and each AS computer is registered. AS computers and the registered persons/organizations can be easily retrieved with further free tools like *ultratools* and many other engines.
For domains and IP addresses, a so-called WHOIS registration exists, often simply available with free search engines. The registration details show company names, addresses, telephone numbers and email-contact addresses. By this, the step from the digital world to the physical world is done, from data to persons and organizations. By this, the researcher may be able to get insight into the 'digital ecosystem' of servers, addresses, registrations, domains etc. of the attacker entity.

Again, even faked registration information is in reality often **re-used** and allows building links between certain attacks. Surprisingly, entering the data into *Google* or any other search engine often leads to further findings which massively increase the chance to find information related to a person with a true real-world identity.

Further, larger organizations reserve **IP blocks**, e.g., packages of consecutive IP numbers[285]. If a suspected IP address is part of such a block, it can help much to enter all the other IP addresses as well into domain search engines etc.

**Real world example:** The security researcher *Krebs* was informed about an IP address belonging to the *Carbanak* group which captured 1 billion US-dollars by intrusion of banking systems[286]. His analysis of the IP address registration showed that the company name was also used for past cyber-attacks with two different types of malwares. The email-address led him to further IP addresses of the *Carbanak* group. The telephone number allowed Mr. Krebs to identify a person with potential relations to the *Carbanak* group, he was even able to have a communication with this person[287].

Note that sophisticated attackers have reacted to this already. One strategy is to exchange IP addresses and servers rapidly with the so-called **fast-flux technology**. Even the shutdown of certain servers can then not stop the attacker. However, a counterstrategy is the use of **sinkhole servers**.

---

[285] There are further technical options, such as giving virtual **IP addresses** within cloud computing and simulating false IP addresses (**IP spoofing**), but in published practical analyses of major cybercrime groups and of Advanced Persistent Threats APT this was not presented as a key issue.
[286] Kaspersky Lab 2015c
[287] KrebsonSecurity 2016

When somebody enters a domain like *www.example.com* into the browser, the computer needs to know the IP address of the target. So-called domain name servers (**DNS servers**) help the computer to find out the IP address.
Sinkhole servers give now intentionally wrong hints (e.g., by saying *www.example.com* is IP address 4.5.6.7 while the true address is 1.2.3.4) and redirect by this the data traffic away from the 'true' computer.
Note that the sinkhole server *can catch* the misdirected data and analyze them. As in larger attacks communication is ongoing for a while, *both* the attacker and the victim data can be collected, which helps to overcome the matter of changing IP addresses. Sinkholing was e.g., used by the Russian security firm *Kaspersky* against the presumably US-based *Equation Group*[288], which on the other hand infected *Kaspersky* with the sophisticated espionage malware *DuQu 2.0* [289].

Another strategy is the use of domains with **difficult-to-track registration**, which was 2017 reported by security firm *Kaspersky Labs* for suspected 'survivors' of the *Carbanak* group. Some countries allow the free sale of domains with their country ending, such as Gabon (.ga) by providers such as *Freenom*. However, any provider is at risk to be approached by national or foreign police or intelligence to give access to their data. There is an enormous variability of cyber security laws and law enforcement procedures worldwide, and there is a never-ending public debate and of court cases in the US going on, who under which circumstances is allowed to request information on users from private companies.

The *European Commission Service* released in Dec 2016 an overview on the current legal situation in EU member states. The survey showed an enormous range on the legal perspectives, e.g., whether a provider must or can cooperate, which extent of information is requested, which ways of law enforcement are used (up to remote access to providers) and whether cooperation between authorities is practiced or not[290].
However, the EU is moving towards a common legal framework with a common legal procedure, the *European Investigation Order EIO* and the European Union considers cyber security investigations as an urgent policy matter.

Smart devices have their own IP addresses. The analysis of incidents with smart devices in the Internet of Things (IoT) allows identifying the manufacturer and the involved products.

[288] Kaspersky Lab 2015a, p.34-35. Unexpectedly, early versions of Equation Group malware showed hard-coded IP addresses in their programs.
[289] Kaspersky Lab 2015b
[290] EU 2016

## *4.3 Hackers*

The cyber world can be differentiated into several actor groups:

- The state with civil authorities, military and intelligence organizations. Hackers may work for these organizations, in some states also in state-linked hacking groups.
- Cyber security firms which are involved in detection, attribution and defense, but also in the construction of cyber weapons and espionage tools. Hackers may also act as **penetration testers** to check security measures of a certain unit.
- In the scientific and commercial sector, hackers may work as **White Hat Hackers** to find and to close security gaps, but also as **Black Hat Hackers** for criminal purposes or for industry espionage.
- **Hacktivists** use their skills for political activities.

Please note that the above-mentioned spheres are not completely separated. In reality, a skilled hacker may be awarded during a hacking contest, then hired by the state and thereafter switching to the private security sector[291].

While the original image of hackers was more anarchic, meanwhile states are intensely and routinely searching for skilled hackers in order to hire them. **IT summer camps, hacking contests, hackathons** (hacking marathons where a certain problem has to be solved) are typical activities. The search for hackers is however only a small part of the search for skilled IT people in general: Skilled IT students may also be directly contacted by states and security firms. 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[292]. As a consequence, recruitment methods for cyber security-related positions are now easier[293].

The typical hacker is now a younger male person who –if involved into larger cyber-attacks- is doing this as a regular job. The dominance of younger males in hacking

[291] Rosenbach 2016, Kramer 2016

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

[293] 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 was available under intelligencecareers.gov/nsa. The NSA presented a new advertisement in 2017: *NSA Cyber Careers – For a Safer Digital World – intelligencecareers.gov. Protect the nation against cyberattacks using state of the art tools & tactics.* The NSA gets over 140,000 applications per year, Shane/Perloth/Sanger 2017. 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.

reflects the dominance of younger males in the IT sector in general. This is meanwhile seen as a problem as this indicates the under-utilization of females for IT. The British cyber intelligence *Government Communication Headquarter GCHQ* is now systematically searching for skilled females by initiating the *CyberFirst Girls Competition* for 13 to 15-year-old girls with tests in cryptology, logic and coding. End of Feb 2017, 600 teams started the competition. Currently, only 37% of the 12.000 employees in the British Intelligence Sector are females[294].

The typical hacker is not a lonesome rider, but interacts with friends and other hackers to exchange tools and experience, to get insights and news from the scene and so on. This is done with cover names in **hacker fora**, on the **black market** and in the **darknet**[295]. These three areas overlap with each other. Sometimes, **defacement websites** exist where hackers post screenshots of the hacked and damaged (defaced) websites as a kind of trophy.

This opens the way to attribution: cover names may appear in several attacks, also the used email addresses. If an individual hacker makes public claims, the risk of being captured is increased, such as the hacker with the cover name *Anna Sempai* who was involved in the *Mirai* botnet attacks and who is probably identified already[296].
Again, it can be helpful to enter the cover name of a hacker into a search engine to get further clues. Practice shows that hackers sometimes use multiple cover names, but not too many of them, because otherwise they lose their 'profile' in the insider scene[297].

**Real world example**[298]**:** In the *Winnti 2.0* attack, a bot communication in *Twitter* used as header the cover name of one of the hackers which also appeared in hacker fora. There, he had email communications with friends who had regular social media websites with all contact details. Also, a short abbreviation in the malware program resulted in further matches in search engines and led to a hacker team, from there to a mail address which then led to a young male person.

The darknet was presented in media in 2016 and 2017 as a major problem. The **TOR system** (derived from *The Onion Router*) is considered my media as the backbone of the darknet, because it allows splitting of data packages over multiple routes and by this a high level of anonymity in the net.

---

[294] Wittmann 2017
[295] For an overview refer to Chiesa 2015
[296] KrebsonSecurity 2017
[297] Research for user identification is permanently in progress, e.g., the *Bio-Catch* method where the Cursor movement pattern (speed direction, breaks) etc. allows identification of user of an online banking account, Gebauer/Wolfangel 2017.
[298] Kaspersky 2013, p.53ff.

However, TOR is increasingly under pressure. A recent paper by the *Naval Research Laboratory* that historically invented the TOR system shows that the takeover of an autonomous system or an IXP node computer (see above) by an adversary would provide enough information to capture a user within weeks or sometimes even within days[299]. While this was presented as statistical modeling, it highlights that the TOR system may not be forever a barrier against detection and attribution.
TOR is in particular vulnerable if the exit node server is under control by an adversary, also certain data may be extracted during the data transfer over the TOR network as theoretically everybody could set up a TOR server.

With respect to darknet[300], one should bear in mind that actors may also be undercover agents[301]. As meanwhile a lot of authorities are using undercover agents for multiple purposes, there is a growing risk of interference or inadvertent interaction between them, e.g., investigating each other instead of adversaries.

Estimates for the size of the **Darknet** in mid-2017 were 5,200 websites, of these 2,700 active and half of them with illegal content[302]. The darknet is the (mostly) anonymous part of the internet and is not to be mixed up with the **Deep Web,** which includes those websites, which are usually not caught and presented by search engines.

In July 2017, two of the largest darknet platforms for illicit drug and arms trafficking, *AlphaBay* and *Hansa*, were shut down in close collaboration between the FBI, the *Drug Enforcement Agency (DEA)* and the Dutch police with the support of *Europol*[303].

*Alphabay* was the largest platform with 200,000 users and 40,000 vendors, and $ 1 billion in sales since 2014. In July 2017, FBI and DEA's *Operation Bayonet* seized the servers and arrested *Alphabay's* central person, a Canadian living in Thailand.
The platform Hansa was secured with the help of the cybercrime center E3C on 20 June 2017, but continued to operate undercover for another month to catch users who switched from *Alphabay*[304].

In the Messenger service *Telegram* offers appeared of $1000 a day for employees of *Moneygram* or Western Union to work with hackers. In general, there is a shift

[299] Johnson et al. 2013
[300] A single darknet platform that was shut down by police in June 2017 had 20,000 users for activities like trade of drugs weapons, credit cards, falsified money, false identity cards, FAZ 2017c. Later in July, another criminal platform (misuse of children) called *Elysium* with 87,000 users could be stopped, Steinke 2017, p.6.
[301] Tellenbach 2017, p.31
[302] Steinke 2017, p.6
[303] Europol 2017
[304] Europol 2017

from darknet to encrypted messenger systems in 2018 with apps and platforms such as *Amir Hack* and *Dark Job*, but investigating authorities already started infiltration[305].

## *4.4 Cyber War Attribution*

The attribution in cyber war is from the theoretical and legal perspective the most important attribution problem as the question "who did it?" may result in retaliation or even war if a certain level of damage is exceeded.
However, the practical relevance of the matter is unclear as there is an **attribution paradox**.

The US and Chinese cyberwar concepts clearly indicate that a conventional strike must be executed simultaneously or very shortly after the cyber-attack if the military action should be successful. This means that the attribution of the cyber-attack will be possible within minutes, because the target state will at the same time exposed to hostile fire, i.e., the attacker will identify himself.

**Real world example:** On 06 September 2007, a suspected nuclear plant in Eastern Syria was destroyed by Israeli air attacks. Israel was technically able to simulate a free heaven to Syrian air defense systems and could thus conduct this attack without disturbance[306].

If a massive cyber-attack would be done without an accompanying conventional strike, the target state has time to restore the systems first and to start attribution in the meantime as well, which with aggressive use of intelligence methods may take less time than attackers expect.
On the other hand, this results in a kind of **reverse attribution**, i.e., from the physical to the digital world. In the era of espionage satellites, the preparation of a large military strike will not be undetected and is typically coming after massive political tensions, i.e., there are clear warning signs in the physical world for coming attacks in the digital world.

[305] FAZ 2018e
[306] Herwig 2010, p.60

# 5. Malware and Advanced Persistent Threats

Meanwhile, several sophisticated hacker units and malware families were discovered and reported which are presented in the following chapters.

## *5.1 Sophisticated malware*

Sophisticated malware 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.
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. Note that this process has a high risk for errors, in larger malware programs it happens that single time stamps were not changed and language settings were not clean enough.
Also, hackers create **digital fingerprints**; these are typical program codes or certain access patterns which allow characterizing a certain group of attackers.[307]
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.) [308]. Also, information can be hidden into small pictures, a method known as **steganography**. Sometimes, attacker servers communicate with victim computers via Twitter or email.

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. However, a growing use of **obfuscation software** to replace names and modification of brackets is observed, too[309]. However, this does not allow clarifying whether an attacker worked on behalf of another state or authority.

Many people consider intrusion as a static event: once the malware is installed, the attacker can lean back and the data flow is going on. In reality, **cyber-attack is a dynamic process**. The attacker may try to expand the access and control rights or push through to other computers of the intruded organization by **lateral movement**, i.e., from one system to the next. Updates have to be made and tailor-made modules are to be uploaded. Instructions have to be sent to the target computer.

[307] Mayer-Kuckuck/Koenen/Metzger 2012, p.20-21
[308] Mandiant 2013
[309] Welchering 2016, p.T4

Intruders have to pay attention that they are not discovered, e.g., by publication of an exploit they used. The extracted data have to be analyzed carefully to identify further needs or to realize when further attack is a waste of time and resources.
From this, it is difficult to mimic the attack of an APT even when the malware of the respective hacker group is available on the black market. The attacker needs to be aware that the cyber security companies do not present their full knowledge to the public, that the intelligence of a member state may also know more about the usage and of course the original hacker group knows their malware better than others and not only *what* it used, but *how* and *when*.

However, an attacker group could of course malware which is available on the black market, but even then, they may show **core characteristics and programs** in use.

Sophisticated hacker units can **check computers for pre-existing infections** (e.g., *Equation Group* and *Waterbug Group*) with their malware and if they detect infections of computers which were neither attacked nor infected earlier, they will be alerted. The hacker units may even be able to inspect the false flag attack and then the mimicking attacker has massive problems both in the digital and the physical world.

In addition to the above analyses, the **chronology** of malware development is important to detect which malware could be derived from precursors and thus be related to the same attackers. For all sophisticated malware groups, such a chronology exists. Note that e.g., the *Stuxnet* malware not only had a long version history, but also massive changes of its structure and targets (originally valves, later centrifuges). [310]

Finally, a cybercrime attack does not end with computer communication, but the money gained by the attacks has to be transferred and hidden as well. This **whitewashing of money** is typically done with multiple transfers between banking accounts to obfuscate the origin of the money. The **use of digital bitcoins** does not really solve the issue, as at the end this has to be exchanged into real money again. The transfer of large sums of money and rapid moves are alert signals.
People who utilize their bank account for transfers of money are the so-called **money mules**, i.e., in addition to hackers, further people are part of the cybercrime group. Experts identified the money transfer of cybercrimes as in important vulnerability of the attackers[311].

[310] McDonald et al. 2013, p.1-2
[311] Baches 2016, p.15

## *5.2 Advanced Persistent Threats (APTs)*

The leading hacker groups are also referred to as **Advanced Persistent Threat (APT)**. The classic definition defines APTs are longer-term attacking groups with defined **techniques, tactics and programs (TTPs)**.
Thus, 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.
Recent years, however, have shown that the definition of espionage and cyberwar is more precise: An APT is a project group within an intelligence unit that develops and applies its TTPs and selects targets along the operational goals of the intelligence unit.
Certainly, as hackers begin to develop, they first see how far they can come and what they can do with their successes, but APTs do not self-evolve, they are formed by putting together appropriate people and aligning their cyber activities to the operational goals.

An APT has its characteristic combination of access vectors, exploits/vulnerabilities, and toolkits which allow differentiation between groups[312]. A widely used term for this combination is TTPs. As each group has a typical set of attack targets, the logic of target selection is also called **victimology**.

The attack tactic varies: Leading techniques are **phishing emails** with infected attachments or links to infected websites. As outlined in the *APT28/Fancy Bear* analysis of the Security Firm *FireEye*, such emails can also be used as traces, such as: ”specific email addresses, certain patterns, specific name files, MD5 hashes, time stamps, custom functions and encryption algorithms”[313].

**Stolen security certificates** and the use of **zero-day exploits** are typical indicators for a sophisticated attacker group.

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.

[312] See also Jennifer 2014
[313] FireEye 2014, p.29

So far, no government or authority has ever officially confirmed a link to a hacker unit. The below groups are the most prominent units in the media, the total number of larger active hacking groups is estimated over hundred groups, the overview shows the best-known APTs.

**Leading APTs**

| Country | Attributions by leading cyber security organizations |
|---|---|
| Russia | APT28/FancyBears/Sofacy/Strontium/Sednit (GRU unit 26165) |
| | APT 29/Cozy Bears/Dukes (SVR) |
| | Waterbug/Turla/Ouroburos/Venomous Bear/Krypton Group (FSB) |
| | Sandworm/Quedagh (GRU unit 74455) |
| | Energetic Bear/Dragonfly (FSB unit 71330) |
| | Trisis/Triton/Temp Veles (Central Scientific Research Institute of Chemistry and Mechanics) |
| China (ca. 20 APTs) | APT 1/Comment Group (PLA) |
| | APT 10/Cloud Hopper (MSS) |
| USA | Equation Group (NSA) |
| | Longhorn/The Lamberts (CIA) |
| North Korea | Lazarus-Group and affiliations |
| Israel | Unit 8200 (IDF) |

All leading groups have multiple names, because analysts typically assign a working name and it appears later that the same group was addressed by different analysts. *Microsoft* uses chemical elements for naming such as *Strontium, Potassium, Barium* etc., other security firms have internal naming conventions, such as *Bear* = presumably Russian, *Panda* = presumably Chinese, *Kitten* = presumably Iran, *Spider* =presumably e-crime etc.; some companies number the APTs, sometimes, codes or terms in the malware trigger the naming, e.g., the name *Sauron* in the recently discovered APT *Project Sauron* (the all-seeing evil eye from *Lord of the Rings*), *Quedagh* or *Ouroburos*.

Most importantly, for the smart industry, Russia has three specialized APTs, namely *Triton* at the developmental level, *Dragonfly* for espionage and *Sandworm* for attacks (in Ukraine). It may be possible that all three APTs are only part of a comprehensive cyber production process. In China, the APT10 is currently regarded as the most successful Industry-focused APT. In North Korea, the so-called *Lazarus* Group is most debated.

From the US security-analyst perspective, Russia has made significant progress with establishing sophisticated units within the last decades. The APTs are under control of the intelligence services. Russia has four services as successors of the former Soviet Intelligence KGB[314]:

[314] Ackert 2018a, p.7

- FSO – Federal Protection Services which includes the Guard of the President in Kremlin
- FSB –Civil Interior Intelligence Service, but still conducting some foreign activities
- SVR - Civil Foreign Intelligence Service, also doing Intelligence Cooperation[315]
- GRU or GU - Military Intelligence Service. The GRU has 4 regional and 11 mission-specific directorates, the 6th directorate for Electronic/Signals Intelligence, the 12th directorate for information operations[316]

In 2018, the *Mueller Indictment* and the subsequent *US Department of Justice (DoJ)* indictment from 2020[317] showed that US was able to monitor and log computer activities of *APT28/Fancy Bears* members as part of the GRU Unit 26165[318]. The *Industrial Control System (ICS)*-focused group *Sandworm/Quedagh* is also attributed to the GRU as Unit 74455, the *Waterbug/Turla/Ouroburos/Venomous Bear/Krypton Group* to the civil intelligence FSB while the *APT29/Cozy Bears* is related the foreign civil intelligence SVR, but anyway Dutch cyber intelligence claimed to have identified the *Cozy Bears* members[319]. The *Dragonfly* group is identical to FSB unit 71330[320].
The Dutch have a *Joint SigInt Cyber Unit* of about 300 members which are coming from the *intelligence AIVD* and the *Military Intelligence and Security Service MIVD*, thereunder an offensive cyber unit of 80-100 people and a defense cyber unit as well. The unit was able to take control of a surveillance camera of a university building near the Red Square where *Cozy Bears/APT29* are physically located with an average team of 10 people[321].

Meanwhile, the Russian APTs related to the GRU could be assigned to their 5-digit field post numbers[322]. The GRU Unit 26165 was in cold war the 85th main special service center responsible for cryptography is now known as *APT28/Fancy Bear*. The GRU Unit 74455 known as *Main Center for Special Technologies* is the Sandworm group. The Unit 54777 known as the *72nd Special Service Center* is responsible for psychological operations, but is also doing cyber support.

For historical reasons the FSB still conducts foreign operations by a special department. Analysts believe that this is done to boost competition, but also to keep

[315] Ackert 2018a, p.7
[316] Bowen 2021
[317] DoJ 2020
[318] Mueller 2018
[319] Paganini 2018a
[320] Kaufmann 2022c
[321] Paganini 2018a
[322] Bowen 2021, Kaufmann 2022c

balance of power between services[323]. The ICS-industry systems-focused group *Energetic Bear/Dragonfly* is the FSB *unit 71330*[324]. A new group *Temp.Veles* was reported in 2018, but as this is a government research institute, is unclear whether this is really an independent APT or only serves as a malware provider for already known APTs.

The *Comment Crew/APT1* and the *Axiom/APT17* were discussed to be linked with China, while the *Lazarus Group* was linked to North Korea by the FBI with support of the cyber security firm *Mandiant* showing that the group used North Korean IP-addresses and a lot of common infrastructure, techniques, codes etc. during various attacks linked to the *Lazarus* group[325].
The *Equation Group* is attributed to the *US National Security Agency (NSA)* based on the leaks of the *Shadow Brokers* group from 2016 which were identical with an unauthorized data collection of NSA software by a contractor named Harold T. Martin[326]. And in 2017, the APT known as *Longhorn Group/The Lamberts* could be linked to the CIA based on the *Vault 7*-leaks. But please note that all respective governments denied or declined to comment.

In practice, the United States were hesitant for a long time to name attackers officially, because this intelligence know-how would have to be exposed to the public. This led to the so-called *Grizzly Steppe* report in 2016/2017 with respect to involvement of Russian actors in the US presidential elections which was criticized for its vague statements. Meanwhile, a decision was made to expose some intelligence knowledge allowing naming attackers precisely. This resulted in the *Mueller indictment* of 2018 and a subsequent DoJ indictment from 2020, which shows the findings from monitoring and logging of computers of Russian intelligence officers as members of *APT28/FancyBears* and of *Sandworm*[327], including the organizational setting (GRU Units 26165 and 74455), the names of the officers and detailed protocols, how, by whom and when the Democratic party was attacked, the stolen data transferred and leaked (spearphishing, *DNC hack, DCLeaks, Guccifer 2.0*).
After *Google* noted increased cyber activities by the Russian military intelligence GRU in a report named "*Peering into the aquarium*" in 2014, not only the monitoring and logging of computers of GRU officers was done, but also conventional intelligence measures were used by the Western intelligence. The activities were massively enhanced after 4 Russians identified as GRU members travelled to the headquarter of the OPCW in Switzerland to observe their investigations on chemical weapons. This included a consultancy of the former

[323] Ackert 2018a, p.7
[324] Kaufmann 2022c
[325] Shields 2018, p.56, 134 and 138
[326] Perloth/Shane 2017
[327] Mueller 2018

GRU member Skripal and other former agents, interception of telephone calls and contacts to the Russian Passport Office and Traffic Police. [328][329]
The combination of these sources allowed identifying the address of a GRU building and of 300 GRU members, because their cars were registered to the address of this building[330].

In the same manner, the *Lazarus* group was analyzed by the FBI in cooperation with the security firm *Mandiant* to identify a North-Korean officer *Park Jun Hyok* as a key member. The group used North-Korean IP-addresses and a lot of shared infrastructure, techniques, codes etc. during various attacks linked to the Lazarus group[331], thus confirming the findings of *Operation Blockbuster* with solid evidence.
But please note that all respective governments denied and declined to comment.

## *5.3 United States*

### 5.3.1 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.

Meanwhile, the existence of a separate *Equation Group* is doubted, as it may only be a working term for the NSA itself[332]. This assumption is supported by the fact

[328] Rüesch 2018, p.4-5
[329] Ackert 2018b, p.3
[330] Ackert 2018b, p.3
[331] Shields 2018, p.56, 134 and 138
[332] Perloth/Shane 2017

that the malware collected in the *Shadow Brokers* incident is treated in the *Harold T. Martin trial* 2017/2018 as original NSA software.

#### 5.3.1.1 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*[333]) 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[334].
Stuxnet is a **worm,** i.e., a program that is able to spread actively to other systems[335].
The infection was started via an infected USB-stick and Stuxnet exploits security gaps in Windows LNK-files to intrude systems[336]. 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[337].
The *Simatic S7*-system of Siemens is running under a Windows environment, also the WinCC software for parameter control and visualization[338]. *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*[339]. 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[340].
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[341]. It was assumed that uranium gas centrifuges needed for construction of nuclear bombs were damaged in Iran, as the number of centrifuges

[333] Shea 2003
[334] Welt online 2010b. Consequently, Siemens expands its cyber war research capacities, Werner 2010, p.7
[335] As Stuxnet has dozens of functions and tools, it sometimes also described as Trojan horse or virus, FAZ2010a.
[336] On 13 Oct 2010 Microsoft released 16 Updates to cover 49 security gaps, Handelsblatt 2010, p.27
[337] Rieger 2010, p.33, who invented the term ‚digitaler Erstschlag' (‚digital first strike').
[338] Krüger/Martin-Jung/Richter 2010, p.9
[339] Schultz 2010, p.2
[340] Kaspersky 2010
[341] Falliere 2010

declined in 2009 and the *International Atomic Energy Agency (IAEA)* reported downtime also in 2010[342], which was confirmed by Iran[343][344].
These issues, the use of several unknown security gaps (**zero-day-exploits**) and the estimated development costs of about 1 million US-Dollars[345] resulted in the theory of a new weapon constructed by secret services to damage the Iranian nuclear program[346].

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 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[347].

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[348]. 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[349]. The reports of the *New York 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) [350].

---

[342] FAZ2010c, p.6
[343] 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.
[344] 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.
[345] Schultz 2010, p.2
[346] Ladurner/Pham 2010, p.12
[347] McDonald et al. 2013, p.1-2
[348] Broad/Markoff/Sanger 2011, p.4
[349] Sanger 2012, p.3
[350] NZZ 2012, p.1, FAZ 2012b, p.7

Erroneously, *Stuxnet* infected the computer of an engineer and then spread over the internet to other countries[351]. 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[352]. 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[353].

*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[354].
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 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*[355]. 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 Bushehr and the debate of the new NATO strategy[356].

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[357]. *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[358]. It was speculated that *DuQu* may have been created to gain information from the target systems for creation of *Stuxnet*[359].
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'[360] in May 2012 named *Flame* that gives very detailed system

[351] Sanger 2012, p.6
[352]Handelsblatt 2010, p.27, Symantec 2010, p.5-7
[353] 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
[354] Rosenbach/Schmitz/Schmundt 2010, p.163; Rieger 2011, p.27
[355] Iran Daily 26 July 2010
[356] Knop/Schmidt 2010, p.20
[357] Goebbels 2011, p.8. The name came from the DQ-prefix used in the program files.
[358] Goebbels 2011, p.8
[359] Welchering 2012, p.T1
[360] *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

information about the infected systems and that again had some technical overlaps with Stuxnet[361]. *Washington Post* reported that *Flame* was already developed in 2007 and also part of the cyber activities against Iran[362]. The program part that allowed the distribution of *Flame* via USB-sticks was first used in *Flame* and then in *Stuxnet*[363].
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*[364].

#### 5.3.1.2 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 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 malware family.[365]

*Kaspersky's* antivirus service was activated by a massively malware-infected private computer in September 2014, with the computer owner turning out to be an NSA contractor[366]. Kaspersky detected the *Equation Group* malware on 11 Sep 2014, but only because the owner had other malware on the computer. A *7zip* archive that was reviewed by *Kaspersky Antivirus* contained *Equation Group* tools that the employee illegally stored on his home computer[367]. The discovery just happened accidentally. The computer owner had 121 other malware programs on his computer[368], including the *Backdoor Mokes/SmokeBot/Smoke loader*, which was known since 2011 in Russian underground forums, but their command-and-control servers were registered in 2014 by a Chinese group called *Zhou Lou*, so there may have been more actors in the computer of the target person[369].
However, people from Israel were already in the computer system of *Kaspersky* with the espionage software *DuQu 2.0* and were able to observe the activities[370].

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

files. Flame is an example, why the conventional differentiation between viruses, worms and Trojans becomes less relevant.
[361] Welchering 2012, p.T1, Graf 2012, p.8, Gostev 2012, p.1
[362] Graf 2012, p.9
[363] Nakashima/Miller/Tate 2012, p.1-4
[364] Focus 2012, Symantec 2012, Mertins 2012, p.10
[365] Kaspersky Lab 2015, p.3
[366] Kaspersky Lab 2017
[367] Kaspersky Lab 2017
[368] Kling 2017c, Weidemann 2017a
[369] Kaspersky Lab 2017
[370] Weidemann 2017a

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[371].

*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[372]. 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[373]. *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. [374]

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[375]. 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 Group* malware family and the *Stuxnet*-related malware family are the following[376]: 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, 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*[377]. 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

[371] Kaspersky Lab 2015, p.5, 8
[372] Kaspersky Lab 2015, p. 10. Already the EquationDrug malware was able to get full control over the operating system, see p.8
[373] Kaspersky Lab 2015, p. 10-12
[374] Kaspersky Lab 2015, p. 13
[375] Kaspersky Lab 2015, p. 15-16
[376] Kaspersky Lab 2015, p. 5
[377] Kaspersky Lab 2015b, p. 3

domain administrator account[378]. The programmers set a series of **false flags** to mislead researchers, these are strings used in other already known malware from other attackers[379]. Also, time stamps were manipulated.

*DuQu 2.0* is meanwhile attributed to Israel and the *Unit 8200*[380]. This program, which was more developed than *DuQu*, was also directed against US targets.
Based on the evidence collected with *Duqu 2.0*, the Israeli intelligence agency observed that Russian intelligence agents were using piggybacking of *Kaspersky* accesses to follow US targets, which is why they warned the NSA[381]. This process was then published by the *Wall Street Journal* in 2017[382], when *Kaspersky* launched its free antivirus version *Kaspersky Free*, which could result in an increased usage of Kaspersky. The Department of *Homeland Security DHS* banned the internal use of Kaspersky software. [383]

This has also been linked to the discovery of *Equation Group* 2014/2015; However, Kaspersky vigorously denied this and pointed out that the detection was only due to the fact that Kaspersky's anti-virus detected a massively malware-infected private computer in September 2014, so the antivirus only did its work and the computer owner turned out to be an NSA contractor[384].

*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[385].
Also, similar to *Equation group*, encrypted virtual file system containers and RC5 encryption is used[386]. *Regin* has multiple properties, such as monitoring traffic, stealing information and collecting data[387]. As in the malware described above, only a few selected high-level targets were attacked[388].

[378] Kaspersky Lab 2015b, p. 4
[379] Kaspersky Lab 2015b, p. 43
[380] Perloth/Shane 2017
[381] Perloth/Shane 2017, Beiersmann 2017e
[382] Lubold/Harris 2017
[383] Beiersmann 2017e
[384] Kaspersky Lab 2017, Beiersmann 2017e
[385] Symantec 2014a, p.3
[386] Symantec 2014a, p.3
[387] Symantec 2014a, p.11
[388] Martin-Jung 2014, p. 17

#### 5.3.1.3 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 a public file with material and offered a second file for 1 million Bitcoins (500 million Euros at that time) in an auction[389]. However, the auction was quickly taken offline, the last offer was 0.12 Bitcoins (60 Euro). [390] 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[391].

The analysis of the public file showed that it was software from 2013[392], 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[393]. *In-Q-Tel* was founded by the CIA as Venture Capital firm in 1999 for strategic investments in start-ups etc. The statement may be 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*[394]. 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[395].

On 31 Oct 2016, the *Shadow Brokers* released a list of servers compromised by the Equation Group with 352 IP-addresses including 32 edu-domains from various countries and seven further tools such as *Orangutan* (which was e.g., detected in Germany) and *Patchicillin*[396].
On 08 April 2017, the long and complex password to encrypted files from 2016 was released which made the previously leaked files accessible[397].

---

[389] Jones 2016
[390] Beuth 2016b, Spiegel online 2016
[391] Jones 2016
[392] Shane/Perloth/Sanger 2017
[393] Ragan 2016
[394] Steier 2016b, Spiegel online 2016, Solon 2016
[395] Steier 2016b
[396] Spiegel online 2016b. In a further message called *Black Friday/Cyber Monday sale* they released a screenshot with a tools file structure.
[397] Kramer 2017

On 14 April 2017, further tools were released including *DoublePulsar, EternalBlue* and *EternalRomance* became possible, which then were used presumably by other actors for preparation of three major cyber-attacks called *WannaCry/WanaDecryptor 2.0*, *Adylkuzz* and *Petya/Non-Petya/Petya2017* (refer later on to *Lazarus* Group in same Section).
In May 2017, the *Shadow Brokers* said that they have data about supervision of SWIFT servers by NSA and about nuclear programs[398].

In September 2017, the *Shadow Brokers* released an older NSA manual for attacks on Windows, *Unitedrake*[399]

In order to clarify possible connections to the *Shadow Brokers*, several NSA employees were subjected to a polygraph test, some were suspended, some had to pass their passport, but the connections to the *Shadow Brokers* could not be clarified.[400]
A special focus was on those people who had previously worked for the CIA to see if there would be a connection between the *Vault7* releases on Wikileaks and the *Shadow Brokers*[401], but this could not be shown so far.

**Harold T. Martin III leak**
Investigations also by the FBI after the Shadow Brokers led to discovery of unauthorized copying of data by Harold T. Martin in August 2016.
The found files would equal 500 million printed pages of material. He stored them at his home in Maryland also at unsecure places, such as the garage and on the backseat of his car despite this was standing openly at the street. Storage comprised of hard disks, computers, USB sticks and print outs[402].

He worked for seven private companies at various agencies, including the *CIA, Cybercom* and ODNI and was last employed at *Booz Allen Hamilton*, where he worked from 2012-2015 as contractor in the *Tailored Access Operations Group TAO* of the NSA[403]. Then, Mr. Martin was enrolled in a cyber security doctorate program at the University of Maryland for which he did further research[404].
It is not clear how the *Shadow Brokers* obtained the hacking tools which -as reported by *Washington Post-* are *identical* to those breached by Harold T Martin, according to former officials[405]. Also, it seems to be virtually the *entire* library of the NSA[406].

[398] Brinkmann 2017
[399] Shane/Perloth/Sanger 2017
[400] Shane/Perloth/Sanger 2017, Mikelionis 2018
[401] Shane/Perloth/Sanger 2017
[402] Ammann 2016, p.3
[403] Marimov 2017
[404] Ammann 2016, p.3
[405] Nakashima et al. 2017
[406] Nakashima et al. 2017

He has over years stolen a massive amount of data from various agencies, i.e., also *outside* the NSA.
Originally, the work of the *NSA Tailored Access Group TAO* was classified as *Exceptionally Controlled Information*, which could only be stored in safes. The rules were later less strict as the amount of information material permanently grew on[407].

Mr. Martin was reported to have access to confidential material from 1996 since his time at the US Navy[408] and at the court, he initially pleaded not guilty[409].
Harold T. Martin pleaded guilty in January 2018 for the first of 20 charges, 19 more points were still being negotiated. A connection to the *Shadow Brokers* could not be shown yet. He had collected files from the NSA, US Cybercom, the CIA and the NRO[410].

### 5.3.2 The Longhorn Group/Lamberts/Vault 7 incident

In March 2017, the platform *Wikileaks* started to release information about the cyber capabilities of the *Central Intelligence Agency CIA* under the name *Vault 7*. The leak comprised 7818 web pages and 943 attachments from the *CIA Cyber Center of Intelligence*[411].
Digital traces pointed investigators to a team of developers formerly working with *CIAs Engineering Development Group*. However, these contractors lost the projects and were reported to be dissatisfied which *may* have been the reason for the leak[412].

From the organization side, the already known *CIA Cyber Center of Intelligence* had an estimated staff of 5,000 people and 1,000 programs in 2016[413].
There are a variety of specialized groups (Branches), such as the Embedded development branch for embedding of implants in VoIP phones, Smart TVs etc., the Network devices branch for routers, the Mobile development branch for mobile phones. The *Cyber Center of Intelligence Europe (CCI Europe)* is reported to be responsible for Europe, the MENA region and Africa[414]. However, it seems that intelligence efforts were pointed to individuals instead of mass spying[415].

The cyber tools disclosed by *Vault7* such as malware archives, obfuscation software, spyware, interdiction etc. reflect the state of the art of cyber intelligence.

---

[407] Shane/Perloth/Sanger 2017
[408] Ammann 2016, p.3
[409] Marimov 2017
[410] Mikelionis 2018
[411] Derespins 2017, Shane/Mazetti/Rosenberg 2017
[412] Harris/McMillan 2017, Deutschlandfunk 2017
[413] Derespins 2017
[414] BfV 2017
[415] Shane/Mazetti/Rosenberg 2017

Key findings were so far:

- Encryption bypass of messenger services and smartphones[416]. Car hacking was only tried, success reports were not available.
- *Weeping Angel* spyware can infect Smart TVs (Samsung Modell F-8000) if agents had physical access to them, which allows to observe TV watchers as the TV is only in a fake off modus.[417]
- The collection of foreign malware has the name *Umbrage*[418]
- In April 2017, the obfuscation software *Marble* was leaked which also can be used for **de-obfuscation**, i.e., to revert the steps made before. *Marble* is able to hide code fragments, also provides texts samples in foreign languages which may confuse analysts. *Marble* Version 1.0 was released in 2015[419].
- In May 2017, the spyware *Athena* was disclosed (together with instruction handbook *Hera)* which can infect all Windows versions with or without internet access and was active since August 2015[420]
- In June it was reported that an advanced CIA firmware has infected Wi-Fi routers starting in 2007. An exploit code named *Tomato* can extract passwords when plug and play modus is on. The malware *CherryBlossom* controls the routers, routers from 10 manufactures are known to be infected[421]. *Brutal Kangooro* is an advanced USB stick malware, which can be sent via internet, then it infects the first USB stick. Once installed, it builds covert networks within a closed network.[422]
- *Highrise* is part of a larger technical platform and is an SMS proxy that can redirect target SMS messages to a listening point[423].
- The Wikileaks release from the end of 2017 mentioned in *Vault 8* reported that the CIA had made messaging with its command-and-control servers by counterfeit Kaspersky security certificates seem unsuspicious. The whole thing is also known as *Project Hive*[424].

In addition, *Symantec* discovered that the *Longhorn Group/The Lamberts*, an APT known since 2011, is linked to the files of *Vault7*[425].
The *Longhorn Group/The Lamberts* is an APT known since 2011 with attacks in 16 countries on targets of strategic interest. The malware *Fluxwire* has strong similarities to data found by Symantec for the *Trojan Corentry*, for the malware

[416] Shane/Mazetti/Rosenberg 2017
[417] Shane/Mazetti/Rosenberg 2017
[418] Goetz/Steinke 2017
[419] Beiersmann 2017a
[420] Kolokhytas 2017
[421] Goodin 2017
[422] Beiersmann 2017b
[423] Beiersmann 2017d
[424] Borchers 2017
[425] Symantec 2017

*Archangel* with *Trojan.Plexor*. *Longhorn* uses two further backdoors *LH1* and *LH2*. The *Longhorn* group had also a program to define at which day of the week the malware had communication with the control server.
In October 2014, a zero-day exploit (backdoor) was discovered by *FireEye* and named *Black Lambert* by *Kaspersky*. Further variants were discovered which were named *White, Blue, Green, Pink* and finally *Gray Lambert* since 2016. The Lamberts share codes, styles, data formats, command and control servers and victims and use names from movies (*Flash Gordon*), computer games, TV series (*Star Trek*) in their codes which is an interesting parallel to the *Sauron* and *Slingshot APT*. The attacks were executed on a small number of computers only and were tailor made to the victims[426].

### 5.3.3 Sauron/Strider and Slingshot

The new *APT Project Sauron* (also known as *Strider*) was discovered in 2016, but the malware properties indicate that the programmers have learned from other sophisticated malware, in particular *Duqu, Flame* (use of *Lua* language)*, Equation* and *Regin*, but at a time where these malware types were not discovered which may indicate a relation between the APTs[427].
*Kaspersky* reported the new *Slingshot APT* having the same complexity like Sauron or Regin, active since at least 2012, using a vulnerability of *Mikrotik* routers (Latvian network hardware provider) to infect victims mainly in Middle East and Africa[428]. References to the book *Lord of the Rings* (Gollum, Sméagol) were made. *Slingshot* is the name of a loader that tries to place modular malware, in particular the *Gollum* App and its supporting *Cahndr (Ndriver)* module that e.g., blocks debugging activities of the victim computer to allow data exfiltration.

Of note, *Sauron* and *Slingshot* APTs share the use of popular culture terms in their codes with the *Lamberts*. On the other hand, the apparently Russian APT *Sandworm/Quedagh* also referred to *Dune*.

## *5.4 Russia*

### 5.4.1 APT28 and APT29

#### 5.4.1.1 APT28 (aka Sofacy, Pawn Strom, Csar Team, Sednit, Fancy Bear, Strontium)

*APT 28 (aka Sofacy, Pawn Strom, Csar Team, Sednit, Fancy Bear, Strontium)* is a group focusing on targets of political relevance for Russia which is observed since 2004[429]. The malware compilation times correspond with Moscow time zone,

[426] Kaspersky 2018b
[427] Kaspersky 2016, p.21, Symantec 2016
[428] Kaspersky 2018a
[429] ESET 2016

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[430]. APT 28 uses a variety of malware droppers (*Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer* and *DownRange*) and also malware for smartphones[431].

APT28 has a typical attack strategy[432]:

- They start with a well-elaborated targeted phishing email.
- This may include a link to an interesting topic; however, the website address (URL) is slightly different to the original URL so the victim is landing on a malicious website (**tabnabbing**). Sometimes, the target user is asked to re-enter log in data. Which seems to be a harmless technical error, is in reality used to get passwords (**Credential Phishing**). The number of fake URLs is high: The security Firm *ESET* discovered an erroneously public list containing around 4,400 URLs that were shortened between March and September 2015 by the *bitly*-method[433]. Several of the domains that APT28 registered imitated NATO domain names, including those of *NATO Special Operations Headquarters* and the *NATO Future Forces Exhibition*[434]
- Also, sometimes, **watering hole** attacks were used. Here, potentially interesting websites are infected, e.g., with the *Browser Exploitation Framework (BeEF)* and during visit, the target person's browser will be attacked.

The malware can be separated into three groups: the first-step software for reconnaissance, the second-step software such as *X-Agent* for spying, while the third step pivot software such as *X-Tunnel* to reach other computers[435]. *FireEye* named in 2014 the downloader *Sourface*, the reconnaissance tool *Eviltoss* and the modular implant *Chopstick*[436].

#### 5.4.1.2 APT29 (aka Cozy Duke/Cozy Bear)

The group is also known as *Dark Halo, The Dukes, Nobelium, Office Monkeys, StellarParticle, UNC2452, and Yttrium*.
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

[430] Weedon 2015, p.71-72
[431] Alperovitch 2016
[432] Hacquebord 2017
[433] ESET 2016
[434] FireEye 2014, p.14
[435] ESET 2016
[436] FireEye 2014, p.14

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[437].

*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*[438]. 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[439]. For this action, multi-step loading and backdoors are available. Remote Access Tools (RATs) include *AdobeARM, ATI-Agent,* and *MiniDionis*[440]. 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, which could be confirmed in 2018.

#### 5.4.1.3 The German Parliament Bundestag hack

The German parliament (Bundestag) is a primary attack target since years[441], but other government units as well, e.g., the German foreign department and embassies,

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[442]. 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[443].
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

[437] Raiu/Baumgartner/Kamluk 2013
[438] Weedon 2015, p.70-71
[439] F-Secure Labs 2015
[440] Alperovitch 2016
[441] Lohse/Sattar/Wehner 2015, p.3
[442] FAZ online 2015, p.1
[443] Wehner 2016a, p.6

European server was going on[444]. Investigations confirmed intrusion of several computers by infected emails[445], including takeover of administrator rights[446].

In 2017, an in-depth analysis was published[447]. On 30 April 2015, parliament members received an email with an article „Ukraine conflict with Russia leaves economy in ruins". Once downloaded, several programs were run by attackers, including the program *Mimikatz* that is searching for admin passwords. A few days later 5 of 6 administrator passwords were under control.
One person noted the impossibility to use the French *accent aigu* on 08 May 2017. The German IT security BSI was alerted and found later the malware *X-Tunnel*. Further analyses showed an IP address which was leased by a firm in Pakistan and was also used later in the *DNC hack*, the *WADA hack* and on the German Party CDU.
Another server could be allocated to a Russian individual named *Roschka* who also seemed to be involved in the Macron hack and who works for *Eureka CJSC* which is known to be a security partners firm of the Russian military intelligence GRU. Also, in an older attack of *Fancy Bears*, a technical problem led to redirection of data flow and could be tracked to a building of the GRU in Moscow. The program used in this older attack was the same used for the Bundestag and DNC hack. However, later on it was found that the WADA hack and the later mentioned *Macron* hack were conducted by the *Sandworm* APT that closely cooperates with the APT28.

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[448]. Interestingly, the attack showed similarities to the cyber-attack on TV5Monde[449].
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[450]. Also, the OSCE hack (which was only one hack of many reported cases such as Czech Republic, Poland, Norway, etc.) discovered in late 2016 showed similarities[451].

In early 2017, the BSI noted unusual traffic and detected a further attack on the Bundestag members, at least 10 members were attacked[452]. This included the

[444] Baumgärtner/Röbel/Schindler 2015, p. 28
[445] Mertins 2015, p.4
[446] Hoppe/Osman 2015, p.1
[447] Beuth 2017, p.13-15
[448] Erk et al. 2015, p.2
[449] FAZ online 2015, see also Wehner 2015, p.1
[450] Baumgärtner/Neef/Stark 2016, p.90-91
[451] Deutsche Welle 2016
[452] Tanriverdi 2017

member of the Green Party Marielouise Beck, whose computer was already infected in 2014 by the malware *Miniduke* from *APT 29/CozyBear*[453].
The attack was done by presenting malicious advertising by a third party on the website of the *Jerusalem Post*, a method called **malvertising**[454].
In 2017, **malvertising campaigns** were a global issue, notably through the *RoughTed* malware, which spread adware, exploit kits, and ransomware[455].

#### 5.4.1.4 The DNC hack/Attacks on voting systems

**Detection history**

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[456].
The APT29 intrusion by the SVR was going back to summer of 2015, while the GRU hackers from APT28 *and Sandworm* 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[457]. 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[458].

Later on, a member of the *GRU unit 74455 aka Sandworm* who presented himself as 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[459]. 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[460].
End of August 2016, it was detected that online voting systems were intruded in Illinois and Arizona, in Illinois data of 200,000 voters were copied[461].
The FBI had detected suspected Russian attempts to penetrate election systems in 21 states and as a warning, a cyber operation was made by the NSA with implanting

[453] Wehner 2016b, p.9
[454] Reuters 2017a
[455] Check Point Research 2017, p.7
[456] Alperovitch 2016, Nakashima 2016a
[457] Alperovitch 2016
[458] FAZ online 2015, see also Wehner 2015, p.1
[459] Baumgärtner/Neef/Stark 2016, p.90-91, DoJ 2020
[460] Lichtblau/Weiland 2016
[461] Nakashima 2016b, Winkler 2016, p.4

computer code in sensitive computer systems that Russia was bound to find[462]. However, also the *Surkov incident* shown in *Section 6.2.3* was discussed to be part of the retaliation.
The *US Intelligence Community Report on Cyber incident Attribution* from 2017 and the preceding assessment by the *Department of Homeland Security* on the operations of *APT28/Fancy Bears* and *APT29/Cozy Bears* as Operation *Grizzly Steppe* was supportive to the attribution of the attacks to Russia[463]. The close cooperation between the GRU units APT28 and *Sandworm* was disclosed in 2020[464].
In April 2017, a Russian was detained at the Barcelona airport who is suspected to be involved in the Russian hack during the US election campaign[465].

**The Mueller indictment from 2018[466]**
The Mueller indictment has presented evidence that *Fancy Bears* are GRU members working in GRU facilities. The *Russian Military Intelligence GRU* has multiple units engaged in cyber operations, including Units 26165 and 74455. 12 known officers of these units are suspected to be involved in the Russian activities of 2016 during the Presidential Elections Campaigns, in particular the *Democratic National Committee (DNC)* hack. Unit 26165 is primary responsible and located in Moscow, while Unit 74455 is located in another Moscow building that the GRU calls the Tower. In 2020, it could be clarified by the US Department of Justice that Unit 74455 is identical to the *Sandworm* group[467].
In March 2016 hacking started with a spearphishing emails. From a hacked computer of a *Democratic Congressional Campaign Committee (DCCC)* employee, the were able to get into the DNC network. In April 2016, files were stolen from the DCCC, the DNC and the Clinton Campaign Team and then in June 2016 released by the fictional actor *Guccifer 2.0* and the *DCLeaks* platform. Within Unit 26165, a department is responsible for development and managing malware including *X-Agent* which was then deployed on DCCC and DNC computers. Also, the *Fancy Bears/APT28* malware *X-Tunnel* was implemented. A Linux-based version of *X-Agent* which was able to communicate to the GRU-registered domain *linuxkrnl.net* and was active until October 2016. The *first Guccifer 2.0* message was prepared on a computer managed by *GRU unit 74455/Sandworm*. *DCLeaks* was hosted on a leased Malaysian server which was funded with bitcoin mining. The same bitcoin

[462] Miller et al. 2017. Details of the intelligence findings were leaked by the Whistleblower *Reality Winner,* an NSA linguist, on the Platform *The Intercept*. As only a very limited group of persons could access and print the files, she was identified rapidly after publication, Gruber/Reinhold 2017 Gruber/Reinhold 2017, Shane/Perloth/Sanger 2017.
[463] ODNI 2017, JAR 2016 of the *Department of Homeland Security DHS* and the *Federal Bureau of Investigation FBI*.
[464] DoJ 2020
[465] Zeit online 2017
[466] Mueller 2018
[467] DoJ 2020

address was used for other GRU operations to purchase servers and domains, e.g., the fake website account-goooogle.com and US-servers. Also, the link *linuxkrnl.net* was renewed by paying with these bitcoins.

#### 5.4.1.5 The Yahoo hacks

The internet firm *Yahoo* reported the hacking of 1 billion user accounts in 2013 and 500 million email accounts in 2014. The United States identified 4 persons, two members of the Russian intelligence FSB and two other hackers who are suspected to have conducted the 2014 hack with a special focus on the accounts of diplomats, militaries and cyber security individuals. One of the suspects is already imprisoned in Russia, probably as part of the *Michailow* incident. However, a link to APT28 or 29 could not yet be established[468]. A new investigation of the 2013 showed in 2017, that all three billion *Yahoo*-accounts were hacked[469].

#### 5.4.1.6 The LoJax firmware campaign

The *LoJack* anti-theft software from the company *Absolute Software* which implements a UEFI/BIOS firmware module to prevent deletion appeared in trojanized versions since at least early 2017. The malicious versions are now known as *LoJax* which is like *LoJack* very deeply embedded into the computer system and also persistent[470]. *LoJax* typically appeared with other *APT28/Fancy Bears* modules, such as the backdoors *SedUploader, X-Agent* and the network proxy tool *X-tunnel*[471].

#### 5.4.1.7 Corona crisis

The British *National Cyber Security Centre (NCSC)* reported that the Russian APT29 targeted various organizations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom[472]. APT29 conducted basic vulnerability scanning against specific external IP addresses, used the *WellMess* malware for shell commands and file handling and the *TWellMail* tool for commands or scripts with data transmission to a hardcoded Command and Control server[473]. The scanning was continued against vaccine research centers in 2020[474]. Also, samples of the *SoreFang* malware were found which specifically targets *SangFor* devices, but this malware was also used by the APT *Dark Hotel*.

---

[468] FAZ 2017a, p.23
[469] DW 2017
[470] ESET 2018
[471] ESET 2018, p.7
[472] NCSC 2020
[473] NCSC 2020
[474] Brühl 2020

#### 5.4.1.8 Further activities

Other activities of the *APT28*/*Fancy Bears* 2017 concerned the release of documents of the *English Football Association* and a breach of the mail system of the United Nations[475].

*Kaspersky* experts noted in 2018 that *APT28*/*Fancy Bears* has now shifted to former Soviet states. They set up multiple servers, use fake phone numbers for domain registration, use privacy services for registration and registrars who accept bitcoin[476].

*Microsoft* has reported in August 2018 that *APT28*/*Fancy Bears* had set up fake websites of conservative Think Tanks to catch user credentials, *Microsoft* was able to block this[477].

Please note that these groups are permanently active, the above events were only the most prominent and 'silence' does not mean that the group is inactive, but that the latest hack may not been discovered yet. In 2019, the new APT 29 malware types *PolyglotDuke, RegDuke* and *FatDuke* were detected and named *Operation Ghost*[478]. Amongst others, the US *Republican National Committee (RNC)* was attacked in 2021.

#### 5.4.1.9 The SolarWinds Espionage Campaign

In December 2020, a massive cyber espionage campaign was reported where - amongst many other organizations- the *US Departments of Treasury and Commerce* were infiltrated, the *SolarWinds, Solorigate* or *Sunburst malware supply chain attack*. This was conducted by the Russian *APT29/Cozy Bears*, the unit of the Russian foreign intelligence SVR[479].

*SolarWinds Orion* is an IT performance monitoring platform that manages and customizes IT systems in hundreds of thousands of organizations. In a cyber-operation going over months, APT29 implanted malware in the *Orion* updates. These poisoned updates were spread between March and May 2020[480].

### 5.4.2 The Waterbug group (aka Turla/Snake/Ouroburos/Venomous Bear/Krypton/Group88)

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

In one source code the term UrObUr()s was used, alternative writings to *Uroburos* are *Ouroburos* and *Uroboros*. Western intelligence attributes this APT to the Russian civil intelligence FSB.

---

[475] The Telegraph 2017, Bild 2017
[476] Paganini 2018b
[477] Tagesschau 2018
[478] ESET 2019
[479] Nakashima/Timberg 2020
[480] Bayak 2020, Krebs on Security 2020

#### 5.4.2.1 The agent.btz attack 2008

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[481]. 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[482].

The multi-functional malware named *Ouroburos/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*[483]. 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[484]. Attackers used *Snake/Ouroburos/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[485].

#### 5.4.2.2 The RUAG attack 2014-2016

*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[486].

#### 5.4.2.3 The IVBB attack 2016-2018

The German government communication system *Informationsverbund Berlin-Bund IVBB* has been in operation since 1999 and is operated by Deutsche Telekom. It covers the Internet and telephone traffic of the Federal Presidential Office, the Federal Chancellery, the Federal Ministries, the Federal Audit Office, security authorities and parts of the Bundestag and the Bundesrat. It is used for the safe transmission of information of the level VS-NfD (confidential-only for service use). The safety of the IVBB is supervised by the German IT security authority BSI. Already after the attack on the computer network of the Bundestag 2015, there were

[481] Glenny 2010, p.23
[482] Brown/Poellet 2012, p.131
[483] Symantec 2016, p.10-11
[484] Fuest 2014a, p.1-3
[485] Weedon 2015, p.72-73
[486] Jürgensen 2016, p.28

longer unexplained irregularities in the telephone network. The extent to which IVBB phone calls could or were intercepted is unclear[487].

There are only two exits, one each in Berlin and Bonn. Transitions to the IVBB Internet and IVBB voice network are protected with package filters of the high evaluation level EAL4. There is a double firewall with content filter and formal filters (IP address blockade) and the *secure network architecture (SINA)* box. iPhones and iPads are only allowed to work with the security solution *SecurePIM*, voice and fax data is encrypted with *Elcrodat 6-2*[488]. Currently, protection programs of the security company *TrendMicro* are also active[489].
2 years ago, the hackers of *Snake/Turla/Ouroburos* manipulated an eLearning learning platform of the *Federal Academy of Public Administration* with spy software, 17 employees then loaded the spy software onto their own computer, and 6 documents were stolen[490].

The aim was Department 2 (Unit 205) of the Foreign Office, responsible for Russia, among other things. In December 2017, Germany was informed about this by a foreign intelligence[491] and then the *Mobile Response Incident Response Team MIRT* of the BSI and the ZITIS analyzed the situation. But then the German press agency reported on the operation at the end of February 2018 and the attacker withdrew. However, the APT tried again in November 2018 to get to email addresses of members of the Bundestag.

#### 5.4.2.4 The attack on the French Navy 2017-2018

*Turla* targeted 12 officers to evaluate the French Navy's oil supply chain in 2017 and 2018, but the French preferred the discrete clarification of incidents instead of public accusations[492].

#### 5.4.2.5 The OliRig attack 2019

In 2019, *Turla* continued its activities. The new malware *Topinambur* was used against individuals who tried to communicate via safe VPN tunnels[493].
Also, they managed to infiltrate the command-and-control server of the Iranian *OilRig* group which is possibly identical to APT34 which allows supervision of their cyber activities[494].

---

[487] Gräfe/Link/Schulzki-Haddouti 2018
[488] Gräfe/Link/Schulzki-Haddouti 2018
[489] FAZ 2018c, p.2
[490] FAS 2018, p.7
[491] FAS 2018; Pinkert/Tanriverdi/Von Bullion 2018
[492] Lawfareblog 2019
[493] Schäfer 2019, p.14
[494] Paganini 2019

### 5.4.3 The Sandworm/Quedagh group (aka Black Energy/Telebots/Voodoo Bear)

The British Intelligence GCHQ associated *Sandworm* and *Black Energy* with the Russian GRU[495] which then was confirmed by the detailed DoJ indictment from 2020 against 6 GRU officers[496]. The group is also known as *Iron Viking, Industroyer, Hades* and *G0034*. The group closely cooperates with APT28, but is also specialized in attacks on *Industrial Control Systems (ICS)*.

#### 5.4.3.1 Sandworm Engagement in 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[497].

The APT29 intrusion was going back to summer of 2015, while the GRU hackers from APT28 *and Sandworm* intruded the network independently in April 2016.

Officers of the Units 26165/APT28 and 74455/Sandworm are suspected to be involved in the Russian activities of 2016 during the Presidential Elections Campaigns, in particular the *Democratic National Committee (DNC)* hack. In 2020, it could be clarified by the US Department of Justice that Unit 74455 is identical to the *Sandworm* group[498].

#### 5.4.3.2 The WADA hack

The newly established *Fancybear.net* Website released in summer 2016 information from *World Anti-Doping Agency WADA* showing that certain athletes got waivers e.g., for use of steroids. The hack was done after doping allegations against Russian athletes [499] The origin was the *Sandworm* group aka GRU unit 74455[500].

#### 5.4.3.3 The Macron hacks

The election campaign of the new French president Macron was attacked and certain documents were leaked. On 15 Mar 2017, the security firm *TrendMicro* detected phishing emails to campaign officials and others which would have linked them to fake websites. On 15 April 2017, also fake websites mimicking the names of the Macron party (*En Marche*!) such as mail-enmarche.fr were registered. The IP numbers behind the websites were part of an IP address block which was attributed

[495] Technology review 2018
[496] DoJ 2020, Bowen 2021
[497] Alperovitch 2016, Nakashima 2016a
[498] DoJ 2020
[499] WADA 2016
[500] DoJ 2020, Bowen 2021

by *TrendMicro* already to APT 28[501], but again the origin was later on identified as the *Sandworm* group aka GRU unit 74455[502].

#### 5.4.3.4 The Olympic Destroyer (false flag) Attack 2018

*Lazarus* was suspected to have conducted a network worm attack with the *Olympic Destroyer* malware on the Olympic Winter Games in Pyeongchang in South Korea which resulted in various inaccessible Olympia websites, but *Kaspersky* showed that this was a false flag by putting a *Lazarus* digital fingerprint into the attacker code by the Sandworm group[503]. In particular: *Lazarus* uses long and reliable passwords and does not hardcode passwords into the malware body. A wiper element was uploaded too late, i.e., two hours after the opening ceremony.

#### 5.4.3.5 The OPCW hacks

The former Russian intelligence member Sergei Skripal and his daughter were intoxicated by the toxic nerve agent *Novichok* at their house in Salisbury, UK. Thereafter, a 2018 hacking campaign took place against UK, Europeans, and the *Organization for the Prohibition of Chemical Weapons (OPCW)* which investigated the nerve agent attack[504]. Moreover, 4 Russians identified as GRU members travelled to the headquarter of the OPCW in Switzerland to observe their investigations on chemical weapons. Later on, the same group conducted 2018-2019 cyber campaign against Georgian media companies and the Georgian parliament.

#### 5.4.3.6 The Black Energy Attack

The *Sandworm* or *Quedagh* group (names resulting from references to science fiction world *Dune)* is using the *BlackEnergy* -which was originally developed as crimeware, but then modified- against target computers.
*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[505]. The *US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)* has identified a malware campaign that since at least 2011 has compromised several ICS systems using a variant of

[501] Perloth 2017a
[502] DoJ 2020, Bowen 2021
[503] GReAT 2018, DoJ 2020
[504] DoJ 2020, Bowen 2021
[505] F-Secure Labs 2014, p.2, 10-11

*BlackEnergy* on Internet-connected human-machine interfaces (HMIs)[506]. Amongst others, the HMIs *GE Cimplicity, Advantech/Broadwin WebAccess*, and *Siemens WinCC* were affected.
In summer 2014, *BlackEnergy* 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[507]. However, NATO confirmed that the classified operational networks were not affected as they are isolated from internet[508].

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[509]. Three further companies were intruded, but had no outages. The intruders were able to open multiple breakers remotely resulting in power outage, which happened in a small-time window in a coordinated manner[510]. **Telephone denial of service attacks (TDoS attacks)** were used to flood hotlines with phone calls to prevent customers from reporting the outage by telephone[511].
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[512].

### 5.4.3.7 The Industroyer Attack

On 17 Dec 2016, the malware *Industroyer/CrashOverride* which was specifically designed for attacks on smart grids caused a blackout in Kiev which was attributed to a new APT called *Electrum* which was linked to the *Sandworm/Quedagh* group[513].
The malware impacted a single transmission level substation by installing a backdoor, then a launcher, thereafter payloads including those with IEC104 protocol commands and finally a wiper malware. The malware used hard-coded proxies including TOR nodes[514]. A similar attack with a slightly modified *Industroyer 2.0* malware in 2022 was ineffective[515], see Section 3.12.14.

[506] ICS-CERT 2016a
[507] BBC 2014, p.1, F-Secure Labs 2014, p.2
[508] BBC 2014, p.2
[509] ICS-CERT 2016b
[510] ICS-CERT 2016b
[511] Zetter 2016
[512] ICS-CERT 2016a
[513] Scherschel 2017a, Dragos 2017
[514] Dragos 2017, p11 and 14
[515] Mäder 2022c, Muth 2022

### 5.4.3.8 The Petya/Not-Petya/MoonrakerPetya Attack

Note that the preceding *MoonrakerPetya* attack was detected after the *NotPetya* attack. While the CIA's assumption of an attribution to the GRU was confirmed by GCHQ (and denied by Russia), it is apparent from the *MoonrakerPetya* attack that this could be attributed to the *Sandworm/Quedagh* group.
The *MoonrakerPetya* attack was only a small one on a few computers, the NSA exploit *EternalBlue* allowed then a large scale-attack.

The *Sandworm/Quedagh* APT released a *NotPetya*-precursor named *MoonrakerPetya* in 2017. In December 2016 the attackers deployed the worm *Moonraker Petya* that probably was a precursor N*otPetya* (also known in as *Petya, ExPetr, Nyetya, EternalPetya).* The worm is a DLL file deployed under the name msvcrt120b.dll in the Windows directory, while the internal name is moonraker.dll. *Moonraker Petya* contains code that makes the computer unbootable, but was used in a small number of cases only[516].

As for *WannaCr*y, first an attack was started with NSA exploits on 23 May 2017 which caused little public attention, as no damage was visible[517].
The NSA exploit *Eternal Rocks* combined 7 exploits from NSA (*EternalBlue, DoublePulsar, EternalRomance, EternalChampion, EternalSynergy, ArchiTouch* and *SMB Touch*). The malware *Petya* used the *EternalBlue* and *EternalRomance* exploit end of June 2017. Before becoming active, it downloads the TOR browser to build a covert communication line to control server.

The malware that initially looked like the already known ransomware *Petya* was quite different, also from another ransomware like *Mischa* and *Goldeneye*. In addition to *EternalBlue* and *EternalRomance*, it used the Ukrainian accounting software *Me-doc* by injecting a malicious update[518]. This was possible due to a falsified Microsoft security certificate. These differences explain why some authors called it *Not-Petya* or *Petya2017*.
Once the new *Petya* had infected a computer, it automatically searched for other computers in the network which could be infected as well[519].
Despite the targets were asked to pay money, it appeared that the userID shown on the request was only a meaningless random number and the malware appeared to be a **Wiper** malware that overwrites the *Master Boot Record*[520] and other files. Due to this, the blocking of the *Posteo*-mail account that was presented as contact address for payment had no impact anymore.

[516] Cherepanov 2018
[517] Kling 2017
[518] Kaspersky 2017b/Scherschel 2017b
[519] Kaspersky 2017b/Scherschel 2017b
[520] Beiersmann 2017c

A large variety of companies was hit, e.g., *Merck* in US, *Maersk* in Denmark, *Milka* in Germany (who then suffered from several days production stop), but it also affected Russian companies and the nuclear plant of Chernobyl.
The use of a falsified security certificate, the complexity of the malware and the lack of profitability, as the victims could not pay anyway, strongly indicated an attack by a state actor. In late 2017 the CIA reported that the *Petya/NotPetya* attack could be attributed to the military intelligence service GRU with high confidence[521].

#### 5.4.3.9 Grey Energy/Bad Rabbit/Telebots

In October 2017, the group also utilized the *BadRabbit* malware family for attacks. Their *Telebots* malware was only used in the Ukraine[522].
The design and architecture of the *GreyEnergy* malware which seemed to exist since 2015 are very similar to those of the *BlackEnergy* malware, but one of the *GreyEnergy* samples was signed with a valid digital certificate from the Taiwanese company *Advantech* that produces ICS and IoT components[523], which may have been stolen.

#### 5.4.3.10 The VPN Filter attack 2018

The new modular malware system *VPNFilter* affected in 2018 at least 500,000 networking devices in at least 54 countries, but in particular in Ukraine by using a specific C2 infrastructure for this country[524]. The malware has overlaps with versions of *BlackEnergy* and infects *Linksys, MikroTik, Netgear* and *TP-Link* networking equipments and *QNAP network*-attached storage devices.
It is a three stage-malware. Stage 1 is the first IoT malware able to persist after a reboot and utilizes command and control mechanisms to contact the stage 2 malware deployment server. The stage 2 malware is for information collection, such as files, command execution, data exfiltration and device management. Some versions of stage 2 have a bricking capability that overwrites a critical portion of the device's firmware with zeros and reboots the device, which makes it unusable. In addition, there are various stage 3 modules as plugins for stage 2. These plugins can e.g., monitor of Modbus SCADA protocols, and to allow stage 2 to communicate over TOR. The C2 communication and additional malware downloads can happen via over TOR or SSL-encrypted connections and a programming bug in the decryption routine was similar to findings in *Black Energy*. In February 2022, Sandworm allegedly released the related *Cyclops Blink* malware.

[521] Nakashima 2018
[522] Cherepanov 2018, p.22-24
[523] Cherepanov 2018, p.2-3
[524] Talos 2018

### 5.4.4 The Dragonfly/Energetic Bear APT

The cyber attacker group *Dragonfly (Energetic Bear/Berzerk Bear/Crouching Yeti/Koala/Group 24/Iron Liberty/Dymalloy/Havex or TeamSpy)* is the FSB unit 71330 and intruded providers of ICS software and injected malware, so that all user companies automatically loaded the malware with the next software update[525]. The 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[526]. 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) [527].

In May and June 2017, the US energy sector was target of cyber attacks. DHS and FBI were investigating this, amongst the targets, the nuclear plant of *Wolf Creek* near Burlington, Kansas was attacked, but its operations were not affected. The attacks were the same as the tactics of *Dragonfly (Energetic Bear/Crouching Yeti/Koala)*, and **fake resumes** for control engineering jobs, watering hole attacks and man-in-the-middle attacks were applied[528], so this attack was also named *Dragonfly 2.0*. Both the original *Dragonfly* and *Dragonfly 2.0* attack exclusively used the malware *Trojan.Heriplor*. Concerns were expressed that the aim of attacks was to take over control to have the option for future sabotage.

*Dragonfly* intruded recently the electric grid networking unit NetComBW of the EnBW energy provider in Southern Germany[529].

### 5.4.5 The Triton/Temp.Veles/Trisis attacks

At the end of 2017, a new ICS malware called *Triton* or *Trisis* was discovered in a Middle Eastern destination.[530] The *Triton/*Trisis malware specifically targets *Schneider Electric's Triconex Safety Instrumented System (SIS)*. SIS systems execute emergency shutdowns or production stops in critical situations, the intrusion can externally enforce such shutdowns from the outside or prevent them in an emergency and thus damage the production[531].
The protection of such a SIS system by a separate firewall may obstruct remote access engineering, so that often there is no such separate protection[532].

[525] Metzler 2015, p.34, Perloth 2017b, Kaufmann 2022c
[526] Campbell 2015, p.11
[527] Symantec 2014b
[528] Perloth 2017b
[529] Kaufmann 2022c
[530] Johnson et al. 2017
[531] Dragos 2017
[532] Dragos 2017, p.5-6

The Israeli cybersecurity firm *Cyber X* reported that it was a Saudi-based target that had been attacked by Iran and that the malware was used against multiple targets.[533]
In late 2018, *FireEye* attributed the malware to Russia. The *Triton* malware development was very likely supported by the *Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM)* for various reasons: A person with links to the institute was involved in this development, the CNIIHM tested malware that is very likely related with *Temp.Veles* activities, the working name of the group using Triton, a CNIIHM IP-address was used for activities around the Triton attack and the institute has research divisions for critical infrastructure and weapon development. Further unique files and tools were identified and *Temp.Veles* tested intrusions already since 2013 finally resulting in the sophisticated *Triton* attack[534].
Finally, language settings and artifacts as well as the primary working time zones fit well with this attribution.
However, it remains unclear whether *Temp.Veles* is really an own APT or only malware provider for already known APTs.
In 2019, it was speculated that new code variants were developed being able to compromise a broader range of safety instrumented systems, but no further incident occurred until 2020[535].

### 5.4.6 Cloud Atlas/Inception/Red October/Rocra

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 from machines using the classified software *acid cryptofile* [536]. In December 2014, a similar malware for smartphones reappeared as *Cloud Atlas/Inception*[537].
Meanwhile, it is assumed that the APT behind this malware at least overlaps or is identical to *Red October* alias *Rocra*.
*Cloud Atlas* continued its activities in 2018/2019 with its new malware *PowerShower*, a malicious *PowerShell* tool used since October 2018[538].

## *5.5 China*

Both the civil and the military sector of China is under control of the Chinese Communist Party. The *Chinas People Liberation Army PLA* is suspected to have specialized cyber units in approximately 6 main locations[539].

[533] Weidemann 2017b
[534] Fireeye 2018b
[535] Giles 2019
[536] Kaspersky Labs 2013
[537] Dilger 2014
[538] Securelist 2019b
[539] Finsterbusch 2013, p.15

The PLAs responsible unit is the *General Staff Department GSD* which consists of 4 Departments. This is Operations in 1st department, department intelligence in 2nd department, signals intelligence and network defense in 3rd department and Electronic Countermeasures and offensive cyber operations in 4th department[540]. The US agency NSA was reported to track about 20 Chinese units in 2014, over half of them PLA cyber units[541] (while the others can thus be assumed to be linked to non-military intelligence).
However, while it is apparent that all APTs have a specialized area of activity, little is known about coordination between the APTs. So, all assignments have to be done with caution, further research may show that certain APTs may only be parts of others or current APTs have to be split into new ones or re-attribution has to be done.
Meanwhile, US believes that the *Ministry of State Security MSS* has taken over the coordination of cyber operations from the PLA in 2015. [542]
In 2018, APT10 was suspected to be linked to the Ministry of State Security.

### 5.5.1 APT1/Comment Crew/Comment Panda/TG-8223

The Third Department of the PLA 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 *Putter Panda/APT2/TG-6952* by security firms and attack activity from Unit 61486 has been linked to Unit 61398 based on shared infrastructure[543].

In 2013, the Cyber security company *Mandiant* presented an in-depth analysis of Chinese cyber activities[544]. 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*'. This person had both a registration of a domain used by APT1 and an available profile as army member.

[540] Mandiant 2013, Sharma 2011, p.64
[541] Perlroth 2014
[542] Langer 2018b
[543] Novetta 2015, p.15, Perlroth 2014
[544] Mandiant 2013

China rejected the accusation, but US media speculated in 2016 that this may have caused the temporary significant decrease on cyber-attacks suspected to come from China[545].
However, other US-Chinese cyber activities continue. Chinese hackers on behalf of the Chinese government allegedly broke in January 2018 into the computers of a U.S. firm, which works for the *Naval Undersea Warfare Center* in Rhode Island. The files were stored in an unsecured network, the 614 Gigabytes information also include a supersonic missile system to be deployed from 2020[546].
Data of 500 million visitors of the *Starwood Hotel* group[547], which includes the *Marriot Hotel* group were copied since 2014 including credit card and passport numbers etc. US government believes that this attack was conducted by China, as the *Marriot* hotels are frequently used by employees of the US government and military. [548]

### 5.5.2 APT17/Winnti/Axiom/Barium

The *APT17/Winnti/Axiom/Barium Group* is also known under many other names, such as *DeepPanda, Shell_Crew, Group 72, Black Vine, HiddenLynx, KungFu Kittens, Winnti Group, Tailgater, Ragebeast, Blackfly, Lead, Wicked Spider, Dogfish, Deputy Dog, Wicked Panda* 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[549].
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 *Adobe*) and from high-tech companies of the security and defense sector in 2009[550].
Other operations included the *Elderwood* platform attack from 2011-2014, the *VOHO Campaign* watering hole 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*[551]. Note that the malware types *Zox* and *Hikit* were only seen in *Axiom* activities, while the other malware used by them was also

[545] Mandiant 2013, Jones 2016, p.5, Nakashima 2016. However, in 2017, the US filed lawsuits against three Chinese hackers who entered US companies between 2011 and 2017, including: the US branch of Siemens, so that this peace seems to be in danger, cf. NZZ 2017b.
[546] Spiegel 2018
[547] Langer 2018a
[548] Langer 2018b
[549] Alperovitch 2014. The company *Crowd Strike* used a kernel sensor (*Falcon host*) deployed on Windows and Mac servers, desktops, and laptops that detected attacks and compared them to a threat intelligence repository for attribution.
[550] Markoff/Barbosa, 18 Feb 2010
[551] Novetta 2015, p.12-13

used by other organizations[552]. Attack targets included a wide range of government organizations, companies from technology sector and academic institutions.
The group also attacks selected targets with *Blackcoffee* malware e.g., to gain military intelligence[553].

In 2019 it was found out that this APT increasingly uses methods to attack multiple users simultaneously.
APT40 was involved in a large attack on ASUS computers known as *Operation Shadowhammer*. They infiltrated a regular *ASUS Live Update*, so tens of thousands of users downloaded the infection on their computers with the update.[554]
In addition, the *Winnti* Group (*Axiom/APT17*) has infiltrated the IT Service Provider *Teamviewer* from 2014-2016, the *Teamviewer* program is used for remote access, e.g., used by IT admins [555].

### 5.5.3 APT10/Red Apollo/CVNX/Stone Panda/menuPass/Potassium

APT10 has done a massive espionage campaign against *Managed Service Providers MSPs* (e.g., companies who provide IT services, Help Desks and other things) which can use the overlap with company-specific infrastructures to infiltrate a large number of Western companies.
The attacks and the new Operation *Cloud Hopper* are done as follows: The tactical malware, *EvilGrab* and now *ChChes*, is delivered through spear phishing and then in case of a relevant target to install sustained malware, *PoisonIvy* (until 2013) and from 2014 on *PlugX* and *Quasar*.[556]

In 2018, the US officially accused two members of this group. Zhu Hua (cover names *Afwar/CVNX/Alayos/Godkiller*) and Zhang Shilong (cover names *Baobeilong/Zhang Jianguo/Axtreep*) were identified as members of the APT10 group, being employees of the *Huaying Haitai Science and Technology Development Company* in Tianjin and associated with the local bureau of the Chinese Ministry of State Security[557]. The group is active at least since 2006. They conducted several campaigns such as an infiltration of *Managed Service Providers (MSPs)* to get access to companies in multiple states, they intruded dozens of technology firms and government institutions in US during a Technology Theft

[552] Novetta 2015, p.20. However, *Novetta* indicated in their *Winnti* attacker group analysis as part of the Operation SMN that *Hikit* was now used to leverage *Winnti* attacks. Whether this meant that *Hikit* malware was now non-exclusive or *Winnti* (that changed from gaming industry to other industry espionage such as *ThyssenKrupp*) was now liaised with *Axiom* was not clear, but now it is assumed that these groups are part of the same APT.
[553] FireEye 2017
[554] Securelist 2019a
[555] Rosenbach 2019
[556] PwC/BAE Systems 2017, p.18
[557] DoJ 2018

Campaign and stole personal data of more than 100,000 members of the US Navy.[558] The indictment provided only examples and highlights of APT10 activities, presumably for protection of sensitive information, but showed on the other hand that the US authorities have more detailed knowledge, e.g. by reporting the number of infected computers, the use of spearphishing and of 1,300 unique malicious domains.

According to reports from June 2019, the NASA *Jet Propulsion Laboratory JPL* was accessed by connecting a *Rapsberry Pi* device, which then allowed to steal data from Mars missions[559]. In 2018, also the *JPL Deep Space Network*, as system of satellite dishes for communication with Nasa spacecrafts was infiltrated. In December 2018, two members of APT10 were indicted for intrusion of the JPL, but it was not stated whether this specific attack was meant.

### 5.5.4 APT 40 (Temp.Periscope) and Thrip

APT 40 is also known as *Temp.Periscope, Temp.Jumper, Bronze Mohawk, Gadolinium, Kryptonite Panda, Leviathan, Feverdream, G0065GreenCrash, Hellsing, Kryptonite Funds* and *Mindcarp.*
Satellite hacks of US satellites were already reported since a decade and China was suspected by the *US-China Economic and Security Review Commission* since a longer time already[560]. In June 2018, *Symantec* reported successful breaches of satellite and defense companies by a new APT called *Thrip* which has been active since 2013. This APT may have overlaps with the APT40.
APT40 is active since 2013 and attacks preferably industries involved into military ship construction. It uses a variety of tools, including spearphishing, spoofing (of *Thyssen Krupp Marine Systems*) and seemed to have taken over TTPs from the Russian groups *Dragonfly* and *APT28* in 2017 and 2018. The group used the *Foxmail* system which was used earlier by another Chinese group named *Luckycat* in 2012[561].

In Dec 2016, the PLA Navy seized an **unmanned underwater vehicle UUV** from US Navy and in parallel to this, cyber activities against naval research units and companies were significantly enhanced.
APT40 is allocated to Chinese IP addresses, command and control servers in China, Chinese working times and China-related WHOIS registrations. It uses dozens of new and different malware programs for initial compromise, maintaining foothold, maintain presence, lateral movement, privilege escalation and reconnaissance.[562]

[558] DoJ 2018
[559] Cimpanu 2019
[560] Menn 2018
[561] Insikt Group 2018
[562] Plan 2019

### 5.5.5 APT 41/Double Dragon/Barium

APT 41 does both espionage and activities for their own profit since 2012. Since that time, they used dozens of unique malware families for their activities. Espionage is focusing on healthcare, telecoms, the high-tech sector while the cybercrime activities focus on ransomware and cryptocurrency operations.
A typical attack method is spear-phishing emails with attachments such as compiled HTML (.chm) files for initial intrusion, followed by further malware deployment[563].

### 5.5.6 Hafnium

The new APT *Hafnium* also known as *ATK233, G0125, Operation Exchange Marauder, Red Dev 13* used *Microsoft Exchange* vulnerabilities[564] to intrude at least 30,000 US Organizations in 2021. The *Microsoft Threat Intelligence Center (MSTIC)* attributed this campaign with high confidence to a Chinese state-sponsored APT that was already active before this incident. In the United States, *Hafnium* uses leased virtual private servers (VPS).

### 5.5.7 Further assumed Chinese APTs

Further assumed Chinese APTs currently are:

- *APT3/Gothic Panda/UPS Team/Pirpi/Clandestine Fox TG-0110/Buckeye*[565]: since 2014 attacking targeted industries with spearphishing and zeroday exploits.
- *APT12/Ixeshe/DynCalc/DNSCalc/Numbered Panda/JoyRAT* targets journalists and military contractors from the United States and Pacific Rim since 2012 by spearphishing and then installing malware such as *Riptide*. Recently the *Etumbot* attack was discovered in Europe which is now a new focus of the APT.[566]
- *APT14* is focusing on information possibly specific to the military and naval sectors[567]
- *APT15/Mirage/Vixen Panda* is now focusing on government and diplomatic targets in Russia and former Soviet republics[568]
- *APT16* is focusing on the Japanese and Taiwanese high-tech sector[569]
- *APT18/Dynamite Panda/Wekby/TG-0416*: The data of 4.5 million members of US-based healthcare organization, *Community Health Systems* was potentially accessed during a breach[570].

[563] FireEye2019
[564] Krebs on Security 2021a
[565] FireEye 2017/Reuters WorldNews 2017
[566] FireEye 2017/Reuters WorldNews 2017
[567] FireEye 2022
[568] Reuters World News 2017
[569] FireEye 2022
[570] PwC/BAE Systems 2017, p.14

- *APT19/Codoso Team:* Several healthcare firms were targeted, *Anthem, Premera Blue Cross and CareFirst* suffered data breaches in 2015.[571] In 2017, they attacked their victims with macro-enabled Excel (xlsm) and rich text format (RTF) attachments
- APT20/*Wocao/Twivy*: According to Fox-IT, the Operation *Wocao* is focusing espionage on government entities, managed service providers and across a wide variety of industries. The attack is typically executed by abusing legitimate access channels, e.g., by abuse of 2FA soft tokens to get into VPN systems[572].
- *APT 21/Zhenbao:* Russian language emails and social engineering to get access to Russian security organizations[573]
- *APT 22/Barista:* military, economic and political targets in USA, Europe and East Asia[574]
- *APT 23:* is focusing on USA and the Philippines[575]
- *APT 24/Pitty Tiger:* is focusing on building construction industry[576]
- *APT 27/Emissary Panda/TG-3390: ThreatConnect* discovered APT 27 activity in Europe in 2016[577].
- *APT30/PLA unit 78020/Naikon*[578]: active espionage since 2004, e.g., at ASEAN summits, modular malware such as *Backspace* to overcome airgaps
- *APT31/Zirconium/Judgment Panda/Bronze Vinewood*: Operation *Iron Tiger* in 2013 was an attack where US government contractors were targeted in the areas of technology, telecommunications, energy and manufacturing[579]. In 2020, APT 31 and the Iranian APT35 were reported to target the US election campaign[580].
- *Mustang Panda*/*Bronze President/HoneyMyte/RedLich* and *Red Delta* Vatican networks were infiltrated by Chinese hackers before the beginning of 2020 talks with China about religious matters. Also, the Catholic Church of Hong Kong was affected. The APT *Red Delta* was assumed to do the attacks[581]. This Group has technical overlaps with the *Mustang Panda* Group which is active since 2017 for example on Mongolian-speaking individuals.

[571] PwC/BAE Systems 2017, p.14
[572] Van Dantzig/Schamper 2019
[573] FireEye 2022
[574] FireEye 2022
[575] FireEye 2022
[576] FireEye 2022
[577] Threat Connect 2016
[578] FireEye 2015
[579] FireEye 2017
[580] SZ 2020
[581] Sanger/Wong/Horowitz 2020

## *5.6 North Korea*

### 5.6.1 The Lazarus group (BlueNoroff, Andariel, Hidden Cobra, Zinc)

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[582]. 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*[583]*,* also known as *BlueNoroff*. The group permanently expands its malware, such as the Trojans *Hangman/Volgmer* in 2014 and *Wild Positron/Duuzer*[584] in 2015.
In summer 2016, the *Lazarus Group* was discussed to be behind the attacks on the SWIFT interbanking system, see below.

However, the *SPE hack* was one of the most controversial debates in the cyber attribution history, resulting from unexpected facts like the initial request for money, data distribution from outside of North Korea etc. etc.[585][586]. Also, the mix of cyber espionage and suspect cyber-criminal activities like the attack on the Interbanking system SWIFT was irritating[587].
However, most of the contradictions could be resolved, if the following assumptions are correct:
1. The *SPE hack* was initially a cyber-criminal activity which was escalated to political matter at a later stage. This would match the communication and attack pattern.

[582] Novetta 2016
[583] Novetta 2016
[584] Guerrero-Saade/Raiu 2016, p.2
[585] Fuest 2014b, p.31
[586] The Security Ledger online 2014, p.1
[587] Brächer 2016, p. 26-27

2. The *Lazarus* group has a core of state-linked hackers which coordinate hackers in South East Asia. This would explain obscure findings like the long work times, the attack locations, overcome the issue of limited network capacities etc.

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[588]. 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[589]. 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[590].

Two other specialized groups could be assigned to the *Lazarus* group, this is *Bluenoroff*, which focuses on foreign financial institutions, while the *Andariel group* has been concentrating on South Korea targets since at least May 2016, including bank cards, online poker and other gaming sites[591].

#### 5.6.1.1 Wiper Malware Attacks

On 15 August 2012, the Saudi-Arabian Oil company *Aramco* was attacked the *Shamoon/Disttrack* malware which is meanwhile assumed to come from the Iranian APT33; 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[592]. The commercially available software *EldoS RawDisk*[593] 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[594].

[588] Novetta 2016
[589] Guerrero-Saade/Raiu 2016
[590] Guerrero-Saade/Raiu 2016, p.6
[591] Kim 2017
[592] 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
[593] Baumgartner 2014, p.2, 4
[594] Darnstaedt/Rosenbach/Schmitz 2013, p.76-80

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[595] (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 cover state-driven activities or as proxies for states[596], these were *Cutting Sword of Justice* (Aramco), *Whois/NewRomanic Cyber Army Team* (for *Darkseoul* hack[597]) 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[598].
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[599]. 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[600]. 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.

#### 5.6.1.2 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[601].

---

[595] As already mentioned earlier, Iranian oil terminals were already attacked with Wiper Malware in April 2012
[596] McAfee 2013
[597] 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.
[598] Novetta 2016
[599] See e.g., Baumgartner 2014, p.4-6
[600] Novetta 2016, p.15
[601] McAfee 2013, p.28

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 and 2011[602]. 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[603].

### 5.6.1.3 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[604] and in December 2014, Sony was hacked by the Group *Lizard Squad*[605][606].

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[607].
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 [608]
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[609].

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

[602] Symantec 2013, p.1-2
[603] Leyden 2014, p.1-3. KHNP confirmed that no critical data were leaked and initiated cyber exercises to enhance security.
[604] Lambrecht/Radszuhn 2011, p.25, Betschon 2014, p.34
[605] 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.
[606] Handelszeitung online 2014, p.1
[607] Fuest 2014b, p.31
[608] Betschon 2014, p.34
[609] Steinitz 2014, p.11

provider in North Korea was *China Unicom*[610]. 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.[611] At Christmas 2014, the movie *The Interview* was then published in a limited number of cinemas. Furthermore, 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[612].

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[613]. 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[614]. Also, the *Sony Hack* and other attacks on South Korea used a common command and control server located in Bolivia[615]

Moreover, North Korea's primary intelligence agency, the *General Reconnaissance Bureau* was reported to have certain cyber capabilities, in particular two units called *Unit 121* and *No. 91 office*. Das *General Reconnaissance Bureau* was founded around 2009-2010 to pool cyber activities.[616]
There are a few reports that due to the limited internet structure persons of these units may work outside North Korea[617]. This would match the findings of a recent report that North Korea has meanwhile several specialized units, amongst them *Unit 180* for cyber operations in the financial sector. Cyber specialists would operate from abroad such as China and Malaysia to block attribution and to utilize the larger internet infrastructure[618]. The Russian company *Russian TransTeleCom* has been providing 60% of North Korean Internet traffic since October 2017, while the only previous Chinese provider *China Unicom* continues to provide 40%. It is estimated that North Korea still does not have much more than 1000 internet connections abroad[619].

[610] 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
[611] SZ2014b, NZZ 2014
[612] Zoll 2015, p.1
[613] 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.
[614] Fuest 2014b, p.31
[615] Robertson/Lawrence/Strohm 2014, p.1
[616] FAZ 2017d, p.6
[617] Robertson/Lawrence/Strohm 2014, p.2
[618] Park/Pearson 2017
[619] Reuters 2017c

Also, it was argued that North Korea had a reasonable political motive[620], but North Korea strongly denied any involvement in the attack[621].

Alternative theories were discussed, because initially intruders asked for money[622] 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[623]. 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[624]. 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[625][626].

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[627]. Thus, the FBI kept its conclusions on the attack origin[628]. 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 initially not officially confirmed[629][630].

#### 5.6.1.4 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 Dollar from the central bank of Bangla Desh to other accounts on 04 Feb 2016[631]. 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

[620] Fuest 2014b, p.31
[621] NZZ 2014
[622] Fuest 2014b, p.31
[623] See SZ 2014c, Bernau 2014, p.1
[624] The Security Ledger online 2014, p.1
[625] See e.g., Bernau 2014, p.1
[626] 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).
[627] Zoll 2015, p.1
[628] SZ 2014c
[629] 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
[630] FAZ 2017d, p.6
[631] Brächer 2016, p. 26-27

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[632]. Meanwhile, more cyber-attacks on SWIFT were reported for banks in Ecuador, Russia, Ukraine and Vietnam[633]. The wiping code used to hide the bank hacks was the same used in the SPE attack[634]. In 2021, the *US Department of Justice* reported that the Swift attacks took even longer from 2015 to 2018 and included also Malta, Taiwan, Mexico and Africa[635].

The SWIFT interbanking attack is of particular importance, because meanwhile it appeared that both the *Lazarus* group and *Carbanak*-related hacks **attacked independently** the same target. The wiping code used by the Lazarus group to hide the bank hacks *was the same* used in the SPE attack[636], while the latter used a new malware *Odinaff*[637].
The *Polish Financial Supervision Authority* was hacked to use their website as watering hole for visitors, the campaign started in October 2016, apparently conducted by the *Lazarus/BlueNoroff Group* and detected in Feb 2017[638].
2017 *BAE Systems* reported, that the *Lazarus Group* seemed to be responsible for taking 60 million $ from the Taiwanese *Far Eastern International Bank*[639].

### 5.6.1.5 The WannaCry/Wanna Decryptor and Adylkuzz Attack

As already mentioned earlier, on 14 April 2017 further tools were released by the *Shadow Brokers* including *DoublePulsar, EternalBlue* and *EternalRomance*, which then were used presumably by other actors for preparation of three major cyber-attacks called *WannaCry/WanaDecryptor 2.0*, *Adylkuzz* and *Petya/Not-Petya/Petya2017.*
Already on 24 April 2017, 183,107 computers were infected with *DoublePulsar* according to Binary Edge[640].
Initially, little public attention was paid to this phenomenon, despite at the same day (24 Apr 2017), the *Adylkuzz* malware attack started[641]. This malware checked computers for a pre-existing infection with *Double Pulsar* and if not, an infection with *EternalBlue* was conducted, if possible[642].
This allowed the creation of a botnet for **virtual money mining**.

---

[632] Storn 2016, p. 29
[633] FAZ 2016b, p.23, Storm 2016
[634] Storm 2016
[635] DoJ 2021a
[636] Storm 2016
[637] Symantec 2016c
[638] Kaspersky 2017a
[639] Boey 2017
[640] WinFuture 2017
[641] PandaSecurity 2017
[642] Kling 2017a

**Virtual money**, such as bitcoin, is created by a sequence of complex calculations which are mathematically linked to the previously created bitcoins, a validation method known as **blockchain**. As a relevant calculation effort is required, those who calculate a new bitcoin are the owners of the new bitcoin. In summary, bitcoin mining is the calculation effort for creating new bitcoins.
The unauthorized use of target computers for bitcoin mining is also known as **cryptojacking** or **collective mining**. In 2017, a wide -spread mining malware was *Coinhive*[643].

*Adylkuzz* now uses infected computers for mining, but transfers the outcome to the control server, is hereby stealing the virtual money from the creating computers. Virtual money is also known as **digital money** or **crypto currency**. As for mathematical reasons the maximum of bitcoins will be limited, further types of virtual money are under development.

**Crimeware** is malware to support cybercrimes. 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*[644].

On 12 May 2017, mass infections of more than 200,000 computers in over 150 countries started with the ransomware *WannaCry*. It was also called *WannaCry 2, Wanna Decryptor 2.0, WanaCrytOr 2.0* and *Wanna Decryptor 2*[645]. Like *Adylkuzz*, this malware checked computers for a pre-existing infection with *Double Pulsar* and *only if not* infected with *DoublePulsar* already, an infection with *EternalBlue* was conducted, if possible[646]. This may have contributed to the rapid mass infection despite the *EternalBlue* exploit was closed by Microsoft already after a warning from the NSA in a patch day in March 2017[647].

[643] Betschon 2017
[644] 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 are 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.
[645] Bodkin/Henderson 2017
[646] Lee et al. 2017
[647] Perloth/Sanger 2017

The ransomware spread was blocked by registering and activating a hard-coded IP-domain by an IT-researcher which was mentioned in the malware code, because its activation induced a pre-programmed stop of the malware spread[648].
Analysis showed that *WannyCry* had remarkable similarities to a functionality of a Trojan used in SWIFT attacks. [649] Technical overlaps were found to the SPE and SWIFT hack, also to the Poland bank attack of Feb 2017 [650].

After the attack, it was discussed why so many old Windows systems are still active, as in particular *Windows XP* was vulnerable. However, often Windows systems are embedded in an institution-specific digital ecosystem of applications and updates bear the risk of damage or collapse which creates in reality high hurdles for system renewal[651].

Phishing emails from North Korea spread a malware that uses an Adobe Flash player gap, according to the *South Korean Computer Emergency Response Team (CERT)* [652].
In one case, bitcoin mining had overstretched the attacked server, so a trace could be secured to North Korea. In addition to Bitcoin mining activities, digital money exchange platforms are increasingly attacked. The damage was estimated by the British intelligence service GCHQ at up to 1 billion dollars per year[653].

In an attack on the Japanese stock exchange *Coincheck* in 2018, 523 million units of the cryptocurrency *XEM* were stolen with an estimated value of 430 million Euros, the attackers could not yet be identified. The money was in a "hot" exchange platform connected to the internet, instead of safer storage in an offline "cold" exchange platform[654].

South Korea's *Coinrail* crypto exchange platform lost 31 million euros in a hacking attack in 2018[655]. Smaller currencies such as NXPS were affected. The money was not secured in a cold wallet, i.e., the money was directly accessible from the Internet.

The security firm *Proofpoint* reported in 2018 on the mining botnet *Smominru*, which also exploits the *EternalBlue* exploit on Windows servers and uses about half a million computers for crypto-mining. Since May 2017, around 8900 units of the

[648] Bodkin/Henderson 2017
[649] O'Neill/Bing 2017
[650] Perloth/Sanger 2017
[651] Steier 2017
[652] Kant 2018
[653] Freidel 2018
[654] Welter 2018, p.8
[655] FAZ 2018f

cryptocurrency *Monero* have been generated, which at the beginning of February 2018 corresponded to about 24 Monero *per day* = about $ 8900 *per day*[656].

#### 5.6.1.6 The Park Jin-hyok indictment from 2018

Experts from *Mandiant* (the same firm which analyzed APT1) supported the FBI investigation on the Lazarus group. A fake person called Kim Hyon Woo used the accounts of the government-owned *Chosun Expo* company and was identified as Park Jin-hyok, believed to be a North Korean intelligence officer for the *Lab 110* of the military intelligence RGB[657]. He used a set of email accounts with the cover name Kim Hyon Woo which were accessed by computers who were utilized in multiple attacks of the Lazarus group, e.g., the *SPE hack*, the *Lockheed* attacks and the attack on the Bangladesh Central Bank.[658] North Korean-owned IP addresses were used as command-and-control address for various malware samples, e.g., for the attack on *Lockheed Martin*[659].
Among further issues, a code snippet re-usage and the use of FakeTLS were noted. The **Transport Layer Security TLS** is a cryptographic protocol and FakeTLS mimics authentic encrypted TLS traffic, so intrusion detection systems do not react. This was used in *WannaCry, Macktruck (SPE hack), Nestegg* and *Contopee* (Banking attacks in Asia) etc. [660] Moreover, multiple technical relations to *Destover*, the *Brambul* worm and *Wannacry* exist[661].

#### 5.6.1.7 Fake Cryptocurrency Platforms

The *Lazarus Group* is still active in 2020. Meanwhile, they have set up faked cryptocurrency trading groups looking similar to those present on *Telegram* to lure victims. *Lazarus* now tries to execute attacks via memory than putting malware on the hard disk to remain undetected[662].

A new strategy was reported in 2022. According to the FBI, *Lazarus* und *APT 38* were responsible for stealing approximately 620 million Dollar cryptocurrency from online game *Axie infinity* where players can earn crypto money by gaming or trading their avatars[663].
In this game, the Vietnam-based firm *Sky Marie* used the *Ethereum* blockchain which is secure, but slow. To allow Axie gamers to sell and buy more quickly, the firm created an in-game currency with a link, the *Ronin bridge*, to the main

[656] Beiersmann 2018a
[657] Cimpanu 2018
[658] Shields 2018, p.6, 134 and 138
[659] Cimpanu 2018, Shields 2018, p.13
[660] Cimpanu 2018
[661] Shields 2018, p.56
[662] The Next Web 2020
[663] France24 online 15 April 2022, Gollmer 2022a

*Ethereum* blockchain which was less secure. The attackers took over 5 of 9 validation nodes for transactions which allowed them to do transactions on their own and 173,600 *Ethereum* units were stolen.

Overall, cryptocurrency theft is meanwhile a global business, a study from *Chainalysis* estimated the amount of stolen currency for 2021 equal to 14 billion US-Dollars[664].

### 5.6.2 APT37 and APT 38

With respect to North Korea, *FireEye* has noted a differentiation of activities within the *Lazarus Gr*oup which led to the emergence of two new APTs 37 (also known as *Reaper, Ricochet Chollima, Group 123* or *Scarcruft*) and APT 38, which both have specific tactics, techniques and procedures and thus a specific profile. Both APTs are specialized on the financial operations, but APT 38 is unique in destroying evidence or victim networks as part of their operations[665].

## *5.7 South Korea*

### 5.7.1 Dark Hotel/Tapaoux

This APT is currently assumed to be located in South Korea[666]. Until now, it is not clear whether this is a nation-state actor, but *DarkHotel* conducts sophisticated economic espionage campaigns.
The group is also known under many other names: *Dubnium, Fallout Team, Karba, Luder, Nemim, Nemin, Tapaoux, Pioneer, Shadow Crane, APT-C-06, SIG25, Tungsten Bridge, T-APT-02*[667].

The APT *DarkHotel* started in 2007 and conducted targeted spear-phishing spyware and malware-spreading campaigns against business hotel visitors, in particular senior executives in luxury hotels in US and Asia, through the hotel-offered WiFi network.

In 2020 as part of the Corona crisis, they tried to break into the *World Health Organization* in March 2020 by password stealing[668]. An overlapping attack method with the Russian APT29 is the use of *SoreFang* malware against *SangFor* devices.[669]

---

[664] Gollmer 2022a
[665] FireEye 2018a
[666] Malpedia 2020
[667] Malpedia 2020
[668] Satter et a. 2020
[669] NCSC 2020

## *5.8 Iran*

### 5.8.1 Pioneer Kitten/Fox Kitten/Parisite

According to Western reports, Iran's cyber sector is rapidly evolving from an organizational perspective as well as with respect to TTPs and malware families.
The current assumed structure is[670]:
The APT *Pioneer Kitten* is breaching into networks. The access is then handed over to the *APTs 33 to 35* which are described below. They expand and stabilize the access. The data gained by *Pioneer Kitten* und the other APTs are then distributed as follows: Strategically important accesses remain in the hands of the other APTs, while the remaining access data are handed over to *Pioneer Kitten* who started selling them to other hackers on respective platforms since July 2020[671].

### 5.8.2 APT33/Elfin Team/Refined Kitten/Magnallium/Holmium/Cobalt Trinity

*FireEye* reported 2017 a new APT numbered APT33 linked to the Iranian government supported by findings that tools like *Nanocore*, *Netwire* and *AlfaShell* are typically used by Iranian hackers, present on Iranian hacking websites and other Iranian cyber actors[672]. The *Dropshot* (also known as *Stonedrill*) malware is used to establish the *Turnedup* backdoor which then is sometimes used to the destructive malware *Shapeshift*, which can be configured to delete files, erase volumes or to wipe disks. *Dropshot* and *Shapeshift* had some Farsi language artifacts.

A man from APT33 with the cover identity *xman_1365_x* could be linked to the *Nasr Institute*, which is suspected by US to be equivalent to *Iran Cyber Army* and which also was suspected to have conducted attacks on US financial institutions from 2011-2013 in an operation called *Ababil*[673]. APT33 attacks were now registered in US, Saudi-Arabia and South Korea with focus on firms who work with the military sector and the energy-petrochemical sector.

A link to the *Shamoon* attack some years ago could initially established, but evidence was growing: *Shamoon* focused on government targets and had elements of Arab-Yemenite language, while *Dropshot* targeted on commercial organizations with Farsi language references. The fact that both attacked Saudi-Arabia, used wipers and anti-emulation techniques was initially not enough evidence. But then technical similarities between *Shamoon* and *Shapeshift* were shown.

---

[670] Uchill 2019
[671] Jung 2020
[672] O'Leary et al. 2017
[673] O'Leary et al. 2017

The *Shamoon* malware was updated and meanwhile *Shamoon-3* is existing[674]. The first version was used in 2012 against *Aramco*, while in 2016 and 2017, upgraded *Shamoon* v.2 and *Stonedrill* wipers were used[675]. In 2018, *Shamoon-3* was used against the Italian oil and gas contractor *Saipem*'s networks. Also, it was used in supply chain attacks.

In February 2020, the US authority FBI released a warning that the *Kwampirs* remote access trojan (RAT) would be used to target companies in the healthcare, energy, and financial sector, but also those supporting Industrial Control Systems (ICS) for global energy generation, transmission, and distribution.[676]
Originally, *Kwampirs* was observed in 2018 and was used by a group called *Orangeworm*, which is active since 2015.
However, despite *Kwampirs* has no wiper function, the forensic analysis of the FBI noted various numerous other technical similarities to *Shamoon*[677].

### 5.8.3 APT34/Helix Kitten

A further Iranian APT is APT34, which operates since 2014 and is using Iranian infrastructure which led to the attribution to Iran and which is possibly identical to the Group *OilRig*. The focus is on strategically relevant companies in the Middle East. They used a specific set of tools (*Powbat, Powrunner, Bondupdater*) to use a meanwhile patched *Microsoft Office* exploit[678]. A similar strategy is used by the *APT39/Chafer*, which is also active since 2014 and which uses a modified *Powbat*-Version[679].

The *US Department of Justice (DOJ)* announced a large-scale attack on 320 universities in April 2018, including 23 universities in Germany, where papers, dissertations and conference reports were published[680]. First the University of Göttingen was attacked, then 22 further universities in Hesse and North Rhine Westphalia with phishing mails and faked library portals. An Institute called *Mabna* in Tehran ran the website *Megapaper*, where the files were found.

[674] PaloAlto2018
[675] Osborne 2018
[676] Cimpanu 2020
[677] Cimpanu 2020
[678] FireEye 2018
[679] FireEye 2019
[680] Diehl 2018, p.58-59

### 5.8.4 APT35/Charming Kitten/Phosphorus/Newcaster/Cleaver

The group is also known under many other names: *Operation Cleaver, Tarh Andishan, Alibaba, 2889, TG-2889, Cobalt Gypsy, Rocket_Kitten, Cutting Kitten, Group 41, Magic Hound, TEMP.Beanie, Ghambar.*

This APT targets entities in the government, energy, and technology sectors that are located in or do business with Saudi Arabia. On 27 March 2020, newspapers reported that Microsoft was able to take over and shut down 99 domains of this group. In 2020, APT 35 and the Chinese APT31 were reported to target the US election campaign[681].

### 5.8.5 APT39/Chafer

Like APT34, the *APT39/Chafer*, which is also active since 2014, uses a modified *Powbat*-Version[682]. Activity areas are telecommunication and travel industry (which may indicate surveillance of certain individuals) and government units in the Middle East.

## *5.9 France*

### 5.9.1 Animal Farm/Snowglobe

The APT *Animal Farm/Snowglobe* has targeted a wide range of global organizations since at least 2009[683]. Unexpectedly, Bernard Barbier, the former head of signals intelligence (SIGINT) at France's foreign intelligence agency (DGSE) confirmed in a speech in 2016 that France was behind *Animal Farm*[684].

## *5.10 Spain*

### 5.10.1 Weevil/Careto/The Mask/Ugly Face

In February 2014, another cyber-attack was reported by *Kaspersky Labs*[685]. The APT *Weevil (Careto/The Mask/Ugly Face)* was able -amongst other many functions- to record Skype VoIP talks and is known to be active since 2007[686]. Careto is a Spanish slang term for mask. As in various other sophisticated cyber-attacks, only a few computers were infected, but the profile of the targets is quite

[681] SZ 2020
[682] FireEye 2019
[683] Malpedia 2020
[684] CFR 2016
[685] Kaspersky 2014
[686] CFR 2019, Malpedia 2020

typical: research units, providers of critical infrastructures, diplomats, embassies and political activists in more than 30 countries. Despite the sophisticated modular approach that has been seen in *Flame* and *Regin*, a clear link to *Equation Group* could not be shown, the origin remained unclear. Meanwhile, it is assumed to be located in Spain[687].

## *5.11 Vietnam*

### 5.11.1 APT32/Ocean Lotus Group

*APT32/Ocean Lotus Group* is a presumably Vietnamese APT which was reported to have a focus on companies with business in Vietnam. Social engineering is used to deploy *ActiveMime* files and malware such as *Soundbite*. [688] The group seems to be active since 2012.
A state-backed APT called *Bismuth* which is at least similar to APT32 deployed malicious coin miners in 2020 in the French private sector and government for the virtual currency *Monero*[689].

## *5.12 Cybercrime groups*

Large Cybercrime groups are the *Carbanak group,* the *Avalanche* ransomware botnet, *EvilCorp/Dridex,* the *Emotet* malware platform, REvil, Darkside and Ransomware-as-a-service (RaaS) groups.
*Kaspersky Labs* identified in 2017 8 groups specialized on ransomware attacks, such as *PetrWrap* and *Mamba*. *PetrWrap* attacks financial institutions, and aimed to encrypt very important files to enhance effect and willingness to pay[690].

### 5.12.1 Carbanak/Fin.7

Also, one of the largest known cybercrime activities, the theft of 1 billion Dollars in total from 100 bank institutes worldwide by the *Carbanak group* was done in that way[691]. Also, they took over the video surveillance and could inspect the institutes before proceeding[692].
The *Carbanak* group used lateral movement to escalate access to banking networks. Despite massive efforts e.g., of the Russian authorities to imprison the group members, residuals of the group continued attacks by attacking SWIFT the *Odinaff* malware in 2016. They used domains with **difficult to-track registration** for their

[687] CFR 2019, Malpedia 2020
[688] FireEye 2017
[689] Kundalia 2020
[690] Scholl-Trautmann 2017
[691] Bilanz 2015, p.50-57
[692] Kaspersky Lab 2015c, p.1

activities. Also, the group intruded hotels to gain information from visitors, in 2018 three members were officially accused for these activities[693].

### 5.12.2 Avalanche

The ransomware-releasing botnet *Avalanche* used the fast-flux technology to avoid detection. Finally, sinkholing allowed catching 130 Terabyte of data. The analysis of this data allowed law enforcement authorities to stop the botnet and to put the *Avalanche* group members into prison. The cooperation of the German *Bundesamt für Sicherheit in der Informationstechnik BSI*, the research unit *Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, The German Police, Europol*, *Eurojust*, the *FBI* and the security firm *Symantec* made this possible despite the misuse of 800,000 (!) domains[694].
Avalanche also took advantage of the drive-by-exploit *Andromeda*, which was still widespread after the coup against *Avalanche*; however, FBI, Europol and other investigators from 25 countries were able to close the *Andromeda* network by the end of 2017[695].

### 5.12.3 EvilCorp/Dridex/Indrik Spider/TA-505

The French CERT group released an in-depth analysis of the *EvilCorp* Group and its lead malware *Dridex* in July 2020[696].
Around 2005-2006, Mr. Bogachev (alias *Slavik, lucky12345*) created the trojan *ZeuS* (alias *Zbot*) which was then used by various groups. For online banking attacks, he created then the malware *JabberZeuS* and cooperated with a cyber crime group called *Business Club*. Hundreds of *ZeuS* variants are known meanwhile. *Business Club* members launched the *GameOverZeuS (GoZ)* botnet with the malware *Cryptolocker*, the FBI was able to shut this down in 2014.
In the same year, *Business Club* members initiated the *Dridex* malware as update version of the older malware *Bugat*, but again, FBI could interfere by arresting an important operator. The *Business Club* however remained active as *Evil Corporation (alias EvilCorp, Indrik Spider)*, headed by Mr. Yakubets, and released further malware, e.g., the ransomware *Bitpaymer* (alias *FriedEx*) which hit a hospital of the *British National Health Service (NHS)*.
In a joint indictment from 05 Dec 2019, the *US Department of Justice* and *Britain's National Crime Agency* identified nine members of *EvilCorp* and said that the group has stolen more than 100 million US-Dollars[697].

[693] Langer 2018a
[694] EUROPOL 2016
[695] Zeit online 2017
[696] CERT France 2020
[697] Fox Business 2019

### 5.12.4 Emotet

The inconsistent activity pattern of actors using the *Emotet/Geodo* malware indicates that *Emotet* is used my multiple groups, cyber criminals as well as nation-state actors. This would then be similar to the history of the *BlackEnergy* malware which was originally developed as crimeware, but then modified and also used by nation state actors. However, there may be links to *EvilCorp* (note the relations to *Bugat* and *Dridex*).

*Emotet* was used by the cyber crime group *Mummy Spider (TA542, Gold Crestwood, Mealybug)*[698] and shared code with the above-mentioned *Bugat/Feodo* malware that was also the precursor of *Dridex*.
*Emotet* got functions for reconnaissance, C2 communication and ability to load other banking trojans such as *Qakbot* and *Dridex*. *Emotet* was offered 2015 in underground forums. *Emotet* sometimes has activity breaks and returns then again, it is still active[699].

In 2020, *Emotet* was used for a high-level espionage attack on the German Army Transportation Service (*BW Fuhrparkservice*) which is responsible for transportation of parliament members. In the previous year, 142.000 transports were made, so that sensitive data of politicians and army members may have been hacked.[700]

In 2021, *Europol* was able to take over the three main servers and to destroy the *Emotet* infrastructure. They used them to send updates to 18,000 victim computers to inactivate the malware. Of course, as *Emotet* is on the black market, it can return as tool from other groups[701].

### 5.12.5 Ransomware-as-a-service (RaaS) groups

A new phenomenon of the 2020ies is the appearance of Ransomware-as-a-service (RaaS) groups. In the RaaS business model, the developers only create the ransomware and sell it then for a provision of 10-20% to the attacker groups.
*BlackCat,* also known as *AlphaV, ALPHV, AlphaVM, ALPHV-ng* or *Noberus*, is a ransomware family written in the easy-to-modify *Rust* language and is used as RaaS. To increase the pressure to pay ransom, the malware can also delete volume shadow copies[702].
The mineral oil traders *Oiltanking* and *Mabanaft* were hit and oil terminals in Rotterdam and Antwerpen were shut down.

---

[698] Malpedia 2020, Wikipedia entry Sep 2020
[699] Proofpoint 2020
[700] Tagesschau online 2020
[701] Mäder 2021a, Tagesschau online 2021
[702] Mäder/Hosp 2022

Other widespread RaaS malware types are now *Quantum* and *Emotet*.
Ransomware attacks can affect everybody: the widespread open-source protocol Log4j which is used worldwide was vulnerable for insertion of malware like *Khonsari*, a compact ransomware written in .NET and targeting Windows servers, but a security patch could be implemented then[703].

### 5.12.6 REvil/GandCrab and Darkside/Colonial hack

The *REvil* group is likely the successor of the *GandCrab/Pinchy Spider/Sodinokibi/Sodin* group in 2019. A probable relationship to the group *Darkside* is under discussion[704]. *REvil* and *Darkside* exempt certain countries, in particular Russian-speaking users from their activities. *Darkside* also uses Russian IP addresses[705].
A new strategy is the **double extortion**: before the ransomware is applied, confidential data are stolen from the victims. If the victim is not willing to pay for unlocking the computer from the ransomware, the data are published.
For this purpose, *REvil* has the website *Happy Blog*, where everybody can bid for the confidential data from 50,000 US Dollar on[706]. In 2021, they attacked the US IT service provider *Kaseya*[707].

*Darkside* is a Russian-language program offering ransomware-as a-service (RaaS) and was responsible for the *Colonial pipeline* hack which resulted in a shutdown of a very important US pipeline on 07 May 2021. This pipeline transports 45% of the East Coast fuel supply. The day before the ransomware was activated the attackers stole a large amount of data from the company. Colonial was forced to pay ransom of almost 5 million Dollars on 08 May 2021.[708]

But the *US Department of Justice DoJ* was able to seize 63.7 bitcoins currently valued at approximately $2.3 million of the ransom in June 2021 and also to catch some servers from *DarkSide* by consequent use of the “Following the money” method as a basic and powerful tool[709]. The DoJ announced that the United States will continue to deter and to disrupt the ransomware ecosystem.

Further Russian groups are active, e.g., the *Conti* group that declared to be patriotic and then attacked not only the *Technical University Berlin*, but also the Western investigation platform *Bellingcat*[710]. The *Killnet* group attacked Norway in 2022[711].

---

[703] Benrath 2021
[704] Krebs on Security 2021b, Da Silva 2021
[705] NZZ online 2021
[706] Da Silva 2021
[707] Von Petersdorff/Finsterbusch 2021
[708] NZZ online 2021, New York Times online 2021
[709] DoJ 2021b
[710] Barker/Tiirmaa-Klaar 2022, Kaufmann 2022a and 2022b
[711] Kirschbaum 2022

### 5.12.7 Smart Contract Hacking/51% attacks

*Ethereum* is a virtual currency whose transactions are tied to execution orders that are **smart contracts**. Execution takes place via a decentralized peer-to-peer network of so-called miners, who profit from the transfer by execution costs called '*gas*'. *Ethereum* can be divided into the smallest units, called *wei* (1 ether = $10^{18}$ wei), which ensures precise execution[712].
Smart contract hacking has already caused damages of up to $ 60 million on a single contract. In the so-called *DAO attack,* a crowdfunding platform was damaged by this amount on 18 June 2016. In simple terms, the attack generated an infinite loop of bookings until the money was gone[713]. There are numerous other vulnerabilities that can affect the contracts, the 'gas', the addresses, and so on.

A new attack method are **51 %-attacks**. The crypto currency miner is using enough computing power to take over the majority of calculation power within a crypto currency system for a certain time (which may be very expensive and complicated for bitcoin, but not for smaller crypto currencies). In this situation the attacker can make payments from the blockchain, but then re-create the block chain without these payments (resulting in a **blockchain fork**). The dominant computer can then implement the falsified blockchain as authoritative version, so that future transactions will use this altered blockchain[714].

The cryptocurrency trading platform *Beanstalk* created a system where the users had shares equal to the invested money. In 2022, unknown hackers leased 1 billion dollars from other sources as flash credit, then they appeared as investors which gave them immediately a two-third majority. This allowed them to transfer the entire money of the trading platform, in total 182 million Dollars, to themselves. Then, they paid back the credit, the estimated net win should be still around 80 million Dollars. The execution of the operation took 13 seconds[715].

[712] Atzei/Bartoletti/Cimoli 2016
[713] Atzei/Bartoletti/Cimoli 2016, p.14
[714] Orcutt 2019
[715] FAZ 2022

# 6. Cyber Defense and Intelligence

## *6.1 Cyber defense*

### 6.1.1 Introduction

Cyber defense can be done on various levels in parallel, as shown below:

| Level | Approach |
|---|---|
| User | Regular updates, careful file handling, virus protection, spam filters, secure passwords, 2-factor authentication with password and a physical device, data encryption, firewalls (control of network access)<br>Research: Key pressing duration and strength and mouse movement patterns as unique individual identifiers |
| Organization | Whitelisting, segmented networks, need-to-know principle, four-eyes-principle for admins |
| Security firms | Threat Intelligence, Intrusion Detection, Penetration Testing, Honeypots, Sandbox Analysis, Data/Knowledge combination |
| Cooperation | Intelligence (e.g., 5-/9-/14-eyes), Police (Europol/FBI), European Cybersecurity (ENISA), Cooperation for Critical Infrastructures, Charter of Trust and so on… |
| Legal | Criminal and liability regulations, safety standards |
| Technology | e.g., DDoS-defense: redirect data traffic, involve provider, switching off own IP, blocking foreign IP (geoblocking), slowing down (tarpitting)<br>One-way street technologies: campus networks (data out, but not in), data diodes (in, but not out) |

Cyber defense starts with yourself as a user, but also at the level of the organizations, the use of cybersecurity companies, by cooperation of authorities and companies, by legal measures and in case of data overload also with purely technical means.

For the users, the most important thing is always to keep their system up to date and to be wary of unclear emails. For password security, a password should not be too simple, but not too short. When in doubt, the most important thing is not to be misguided by curiosity, even if that is sometimes difficult. Organizations may, inter alia, apply **Whitelisting**, i.e., what has not been explicitly allowed by IT is forbidden on company computers, it may make sense to separate important network sections, limit the access of the employees to the most necessary (**need to know**), administrators can monitor each other during important interventions.
Security firms can use Threat Intelligence to match attacks with attack pattern databases, but also use **Intrusion Detection** to scan traffic for unusual events and statistical issues.

**Threat Intelligence** repositories compare incoming information with known IP-addresses, domain names, websites and also with lists of known malicious

attachments[716]. This allows immediate detection and sometimes even attribution of an incoming attack. Newly discovered malware can be integrated with so-called **Indicators of Compromise IOC**, i.e., numbers that allow detection in a certain computer.

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[717]:
The **Continuous Diagnostics and Mitigation (CDM)** program provides real-time capacity to sense anomalous behavior and to create reports to administrators on a dashboard.
**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[718].

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[719]. 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.

Administrators can test system security by hackers as **penetration testers**, or lure foreign hackers through **honey traps**, seemingly vulnerable computers, to analyze their actions. One can run detected malicious programs in virtual environments, the

[716] The company *Crowd Strike* uses a kernel sensor (*Falcon host*) deployed on Windows and Mac servers, desktops, and laptops that detect attacks and compare them with a threat intelligence repository for attribution.
[717] Gerstein 2015, p.4-5
[718] Welchering 2014b, p. T4
[719] Beuth 2016a, p.1-3

so-called **sandboxes**, to understand their function and finally, which is more common, combine knowledge.
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[720], 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.

Cooperation may happen, to name just a few examples, e.g., between the intelligence services, with Germany being one of the wider groups of 14-eyes in the US system. The police closely cooperates via *Europol* with the FBI, the Europeans in the *network agency ENISA*, German companies and authorities in the *Working Group for Critical Infrastructures (AK KRITIS)* and large German companies have joined forces to establish safety standards for suppliers in the *Charter of Trust*.

An important progress is the formation of further large **Cyber alliances**, e.g., the *Cyber Threat Alliance* of the security firms *Fortinet, Intel Security, Palo Alto Networks* and *Symantec* to fight against ransomware. More and more private security firms merge collected data and do-long-term analyses to identify certain groups. Examples are the large forensic Operations *SMN* and *Blockbuster*, more details will follow below. 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. Also, large private companies coordinate their cyber defense.

### 6.1.2 Defense against DDoS attacks

General recommendations against DDoS attacks were given by the German IT security authority BSI[721]. 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 and re-routed, 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.

[720] Dohmen 2015, p.75
[721] BSI 2012

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.

### 6.1.3 Automated Cyber Defense

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[722]. The research budget for Plan X was 110 million US-Dollars.

The **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[723].
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 [724]

*DARPA* was satisfied with the results; it was a first step forward to an automated defense and response system[725]. As the number of vulnerabilities is meanwhile immense[726], 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 computer to get inactive or misconstructed patches may slow down the defense system.

[722] DARPA 2012, Nakashima 2012b
[723] DARPA 2016
[724] Atherton 2016
[725] DARPA 2016
[726] 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

## *6.2 Human Intelligence*

The identification of an attacker is sometimes out of reach for digital attribution methods. Human intelligence methods can help to find the missing link.

The following methods are most important in the practice of attribution:

- Cyber intelligence
- Intelligence cooperation for information exchange
- Conventional intelligence.

### 6.2.1 Cyber intelligence

Cyber intelligence can use a broad range of methods (see also Section 2):
In military sector, *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[727]. As an example, the NSA put implants into Iranian networks (*Nitro Zeus*) [728] and as described above into Russian networks as a warning sign.

**Hack the hackers:** If the attackers are identified, it may make sense to intrude them to find out more about their activities.

**Data analysis:** large server farms can also be used for analysis of large data volumes, also known as **big data**. As shown earlier, the main problem is not to gain information, but to store[729] 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, the terrorist network involved in the Madrid 2004 attack could be represented by analysis of connection data[730].
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[731].
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[732]. More than 90% of the BND search terms

[727] Sanger 2015, p.5
[728] Gebauer 2016, p.17
[729] The storage volume discussed for the NSA data center in media is in Yottabytes, this is $10^{24}$ bytes, Juengling 2013, p.52.
[730] Hayes 2007. The network identification is also known as **community detection.**
[731] Tomik 2013a, p.6
[732] Amann 2013, p.17

are formal terms such as telephone numbers, email- or IP-addresses of users or companies under suspicion[733].

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[734]. 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[735].

Another approach is the **digital dust analysis**. If in Russia or China a new US embassy member is announced, not only the amount, but also the spread of digital information is checked. If the newcomers' digital footprint is too small this is social media posts, cell phone calls and debit card payments, then the diplomate is flagged as an undercover CIA officer[736].

After 2010, 18 to 20 CIA sources were killed or imprisoned in China. The encrypted communication to CIA agents may have been cracked, this however competes with other theories such as leaks by a traitor or mistakes (using the same travel routes too often, eating in restaurants with listening devices and waiters employed by Chinese intelligence). [737]

Meanwhile, a former Hong Kong-based former CIA employee named Lee was arrested, and in 2013, information about Chinese CIA employees had been found in his notice book by the FBI, but it seems that the investigators were now certain enough to arrest him when entering the United States 2018[738].
Lee's case was the third case involving US agents in China in less than a year and Lee has admitted meanwhile.[739]

### 6.2.2 Intelligence Cooperation

Media reports 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

[733] Schulz 2013, p.6
[734] Spiegel 2013d, p.111
[735] Süddeutsche Online 2013
[736] Rohde 2016
[737] Mazetti 2017
[738] Winkler 2018, p3
[739] BBC 2019

derived from *human intelligence (HumInt), imaging intelligence (ImInt)* and *open-source intelligence (OsInt)*[740].
Theoretically, espionage is illegal and the presence of foreign agents as well,[741] but the customary international law accepts the right of sovereign states to do espionage which allows intelligence cooperation.

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 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[742]. 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, his office is known as *ODNI*) coordinates all organizations, 8 of them are forming the military umbrella organization *Defense Intelligence Agency DIA*[743].

The second level is a network of **bilateral intelligence cooperation**, e.g., Germany has relations with more than 100 countries[744]. 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

[740] Best 2009
[741] Radsan 2007, p.623
[742] Carmody 2005
[743] 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
[744] Daun 2009, p.72

capacities to achieve a global coverage. The information mode is typically as follows[745]:

- **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[746].

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 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[747].
When looking on the map, this arrangement reflects not only a preference order, but also a geographical logic. The 9-eyes partners are located at the Eastern and Southern flank of the United Kingdom, while the 14-eyes group are the surrounding neighbors of the 9-eye states, forming together a territorial block. This allows establishing a European platform and to protect surveillance and physical presence in these countries.

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*)[748] is analyzing information provided by member state organizations, counter-terrorist working groups etc. [749]
Meanwhile, the *SitCen* is part of the *European External Action Service EEAS* and now called *Intelligence Center (INTCEN),* which is organized in 4 units *Intcen 1-4* for analysis, OSINT; situation room and consular crisis management. Also, the EEAS has an internal security service for the security of the EEAS itself[750]. The Military Intelligence is coordinated in the *EU Military Staff (EUMS)*. The EU INTCEN is part of the *Single Intelligence Analysis Capacity (SIAC)*, which combines *civilian intelligence (EU INTCEN)* and *military intelligence (EUMS*

[745] Jäger/Daun 2009, p.223
[746] Wetzling 2007
[747] See e.g., Shane 2013, p.4
[748] 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).
[749] Scheren 2009
[750] Tagesschau online 2019

*Intelligence Directorate)* and is linked to the *European Union Satellite Centre*. European intelligence is also cooperating in the *CdB (Club de Berne)* since 1972[751]. The EU command and control (C2) structure is directed by political bodies composed of member states' representatives, and generally requires unanimous decisions.
Africa has established the multinational cooperation *Committee of Intelligence and Security Services of Africa CISSA* as a part of the African Union (see Section 9.12).

### 6.2.3 Conventional intelligence

Recent events from 2016 illustrate the relevance of conventional intelligence activities for attribution. As shown above, the tensions between Russia and US were already ongoing, as the Russian security firm *Kaspersky* used sinkholing against the presumably US-based *Equation Group*[752], while they on the other hand infected *Kaspersky* with the sophisticated espionage malware *Duqu 2.0* [753].

In August 2016, a previously unknown group called *Shadow Brokers* claimed to have cyber weapons from the *Equation Group* (which is suspected to have relations to US) and published material.

The **Michailow incident:** End of August 2016, it was detected that online voting systems were intruded in Illinois and Arizona, in Illinois data of 200,000 voters were copied[754]. Media speculated that this was part of a Russian campaign, but definite evidence was not found.[755] But then it was detected that a company named *King Server* leased six servers for this attack from a company called *Chronopay*. The Russian owner of *Chronopay* was already under investigation by *Sergej Michailow*, a member of the Russian *Intelligence Cyber Unit CIB* of the intelligence service FSB who (according to reports e.g., from the newspaper *Kommersant*) informed US authorities about this matter[756]. *Russia Today* confirmed that there are issues with Mr. Michailow without confirming the details of the information leak, but clarified that the case together with others is still under investigation by Russian authorities[757]. Also, a cyber security expert named *Ruslan Stojanow* from *Kaspersky Labs* was involved. While details remain unclear, Russian newspapers reported an affair with unauthorized disclosure of up to hundred IP-addresses of the Russian Ministry of Defense against payment of a high amount of money presumably by a foreign intelligence. However, *Kaspersky Labs* as organization was not involved[758].

---

[751] Scheren 2009
[752] Kaspersky Lab 2015a, p.34-35
[753] Kaspersky Lab 2015b
[754] Nakashima 2016, Winkler 2016, p.4
[755] Winkler 2016, p.4
[756] FAZ 2017a, p.5
[757] Russia Today (RT Deutsch) online 27 Jan 2017
[758] Russia Today (RT Deutsch) online 27 Jan 2017

The **Surkov incident:** In mid of October 2016, US Vice President *Joe Biden* announced that US seriously considers a cyber retaliation against Russia due to their suspected involvement in the *DNC hack* and other issues[759]. A few days later, i.e., before the Presidential Elections in US, a Ukrainian Group named *CyberHunta* presented the hack of the email box of the Bureau of the Russian President's top advisor *Vladislav Surkov*. At least parts of the material could be verified as real, i.e., as not fabricated. However, US media doubted that such a top-level operation could be done by a Ukrainian Group without respective hacking history, but that this was instead a warning by US intelligence[760].

The *US Intelligence Community Report* on Cyber incident Attribution from 2017 which was in line with the preceding assessment on the operations of *APT28/Fancy Bears* and *APT29/Cozy Bears* as Operation *Grizzly Steppe* strongly emphasized the political motivation of Russia as argument for the attribution of the attacks to Russia[761]. This was criticized in media as limited evidence, but the *Michailow* and *Surkov incidents* indicate that there was possibly more behind the scene than only digital attribution and analysis of political motivations.

# 7. Artificial Intelligence

## *7.1. Introduction*

Artificial Intelligence (AI) is commonly understood as the ability of machines to perform tasks that normally require human intelligence and is a key area of advanced computing. Important AI-related techniques include neural networks, deep learning, machine learning, Edge computing and robotics.

## *7.2 What is Artificial Intelligence?*

### 7.2.1 The DoD Working Definition

Even for human intelligence, there is no standard definition. However, the core of human intelligence definitions includes the mental capacity to recognize, analyze and solve problems, and a human being is then more intelligent if this can be done faster and/or for more complex problems.
Historically, the concept of Artificial Intelligence (AI) focused on machines could be used to simulate human intelligence. A practical definition which covers the common understanding of AI was made by the US *Department of Defense (DoD)*.

[759] Zeit online 2016a
[760] Shuster 2016
[761] ODNI 2017, JAR 2016 of the Department of Homeland Security DHS and the Federal Bureau of Investigation FBI.

The summary of the 2018 DoD AI strategy states that "*AI refers to the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action— whether digitally or as the smart software behind autonomous physical systems*."[762]

Many definitions focus on activities that require human intelligence, but strictly spoken, already the simple pocket calculators of the 1970ies made something that normally requires human intelligence. However, it is evident from literature, the AI researchers mean advanced and autonomous computing when they talk about AI. Therefore, **intelligent agents** are all devices that can perceive the environment and maximize the chance of goal achievement. When a computing application becomes normality, it is typically not considered as AI anymore (**AI effect**), past examples are e.g., pocket calculators, translation computers and chess computers, current examples are navigation systems and home assistant systems like *Alexa, Siri* etc.

The FY2019 National Defense Authorization Act (NDAA) provides a formal definition of AI with 5 types of AI systems[763]:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action
3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting.

### 7.2.2 'Strong' and 'Weak' AI

The so-called 'weak' AI can reproduce an observed behavior and can carry out tasks after training[764], i.e., systems that use machine learning, pattern recognition, data mining or natural language processing. Intelligent systems based on 'weak' AI include e.g., spam filters, self-driving cars, and industrial robots. In contrast, 'strong' AI would be an intelligent system with real consciousness and the ability to think.

The current AI of 2020 is still 'weak' AI with programmed machines that do fast calculations, which allows them to interpret, mimic or predict actions by using data

[762] DOD 2018, p.5
[763] NDAA 2019, Section 238
[764] Perez at al 2019, p.6

bases and statistical models, but still have no idea of itself and cannot reflect, i.e., they cannot really think or say "I" and "why".

On the other hand, human actions include a lot of repetitive and routine activities which can be standardized and are thus accessible for AI already now. Furthermore, decision making is often only the choice between standard options. Even things that human beings perceive as complex activity, e.g. driving a car from town A to town B, are mostly long sequences of routine activities and standard decisions, for example: The car comes to a traffic light: stop or go?, ….then driving…. a crossing comes: turn left or right?...then driving again… and so on…
This is in a similar way also applicable for industry production and machine activities.

In summary, already current AI systems are able to support or replace human activities in significant parts of daily life, communication, commerce, industry etc. and to support or control all kinds of machine use which explains the massive growth of AI and its enormous potential.
The AI program *GPT-3 (Generative Pretrained Transformer)* von *OpenAI* in San Francisco can on request generate complex and logically and grammatically correct sentences or expand existing texts, on *Youwrite* it already can prepare short papers to topics for school presentations. The AI program *Dall-E2* can create design, advertising photos, comics, illustrations and can use or modify existing styles[765].
It takes only minor modifications to have **dual-use AI**. If a drug research program is changing from avoiding toxicity to looking for toxicity, the combination of toxicity and bioactivity reveals thousands of new molecules with chemical weapon potential, even more toxic than VX[766].

### 7.2.3 AI-related Techniques

Important AI-related techniques are **neural networks, deep learning, machine learning Edge computing** and **robotics.**

**Neural networks:** The human brain is processing input with interlinked nodes of nerve cells, the neurons. The processing includes signal transfer, but also filtering by inhibitory neurons. Finally, incoming input patterns can be compared with known patterns to create a reaction. As a simplified example, when the eyes see on the street an object with four wheels, signals are transferred from the eyes' retina to the optical cortex in the posterior brain and from there to the neighbored interpretative cortex and memory areas in the Hippocampus region which finally

[765] Böhringer 2022, Schneier 2022
[766] Urbina 2022

allows to classify the object as 'car', even if the specific car model was never seen before.
The same principle is used in AI applications: The input is transferred and filtered through multiple hidden layers of computer areas (nodes), before the output (e.g., object classification, decision) is given.
Neural networks can be acyclic or **feedforward neural networks** where the signal passes in only one direction and **recurrent neural networks** with feedback signals and short-term memories of previous input events.
**Deep learning** means learning of long chain of causalities based on neural networks while the related concept of **Machine learning (ML)** is focusing on memory (experience) by developing computer algorithms that improve automatically through experience. **Fuzzy logic** focuses on the manipulation of information that is often imprecise, e.g., "put it a bit higher" where algorithm help to transform it into a more precise information.
**Natural language processing** includes algorithms to understand human language by systematic analysis of the language elements and their relations. A related area is **voice processing**.

A new AI area are **Bio-Inspired Computation Methods** which uses collections of intelligent algorithms and methods that adopt bio-inspired behaviors and characteristics such as genetic algorithms (GA =mutation, recombination and selection of algorithms), evolution strategies (ES), ant colony optimization (ACO), particle swarm optimization (PSO), and artificial immune systems (AIS)[767].

**Edge computing** is a layer of distributed computers between clouds and users that brings computation and data storage closer to the location where it is needed, to improve response times.

The key concept of **AI and Robotics** tries to optimize the robots' level of autonomy through learning to enhance the ability to manipulate, navigate and collaborate. Robots can sense the environment by integrated sensors or computer vision which is also a field of AI[768]. In practice, a rise of **co-bots** (co-worker robots) can be observed which support human beings e.g., by taking over repetitive activities such as sorting or carrying things, room disinfection etc.[769].

Historically, AI, machine learning, pattern recognition, robotics etc. were relatively independent research areas, but meanwhile they are increasingly confluent, so a wider understanding of AI includes these areas into the discussion.

[767] Truong/Diep/Celinka 2020, p.24
[768] Perez et al. 2019, p.24
[769] Jung 2020, p.70-71

The modern concept of automated systems thus includes the originally separate, but now overlapping concepts of autonomy, robotics and AI[770].

### 7.2.4 AI-driven Engineering

#### 7.2.4.1 Computers and Machines

Currently, the typical construction process of larger machines is to embed various computing elements and to connect them to control the machine. A *Eurofighter* Jet has more than 80 computers and 100 kilometers wires[771].
However, this construction leads to a very complex computing environment with a lot of interfaces which increases the risk for communication and compatibility problems as well as software problems, makes it difficult to keep all systems up to date and offers a lot of vulnerabilities for cyber-attacks.

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[772]. However, this would mean to delegate the IT security to multiple suppliers. 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 would need to be secured individually[773].

The trend is now going forward to create a fully integrated computing system with embedded artificial intelligence elements first and then to align and adapt the machine environment to this as e.g., done in the latest *Tesla* car models[774].
This allows a significant simplification of the IT environment combined with larger data flows and may be an option for other machines as well as e.g., military machines and air planes which are meanwhile (over)loaded with complex computed elements.

#### 7.2.4.2 Computers and Biologic Systems

The embedding of computers is also an issue for biologic organisms. In strict definitions, a **cyborg** (cybernetic organism) is a biologic organism with integrated machine elements. Retinal and cochlear implants as well as pacemakers fulfill this definition already. Note that cyborg development is going much slower than expected, because this approach has a very limited potential. Among other problems, the interfaces between living and computer sections are challenging. Another issue is the energy supply for the machine parts as any heat or radiation

[770] Hoadley/Sayler 2019, p.4
[771] Köpke/Demmer 2016, p.2
[772] Leithäuser 2016, p.8
[773] Mahaffey 2016, p. V6
[774] Floemer 2020

would damage the surrounding tissue. The immune system and the surrounding tissue tend to react against the implants with inflammation, rejection and fibrosis. Maintenance and repair requirements are already used as backdoors for cyberattacks. In summary, the amount of machine parts that an organism may be able to carry seems to be quite limited.

Compared to this, **autonomous biohybrids**, free combinations of biological and synthetic materials seem to have a much larger potential. Here, tailor-made biologic material is composed around computed machines elements and artificial intelligence could provide the autonomy to this system.
In 2016, a swimming robot that mimicked a ray fish was constructed with a microfabricated gold skeleton and a rubber body powered by 200,000 rat heart muscle cells[775]. 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.

Currently, three key technologies are in development which may enable advanced biohybrids, these are **artificial cells**, **organoids** and **synthetic/artificial genomes**.
Since 2010, a **minimal genome** cell is developed, this is the smallest possible genome that allows autonomous life and replication[776]. In 2016, a new cell, called *Syn 3.0*, was created by replacing the genome of *Mycoplasma capricolum* with the genome of *Mycoplasma mycoides*, with removal of unessential DNA[777]. After it was found that a slightly larger genome than the smallest possible leads to improved cell growth, a modified minimal cell was created which allowed to reduce the number of genes with unknown function to 30 in the year 2019[778]. If the function of these 30 genes could be clarified, the basic mechanisms of living cells are identified and could then be used to create freely **designable artificial cells**.
Also, the control of cell differentiation has made substantial progress: **Organoids** are small **artificial organs** created by targeted application of growth factors and hormones to stem cells with many functionalities of the original organ, e.g., lungs and airways[779] for studies of coronavirus infections, but also other organoids like small brains.
The other matter is **synthetic genomes**[780]. The rapid technical progress of DNA synthesis allows meanwhile a synthesis of **artificial chromosomes** for *Yeast (S. cerevisiae)*. Together with designable cells this technology may allow large-scale genomic variation and optimization.

[775] Park et al. 2016
[776] Kastilan 2010
[777] Danchin/Fang 2016
[778] Lachance et al. 2019
[779] Elbadawi/Efferth 2020, Heide/Huttner/Mora-Bermudez 2018
[780] Wang/Zhang 2019, p.23

## *7.3 AI Strategies*

### 7.3.1 Introduction

The United States and China compete for technology leadership in AI, followed by Europe as third largest actor.

As for other advanced technologies, research is done by three groups, i.e., state, private companies and academic research. In complex projects, these groups cooperate with each other and the state tries to coordinate and fund the AI projects of highest strategic value. In the security sectors, this means those applications with highest impact on military and intelligence capabilities.

The key strategic challenge is to identify these strategic AI applications and to ensure coordination for rapid development and deployment.

### 7.3.2 The AI Strategy of the United States

The *Presidential Executive Order on Maintaining American Leadership in AI*[781] was signed on 11 February 2019. The executive order emphasized the importance of continued American leadership in AI for its economic and national security and for shaping the global evolution of AI in a manner consistent with its values, principles, and priorities. At the same time, the DoD released an unclassified summary of its AI strategy with a clear focus on the *Joint Artificial Intelligence Center (JAIC)* for strategy implementation[782].

Note that a primary strategic direction for the future is the cooperation with the Intelligence Services (here meaning secret services) of the *Five Eyes*-Group (US, UK, CDN, AUS, NZ) and then secondary within the NATO[783].

In June 2019, the *White House Office of Science and Technology Policy's National Science and Technology Council* released the National *AI R&D Strategic Plan* which defined key strategies for Federal AI R&D investments[784].

The United States systematically expanded the institutional framework for AI research and funding[785].

| Sector/Administration | Institution | AI impact |
|---|---|---|
| **Military** | | |
| Department of Defense DoD | Joint Artificial Intelligence Center (JAIC) since 2019 | coordinates the efforts to develop, mature, and transition artificial intelligence technologies into operational use |
| | National Security Commission on Artificial Intelligence (NSCAI) since 2019 | assessment of militarily relevant AI technologies and provides recommendations |

[781] Trump 2019
[782] DoD 2018, p.9
[783] NSCAI 2020, p.4
[784] OSTP 2020, p.6
[785] Hoadley/Sayler 2019, p.9-10, RAND 2019, DoD 2018, OSTP 2020, NSCAI 2020

| | | |
|---|---|---|
| | Defense Advanced Research Projects Agency (DARPA) for 60 years | Currently over 20 AI programs |
| | Defense Innovation Unit DIU since 2016 | DIU works with companies to prototype commercial solutions against DoD problems. Contracts are typically awarded in less than 90 days |
| **Intelligence** | | |
| Office of the Director of National Intelligence ODNI | Intelligence Advanced Research Projects Agency (IARPA) since 2007, integrated precursor agencies from NSA, NGA and CIA | Similar purpose like DARPA, but with focus on intelligence. Initiated the Algorithmic Warfare Cross-Functional Team (Project Maven) which will be transferred to JAIC.<br>*Project Maven*: since 2017 for automating intelligence processing with computer vision and machine learning algorithms for target identification from drone data<br>Other AI programs include developing algorithms for multilingual speech recognition and translation in noisy environments, geo-locating images without the associated metadata, fusing 2-D images to create 3-D models, and analysis tools to infer a building's function based on pattern-of-life analysis |
| Central Intelligence Agency CIA | [has own firm In-Q-Tel for cooperation with start-ups] | Around 140 projects focusing on AI e.g., for image recognition and predictive analytics |
| | CIA federal lab since Sep 2020 | artificial intelligence, bioscience, virtual and augmented reality, quantum computing and advanced materials and manufacturing[786] |
| **Civil Sector** | | |
| Department of Energy DOE | Artificial Intelligence and Technology Office | to accelerate DOE's AI capabilities, ensuring the national and economic security |
| **Government** | | |
| National Science and Technology Council NSTC | The Select Committee on AI since 2018 | Consists of heads of departments and agencies principally responsible for the government's AI R&D (Research and Development) under the Information Technology R&D (NITRD) Subcommittee |
| | The Machine Learning and Artificial Intelligence (MLAI) Subcommittee | The MLAI Subcommittee monitors the state of the art in machine learning (ML) and artificial intelligence (AI) and reports to the NSTC Committee on Technology and the Select Committee on AI |
| | The AI R&D Interagency Working Group | It operates under the NSTC's NITRD Subcommittee and consists of research program managers and technical experts from across the Federal Government and reports to the MLAI and NITRD Subcommittees |

According to the 2017 *New Generation AI Development Plan*, China is aiming to become the global AI leader and develop a domestic AI market worth USD 150 billion by 2030[787]. The Chinese government views AI as an opportunity to "leapfrog" the United States by focusing on AI for enhanced battlefield decision-

[786] Coleman 2020
[787] Hoadley/Sayler 2019, p.1, NATO 2019, p.10

making, cyber capabilities, cruise missiles, and autonomous vehicles in all military domains[788].
In 2017, a civilian Chinese university demonstrated an AI-enabled swarm of 1,000 uninhabited aerial vehicles at an airshow. To accelerate the transfer of AI technology from commercial companies and research institutions to the military as *Civil-Military Integration (CMI)*, the Chinese government created a *Military-Civil Fusion Development Commission* in 2017[789].
The concept as given in the *Defense White Paper (DWP)* from 2019, it the development of warfare from mechanization to 'informationisation' and now with A.I. to 'intelligentisation'. Thus, for the Chinese army PLA, AI is essential for "**intelligentised warfare**"[790]. The practical strategic approach is to provide directions and resources centrally, but to implement locally, so that competition between Chinese cities and regions for AI-research is activated. To strengthen academic capabilities, hundreds of new AI professorships were established.
The military AI research focus is on Command and Control and on a broad spectrum of unmanned vehicles.
China is further investing in U.S. companies working on militarily relevant AI applications, potentially granting it lawful access to technology and intellectual property, but U.S. is still concerned that industrial and cyber espionage may be conducted also[791].
The largest AI project at the moment is the civilian **China Social Score System**, where health data, financial data (which includes consumption habits), digital data, mobile data and surveillance camera pictures are combined to create behavior, movement and content profiles. Based on output, lower interest rates, easier travel and other advantages (promotions, job offers, better positions in dating platforms thus improving the chance to reproduce) are granted for people with good score, with corresponding disadvantages for people with low scores. The idea is the automated management of a large society[792].

### 7.3.4 The Cross-Dependence of the United States and China

Both states are linked to each other with respect to human and technical resources. A cold war-like split into two separate cyber and AI worlds may cause significant problems for both states and the progress of AI as well[793].
Currently, many top Chinese researchers, i.e., those who delivered top papers at AI conferences, work in the US instead of China, even if they made their first academic degree in China. China tries to attract AI researchers with very good job offers, as

[788] NATO 2019, p.10
[789] Hoadley/Sayler 2019, p.20-22
[790] Bommakanti 2020, p.3-4
[791] Hoadley/Sayler 2019, p.22-23
[792] Westerheide 2020
[793] Mozur/Metz 2020

even after the Doctorate many Chinese researchers stay for a longer time in US instead of returning to China.
The DoD A.I. key *Project Maven* was developed with the help of a dozen *Google* engineers, many of them Chinese citizens. In particular, oversight was done by the Stanford Professor Dr. Fei-Fei Li. The Pentagon said that they were only working with unclassified data and were the best qualified to do this[794].

Both states are major cyber powers: China is the main producer of physical electronics in computers and smartphones, even US firms outsource their production often to China.
China has the impression that US dominates the cyberspace while US feels threatened by Chinas actions in cyberspace, see 5G and *Huawei* dispute in 2019[795]. Also, the NSCAI believes that US has still no credible alternative to the Chinese provider *Huawei* use in 5G[796] which is a major security problem because 5G networks will be a kind of "connective tissue" between AI applications.[797]

### 7.3.5 The Balance between Cyber and Physical Power

Computing and AI can support and replace human activities and by this leverage the intelligence and military capacities of a country. This method allows high-tech nations with large economies to consolidate and expand their power.

But in 2017, the Pentagon, more specifically, the *Strategic Studies Institute (SSI) of* the *U.S. Army War College*, a study based on the so-called **post-primacy scenario**[798], in which the US is still the largest economic and military power, but is no longer able to shape world order due to rising competitors such as China. Thus, geostrategy now has to be re-thought for an unstable, multipolar world that is not necessarily dominated by Western values anymore.

---

[794] Mozur/Metz 2020
[795] Security concerns against the Chinese company *Huawei* were expressed by Western countries, as this is meanwhile one of the largest global smartphone producers and also one of the largest infrastructure providers, in particular radio masts for smartphones and other data traffic. The next Internet communication generation **5G** is coming which will allow the first time a broad implementation of **the Internet of Things** and of smart home and smart city solutions, in particular by much higher data flows, real-time transfer massively reduced latency times (transmission delays) under 1 millisecond and also reduced energy need for transfer per bit, refer to Giesen/Mascolo/Tanriverdi 2018
[796] NSCAI 2020, p.54
[797] NSCAI 2020, p.55
[798] Lovelace 2017 writes in his foreword: *"The U.S. Department of Defense (DoD) faces persistent fundamental change in its strategic and operating environments. This report suggests this reality is the product of the United States entering or being in the midst of a new, more competitive, post-U.S. primacy environment. Post-primacy conditions promise far-reaching impacts on U.S. national security and defense strategy. Consequently, there is an urgent requirement for DoD to examine and adapt how it develops strategy and describes, identifies, assesses, and communicates corporate-level risk"*

An Australian military study on the US capabilities[799] showed that America's capacity to enforce the liberal order has declined, as the US and its allies accounted for 80% of world defense spending in 1995, which is now down to 52%[800]. The military equipment is overused and overaged with increased accidents due to near-continuous combat in the Near and Middle East region and budget instability caused by debt crisis and parliamentary disputes, training cuts[801]. There is a growing mismatch between strategy and resources.
The conclusion is that this *"...requires hard strategic choices which the United States may be unwilling or unable to make. In an era of constrained budgets and multiplying geopolitical flashpoints, prioritizing great power competition with China means America's armed forces must scale back other global responsibilities. A growing number of defense planners understand this trade-off. But political leaders and much of the foreign policy establishment remain wedded to a superpower mindset that regards America's role in the world as defending an expansive liberal order."* [802] Trade-off means to reduce the burden in dealing with multiple secondary priorities to achieve the primary goal.

In summary, the focus on cyber and AI activities will only expand the power of a state, if also the physical capabilities are maintained and aligned, otherwise the freedom of action is in danger despite improved knowledge and technology.
Also, there is an ongoing discussion, whether cyber intelligence may be a less risky, remote and cheaper way to do the espionage, but cyber espionage can only complement conventional espionage work and cannot replace the presence of local agents.

### 7.3.6 The AI Strategy of the European Union

The European Commission recently released a *White Paper on Artificial Intelligence* and supports a regulatory and investment-oriented approach with the objectives of promoting AI and of addressing the associated risks against (citation) "a background of fierce global competition".[803]
The aim is to become a global leader in innovation in the data economy and its applications, but with a regulatory **ecosystem of trust** into these rapidly evolving technologies.
To achieve this, the Commission established a *High-Level Expert Group* that published Guidelines on trustworthy AI in April 2019 with seven key requirements: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and

[799] United States Studies Centre 2019
[800] United States Studies Centre 2019, p.11
[801] United States Studies Centre 2019, e.g. p.47-48 amongst others
[802] United States Studies Centre 2019, p.9
[803] EC 2020

environmental wellbeing, and accountability. Further, a *Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics* was prepared. However, the EU has so far no clear strategy for the military dimension of AI[804].
The European Union permanently improves funding, but emphasizes the need to enhance efforts, as some €3.2 billion were invested in AI in Europe in 2016, compared to around €12.1 billion in North America and €6.5 billion in Asia[805].

## *7.4. Military Aspects*

### 7.4.1 An Introductory Case Study: The Eurosur Project

This project was for not for military purposes, but it shows very clearly the vision of fully integrated autonomous control systems. 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[806] 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[807]:

- 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 server would be the key vulnerability and would need to be maximum secure and resilient.
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

[804] Franke 2019
[805] EC 2020, p.4
[806] Welchering 2013, 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.
[807] Oparus 2010, SEC 2011, p.7, Talos Cooperation 2012

borders that are difficult to control. Similar approaches are currently developed in Saudi-Arabia (by EADS) [808] and in certain sectors of the US border[809].
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[810].

## 7.4.2 Practical Applications

### 7.4.2.1 Unmanned Aerial Vehicles (UAVs, Drones)

Drones aka **Unmanned Aerial Vehicles (UAVs)** are meanwhile advanced weapons with growing system autonomy. On the other hand, the defense against drones has also made significant progress.
**Drones** are not only used for reconnaissance, but also for active fighting. Drones are used for all kinds of operations that are „dull, dirty, dangerous or difficult“[811].
Drones allow observation and/or targeted killing of adversaries as *Lethal Autonomous Weapons Systems (LAWS)*[812]. However, the technical progress allows more and more **assistance functions**, i.e., the human decision making is increasingly supported and influenced by computers[813]. Meanwhile, the creation of a legal '**machine liability**' is now under discussion[814]. Any progress to fully automated drones would require enhanced cyber security efforts to avoid that machines are taken over by adversary hackers[815]. 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[816].

The *Drone Databook* from 2019 summarizes the drone availability and research of 101 countries and uses the *NATO Standardization Agreement 4670* classification ranging from I to III based largely on their maximum take-off weight: Class I (less than 150 kilograms, typically Micro, Mini, and Small Drones), Class II (150 to 600 kilograms, typically "tactical" UAVs), and Class III (more than 600 kilograms as *"medium-altitude long-endurance" (MALE)* or *"high-altitude long-endurance" (HALE)* UAVs) [817].

---

[808] Hildebrand 2010, p.6
[809] Miller 2013, p.12-13
[810] Wysling 2014, p.5
[811] Jahn 2011, p.26
[812] Thiel 2012, p. Z2
[813] 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
[814] In the civil sector, this is discussed in US for self-driving cars (i.e., cars with autopilot functions), Burianski 2012, p.21
[815] 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).
[816] Gettinger 2019, p.IV
[817] Gettinger 2019, p.IV

Most importantly, at least 24 countries are currently developing new military unmanned aircraft (10 Class I systems, 12 Class II systems, and 36 Class III systems). At least seven countries are exploring next-generation drones, including stealthy aircraft (US, China, Russia, and France), high-altitude pseudo-satellites (US, China, UK), swarms (US, China, UK), and manned-unmanned teaming systems (Australia, Japan, UK, China, and the U.S.) [818].
**Swarms** are AI-based drones which are autonomous (not under centralized control) capable of sensing their local environment and other nearby swarm participants, able to communicate locally with others in the swarm and able to cooperate to perform a given task[819].

Chinas drone development focus is on a large variety of Class III drones[820]. Three current US projects for AI drones are *Valkyrie, Skyborg* and *Gremlins*[821].

- The XQ-58A *Valkyrie* is a jet-powered Class III UAV of the Air Force's *Low-Cost Attritable Strike Demonstrator (LCASD)* aka *Loyal Wingman* which can accompany manned aircrafts into combat and e.g., attack enemy air defenses. The first flight took place in 2019.
- *Skyborg* is an Air Force concept for an autonomous low-cost strike drone that could serve as a vessel for testing different artificial intelligence technologies that would enable complex, autonomous operations. A future *Skyborg* UAV could operate alongside the *Valkyrie*, test fights with manned aircrafts are expected for 2021.
- *Gremlins* is a DARPA program to develop a swarm of low-cost, reusable Class I UAVs which could e.g., used for reconnaissance or electronic warfare.

In August 2019, DAPRA selected eight contractors for competitions[822]. In August 2020, the Heron system won against the seven other teams in two days and in the *AlphaDogfight* contest, the Heron system won five to zero against a human jet pilot (virtual reality helmets were used). The system is based on deep reinforcement learning, i.e., endless training cycles with 4 billion simulations which equals 12 years flight experience.

The functioning of autonomous devices is dependent on the underlying programs which can result in ethical and practical dilemmas[823]. If the programmed habit is

[818] Gettinger 2019, p.XV
[819] Hoadley/Sayler 2019, p.14
[820] Gettinger 2019, p.16
[821] Gettinger 2019, p.245
[822] Defense One 2020
[823] Hevelke/Nida-Rümelin 2015, p.82

known, e.g., drones (like cars) could be intentionally misled, captured or destroyed by mimicking certain situations or objects.

The most important ways to attack drones are:

- **Drone hacking**: by using the **Battle Management Language** commands which are sent on predefined frequencies. The limited costs and efforts needed for such attacks are a key security concern for militaries[824].
- **GPS-spoofing of drones:** sending false coordinates to the drones may mislead them or even urge to do an emergency landing
- **Jamming of drones:** Flooding with electromagnetic signals can induce an emergency landing which allows destruction or even capture of the attacked drones.
- **Physical attacks:** Shooting of drones, but also capturing of drones, even by trained animals, is a growing market for security firms. Also, laser defense is under development.
- **Loss of Communication:** The *EuroHawk* drone combined drone technology derived from the *Global Hawk* drone provided by *Northrop Grumann* and a new advanced reconnaissance technology called *ISIS (Integrated Signal Intelligence System)* from the EADS affiliate *Cassidian*. During a flight to Europe, this drone showed temporary losses of communication for a few minutes which constitute potential windows of opportunity for (cyber) attacks from adversaries. In general, loss of communication can enforce the unplanned landing and require destruction, if there is a relevant danger of takeover by adversaries.

Iraqi insurgents were able to use commercially available software to intrude U.S. drones which allowed them to view the videos of these drones[825]. 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[826]. Also, Iran was able to capture a US drone (type RQ-170) in 2011[827]. The vulnerability of drones depends also on the drone type with can have different control modes and grades of system autonomy[828]. The drone technology itself could cause losses of relevant number of drones. So far, most drone losses were caused by handling errors and conventional technical problems. 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

[824] Welchering 2017
[825] Ladurner/Pham 2010, p.12
[826] Los Angeles Times 13 October 2011
[827] 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.
[828] Heider 2006, p.9

previous decade[829]. 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[830].

Tests in New Mexico 2012 have shown that drones are vulnerable for **GPS spoofing**. The same could be shown for *Automatic Dependent Surveillance 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.[831]

The company *Airbus* develops a drone defense system with a detection range of 10 kilometers with radar and infrared cameras[832]. 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[833]. 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[834]. **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.

The selling of a certain drone model to more than one state results in sharing knowledge of the capabilities and vulnerabilities[835]. To protect critical knowledge,

[829] Gutscher 2013, p.4, Spiegel 2013a, p.11
[830] Whitlock 2014
[831] Humphreys/Wesson 2014, p.82
[832] Lindner 2016, p.24, Heller 2016, p.68
[833] Marsiske 2016
[834] Brumbacher 2016, p.5
[835] 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,

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[836]. 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[837].
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[838].

The meanwhile suspended[839] *EuroHawk* drone combined drone technology derived from the *Global Hawk* drone provided by *Northrop Grumann* and a new advanced reconnaissance technology called *ISIS (Integrated Signal Intelligence System)* 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.
Germany discussed in 2018 the acquisition of the *Triton drone* from the Navy and NASA, which can operate at an altitude of 18 kilometers over 30 hours and 15,000 kilometers of flight distance and which has a sense- and avoid collision detection system and the *ISIS system (Integrated Signal Intelligence System)*, which can be used to operate signal intelligence from the air. Germany has not been able to do so since 2010, because it decommissioned three *Breguet Atlantic* aircrafts, despite those had SigInt-capabilities[840].

### 7.4.2.2 Autonomous Vehicles

Both US and China are working to incorporate AI into **semiautonomous** and **autonomous vehicles**, in US this includes fighter aircraft (such as the Project *Loyal Wingman*), drones, ground vehicles (such as the remote-controlled *Multi-Utility Tactical Transport MUTT* of the Marine Corps), and naval vessels such as the *Anti-*

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
[836] Löwenstein 2013, p.5, Hickmann 2013, p.6
[837] Hein/Schubert 2016, p.22
[838] FAZ 2016a, p.29
[839] 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.
[840] Seliger 2018

*Submarine Warfare Continuous Trail Unmanned Vessel* prototype known as *Sea Hunter*[841].

### 7.4.2.3 Intelligence, Surveillance, and Reconnaissance (ISR)

AI is expected to be particularly useful in **Intelligence, Surveillance, and Reconnaissance (ISR)** due to the large data sets available for analysis as in the above-mentioned *Project Maven*. But **Imaging Intelligence** is more than target identification or face recognition, the *Defense Intelligence Agency (DIA)* and the CIA for example supervise adversary buildings with restricted access to analyze activities[842]. Satellites for example daily check Chinese hospitals activity by precise counting of the cars on surrounding parking lots. In a recent study, a massive peak was observed in autumn 2019 which may have been an early sign of the Coronavirus pandemic, because an analysis of the Chinese internet in the same study showed that Chinese users in Wuhan increasingly searched with *Baidu* for the terms cough and diarrhea.

### 7.4.2.4 Command and Control

**Command and Control** programs with use of AI are evaluated in China and US. The Air Force is developing a system for *Multi-Domain Command and Control (MDC2)* to centralize planning and execution of air-, space-, cyberspace-, sea-, and land-based operations.[843]

### 7.4.2.5 Logistics

AI may also support military logistics[844], the *Defense Innovation Unit (DIU)* and the *US Air Force* are working with the JAIC on **Predictive Maintenance** solutions for maintenance needs on equipment, instead of making repairs or to be stuck to standardized maintenance schedules[845]. For the F-35 jet, real-time sensor data embedded in the aircraft's engines and other onboard systems are put into a predictive algorithm to determine when technicians need to inspect the aircraft or replace parts[846].

[841] Hoadley/Sayler 2019, p.14
[842] Folmer/Margolin 2020
[843] Hoadley/Sayler 2019, p.12
[844] Hoadley/Sayler 2019, p.10
[845] DoD 2018, p.11
[846] DoD 2018, Hoadley/Sayler 2019

## *7.5 Security Aspects*

### 7.5.1 Brief Introduction

AI-systems can be manipulated, evaded, and misled resulting in profound security implications for applications such as network monitoring tools, financial systems, or autonomous vehicles[847]. AI has to do with computers, hardware and software, so all common threats to digital systems represent common threats for AI systems as well.

Besides this, there are AI-specific threats which need to be presented in more detail. As the complexity of AI systems is rapidly increasing, it is uncertain whether these problems could be resolved or may be even aggravated in future. The software of AI systems can be stolen, i.e., cyber espionage can eliminate the whole advantage by AI systems.

On the other hand, AI can substantially improve the cyber defense up to automated cyber defense and be a weapon in information warfare.

### 7.5.2 Key Vulnerabilities of AI Systems

#### 7.5.2.1 General AI Problems

The early AI systems were simple and thus easily explainable. However, meanwhile **Deep Neural Networks** have arisen, which show very good results, but are based on Deep Learning models which combine learning algorithms with up to hundreds of hidden 'neural' layers and millions of parameters, which makes them to opaque black-box systems, this is known as **Explainability** Issue[848].

The types of AI algorithms that have the highest performance are currently unable to explain their processes. For example, *Google* created an effective system to identify cats in movies, but nobody could explain which element of a cat allowed the identification. This lack of so-called "explainability" is common across all such AI algorithms[849]. But there is a discussion that machines sometimes see common patterns or structures in object classes which human beings simply did not note before.

As a result, nobody can predict when and for what reason an error may occur and AI systems have a limited **predictability**.

**Systematic errors**: AI system failures may create a significant risk if the systems are deployed at scale, i.e., AI systems may fail simultaneously and in the same way, potentially producing large-scale or destructive effects.

[847] NSTC 2020, p.1
[848] Arrieta et al. 2020, p.83
[849] Hoadley/Sayler 2019, p.31

**Communication issues:** 5G networks will be a kind of "connective tissue" between AI applications which means that everyone who can access the 5G networks can influence (alter, disrupt) the communication.[850]
**Misuse of Computing Power:** the pure speed of AI makes the systems highly attractive for misuse, e.g., for mining of crypto currency which requires a lot of calculations.[851]

#### 7.5.2.2 Mission Stability

A specific military AI problem is the **mission stability**[852]. Autonomous military systems can improve reconnaissance and intelligence and can speed up decision making and may also allow rapid reaction, but also may destabilize military missions.
Examples:

- An autonomous drone may decide to attack a relevant target, but by this disclose the military presence and jeopardize Special Forces or Intelligence Operations.
- In the *DARPA Cyber Challenge* of 2016, the best computer was a machine that defended itself on the expense of the defense systems.
- A computer may decide that a combat at a certain location may be a waste of resources and withdraw e.g., a drone swarm, but may never understand that sometimes a certain location has a symbolic and psychological value, or is maybe foreseen as anchor point of a new front line or that the fight is only done to distract adversaries from more important areas. The question is: will an advanced military AI really be able to think strategically or only tactical? Context is still very poorly understood by the systems, i.e., they lack common sense[853].
- Mission authority problem: In civil airplanes, pilots already had to fight against defect autopilots which could not be overridden in critical situations[854].
- An AI may decide to fight too quickly, leaving the conventional forces unprepared or closing the door to a peaceful solution.
- An intruded AI system can be turned against its controller or used as double agent (i.e., it sends observations of both sides to both sides)

---

[850] NSCAI 2020, p.55
[851] Goddins 2020
[852] Masuhr 2019, Johnson 2020
[853] Wright 2020, p.7
[854] Voke 2019 wrote in his analysis on page 33: *„Moreover, if AI is showing improper intentions or acting poorly, humans must be able to override its behavior. Although the system did not perform as required, the human must be able to exercise control once recognition of a hazardous situation occurs. Transparency is a requirement for control, and control is a requirement for trust."*

Conclusion: The more advanced a military AI will be, the higher the risk for mission instability which may suddenly appear in microseconds.

#### 7.5.2.3 Data Manipulation

- **Manipulated images** can confuse of autonomous systems. Small stickers on the street were enough to drive the autopilot of a *Tesla* vehicle on the opposite lane[855]. Meanwhile, there are pixel-style camouflage paintings on modern Chinese military vehicles, but also on Russian helicopters.
  Already smallest -for human eyes invisible- changes in digital images can cause systematic misinterpretation by AI, a process known as **adversarial machine learning**[856].
- **Data poisoning:** machines can be systematically misled by mislabeled data. This can be done by tapes in stop signs for traffic[857], but maybe the misuse of military flags and symbols could be another option.
- **Object Dummies** would certainly be able to mislead even autonomous combat drones.
- **Spoofing**: misleading of *Global Positioning System (GPS)* controlled systems by sending a false GPS signal which overrides the right signal, e.g., against drones or ships

### *7.6. Ethics and Machine Logic*

There are many aspects of AI which may cause ethical problems, e.g., in the military sector, if automated decision-making may end in killing of adversaries. It is common sense that for AI systems a human oversight or at least an emergency override function in case of apparent malfunctions is included.

Another challenge is the **predictability** and **explainability** issue. The specific characteristics of many AI technologies, including opacity ('black box-effect'), complexity, unpredictability and partially autonomous behavior, may make it hard to verify compliance with, and may hamper the effective enforcement of, rules of law to protect fundamental rights[858]. Certain AI algorithms, when exploited, can display gender and racial bias, e.g., for facial analysis. Human decisions can also be biased but, the same bias in widely used AI systems could have a much larger effect, affecting and discriminating many people[859].

While it is possible that AI researchers and their countries are committed to ethical and societal values, it is currently, where AI has limited understanding of situation contexts, very difficult to imagine an AI with embedded values. For example,

[855] FAS 2019, p.21
[856] Wolff 2020
[857] Wolff 2020
[858] EC 2020, page 11-12
[859] EC 2020, page 11-12

human beings usually have a clear idea what dignity, justice and fairness means to them, but what are these terms in program code or machine language?
A classic problem of machine ethics and logic is the **collision dilemma** of autonomous cars[860]: a pedestrian may suddenly cross the street and the autonomous car system may be confronted with two options, i.e., dodge and risk the death of the driver or move and risk the death of the pedestrian.

A strong AI system with the ability to ask for the rationale and with an independent understanding of itself (*cogito ergo sum*) may –based on superior knowledge and intelligence- probably not follow human logics and ethics anymore. In the DARPA contest 2016, the machine has won that rescued itself instead of keeping the defense systems permanently active.

[860] Hevelke/Nida-Rümelin 2015

# 8. Cyber security of digital technology

## *8.1 Introduction*

The number of smart devices is rapidly growing, but the long-term development is already going beyond the **Internet of Things (IoT)**, it is heading to the **Internet of everything (IoX)** which will connect everybody and everything everywhere.
In 2020, at minimum 50 billion IPv6 addresses will be reserved, and the trend is going forward to 8 to 20 IP addresses for each human individual[861].

The number of digital devices and vulnerabilities is growing. The security firm *Palo Alto* has discovered the malware *Amnesia* (a variant of the malware *Tsunami*) which can infect digital videorecorders and build IoT botnets. To prevent analysis, it can detect and delete virtual machines (sandboxes).[862]

## *8.2 Smartphones*

Eavesdropping of government smartphones[863] 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[864], energy supply by smart grid and later on also for control of cars in the upcoming **e-mobility** projects[865]. 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.[866] 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. Another concept is **Company owned personally enabled (COPE)** where employees can run private applications on company devices. The BYOD and COPE philosophy creates a kind of **shadow IT** in companies which is quite difficult to control and to protect[867].

[861] Chiesa 2017
[862] Kling 2017b
[863] Graw 2013, p.4-5. Respective incidents were e.g. reported for Indonesia, Germany, Brazil.
[864] RWE 2013
[865] Heinemann 2013, p.3
[866] Langer 2014a, p.7
[867] Müller 2014, p.16

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) [868] are simple collection of electromagnetic waves by radio masts (GSM standard is not secure[869]), mimicking radio masts by **IMSI-Catchers**, access to node servers or cables of node servers[870], implanting viruses and Trojans by infected Apps, unauthorized data use by hidden App properties[871], or sending invisible and silent SMS messages (**stealth SMS**) to transfer spyware such as *Flexispy* [872]. 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 to take over audio and video functions[873]. 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[874].

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[875]. Meanwhile German ministers are advised to use **one-way mobile phones** that are only used during one travel and then destroyed.[876]

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[877]. 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-

[868] Ruggiero/Foote 2011
[869] FAZ 2013c, p.14
[870] Wysling 2013, p.5
[871] Focus online 2013
[872] Welt 2013, p.3, Opfer 2010
[873] Steler 2015
[874] Drissner 2008, p.4, Opfer 2010
[875] See also Dohmen 2015, p.75
[876] Der Spiegel 2015, p.18
[877] Der Spiegel online 2014, p.1, Zeit online 2014a

machine communication and which allows "over the air" access to SIM cards to allow change of operators[878].

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.[879]
A problem is 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 2015 via an infected **software development kit (SDK)** for App programming. More than 250 infected Apps were removed from App stores[880]. In August 2017, 500 infected apps were removed from the *Google Playstore*, which together had more than 100 million downloads[881].
Apps can sometimes leak sensitive data as well, such as *Strava*, a fitness tracker often used by soldiers which unintentionally exposed military bases[882].

**QR codes** (Quick Response Codes), i.e., matrix or two-dimensional barcodes may redirect smartphones to malicious websites during scanning[883]. 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[884].

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[885].
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[886]. 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[887].

[878] 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
[879] Spehr 2015, p. T4
[880] T-online 2015
[881] Janssen 2017, p.22
[882] Holland 2018
[883] Beuth 2016a, p.1-3
[884] Lemos 2015
[885] FAZ online 2016
[886] Die Welt online 2016
[887] Die Welt online 2016, FAZ online 2016

*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[888].

In 2017, the Cyber security company *Cellebrite* was hacked and data were published. These showed that 40,000 licensed clients (intelligence, border police, police, military units, finance organizations) used e.g., the *Universal Forensic Extraction Device UFED* that allows access to smartphones by utilizing security gaps (exploits). Further exploit collections for *iOS, Android* and *Blackberry* were released[889].
Mass infections of smartphones are a new trend. A motive for this is building smartphone botnets, which e.g., for the smartphone to click on certain advertisements or to approach websites in the background. The malware *Gooligan* was downloaded more than 1 million times from App Stores and allows control of the smartphone[890]. Further mass infections of smartphones were reported in the previous months, e.g., with the malware types *DVMAP* and *VoVA*.
In 2018 the security company *Grayshift* offered large-scale iPhone cracking packages: 15,000 US-Dollar for 300 iPhones or 30,000 Dollar for an offline cracking black box with unlimited use[891].

## *8.3 Smart Industry (Industry 4.0)*

### 8.3.1 Overview

**Smart Industry (Industry 4.0)** refers to the digital (networked, computerized, intelligent) production, typically with remote maintenance and control systems (*Industrial Control Systems ICS/Supervisory Control and Data Acquisition SCADA*). It is a sector of the smart technologies (smart home, smart cities, smart grid/smart meter, smart cars etc.) and of the **Internet of Things IoT**, i.e., of all devices connected with the internet.

A key element will be the **5G technology** which will connect all these elements and which is characterized by energy-saving work, connection with approx. 1 million devices per km2 and a minimal latency time during the signal transmission, will develop the full potential of all smart technologies and the IoT. In Germany, a secure one way-street communication system, the **5G campus network** (Campusnetzwerk) was developed where people within the secure network can communicate with outsiders, but not data can be sent into the secure sector. Earlier,

[888] Jansen/Lindner 2016, p.28
[889] Kurz 2017, p.13
[890] NZZ 2016
[891] Betschon 2018a, p.7

the **data diode** (data can come in, but not out) was presented as other secure one way-street technology.

This is a challenge for cybersecurity, because users and companies face an exponential growth of devices, interfaces, updates, and variants which can hardly supervised or controlled. Another problem is the **open systems**: In order to perform tasks such as monitoring, maintenance and updates, the systems must be accessible from the outside. In addition, companies want to be able to study the user behavior for product development and, finally, intelligence services sometimes require backdoors in the system. In the end, networking always means that a system usually does not belong to a user alone, because there are third parties who have to maintain, protect, update and administer it, so that one's own safety always depends on third parties.

Most dangerous is the **unnecessary connection to internet**. The search engine *Shodan* is looking for networked smart devices of all kinds and security researchers found at first tests freely accessible control systems in companies, train stations and airports that they could click and change directly, but also saw babies in their beds, which were monitored by unprotected webcams. However, *Shodan* can be used to check the own organization for unprotected devices. Another problem is the **low password protection** by factory default passwords or even hard-coded (unchangeable) passwords, which invite straight to the misuse of the device.

The DoD agency *Defense Advanced Research Projects Agency DARPA* has 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[892].

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[893]. SCADA systems often do not have automatic security updates or virus scans and firewalls can often not be implemented, because

[892] 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
[893] Betschon 2013a, p.38

this interferes with the liability of the manufacturer of the SCADA-driven machine[894].

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[895].
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[896].

The *US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)* recommends[897] 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.

## 8.3.2 Cyber-attacks in the Smart Industry

### 8.3.2.1 Background

- Infiltration > lateral movement > escalation > manipulation
- Development of the attack takes years (including tests) and requires the cooperation of computer scientists and engineers
- Hacking alone is not enough, you also have to know the system (otherwise discovery, accidental sabotage)
- Usually only spying, not sabotaging (in cybercrime, however, ransomware and botnets)
- The primary goal is the (industry) espionage, the cyberwar an option

Some key principles of attacking the smart industry are: you do not have to attack production directly. It is also possible -as in a true incident- to progress from the infected office computer into the control of the blast furnace by lateral movement.
The development of a major attack takes years (including tests) and requires the cooperation of computer scientists and engineers. The hacker knows how to get into a computer, but what he then can see, only the engineers really know. If a hacker accidentally presses the wrong button, the damage can be immense and he has also unmasked himself.
Generally, espionage is frequent, attacks are avoided. This explains the excessive espionage, but the few attacks. Otherwise, the opponent could retaliate by turning

[894] Striebeck 2014
[895] Reder/van Baal 2014, p. V2
[896] Krohn 2014, p.24
[897] ICS-CERT 2016a

off the electricity or paralyze a nuclear power plant, which is why care is practiced in practice.
The typical industrial attackers are cybercriminals who want to blackmail money with the help of blockages, by ransomware (blocking screens) or by botnets (flooding of systems with queries).
So, the primary goal is (industrial) espionage, but cyberwar is always an option. The infiltration of a controller not only provides valuable information about the controller itself, but also provides insights into the production process, including potential problems that can be learned from in advance.

#### 8.3.2.2 Important cyber attacks

The following list presents the most important Smart Industry Attacks, for background and details refer to Section 5:

- *Stuxnet (2005-2010):* originally valves, then frequency modulation of uranium centrifuges by targeted attack on *Simatic S7-SPS* and *process visualization WinCC*
- *Shamoon* attack on Aramco (2012), wiper attack on Iran (2012)
- 2020 *Kwampirs* malware warning by FBI. A successful cyber-attack on an Israeli water pump in 2020 led to cyber retaliation against an Iran port
- *Cloud Hopper (2006-2016):* attack on *Managed Service Providers MSPs* (Clouds, IT Services, Help Desks etc.), in addition on technology firms and the US Navy
- *Lazarus-Group (2012-today):* since years use of wipers as logic bombs or to eliminate traces, use of destructive ransomware *(WannaCry) 2017*
- *Triton/Trisis/Temp.Veles (2017):* Malware *Triton/Trisis* against *Schneider Electrics Triconex Safety Instrumented System (SIS)* in Saudi-Arabia, manipulation of emergency shutdowns
- *Dragonfly/Energetic Bear:* infected ICS Provider with Malware *Havex* for surveillance and manipulation of ICS/SCADA-Systems (ca. 2000 cases)/ *Wolf Creek-incident* 2017 with spearphishing using fake resumes
- *Sandworm/Quedagh* (since 2011): Modified multi-function Malware *BlackEnergy3* against *Human-Machine-Interfaces HMI*
  - 2015 Power failures in the Ukraine by disconnecting power connections and Telephone Denial of Service (TDoS)-attacks to block alert hotlines and use of Wipers *(Killdisk)*
  - 2016 *Industroyer*-Attack Wrong IEC-104 protocol orders to a single infiltrated transmission substation led to a power outage in Kiev. A similar attack with a slightly modified *Industroyer 2.0* malware in 2022 was ineffective[898].
  - 2017 *Petya/Not-Petya/Moonraker-Petya* Use of NSA exploits for destructive ransomware

[898] Mäder 2022c, Muth 2022

- 2018 *VPN-Filter* reboot-resistant IoT-Malware for network devices for surveillance of SCADA protocols with bricking option.

## 8.4 Internet of Things

**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.).

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[899].

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[900].

A substantial new threat is **Home Assistant Systems** (such as *Alexa, Siri, Google Assistant etc.*). A frequent problem is **inadvertent command execution** if the systems hear something which is not directed to them, e.g., from TV. Data and privacy issues may appear, too.
Meanwhile, intruders can send **‚silent' commands** (using the range above 20 kHz) from outside the building and by this take over control about the home assistant, and if settings allow, about the entire smart home arrangement, e.g., opening doors. The detection of existing smart home technology is technically simple[901].

The Internet of Things (IoT) botnet *Mirai* (named after the anime *Mirai Nikki*) utilized webcams, babyphones and other devices to create a DDoS attack on the US internet infrastructure provider *Dyn* with data flow rates of more than 1 Terabit per second in October 2016. The IP addresses led to the manufacturer *Xiong Mai*.
Some days before, a hacker with the cover name *Anna Sempai* released 62 passwords for access to the devices. Meanwhile, solid evidence was found by security researcher *Krebs* that *Anna Sempai* was involved in the Mirai precursors,

[899] Market Wired 2014, p.1-2
[900] Weber 2016, p. T1
[901] Niewald 2018

in particular *QBot*, while for the *Dyn* attack another group *New World Hacker* claimed responsibility[902]. *Mirai* was derived from precursor botnets such as *QBot* and *Bashlite*. These botnets were originally utilized to attack *Minecraft* (a popular online game) servers to push them out of the attractive *Minecraft* hosting server market. The *Mirai* worm was programmed in the specific language *Golang*.

Later in 2016, the *German Telekom* was massively attacked. Here, a new *Mirai* variant was utilized and analysis showed that again only selected devices (so-called *Speedport* routers) from the Taiwanese manufacturer *Arcadyan* were affected. The attack failed only due to a technical error caused by the malware[903].

On 22 Feb 2017, a young Briton was detained at the London airport who is suspected to have caused the *Mirai* attack on *Telekom*. This was a successful cooperation of authorities from Germany, United Kingdom and Cyprus.
The attacker pleaded guilty. *Mirai* aimed at the remote maintenance access port 7547, In Liberia, the telecom company *Lonestar* was attacked, at the *German Telekom* their *Speedport* routers. The attack on the Telekom router failed, but interfered with their function. Nevertheless, he got up to 600,000 routers in Germany, Britain and South America under control to attack *Lonestar*. The Telekom was attacked to have more routers for later attacks[904].

However, Mirai-related attacks continued, as the **DNS Query Flood** *(Mirai DNS Water Torture Attack)* on 15 Jan 2017 which targets DNS servers, i.e., computers to solve questions which domain belongs to a certain IP address. A randomized 12-character alphanumeric subdomain is prepended to the target domain to prevent response by local servers. The attacking bots send their queries to their locally-configured DNS servers, which then ask an authoritative DNS server, the real target of the attack and which is then overflooded with requests[905].

A new attack method in IoT is **Bricking.** Here the malware attacks smart devices, gives instructions to alter settings and overwrites the firmware which leads to factual destruction of the device.
The attack with *BrickerBot.1* und *BrickerBot.2* used hard-coded passwords of cameras and devices of the company *Dahua*, which gave the attackers easy access to the devices[906].

[902] KrebsonSecurity 2017, Radio Free Europe 2016
[903] Alvarez/Jansen 2016
[904] Jung/Jansen 2017, p.24
[905] Akamai 2017, p.8
[906] Böck 2017

## 8.5 Smart Grids

The **smart grid** is the digital version of the conventional electric grid, that is needed to produce electricity at power plants, to transmit this energy to local station where it is stepped down to lower voltage to distribution networks to power customers. Dominant smart grid network protocols are *IEC 104*, a TCP-based protocol, and its serial protocol companion *IEC 101* are used in Europe and Asia while the *Distributed Network Protocol 3 (DNP3)* is typically used in US.
A specific risk of the smart grid is **domino effects** as the voltage of the transmitted electricity has to be kept stable in a very narrow range. Any volatility e.g., caused by a cyber-attack can destabilize large regions up the entire European Union which makes the smart grid defense to a priority of cyber security efforts.

## 8.6 Nuclear plants

During the power failure of 2003 in the US, it was discussed whether this was caused by a computer virus[907]. 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[908]. Since 2006 nuclear power plants were shut down two times after cyber-attacks[909]. In April 2009, hackers successfully intruded the US electricity net control[910] and installed programs that allowed manipulation and turn-off. China was suspected, that denied and also Russia.
In October 2016, the *International Atomic Energy Agency (IAEA)* Director Amano said that two to three years ago a nuclear power plant was hit by a disruptive attack, whoever it did not need to shut down. After the cyber-attack in South Korea 2014 (see Section 5 *Lazarus Group*) and a computer virus found in German nuclear plant Grundremmingen in April 2014 (in the office, not the nuclear section). End of June 2017, the Ukrainian nuclear plant Chernobyl was affected by the *Petya* malware attacks[911].
In May and June 2017, the US energy sector was target of cyber attacks. DHS and FBI were investigating this, amongst the targets, the nuclear plant of *Wolf Creek* near Burlington, Kansas was attacked, but its operations were not affected. The attacks were the same as the tactics of *Dragonfly (Energetic Bear/Crouching Yeti/Koala)*, and **fake resumes** for control engineering jobs, watering hole attacks and man-in-the-middle attacks were applied[912].

The French company *Ingerop* which constructs buildings, was affected in 2018 by a phishing attack of unknown actors who stole 11,000 files, thereof files with respect

[907] Gaycken 2009 with picture of power failure in Northeast USA 2003
[908] Wilson 2008, p.22
[909] ArcSight 2009
[910] Goetz/Rosenbach 2009, Fischermann 2010, p.26
[911] Shalal 2016
[912] Perloth 2017b

to nuclear waste facilities, prisons and other critical infrastructure[913]. A trace led investigators to a server in Dortmund and it may be possible that hacktivists were involved.

In June 2019, it was reported that since at least 2012, US has put reconnaissance probes into control systems of Russian electric grid. In addition to *Wolf Creek*, attempts were made to infiltrate Nebraska Public Power District's *Cooper Nuclear Station* where they reached communication networks, but not the reactor system[914].

## *8.7 Cars and Air Planes*

Digitalization of cars is rapidly moving forward, e.g., for driving assistance, motor diagnostics, information, navigation and entertainment, security and camera systems[915]. 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[916]. Eighty percent of new cars in Germany will have internet access in 2016[917]. From 2018, new 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[918].

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[919].

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[920]. Until now, all these hacks were done in research environments, typically by ethical hackers who notified the affected companies to allow early closure of security

[913] Eckstein/Strozyk 2018
[914] Sanger/Perloth 2019
[915] Hawranek/Rosenbach 2015, p.65
[916] Fuest 2015, p.34-35
[917] Schneider 2014
[918] Fromme 2015, p.17
[919] Karabasz 2014, p.14-15
[920] Lewicki 2014, p.62

gaps[921]. 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[922].

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[923], but such signals can be easily detected and reproduced by attackers using a **repeater** device[924].

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[925], but also allows rapid security updates[926]. 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[927]. Meanwhile an investigation showed that the driver ignored warnings of the autopilot[928].

In future, cars will have additional features[929]. A study of the automobile association FIA showed that BMW models 320 and i3 captured driving behavior, mobile phone contacts, navigator targets, usage of seats, location and parking positions. *Mercedes* commented that their cars would know the driving style, the drivers‘ calendar and his music preferences. However, in public traffic e-tickets can store the movement profile of the ticket owner.

Apps from other providers are a potential vulnerability. A 19-year-old German could use *Tesla Mate*, an application for analysis of driving data, as entry to access 25 *Tesla* cars in 13 countries and was able to control the cars remotely[930]. The vulnerability was closed as the hacker alerted *Tesla* and *Tesla Mate*.
In future, a potential risk for all kind of cars could be Cloud Services where manufacturer communicate with the cars.

---

[921] Meanwhile car manufacturers hire hackers to check the security such as the British telecommunication company BT, FAZ 2015b, p.18
[922] 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.
[923] Rees 2016, p.2
[924] Heute 2016
[925] 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
[926] Becker 2016, p.78
[927] Fromm/Hulverschmidt 2016, p.25
[928] SZ online 2017
[929] Spehr 2017, p. T1
[930] Schmidt/Mäder 2022

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[931]. 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.[932]

The German Air Traffic Control *Deutsche Flugsicherung DFS* is setting up a control center in Leipzig from which the Saarbrücken Airport will be remotely controlled as a **Remote Tower Control (RTC)** from 2019; a trend emerging in Europe after a long pre-test period[933].

## *8.8 Cloud Computing*

A new area of concern is the rapid growth of **cloud computing** where data may be stored on external computers under a foreign jurisdiction.

The storage and handling of data in large servers of external providers has various advantages:

- All programs and computers of the organization can be updated and patched in one step.
- The deployment of new computers and location is less problematic, organization are more flexible.
- The own IT infrastructure can be significantly reduced.

However, there are also security issues:

- The cloud provider has the physical control of the data, which requires high standards of trust and (technical) reliability.
- The cloud provider must be able to defend the data against attacks.
- Depending on local and legal settings, third parties may have legal access to the data.

In 2019 there were estimated 3000-4000 **Cloud Service Providers**, the leading providers, the **Hyperscalers**, are all located in US: *Amazon Webservices AWS,*

[931] Rosenbach/Traufetter 2015, p.72f.
[932] GAO 2015, p.1
[933] FAZ 2018d

*Microsoft Azure, Google Cloud Platform, IBM SoftLayer, Oracle Cloud, Salesforce* and *VMware*[934].

The *US Cloud Act* allows since 2018 access to overseas data under certain circumstances, e.g., if needed to clarify crimes that happened in US.

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[935]. The cloud provider represents an additional entrance gate for attacks, with may be difficult to control by the outsourcing company[936]. 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[937].

**Multicloud-Solutions** are selected by many firms to reduce dependency. Other methods to improve security can be the choice of server locations, data splits, and data encryption).

In addition to the above-mentioned APT10 *Cloud Hopper*, which uses cloud access to cloud users, fuzzing research has revealed the *SpectreNG* gap in chips that makes it possible to penetrate from the virtual machine into the cloud itself.

In addition to the various security issues[938] uncertainties about rights and responsibilities on cross-border situations[939] 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"[940].

Cloud services are also used by the intelligence services. *Amazon Web Services (AWS)* set up a **top-secret region** in 2014 to store classified materials as a result of a $ 600 million CIA contract. At the end of 2017, AWS also set up a S**ecret Region**, where software and data with the respective level of secrecy are available cloud-based. The cloud services of AWS and *Microsoft Azure* were certified as eligible by the US Government.[941]

[934] Müller 2019, p.14
[935] FAZ 2010f, p.17
[936] Menn 2010, p.H12-H13
[937] Postinett 2013b, p.12
[938] ENISA 2009b
[939] EU2011
[940] EU 2012a, p.5
[941] Beiersmann 2017f, p.1

## *8.9 Satellites*

### 8.9.1 Introduction

A satellite is an object that has been intentionally placed into orbit, in 2019 several thousand satellites are assumed to be in orbit, less than half of them approximately still operational. They are used by more than 100 governments as well as commercial entities from more than 50 countries[942]. However, tens of thousands of small satellites are projected to launch in this decade for communications and Earth observation[943].

### 8.9.2 Global Coverage

The leading nation working with any kind of satellites are the United States. A recent count estimated for the US 154 military satellites and 49 satellites of the satellite-based intelligence organization *National Reconnaissance Office (NRO)*. China had in the same count 63 and Russia 71 (known) satellites, while other countries had less than ten each.
The Intelligence, Surveillance, and Reconnaissance (ISR) satellites ('spy satellites') can for examples detect and record hundreds of thousands of cell phone calls simultaneously and produce highest-quality images of the earth[944].

### 8.9.3 Satellite Hacking

An increasingly important weapon is satellite hacking which can be done as direct attack on satellites or as attack on the ground station and or providers. Little is published, but one can say that direct takeover of satellites in space is cumbersome and has little effect, while hacking of space control centers on earth has led to a substantial increase of satellite hacking activities.

Satellite hacks of US satellites were already reported since a decade and China was suspected by the *US-China Economic and Security Review* Commission since a longer time already[945]. In 2011, a report of this Commission stated that two US satellites had been compromised in 2007 and 2008 through a ground station in Norway and in 2014, the *US National Oceanic and Atmospheric Administration confirmed* that one of its satellites had been hacked[946].

The *Waterbug group* (aka *Turla/Snake/Ouroburos/Venomous Bear/Krypton/Group88*) is the name for the actors who use the malware *Wipbot/Tavdig/Epic Turla, Uroburos/Turla/Snake/Carbon* and *agent.btz/Minit.* In one source code the term UrObUr()s was used, alternative writings to *Uroburos* are

[942] CRS 2019
[943] Pekkanen 2019, p.93
[944] Abbany 2020
[945] Menn 2018
[946] Rajagopalan 2019

*Ouroburos* and *Uroboros*. Western intelligence attributes this APT to the Russian civil intelligence FSB. The group owns a malware family that could be backdated to 2005. The group is utilizing satellite-based internet links for action[947].
Simply spoken, a sender sends data to a satellite as uplink, the satellite then sends data back to one or more receivers as downlink. The *Waterbug/Turla* group hijacks *DVB-S (digital video broadcasting satellite)* links with their own satellite dish by inserting their own data packages into the downlink signal to control their botnet. This method allows to act highly anonymously as the signal seems to come from a legitimate sender[948].

While in the past people thought that future wars on earth would be decided in space, it seems now that future wars in space may still be decided on earth: the hacking of space control centers could be used for sabotage, i.e., by sending false commands to move satellites resulting in damage, collision or loss. This does not only affect satellites, but is also applicable for all kinds of space robotics in general. Cyber-attacks included:

- The German Space Center *Deutsches Luft- und Raumfahrtzentrum DLR* was hacked in April 2014, presumably for technology espionage[949].
- In 2015, the French Television *TV5Monde* was temporarily taken offline by the Russian cyber group *APT28 (Fancy Bears)*[950]. 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[951].
- According to reports from June 2019, the NASA *Jet Propulsion Laboratory JPL* was accessed by connecting a *Rapsberry Pi* device, which then allowed to steal data from Mars missions[952]. In 2018, also the *JPL Deep Space Network* as system of satellite dishes for communication with Nasa spacecrafts was infiltrated. In December 2018, two members of the Chinese cyber group *APT10* were indicted for intrusion of the JPL, but it was not stated whether this specific attack was meant.
- In addition to ground stations, suppliers and stakeholders are also a security risk[953]. In June 2018, *Symantec* reported successful breaches of satellite and defense companies by a new espionage hacking group *(Advanced Persistent Threat APT)* called *Thrip* which has been active since 2013. *Thrip* may have overlaps with APT40 which is active since 2013.

[947] Weedon 2015, p.72-73
[948] Paganini 2015
[949] Die Zeit online 2014
[950] FAZ online 2015, p.1
[951] Wehner 2016a, p.6
[952] Cimpanu 2019
[953] Hlavica 2019

In the early morning of 24 Feb 2022, modems of the KA-SAT satellite of the US telecommunication firm *Viasat* were blocked to stop communication which affected Ukraine military and police units[954], but also thousands of German wind energy systems that used the satellite as well. The attack showed similarities to some activities of the Sandworm APT, the GRU unit 74455[955].
*Starlink* is a satellite-based network with low-orbit satellites. The users need a receiver and routing device to get the data which are transported with light. The low-orbit allows a reliable and fast data transfer. This makes senders and users independent from the physical internet. This was the reason why the owner Elon Musk provided it to the Ukraine shortly after the Russian attack[956].

### 8.9.4 Space Resilience

Based on the increasing threats, there is need for a concept of **space resilience** as the technical backbone of space defense. There is no official NATO definition, but resilience (or resiliency) is commonly understood as robustness and survivability[957].
The **space defense** needs to cover the **space segment** with spacecrafts, the **ground segment** with control center, ground station and remote centers as well as the IT facilities and the launch facility, and finally the **user segment** with customer terminals (such as satellite TVs)[958].

[954] Reuters exclusive 11 March 2022
[955] Mäder 2022b
[956] DW 2022
[957] Console 2018
[958] Console 2018

# 9 The Key Actors in Cyberspace

## *9.1 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.

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[959].
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[960].

## *9.2 The United States of America*

### 9.2.1 Overview

Intelligence:
The largest Intelligence Community is in the US where the *Director of National Intelligence DNI* (since 2004 in response to 9/11, his office is known as *ODNI*) coordinates all organizations, 8 of them are forming the military umbrella organization *Defense Intelligence Agency DIA*[961].

Within intelligence, four organizations have a prominent role in the cyber sector:

- The *National Security Agency NSA* as signal intelligence agency, which is combined by having the same director to the *US Cyber Command Cybercom*. The most frequently reported NSA unit is the *Tailored Access Operations (TAO) group,* an elite hacker unit for gaining access to systems of adversaries. Media reports suggest a link to the so-called *Equation Group*, which remains unconfirmed, refer to Section 5.

Non-military organizations are

- the *Central Intelligence Agency (CIA)*,
- the *Department of Homeland Security DHS* and the
- *Federal Bureau of Investigation (FBI)*.

[959] Wilson 2008, p.12
[960] 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
[961] DNI Handbook 2006

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[962]. The key unit is the *CIA Center for Cyber Intelligence*, refer to Section 5. Media reports suggest a link to the so-called *Longhorn Group*, which remains unconfirmed.

Military:
The military cyber unit is the *US Cyber Command Cybercom* that is subordinated to the Strategic Command *US STRATCOM* that plans and executes Cyberspace Operations[963].
*Cybercom* is the umbrella for the previously units of the navy, the army and air force which were founded between 1996 and 1998. *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'[964]. The US-CERTs are also working with the DHS.
For military research including cyber sector, the *US Department of Defense DoD* has established the agency *Defense Advanced Research Projects Agency DARPA.*

Technical aspects:
There are three internet security levels:

- the normal civil net as Non-classified Internet Protocol Router Network NIPRNET,
- the secured Secret Internet Protocol Router Network SIPRNET for critical infrastructure and government and close-to-military institutions and the
- *Joint Worldwide Intelligence Communication System JWICS* as third maximum security level for military operations [965].

Security partners:
The platform for cooperation between state and private sector is since 2005 the *Intelligence and National Security Alliance (Insa)*, which was formerly known as *Sasa (Security Affairs Support Association)* [966].

The NSA started the privatization within 1999-2005, the contractor companies settled in a commercial area one mile away from the NSA headquarter. The entire internal IT of the NSA was outsourced to the company *CSC*[967].

The US intelligence community has long-standing cooperation with firms who provide services or contractors to support the state organizations. In 2013, the 4

[962] Die Welt 2015 online, p.1, Tagesschau 07 Mar 2015
[963] USAF 2010, p.21-22
[964] Porteuos 2010, p.7
[965] in Germany the Herkules platform is similar to SIPRNET and the JASMIN database to JWICS.
[966] Wendt 2014
[967] Cyrus 2017

main providers were[968] *Booz Allen Hamilton BAH, CSC, SAIC/Leidos and L-3 communications.*
Armament Companies with large IT-service units are e.g., *Lockheed Martin*, *Northrop Grumman, General Dynamics and Raytheon*[969].

New figures from 2016 show that only 5 companies (*Leidos, BAH; CSRA, SAIC* and *CACI International*) employ 80% of the 45,000 external US-Intelligence staff, in total the agencies have 183,000 employees[970]. In the military *Defense Intelligence Agency (DIA)* 35% of the employees are external, in the *National Reconnaissance Organization (NRO)* even 95%[971].

The CIA runs the venture capital firm *In-Q-Tel* which supports companies in the IT sector, in 2013 these were 60 enterprises[972]. A prominent example is the joint venture *Recorded Future*. The CIA started its own federal lab in Sep 2020, which covers amongst others artificial intelligence, bioscience, virtual and augmented reality, quantum computing and advanced materials and manufacturing[973].
As already shown in various sections, the US also have a strong scene of cyber security firms.

### 9.2.2 Capacity building

The USA has systematically developed their cyber war capacities in the last 2 decades[974].
In 1988, the *Department of Defense DoD* established a *Computer Emergency Response Team CERT* at the Carnegie-Mellon University[975].
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*.

[968] SZ 2013, p.8-9
[969] SZ 2013, p.8-9. China believes that the United States and other Western countries are actively using defense contractors such as Lockheed Martin, Boeing, Northrop Grumman, and Raytheon for cyber-weapon development and deployment; Zhang 2012, p.805
[970] Cyrus 2017
[971] Cyrus 2017
[972] Buchter 2013
[973] Coleman 2020
[974] Hiltbrand 1999
[975] Porteuos 2010, p.3

Thereafter, Cyber Commands were established within the military branches[976] and consequently, a central *Cyber Command* (US CYBERCOM) was established in May 2010 with an estimated staff of 1,000 people and which was first led by the director of the National Security Agency NSA, General Keith Alexander[977]. Also, it is co-located with the NSA[978].
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[979]. In 2018, Army General Paul Nakasone took over the command.
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[980].

On the military level, capacity building 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[981].
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[982]. 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[983].

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[984].
In 2012, DoD started to build the *Cyber Mission Force (CMF)*, which is planned to include 6,200 military, civilian and contractor employees[985].

---

[976] 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
[977] Hegmann 2010, p.5, The Economist 2010, p.9/22-24, Glenny 2010, p.23
[978] DoD 2011, p.5
[979] Winkler 2014b, p.3
[980] Gierow 2016, p.1-2
[981] Barnes 2012
[982] 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.
[983] Black cited by Schanz 2010, p.52
[984] Matthews 2013, p.8
[985] DOD 2015, p.6

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 *Cybercom*.

### 9.2.3 Strategies and concepts

The primary aim of actors is to achieve and maintain **electromagnetic dominance** and **cyberspace superiority**[986] 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 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 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[987].
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.[988]
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[989]. However, the activities for cyber defense are still going on[990].

---

[986] USAF 2010a, p.2
[987] White House 2011, in particular p.5 and 9
[988] DoD 2011, p.8-9
[989] 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
[990] 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

In April 2015, the *US Department of Defense* released the *DOD Cyber Strategy*. 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[991].
The *DOD Cyber Strategy 2018* continues this strategy[992].

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[993].
On 11 May 2017, President Trump signed an Executive Order to strenghten cyber security of federal networks and critical infrastructures which orders the authorities to cooperate with private companies for defense and risk mitigation[994].

Under President Biden, the US government is utilizing the *Cyber Unified Coordination Group UCG* including private companies in 2021. The *Industrial Control System Initiative* was started with the *Electricity Subsector Action Plan* which will be followed by similar plans for pipelines, water and chemicals.

### 9.2.4 Cyber Exercises

A first large cyber exercise was the so-called *electronic Pearl Harbor* of the US Navy in 2002, where a massive attack on critical infrastructures was simulated. Since that time, the term ‚electronic Pearl Harbor' is often used as figure of speech for the consequences of cyber-attacks.
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 *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*[995].

Regular exercises are the *Cyber Storm* exercises which were organized by the *Department of Homeland Security (DHS)* and again, the capability to defend against

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.
[991] DoD 2015, p.8
[992] DoD 2018
[993] White House 2013
[994] Perloth 2017b
[995] 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.

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[996]. It was planned to test these codes in California, but not done to avoid unintended internet breakdowns[997]. Such internet shutdown tools also known as "**kill switches**" [998].

## *9.3 The Peoples Republic of China*

### 9.3.1 Overview

Both the civil and the military sector of China is under control of the Chinese Communist Party. The Chinas *People Liberation Army PLA* is suspected to have specialized cyber units in approximately 6 main locations[999].
The PLAs responsible unit is the *General Staff Department GSD* which consists of 4 Departments. This is Operations in 1st department, department intelligence in 2nd department, signals intelligence and network defense in 3rd department and Electronic Countermeasures and offensive cyber operations in 4th department[1000].

China has adopted the *"Integrated Network Electronic Warfare" (INEW)*, a formal information warfare strategy for *computer network operations (CNO) for both computer network attack (CNA)* and *Electronic Warfare (EW)* in 4th department of the GSD, while the computer network defense (CND) and intelligence is located in the 3rd Department[1001].
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[1002]. Chinese APTs were presented earlier in Section 5.

From 2017 on, a new Cyber security law requires for critical infrastructure sectors that hard- and software is undergoing a security check by the state before delivered by foreign companies. Also, data storage will from now only be allowed on Chinese servers[1003].

Meanwhile, US believes that the *Ministry of State Security MSS* has taken over the coordination of cyber operations from the PLA in 2015. [1004] The MSS conducts

[996] Welchering 2011, p. T2
[997] 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.
[998] von Tiesenhausen 2011, p.11
[999] Finsterbusch 2013, p.15
[1000] Mandiant 2013, Sharma 2011, p.64
[1001] Sharma 2011, p.64
[1002] Kremp 2011
[1003] Müller 2016, p.3
[1004] Langer 2018b

cyber operations through its 13th Bureau, which is known publicly as the *China Information Technology Evaluation Center (CNITSEC)*.
The persons working for and cooperating with the MSS are at least partially embedded into companies or universities, for examples persons linked to APT 40 in the *Hainan University*, to APT17 in the *Southeast University*, to APT3 in the *Xidian University* and to APT1 in the *Shanghai Jiao Tong University*, the *Zhejiang University* and the *Harbin Institute of Technology*. All six academic institutions are active in AI and machine learning research[1005].
The MSS has multiple front companies such as *Hainan Xiandun* from where four MSS members were spying for trade secrets, sensitive technologies etc.[1006]

### 9.3.2 Strategic goals

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[1007]. 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.[1008]

An analysis of the US 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[1009]. From this perspective, it is necessary to rethink the research focus on defensive tools[1010]. The NSA plans to handle Chinese cyber war issues in a more offensive way[1011].

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

[1005] Dakota 2021
[1006] DoJ 2021c
[1007] Krekel et al. 2009
[1008] Tinner et al. 2002
[1009] 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."
[1010] 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
[1011] Barnford 2010

conventional weapons („leapfrog strategy"). Cyber war cannot replace conventional capabilities, but helps to expand the own options quickly and also fits well with the concept of ‚**active defense**', where the early and quick elimination of possible retaliation of the enemy is an essential aim[1012].
Also, China is surrounded by states which have critical relations with China or are even allies of the USA[1013], 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.

## *9.4 Russia*

### 9.4.1 Overview

The APTs are under control of the intelligence services.
Russia has four services as successors of the former Soviet Intelligence KGB[1014]:

- FSO – Federal Protection Services which includes the Guard of the President in Kremlin
- FSB –Civil Interior Intelligence Service, but still conducting some foreign activities
- SVR - Civil Foreign Intelligence Service, also doing Intelligence Cooperation[1015]
- GRU or GU - Military Intelligence Service

.
As mentioned earlier, these services are believed by the West (and denied by Russia) to be linked to APT28 and APT 29 as well as to three units with focus on industry, the *Waterbug/Turla* Group, the *Sandworm/Quedagh* group and the *Energetic Bear/Dragonfly*[1016]. The existence of further APTs is under discussion.
The most prominent security firm is *Kaspersky Labs*, which has a good working relationship to the Russian state[1017], but strongly denies installing backdoors for the Russian state or similar measures.

Little is published about the **cyber troops** within the Russian army which are believed by media reports to exist since 2014 (meanwhile assumed to be GRU

[1012] Kanwal 2009, p.14
[1013] Rogers 2009
[1014] Ackert 2018a, p.7
[1015] Ackert 2018a, p.7
[1016] See e.g., Jennifer 2014
[1017] Russia Today (RT Deutsch) online 27 Jan 2017

members). 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"[1018]. In addition, an All-Russian hacker competition was initiated to recruit skilled young cyber professionals[1019].
In 2015, the Russian army has established *Science Squadrons*[1020]. Each squadron is planned with 60-70 soldiers.
Staffing is done from leading universities such as Moscow, St. Petersburg, Novosibirsk, Rostov and Far East. Activity areas include amongst others aviation, laser technology, software research and biotechnology.
The *Military Scientific Committee of the Armed Forces* has control which is affiliated to the *National Defense Management Center NDMC* which also is hosting the most capable military supercomputer which operates in the petaflop range. The results will be mostly classified, but it was reported that in IT security already 45 new software programs were developed.

Western analysts believe, also from the recent detainments of various Russians (*Yahoo hack, Michailow incident, US elections*), that Russia would have a distinct advantage in the cyber realm because it would engage the services of non-governmental cybercrime entities, which masks its role in cyber-attacks[1021]. According to the United Kingdom and other NATO intelligence services, the cyber potential of Russia comprises one million programmers and 40 cybercrime rings[1022].

As shown in the next chapter, cyber war includes from Russia's perspective also information warfare, see also *Section 2.2.6* with respect to the assumed role of **cyber trolls** and **social bots**. From the Russian point of view, Western states try to dominate information flow and to undermine Russia and other actors.

Russia has significantly strengthened its cyber security in this decade. Russia uses the surveillance system *SORM* for supervision of data traffic[1023]. 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[1024].
Russian authorities (*FSB and Federal Service for Technical and Export Control FSTEC*) asked providers increasingly since 2014 for source code to ensure that no backdoors and other security gaps are existing. Cisco, IBM and SAP do so while

[1018] Citation in Pravda 2012
[1019] Pravda 2012
[1020] Gerden 2015, SCMagazine 2015
[1021] Johnson 2016
[1022] Johnson 2016
[1023] FAZ 2010h
[1024] Wechlin 2016, p.6

*Symantec* has stopped cooperation. The review of source code is done only in rooms where code cannot be copied or altered[1025].

### 9.4.2 The cyber war concept of Russia

**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[1026].

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*." [1027] This definition is consistent with the information security doctrine given by President Putin in the year 2000[1028] 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*." [1029]

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[1030].

**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[1031]. 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[1032]. Also, lack of control may lead to de-stabilization and destruction[1033].

---

[1025] Reuters 2017b
[1026] Bazylev et al. 2012, p.10
[1027] 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.
[1028] 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.
[1029] Annex I, cited by Bazylev et al. 2012, p.11
[1030] Bazylev et al. 2012, p.11-15
[1031] Maliukevicius 2006, p.121
[1032] Maliukevicius 2006, p.125ff.
[1033] Bazylev et al. 2012, p.12

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[1034].

**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[1035] 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 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) [1036].
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.

### 9.4.3 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[1037]. 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")*[1038], the opinion that the various technologies cannot be separated in

[1034] 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).
[1035].
[1036] 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".
[1037] WCIT2012 presentation, introductory section
[1038] WCIT2012 presentation, section myths and misinformation

practice[1039] 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[1040].

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[1041]. While media reports focused much on the internet issue, the draft document suggested by these states also used the term ICT[1042]. 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[1043]. 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[1044] 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[1045].

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*"[1046]. Also, new ITRs were adopted, but a consensus could not be reached[1047]. As a consequence, the United States, the states of the European Union, Australia and many other states did not sign the new ITRs[1048]. The hard dispute between two large groups of states gave to some observers the impression of a **digital cold war**.

---

[1039] 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*"

[1040] ICT is mentioned in the WCIT2012 presentation, section myths and misinformation

[1041] Touré 2012

[1042] WCITleaks 2012. Please note that this was a 'leaked' draft only and not an official presentation

[1043] EU 2012b (Position Paper of the EU)

[1044] Kleinwächter 2012, p.31, Lakshmi 2012, p.1

[1045] Touré 2012

[1046] WCIT 2012 Resolution Plen/3

[1047] WCIT 2012 Final Acts

[1048] Betschon 2012, p.4, Lakshmi 2012 estimated that 113 of 193 member states will sign, 80 not.

In addition to the issues discussed above, the Internet Governance also influences the cyber capabilities. Recently, the US Air Force analyzed this as follows:[1049] "*Failure to pay attention to our vulnerabilities from Internet governance and friendly contest may provide our adversaries with a strategic advantage in cyber conflict. Our own cyber-attacks will also become complicated as networks that are not based on protocols and standards developed by US-entities are deployed by our competitors. […] The United States currently enjoys technological dominance through its position of developer and core provider of Internet Services made possible by the ICANN and the top-level Domain Name System.*"

## *9.5 Israel*

Israel is one of the leading cyber actors. Based on former officers from the military cyber unit *Unit 8200* and on a dynamic academic environment such as the University Tel Aviv there is a rapidly growing scene of cyber security firms such as *Cellebrite and NSO group*, which have e.g., demonstrated their ability on smartphone intrusion and decryption. For example, the founders of the security firms *CheckPoint* and *CyberArk* served in the Unit 8200[1050].

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[1051].

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[1052].

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*[1053].

## *9.6 The Federal Republic of Germany*

### 9.6.1 Overview

Civil sector:

*Federal Ministry of the Interior (Bundesministerium des Innern BMI)* with

[1049] Yannakogeorgos 2012, p.119-120
[1050] FAZ 2018e
[1051] Croitoru 2012, p.30
[1052] EPRS 2014, p.5/6
[1053] Rößler 2016, p.6

- *Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik BSI)* for protection of government IT infrastructure
- *"Zentrale Stelle für Informationstechnik im Sicherheitsbereich" (ZITIS), i.e., Central Service for IT in the security sector* for decryption services (BSI acts as code maker, Zitis as code breaker).[1054]
- The *Agency for cyber security innovations (Agentur für Innovation in der Cybersicherheit)* as civil-military cooperation between ministries of the Interior BMI and of Defense BMVg started in August 2020[1055].

Military sector:

- *Cyber and Information Space Command (Cyberinformationsraum-kommando CIR)* with *German Army Secret Service for Exterior Affairs (Kommando Strategische Aufklärung KSA)* with the sublevels for electronic warfare, *cyber network operations (CNO)* and the satellites (with the whole *Geoinformation GeoBw*).

Intelligence sector:

- Germany's foreign intelligence agency (*Bundesnachrichtendienst BND*) with department T4 (Abteilung T4) for cyber operations[1056]
- Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz BfV*) for domestic intelligence
- *Military Counterintelligence Agency (Militärischer Abschirmdienst MAD)* for the protection of the German army

Security partners include:

- *Secunet* for *Secure Inter-Network Architecture (SINA)* (Sichere Netzwerkarchitektur SINA)
- *Rohde and Schwarz* for cryptology
- *Genua* (owned by Bundesdruckerei) for VPN and firewalls

A state-related research unit is the *Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE*.

### 9.6.2 Background and details

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

[1054] Kirchner et al. 2017, p.5
[1055] BMI 2018
[1056] Mascolo/Steinke 2019, p.9

central role of the BSI for information security matters in Germany, in section 5 of the amendment also for the government communication[1057].

Important responsibilities and projects are e.g.,[1058]:

- member of the German Critical Infrastructure working group (AK KRITIS)[1059]
- 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[1060]
- document protection within Government procedures
- 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[1061]
- Work on **computer resilience**[1062] 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[1063]. The efficacy of the cyber defense center was so far affected by coordination issues between member authorities (Government, Intelligence, Police etc.)[1064].
- Also, a *National Cyber Security Council* that consists of the State Secretaries of all large federal ministries was established[1065].

---

[1057] Act to Strengthen the Security of Federal Information Technology dated 14 August 2009

[1058] Refer to Annual reports of the BSI 2005, 2006-2007 and 2008-2009 and 2010

[1059] 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)

[1060] Steinmann 2010, p.10

[1061] To control problems such as the computer radiation which allows to detect the information that is shown on the computer screen, Schröder 2008

[1062] Resilience means permanent availability. Not only cyber-attacks, but physical damages by an **electromagnetic pulse** are relevant issues here.

[1063] FAZ 2010g, p.4, Tiesenhausen 2011, p.11, BMI 2011

[1064] Goetz/Leyendecker 2014, p.5

[1065] 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

From 2016 on, a new decryption office was 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[1066].
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[1067], also known as '*Cyberfeuerwehr*'.
Security services for the federal government are usually derived from framework contracts of the BSI and the procurement office (Beschaffungsamt), including contracts with *Symantec*, which are in 2018 further supervised by *Trend Micro*.

Within the Intelligence Sector, the Federal Office for the Protection of the Constitution (German: *Bundesamt für Verfassungsschutz BfV* and *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[1068]. 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[1069] and which has key functions in military intelligence since 2008. In 2010 it had a workforce of 6,000 people[1070] and is responsible for

- the electronic warfare (Elektronische Kampfführung EloKa),

[1066] Heil/Mascolo 2016, Mascolo/Richter 2016, p.2
[1067] Biermann/Beuth/Steiner 2016
[1068] Rühl 2012, p.10
[1069] Eberbach 2002
[1070] Bischoff 2012

- since 2007, the KSA has a *computer- and network operation (CNO) unit*[1071] which is also responsible for cyber war issues[1072] and since 2012 ready for operations[1073]
- the new military satellites Synthetic Aperture Radar (SAR-Lupe)[1074] 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[1075]. 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-Systeme der Bundeswehr (BITS)*[1076]. The military cyber intelligence is handled by the MAD; the offensive capabilities are located in the KSA as CNO[1077].

The activities in the cyber and information space[1078], are now organized in a central Cyber and Information Space Command ('*Cyberinformationsraumkommando*'[1079]). The new command is now 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[1080]. The CNO capacities will be expanded to allow **Red teaming**, i.e., to train cyber-attacks[1081].

[1071] Bischoff 2012
[1072] 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.
[1073] Steinmann/Borowski 2012, p.1
[1074] 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.
[1075] Handelsblatt 2014, p.16
[1076] BmVg 2015a
[1077] BmVg 2015a
[1078] Leithäuser 2015b, p.4
[1079] Köpke/Demmer 2016, p.2
[1080] BmVg 2016
[1081] BmVg 2016, p.28

The capabilities for a hackback are planned to be expanded by an increase from 100 to 300 employees after 2018. A future threat, according to BMVg, are quantum computers, as all relevant actors run quantum projects[1082].

In 2015, the German military reported[1083] 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[1084].

The BND has established a cyber intelligence department in 2013[10851086]. 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[1087]. Also, it is planned to give more support to cyber defense, i.e., the information gained should help to prepare for cyber-attacks. Also, until 2022 the BND will get own espionage satellites[1088]. The BND will receive two satellites with the system *Secret Electro-Optical Reconnaissance System Germany (Georg)* by 2022. So far, BND and Bundeswehr are represented with liaison officers at the *National Geospatial Agency (NGA)*, from which they sometimes receive aerial photographs[1089].

The *Agency for cyber security innovations (Agentur für Innovation in der Cybersicherheit)* as civil-military cooperation between ministries of the Interior BMI and of Defense BMVg started in August 2020[1090] with a planned staff of 100 employees and will support research in this sector. This will not be a formal authority, but a government-owned agency which will be led by the BMI and

[1082] Der Spiegel 2018, p.12
[1083] Köpke/Demmer 2016, p.2
[1084] Spiegel online 2011
[1085] Flade/Nagel 2015, p.4
[1086] Spiegel 2013b, p. 22, also Spiegel 2013c, p.15
[1087] SZ 2014a, p.1
[1088] Lohse 2016, p.4
[1089] Biermann/Stark 2018, p.7
[1090] BMI 2018

BMVg. The original name was „disruptive innovations“ thus emphasizing cyber weapon research, but this was not used then.

### 9.6.3 The Doxing attack of 2018/2019

**Doxing** or **Doxxing** is used to violate the privacy of target persons by publication of private documents (term derived from docs = documents).
At the evening of 03 Jan 2019, it was revealed that an initially unknown attacker who was a 20-year-old school boy from the German region Hesse, who used Twitter with the cover names *G0d* (G0d is probably a reference to the online game *Minecraft*) alias *Orbit/Troja/Power/Orbiter* to put private data of 994 German politicians and celebrities online with the account @_ orbit[1091].

The first activities began as early as 19 Jul 2017 and on 24 November 2018 the user announced that he created an advent calendar with private data (such as secret phone numbers, testimonials and other personal data, but also internal party papers and copies of passports and diplomatic passports, from 2011-2018) [1092]. From 01 to 24 Dec 2018, data were actually gradually released, e.g., including information on Chancellor Merkel and President Steinmeier. Despite about 17,000 followers (at least some of them may be from the time before the account was taken over by the attacker[1093]), the action initially did not attract public attention.
The user *G0d* had been known in the hacker scene since years[1094] and e.g., hacked You-Tube accounts. *G0d* hacked and took over in 2015 the account of Yannick Kromer alias *Dezztroyz* to spread data and later on, he hacked the account of the well-known YouTuber Simon Unge to gain an increased public attention[1095].

The doxxing was possible through a combination of collection of public data and conventional password hacking[1096]. To prevent deletion of data, they were stored on up to 7 Asian and Russian download servers[1097], also he placed the links to the data on multiple accounts which are probably owned by the attacker as well, such as r00taccess, Nullr0uter, nigzyo etc.[1098]

One parliamentarian reported in December 2018 abnormal communication activity to the IT security authority BSI, which tried to resolve it with the MIRT-team, but at that timepoint they did not know that this was part of a larger attack. After the

[1091] Bender et al. 2019, Ludwig/Weimer 2019
[1092] Bewarder et al. 2019a and b
[1093] T-online exklusiv 2019
[1094] T-online exklusiv 2019
[1095] vgl. Bender et al. 2019, Ludwig/Weimer 2019
[1096] Decker/Köpke 2019, p.2
[1097] Bewarder et al. 2019b/Bender et al. 2019
[1098] Bewarder et al. 2019b/Bender et al. 2019

Social Democratic politician Martin Schulz was also affected[1099], a crisis meeting of the *National Cyber Defense Center* took place on 04 Jan 2019. Intense investigations were started under the direction of the Police Cybercrime Unit *Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT)* and it was reported that America, i.e., the NSA, was asked for help[1100].

The authorities did not find evidence of a breach into the government network and an individual attacker was suspected[1101].
Attribution was quicker than expected. A first trace was a photo on his Twitter account which apparently was a real photo showing him as a young teenager[1102].
The attacker used for his *Telegram* messages an account which was registered on the real number of his *German Telekom* mobile phone. Also, in a screenshot of an intruded *Amazon* account, he showed by error his *Windows 10* environment with a lot of icons of utilized programs and add-ons (such as *Perfect Privacy, Ghostery* and *ABP*) and the precise login date and time which allows *Amazon* to check which IP address communicated with this account[1103].

Despite the events, he still exchanged emails[1104]; he informed the YouTuber Jan Schürlein by an encrypted message on 05 Jan 2019, that he destroyed all hardware related to this event[1105]. On 06 Jan 2019 in Heilbronn, Jan Schürlein who had contact to the hacker was interviewed by the police[1106]. At the same day, the police could find the attacker who fully admitted the attack on 07 Jan 2019. No hints for foreign actors were found, instead the attacker stated he was angry about certain persons[1107].

The German government has immediately decided to strengthen the BSI by a staff increase from 800 to 1,300 and also the *National Cyber Defense Center* by giving coordination responsibilities and new analysis capabilities[1108].

## *9.7 United Kingdom*

The **United Kingdom** has done massive investments as part of their Cyber Strategies, the current National Cyber Security Strategy 2016 states that until 2021 £1.9 billion will be invested[1109].

[1099] Schubert 2019
[1100] Schmiechen 2019, Ludwig/Weimer 2019
[1101] Bild 2019
[1102] Bender et al. 2019
[1103] Denker et al. 2019
[1104] T-online exklusiv 2019
[1105] Van Lijnden 2019
[1106] Van Lijnden 2019
[1107] Decker/Köpke 2019, p.2
[1108] FAZ 2019a, p.1
[1109] National Cyber Security Strategy 2016

Current structure:

- *National Cyber Security Centre (NCSC)* as authority on the UK's cyber security environment, sharing knowledge, addressing systemic vulnerabilities and providing leadership on key national cyber security issues. The military *Cyber Security Operations Centre* will work closely with the NCSC.
- The *National Cybercrime Agency NCA* is fighting cybercrime.
- The *Defence Intelligence (DI)* as part of the *Ministry of Defence (MOD)* focuses on gathering and analyzing military intelligence and will be the place for the new cyber warfare unit
- The DI is not part of the UK's intelligence agencies (the MI6*, Government Communication Headquarters GCHQ* and MI5); of these, the GCHQ is specialized on cyber intelligence[1110].

## 9.8 France

The *Strategic Review for Defense and National Security* in 2017 was the starting point. There is a clear separation between military and civil defense.
The *National Cyber Security Agency ANSSI* coordinates the state's cyber security.

Also, **France** launched its first cyber-warfare unit to take on hackers. The French unit started work in Jan 2017[1111]. The *Commandement de Cyberdefense (Comcyber* or *Cocyber)* includes more than 3,200 Soldiers of Army, Navy and Air Force, before this cyberdefense departments existed since 2011. *Comcyber* is responsible for cyber operations, reconnaissance and defense, except the foreign intelligence DGSE which remained autonomy and which was reported to do offensive cyber-attacks as needed[1112].

The Russian *Turla* APT attacked 12 officials to unveil the French Navy oil supply chain in 2017 and 2018. France however prefers discrete problem solution and avoids naming and shaming [1113].

## 9.9 Further actors

**Iran** is also an active cyber actor. A recent example is the establishment of a *High Council of Cyberspace* (*Shoray-e Aali-e Fazaye Majazi*) which now gives directions to all other authorities involved in cyberspace[1114]. Before that, already a *Cyber*

[1110] National Cyber Security Strategy 2016, Ross 2016
[1111] AFP 2016
[1112] vgl. Lawfareblog 2019
[1113] vgl. Lawfareblog 2019
[1114] Nligf 2012, where also the existence of an informal 'cyber army' was noted.

*Defense Command* was established in 2010 for protection of critical infrastructures after the *Stuxnet* events.
For further cyber activities of Iran, please refer to Section 5.

A 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[1115].

## *9.10 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* had in 2012 only 12 member states (Finland, France, Germany[1116], Netherlands, Norway, Hungary, Spain, Sweden, United Kingdom with 2 CERTs, Switzerland, Austria and Denmark)[1117] [1118].
Meanwhile, a CERT-EU team for the security of EU IT infrastructure was permanently established in 2012 [1119]

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*.)"[1120]

---

[1115] Chhabra 2014, p.66-67
[1116] The German group CERT-Bund is presented on the BSI Website.
[1117] IT Law Wiki 2012b, p.1.
[1118] ECG 2008, Website of the ECG Nov 2010. Further CERT-Fora with involvement of the German CERT-Bund are FIRST (*Forum of Incident Response and Security Teams)* und TI (Trusted Intruder).
[1119] EU2013b, p.5
[1120] 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

The focus is now on the *ENISA (European Network and Information Security Agency,* since 2019 *European Union Agency for Cybersecurity*), that was founded in 2004 with regulation 460/2004 with a budget of 33 Mio. Euro and 50 employees. ENISA became operational in 2005 and was located in Heraklion/Iraklion, the capital of Crete, at the Southern EU border, which was perceived as a suboptimal solution[1121]. Meanwhile, it was renamed under EU Regulation No 2019/881 to *European Union Agency for Cybersecurity* and has its main office in Athens. In 2019, the budget was 17 Mio. Euro and it had 70 staff members.
The ENISA works on network security studies, encryption tools, etc. Cryptography is also part of the current EU research program[1122]. The focus is still on network and information security of the EU.
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[1123],
- 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[1124].
- In line with the European Commission Communication on Critical Information Infrastructure Protection 2009,[1125] 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[1126]. However, the exercise showed the uneven and uncoordinated national approaches and insufficient preparedness of smaller member states[1127]. The *Cyber Europe* exercise is now taking place regularly.

implemented. Taking these facts into consideration, the discussed development of an international **cyber war convention** seems to be unlikely, Dunlap 2011, p.83
[1121] EU-ISS 2007
[1122] ENISA 2007
[1123] EU 2007, EU 2009b
[1124] ENISA 2009a
[1125] EU 2009b
[1126] ENISA 2010a, ENISA2010b
[1127] 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."

The *European Cybercrime Centre E3C* as unit of *Europol* cooperates with ENISA and the *European Defense Agency EDA* to enhance cooperation for NIS matters[1128]. On 03 Sep 2014, it was officially announced that a new *Joint Cybercrime Task Force J-CAT* will be established at *Europol* as a joint effort of *Europol, the European Cybercrime Taskforce,* the *FBI* and the *British National Crime Agency NCA*.

In July 2020, the European Council imposed for the first time sanctions against cyber attackers, here six individuals and three entities for the attempted cyber-attack against the *OPCW (Organization for the Prohibition of Chemical Weapons)* by two GRU members which was disrupted by the Dutch Military Intelligence MIVD, against two members of the *Lazarus Group* for 'WannaCry' and 'NotPetya' and two APT10 members for the *'Operation Cloud Hopper*'. The sanctions imposed include a travel ban and an asset freeze[1129].

## *9.11 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[1130].

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[1131].
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*[1132] includes 3 cyber defense elements, these are

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

[1128] EU2013b, p.18
[1129] CFSP 2020
[1130] Schuller 2010, p.6
[1131] NCSA 2009a-c
[1132] NATO 2015

- 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[1133], Estonia with a staff of 30 people, which was in the first years supported by Estonia, Lithuania, Latvia, Italy, Spain, Slovakia and Germany[1134]. 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.
The CCD COE is responsible for the planning and coordination of training and further education solutions in cybersecurity for the entire alliance since January 2018.
NATO Cyber Defense exercises were *Digital Storm* and *Cyber Coalition* and were managed by the CCD CoE together with the NCIRC and other NATO bodies[1135]. The exercise Cyber Coalition (CC) is now done annually. *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"*)[1136].

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

[1133] In reality, the CCD CoE became operational already in 2006 after an Estonian initiative in 2004; CCDCoE 2010a
[1134] The NATO plans to rely on consultations after a cyber-attack; von Kittlitz 2010, p.33
[1135] Wildstacke 2009, p.28/29, CCDCoE 2010b
[1136] NATO 2010. For the NATO, not only cyber war, but all kinds of cyber-attacks are relevant, Hunker used 2010 the term **cyber power**.

internet and social media on one hand and cyber-attacks on the other hand[1137]. As a result, there is need for intense review of security policy with a particular focus on cyber resilience[1138]. 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[1139].
Analysts of the German Foreign Intelligence BND concluded that in armed conflicts cyber activities are particularly important in the early stage of the conflict[1140]. 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.

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[1141].
*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[1142].

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[1143]. However, this would mean to rely on the security efforts of multiple vendors, i.e., it is difficult to delegate the IT security. 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).

## *9.12 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

[1137] NATO 2014, BMVg 2015b
[1138] BMVg 2015b
[1139] Jones 2014, p.1
[1140] Leithäuser 2015a, p.8
[1141] Leithäuser 2015b, p.4
[1142] Sanger 2015, p.5
[1143] Leithäuser 2016, p.8

develop and implement National Information Communication (NICI) policies and plans[1144].
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)[1145].
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 2011[1146]. The convention is dealing with electronic commerce, data protection and processing and cybercrime in general, but does not contain specific provisions on cyber war[1147].

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*[1148].
A main topic in many documents is the need for intensified Inter-African Cooperation and to enhance cyber security awareness[1149].
South Africa already started the development of a *National Cyber Security Policy Framework* in 2010 which was approved by the cabinet in March 2012[1150]. One of the primary aims of this policy was the coordination of various national authorities dealing with cyber security[1151].

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 above[1152].

The headquarters of the African Union, which was built with the help of China in Addis Ababa, were regularly attacked by hackers, which are said to have come from Shanghai from 2012 to 2017. China vigorously denied this, but the Chinese IT technicians were replaced[1153].

---

[1144] ECA 2012, p.1
[1145] 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
[1146] ECA 2012, p.3, AU 2011
[1147] AU 2011
[1148] ECA 2012, p.4
[1149] 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.
[1150] South Africa 2012
[1151] South Africa 2010, p.6
[1152] Puhl 2013, p.118f.
[1153] FAZ 2018b

# 10 Cyber war and biologic systems

## *10.1 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[1154]. 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[1155].

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[1156]. 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[1157]. The challenge is to balance security/privacy with medical safety/usability[1158].

The Cybertech firm *Xtrap* in California found during a check that all 60 of 60 hospitals were already infected with malware.[1159] The FDA released in 2015 a warning for an internet-connected insulin pump from *Hospira* due to potential risk of hacking, in 2016, *Johnson and Johnson* warned 11,400 patients for their connected insulin pump as well[1160].

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-

[1154] Gupta 2012, p.13
[1155] Xu et al 2011, Gollakota et al 2011.
[1156] FDA 2013a
[1157] FDA 2013b, p.2
[1158] Gupta 2012, p.26
[1159] Lindner 2017
[1160] Jonas 2016, p.22, Lindner 2017

malware and to ensure secure data transfer to and from the device, and when appropriate, use accepted methods for encryption[1161].

Meanwhile, deep brain neurostimulators were developed that can measure the brain activity, emit signals out of the brain ('brain radio') and influence the brain by giving electric stimulation[1162]. 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[1163]. 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[1164].

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[1165]. Recently, cardiac pacemakers were developed that could utilize organ movements to win energy[1166]
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[1167]. 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[1168], 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[1169]. Intruders could not only track the individual user, but also use the

[1161] FDA 2013b
[1162] Young 2013, p.1, Medtronic 2013
[1163] LFP signals were found to encode dynamic aspects of behavior, unrelated background dynamics with distinct state fluctuations, and possibly other aspects, refer to Stamoulis/Richardson 2010, p.8
[1164] ClinicalTrials.gov 2013
[1165] Jürisch 2013, p.10
[1166] Welt online 20 Jan 2014
[1167] Stingl et al 2013
[1168] Such as delivery of electric shocks, see Gollakota et al 2011, p.1
[1169] Postinett 2013a, p.30

glasses to observe others[1170]. 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[1171].

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.

## *10.2 Relations between cyber and biological systems*

### 10.2.1 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 its 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[1172]. 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[1173]. The excessive release of cytokines, known as **cytokine release syndrome** or 'cytokine storm' can result in potentially fatal shock-like conditions (circulation failure, organ failure, blood clotting etc.)[1174].

---

[1170] Also, RFID chips are meanwhile implanted e.g., in expensive horses to prevent stealing and in some children to prevent kidnapping.
[1171] The analysis of user condition could also be done by cameras, such as in the new Microsoft X-Box, Mähler 2013, p.38
[1172] Haller 2009, p.57
[1173] Kash et al 2011, Stegemann-Koniczewski 2012
[1174] 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

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.
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[1175]. The *Sputnik* virophage is directed against the *Mimivirus* that can cause human pneumonia[1176], meanwhile the related *Zamilon* virophage was discovered[1177]. 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[1178], 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[1179].
The number of virophages is permanently growing, so several virophage genome sequences have been partially or fully assembled from metagenomic datasets, e.g., from two Antarctic lakes and the Yellowstone Lake[1180].

### 10.2.2 Bacteria

Bacteria are single-cell microorganisms that can infect other organisms such as humans[1181]. Some of those who cause relevant infections in humans can form liquid platforms called **biofilms**[1182] 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[1183].

Biotechnology allows to change genes or to introduce new genes into organisms, which raised concerns that new dangerous organisms maybe created

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
[1175] Zhou et al. 2012
[1176] Zhanga et al. 2012
[1177] Krupovic et al. 2016
[1178] Shah 2014, p.27
[1179] Scheubeck 2014, p.7
[1180] Krupovic et al. 2016
[1181] 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.).
[1182] Bakaletz 2012, p.2
[1183] Gebhardt 2013, p.38.

intentionally[1184] or inadvertently. In the last decade, a new phenomenon called **bio-hacking** was observed[1185]. 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[1186]. However, there are high structural, functional and energetic hurdles for achieving stable modifications of genes or organisms. Genetic modifications of bacteria typically result in microscopic variations of surface glycoproteins which could be used for production plant attribution like a fingerprint[1187].

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[1188]. 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[1189]. 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[1190]. Bacteriophage enzymes may have also military relevance, as one

[1184] 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).
[1185] Kunze 2013, p.19-20
[1186] 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.
[1187] 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. Young moths (*Galleria melonella*) also consume Polyurethan at much higher rates than Ideonella, Neuroth 2017. For 2019, the abstract is available under Biological Warfare - The Reference Module in Biomedical Sciences 2019. Elsevier ScienceDirect. https://doi.org/10.1016/B978-0-12-801238-3.62160-8
[1188] Yang et al. 2013, p.46ff
[1189] Mandal 2014
[1190] WHO 2014, Verbeken et al. 2014

bacteriophage product was effective against the standard bioweapon *Bacillus anthracis*, more commonly known as Anthrax[1191].

### 10.2.3 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 behavior and decision making[1192]. However, there are some limitations of potential cyborg[1193] scenarios:

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[1194]. 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[1195].

An example is the *tiger mosquito* that transmits *yellow fever, Dengue virus* and *Zika virus*[1196]. The attack program starts with the detection of carbon dioxide, then switches to the smell of unprotected skin and to darker colors; only after all criteria are met, the mosquito is landing and starts the blood sucking after injection of anesthetics and anticoagulants to ensure and easy and undisturbed sucking. When the stomach is filled with blood, the mosquito stops and flies away. The *Dengue virus* changes this program in a way that the mosquito more often takes incomplete meals. The increased frequency gives the dengue virus more chance for infection

[1191] Zucca/Savoia 2010, p.83
[1192] Jüngling 2014, p.63
[1193] 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 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.
[1194] 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
[1195] Perrot-Minnot and Cézilly 2013, p136-137
[1196] Feldmeier 2022

and replication. However, also here the virus is not "controlling" the animal, but it is disturbing regular procedures.

In humans, the parasite *Toxoplasma gondii* has been shown to influence human behavior (such as affects, novelty seeking, schizophrenia risk, dominant attitude of infected males etc.) significantly by infecting the brain[1197] as evaluated by several standard psychological questionnaires. The behavioral influence is based on changing dopamine and testosterone levels[1198], 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 behavioral changes facilitate enhance transmission to the feline definitive host[1199]. Also, it is not yet clear which effects in humans are really targeted manipulations or just side effects of the chronic infection[1200].

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[1201]. The DBS works by sending electric signals to groups of specialized nerve cells, so-called nuclei, which are located deeply in the brain and where the probe is located[1202]. 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 influence by as the nuclei below the cortex are involved in the emotional and hormonal system[1203] 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[1204]. Recently, a chip became commercially available which after connection allows control cockroach movements by smartphones, here as *RoboRoach* from the firm *Backyard Brains*.

---

[1197] Adamo and Webster 2013, p.1, Flegr 2013, p.127f.

[1198] 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.

[1199] Adamo and Webster 2013, p.2, Flegr 2013, p.128

[1200] Flegr 2013, p.127

[1201] 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

[1202] VNS stimulates the tenth brain nerve, the vagus nerve, the stimulation is done beyond the brain.

[1203] 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

[1204] Hummel 2014b

The cockroach species is *Blaberus Discoidalis*[1205]. 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[1206]. Electric signals to the antennae induce a movement change of the cockroach by remote control via smartphone and Bluetooth[1207]. 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[1208]. 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.

## *10.3 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 data are leaving the computer (or the smartphone) in the background, also not why, to whom and to which extent[1209]. 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.

---

[1205] Hummel 2014a, p.1

[1206] Hummel 2014a, p.2

[1207] 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

[1208] Park et al. 2016

[1209] Even the television may record and export all user data without knowledge if designed as Internet-TV (IPTV), SZ online 2013b

# 11 Literature references


Abbany, Z. (2020): Modern spy satellites in an age of space wars. Deutsche Welle online 25 Aug 2020 Article a-54691887

Abdollah, T. (2019): US launched retaliatory strike against Iranian military computers, as cyber war escalates. The Sydney Morning Herald 23 Jun 2019

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

Ackert, M. (2018a): Russlands Geheimdienst fürs Grobe. Neue Zürcher Zeitung, 26 Sep 2018, p.7

Ackert, M. (2018b): Russlands Militärgeheimdienst wird bloßgestellt. Neue Zürcher Zeitung, 08 Oct 2018, p.3

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

AFP (2016): France launches first cyber-warfare unit to take on hackers. 13 Dec 2016

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

Akamai (2017): akamai's [state of the internet] / security Q1 2017 report 26 pages

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

Alvarez, S., Jansen, F. (2016): Hackerangriff auf die Telekom. Der Tagesspiegel online 28 Nov 2016

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

Ammann, B. (2016): Genug Daten für eine Doktorarbeit. Neue Zürcher Zeitung 24 Oct 2016, p.3

Ankenbrand, H. (2020): Trumps Angriff auf Chinas Herzstück. Frankfurter Allgemeine Zeitung, 08 Aug 2020, p.24

Ankenbrand, H., von Petersdorf, W. (2020): Huawei droht der Todesstoß. Frankfurter Allgemeine Zeitung, 19 Aug 2020, p.16

Ankenbrand, H., Finsterbusch, S. (2022): Chinas Chip-Pläne stecken in der Sackgasse. Frankfurter Allgemeine Zeitung 18 Aug 2021, p.22

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

Arrieta, A.B. et al. (2020): Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities, and challenges toward responsible AI. Information Fusion 58 (2020), p. 82–111

Asendorpf, D. (2017): Error. Die Zeit 27 Jul 2017, p.33

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

ATP 3-12.3 (2019): Army Techniques Publication No. 3-12.3. Headquarters Department of the Army. Washington, DC, 16 July 2019. Approved for public release; distribution is unlimited.

Atzei, N., Bartoletti, M. Cimoli, T. (2016): A survey of attacks on Ethereum smart contracts. Universita degli Study di Cagliari; Cagliari Italy, Working Paper 2016, 24 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

Baches, Z. (2016): Wie Hacker eine Notenbank knacken. Neue Zürcher Zeitung, 10 Oct 2016, p.7

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

Barker, T., Tiirmaa-Klaar, H. (2022): Russlands Cyberkriege. Welt Am Sonntag 19. March 2022, p.27

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

Bayak, F. (2020): Hack may have exposed deep US secrets. Damage yet unknown. AP News online 15 Dec 2020

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

BBC (2019): Ex-CIA agent Jerry Chun Shing Lee admits spying for China. BBC online 02 May 2019

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

Becker, L. (2018): "Black Dot Bug" in iOS11: Zeichenfolge legt Nachrichten-App auf iPhone lahm. Mac & I news 04 May 2018

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

Beiersmann, S. (2017a): Wikileaks macht Tool zur Erkennung von CIA-Malware öffentlich. ZDNet 03 Apr 2017

Beiersmann, S. (2017b): Brutal Kangoroo: Wikileaks enthüllt weiteres Hacking Tool der CIA. ZDNet 26 Jun 2017

Beiersmann, S. (2017c): Sicherheitsforscher: Petya 2017 soll Daten zerstören und nicht verschlüsseln. ZDNet 29 Jun 2017

Beiersmann, S. (2017d): HighRise: CIA-Malware für Android fängt SMS-Nachrichten ab. ZDNet 17 Jul 2017

Beiersmann, S. (2017e): NSA verliert erneut wichtige Daten. ZDNet. 06 Oct 2017

Beiersmann, S. (2017f): Amazon kündigt AWS Secret Region für Geheimdienste an. ZDNet 21 Nov 2017

Beiersmann, S. (2018a): EternalBlue: Botnetz nutzt NSA-Exploit für Kryptomining. ZDNet 03 Feb 2018

Beiersmann, S. (2018b): GitHub trifft weltweit größter DDoS-Angriff. ZDNet 02 Mar 2018

Beiersmann, S. (2018c): GitHub Hacker steigern DDos-Rekord auf 1,7 Terabit/s. ZDNet 07 Mar 2018

Bender, J. et al. (2019): Erst Flop, dann Staatsaffäre. Frankfurter Allgemeine Zeitung 05 Jan 2019, p.3

Benrath, B. et al. (2021): Der Fukushima-Moment. Frankfurter Allgemeine Zeitung 15 Dec 2021

Benrath, B., Finsterbusch, S., Heeg, T. (2022): Russlands Cyberwaffen. Frankfurter Allgemeine Zeitung vom 26 Feb 2022, No. 48, page 28

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

Betschon, S. (2017): Raub von Rechenleistung. Neue Zürcher Zeitung 18 Oct 2018, p.37

Betschon, S. (2018a): Saisonschlussverkauf der iPhoneHacker. Neue Zürcher Zeitung 19 Mar 2018, p.7

Betschon, S. (2018b): Intel-Prozessoren veruntreuen Daten. Neue Zürcher Zeitung 22 Aug 2018, p.37

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

Beuth, P. et al. (2017): Merkel und der schicke Bär. Die Zeit No.20 11 May 2017, p.13-15

Bewarder, M. et al. (2019): Hackerangriff erschüttert das politische Berlin. Die Welt 05 Jan 2019, p.1

Bewarder, M. et al. (2019b): Gods Werk und Twitters Beitrag. Die Welt 05 Jan 2019, p.4

BfV (2017): Cyberbrief 01/2017, 6 pages

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

Biermann, K, Stark, H. (2018): Merkel sieht alles. – Der BND bekommt eigenen Satelliten. Die Zeit No. 8/2018, p.7

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

Bild (2017): Russen-Hacker führen deutschen Diplomaten vor. Bild 20 Nov 2017, p.1 and 3

Bild (2019): Wer steckt hinter den Angriffen? Bild 05 Jan 2019, p.2

Bing, C., Taylor, M. (2020): Exclusive: Chinese-backed hackers targeted COVID-19 vaccine firm Moderna. Reuters online 30 July 2020

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

BMI (2018): Bundesministerium des Innern (Federal Ministry of the Interior): Agentur für Innovation in der Cybersicherheit. 29 Aug 2018

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

Bodkin, H, Henderson, B. (2017): NHS cyber attack spreads wordwide. The Telegraph online 12 May 2017

Böck, H. (2017): Hacker sabotieren das Internet der unsicheren Dinge. Die Zeit online 07 April 2017

Böck, H. (2019): Linux-Rechner übers Netz abschießen. Golem.de 18 Jun 2019

Böhringer, H.C. (2022): Wer hat Angst vor Dall-E2? Frankfurter Allgemeine Zeitung, 29 Aug 2022, No. 200, p.11

Boey, D. (2017): North Korean Hacker Group linked to Taiwan Bank Cyberheist Bloomberg Technology online Oct 2017

Bommakanti, K. (2020): A.I. in the Chinese Military: Current Initiatives and the Implications for India Observer Research Foundation (ORF) Occasional Paper 234 February 2020

Borchers, D. (2017): Wikileaks: CIA tarnt Spionage-Software mit gefälschten Kaspersky-Zertifikaten. Heise online 11/2017

Bost, B. (2022): Möglicherweise eine Art Überlebensgarantie. Preußische Allgemeine Zeitung. 19 Aug 2022, p.7

Bowen, A.S. (2021): Russian Military Intelligence: Background and Issues for Congress. CRS Report R46616

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

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

Brühl, J., Tanriverdi, H. (2018): Einbruch per email. Süddeutsche Zeitung Nr. 51 vom 02 Mar 2018, p.2

Brühl, J. (2020): Corona-Impfstoff im Visier der Spione. Süddeutsche Zeitung No. 163, 17 July 2020, p.9

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

Brundage, M. et al. (2018): The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute University of Oxford/Centre for the Study of Existential Risk University of Cambridge/Center for a New American Security/Electronic Frontier Foundation/OpenAI February 2018

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

BSI (2022): BSI Homepage Emission Security (English version). Last retrived 22 Sep 22. https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Geheimschutz/Abstrahlsicherheit/abstrahlsicherheit_node.html

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

Buchter, H. (2013): Die Profiteure. Die Zeit No. 33/2013, p.21

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

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

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

Campbell, D. et al. (2013): Revealed: Britain's secret listening post in the heart of Berlin. The Independent online 05 Nov 2013

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

CERT France (2020): The Malware Dridex: Origin and Uses. 17/07/2020 https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

CFR (2016): Shouting at Americans: A Peek Into French Signals Intelligence. Council of Foreign Relations 15 Sep 2016

CFR (2019): Cyber Operations Website: Careto. www.cfr.org/cyber-operations/

CFSP (2020): Council Decision (CFSP) 2020/1127 of 30 July 2020 Amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

Cherepanov, A. (2018): GreyEnergy - A successor to BlackEnergy. ESET White Paper, October 2018, 31 pages.

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

Check Point Research (2017): Mid-Year Report Cyber Attack Trends 2017, 19 pages

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

Chiesa, R. (2015): Lectio Magistralis Hacking Cybercrime e underground economy (con u po di cyber espionage) Arcetiri, Firenze, INFN 5 Novembre 2015

Chiesa, R. (2017): IoT & IoX Cybersecurity: are you ready for the very first Hackmageddon? Presentation in Milan, 17 May 2017

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

Cimpanu, C. (2018): How US authorities tracked down the North Korean Hacker behind Wannacry. ZDNet 06 Sep 2018

Cimpanu, C. (2019): NASA hacked because of unauthorized Rapsberry Pi connected to its network. ZDNet 21 June 2019

Cimpanu, C. (2020): Exclusive: FBI alerts US private sectors about attacks aimed at their supply chain software providers. ZDNet 10 Feb 2020

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

Coleman, J. (2020): CIA creates its own federal lab 21 Sep 2020

Console, A. (2018): Space Resilience – Why and How? The Importance of Space Resilience and the Current Approach. Joint Air Power Competence Centre (JAPCC) Journal Edition 27/2018, p.10-16

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

CrowdStrike (2016): Danger close Blog Nov 2016

CRS (2019): "Space Force" and Related DOD Proposals: Issues for Congress. Congressional Research Service CRS Paper 08 April 2019

CSA (2022): Joint Cybersecurity Advisory (CSA) Destructive Malware Targeting Organizations in Ukraine Product AA22-057A February 26, 2022

CT (2018): Super-Gau für Intel: Weitere Spectre-Lücken im Anflug. CT online 03 May 2018

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

Cyrus, O. (2017): Geheimdienste auslagern - ein Spiel mit dem Feuer, Neue Zürcher Zeitung 13 Oct 2017, p.16

Da Silva, G. (2021): REvil begann als ungeschicktes Startup. NZZ 08 July 2021, p.14-15

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

Dakota, C. (2021): Academics, AI, and APTs Center for Security and Emerging Technology (CSET) Issue Brief March 2021

Danchin A., Fang, G. (2016): Unknown unknowns: essential genes in quest for function. Microb Biotechnol. 2016 Sep;9(5):530-40. doi: 10.1111/1751-7915.12384. Epub 2016 Jul 20

Van Dantzig, M., Schamper, E. (2019): Operation Wocao. Shining a light on one of China's hidden hacking groups 19 Dec 2019 Fox-IT

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

Decker, M., Köpke, J. (2019): Ein Schüler hackt das Land. Neue Westfälische 09 Jan 2019, p.2

Defense One (2020): An AI Just Beat a Human F-16 Pilot In a Dogfight — Again 21 Aug 2020 https://www.defenseone.com/technology/2020/08/ai-just-beat-human-f-16-pilot-dogfight-again/167872/

Demchak, C.C. and Shavitt, Y. (2018): China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking. Military Cyber Affairs: Vol. 3: Iss. 1, Article 7. 9 pages

Denker, H., Roodsari, A.V., Wienand, L., Kartheuser, B. (2019): Wie konnte ein 20-Jähriger den Riesenhack schaffen? T-Online Nachrichten 08 Jan 2019

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

Derespins, C. (2017): Wikileaks releases entire hacking capacity of the CIA. FOX News US 07 Mar 2017

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

Der Spiegel (2018): Gerüstete Cyberkrieger. Der Spiegel No. 25/2018, p.12

Deutsche Welle (2017): Hackerangriff auf OSZE Deutsche Welle online 25 Dec 2016

Deutschlandfunk (2017): CIA verdächtigt ehemaliges Vertragsunternehmen Deutschlandfunk online 13 Mar 2017

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

Diehl, J. et al. (2018): Teherans Papierdiebe. Der Spiegel No. 17/2018, p.58-59

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

Die Welt online (2015): CIA plant Großoffensive gegen Cyberangriffe. 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

Die Zeit online (2014): Cyberangriff: Hacker spionierten Luft- und Raumfahrtzentrum aus. 13 Apr 2014

Die ZEIT online (2017): Mutmaßlicher russischer Hacker in Spanien festgenommen. 10 April 2017

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

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

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

DoD (2018): Summary of the 2018 DoD Cyber Strategy, 10 pages. Published by US Department of Defense (DoD)

DoD (2018): U.S. Department of Defense, Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity

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

DoJ (2018): Indictment United States of America versus Zhu Hua and Zhang Shilong. United States District Court - Southern District of New York. Unsealed on 20 Dec 2018.

DoJ (2020): Indictment against 6 Russian GRU officers from GRU unit 74455, unsealed 19 Oct 2020, 50 pages

DoJ (2021a): Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Around the Globe. 17 Feb 2021

DoJ (2021b): Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside. Monday, June 7, 2021

DoJ (2021c): Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research July 19, 2021

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

Dragos Inc. (2017): CRASHOVERRIDE. Analyzing the Threat to Electric Grid Operations. 35 pages

Dragos (2017): TRISIS malware. Dragos version 1.2017213, 19 S.

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

DW (2017): Yahoo-Datenklau viel größer als gedacht. Deutsche Welle online

DW (2019): France details military command of space plans to protect satellites. Article a-49747318

DW (2022): So funktioniert Starlink - auch in der Ukraine. DW online 15 Jun 2022

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

EC (2020): White Paper On Artificial Intelligence - A European approach to excellence and trust Brussels, 19.2.2020 COM(2020) 65 final

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

Eckstein, P., Strozyk, J.L. (2018): Hacker erbeuten Pläne von Atomanlagen. Tagesschau online 01 Nov 2018

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

Elbadawi M., Efferth T. (2020): Organoids of human airways to study infectivity and cytopathy of SARS-CoV-2. Lancet Respir Med 2020 Published Online May 21, 2020 https://doi.org/10.1016/S2213-2600(20)30238-1

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

ESET (2016): En Route with Sednit Part 1: Approaching the Target. Version 1.0 October 2016, 40 pages ESET

ESET (2018): LOJAX - First UEFI rootkit found in the wild, courtesy of the Sednit group. ESET Research Whitepapers, September 2018 24 pages

ESET (2019): Operation Ghost: The Dukes aren't back – they never left. ESET Research. 17 Oct 2019

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 (2016): Commission Services Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace. Brussels, 2 December 2016 15072/16

EU (2019): EU Space Policy Fact Sheet of the European Commission.

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

EUROPOL (2016): ‘Avalanche’ Network dismantled in International Cyber Operation. Press Release 01 December 2016

Europol (2017): Massive blow to criminal dark web activities after globally coordinated operation. 20 July 2017

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

FAS (2018): Lernende Spione. Frankfurter Allgemeine Sonntagszeitung No. 9/2018, p.7

FAS (2019): Sicherheitsexperten manipulieren Teslas Autopiloten. Frankfurter Allgemeine Sonntagszeitung No. 9, 03 April 2019, p.21

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

FAZ (2000): Amerikaner hören angeblich Datenleitungen in Europa ab. FAZ 24 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

FAZ (2017a): Geheimdienstler verhaftet. Frankfurter Allgemeine Zeitung, 28 Jan 2017, p.5

FAZ (2017b): Russische Spione wegen Cyberangriffs auf Yahoo angeklagt. Frankfurter Allgemeine Zeitung 16 Mar 2017, p.23

FAZ (2017c): Schlag gegen Darknet-Handel. Frankfurter Allgemeine Zeitung 13 Jun 2017, p.4

FAZ (2017d): Amerika: Hinter Wannacry steckt Nordkorea. Frankfurter Allgemeine Zeitung 20 Dec 2017, p.6

FAZ (2018a): Die gefährlichste Sicherheitslücke aller Zeiten und ihre Entdecker. Frankfurter Allgemeine Zeitung 08 Jan 2018, p.22

FAZ (2018b): Hat Peking spioniert? Frankfurter Allgemeine Zeitung 31 Jan 2018, p.18

FAZ (2018c): Wie die Schlange vor dem Kaninchen, Frankfurter Allgemeine Zeitung No. 52/2018, p.2, 02 Mar 2018

FAZ (2018d): Der Flughafen Saarbrücken wird bald ferngesteuert. Frankfurter Allgemeine Zeitung No. 91/2018 vom 19 April 2018, p.21

FAZ (2018e): Wie sich Hacker in der Telegram-App zusammentun. Frankfurter Allgemeine Zeitung No. 107/2018 vom 09 May 2018, p.22

FAZ (2018f): Bitcoin-Kurs verliert nach Hackerangriff 13 Prozent. Frankfurter Allgemeine Zeitung 20 Jun 2018 online

FAZ (2018g): Mit Sicherheit aus Israel. Frankfurter Allgemeine Zeitung 26 Nov 2018, p.20

FAZ (2019a): Bundesregierung will nach Datendiebstahl Cyberabwehr verbessern. Frankfurter Allgemeine Zeitung 08 Jan 2019, p.1

FAZ (2019b): Amerika will mehr seltene Erden fördern. Frankfurter Allgemeine Zeitung, No.130, p.17

FAZ (2022): Hacker stehlen 182 Millionen Dollar. Frankfurter Allgemeine Zeitung 21.04.2022 No. 92, S.25

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

Feldmeier, L. (2022): Das Virus steuert die Mücke. NZZ, 06 Jul 2022, p.25

Financial Times (2019): Beijing orders state offices to replace foreign PCs and software 08 Dec 2019 https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406

Finkbeiner, A. (2021): Kampf im Orbit. Spektrum der Wissenschaft 17 Mar 2021

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

Finsterbusch, S. (2021): Cyberbanden und ihre Waffen. Frankfurter Allgemeine Zeitung, 14 May 2021, p.18

FireEye (2014): APT28: A Window into Russia's Cyber Espionage Operations? 45 pages

FireEye (2015): APT30 and the mechanisms of a long-running cyber espionage operation. 12 April 2015

FireEye (2017): APT overview in www.fireeye.com/current-threats/apt-groups.html

FireEye (2018a): APT overview in www.fireeye.com/current-threats/apt-groups.html

Fireeye (2018b): Triton Attribution: Russian Government-owned Lab most likely built tools. FireEye-Intelligence online 23 Oct 2018

FireEye (2019): APT39: An Iranian Cyber Espionage Group Focused on Personal Information. 29 Jan 2019

FireEye (2022): APT overview in www.fireeye.com/current-threats/apt-groups.html

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

Floemer, A. (2020): Teslas Modell 3 ist VW und Toyota technisch um sechs Jahre voraus. Welt Online 19 Feb 2020

Flückiger, J. (2014): Staatstrojaner mit Risiken und Nebenwirkungen. Neue Zürcher Zeitung 03 July 2014, p.27

FM (Field Manual) 3-36 (2012): Electronic Warfare. Headquarters Department of the Army. Washington, DC, 9 November 2012. Approved for public release; distribution is unlimited.

FM (Field Manual) 3-38 (2014): Cyber Electromagnetic Activities. Headquarters Department of the Army. Washington, DC, 12 February 2014. Approved for public release; distribution is unlimited.

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

Folmer, K., Margolin, J. (2020): Satellite data suggest Coronavirus may have hit China earlier: Researchers. ABC News online, 08 June 2020

Fox News (2017): John Kasich: OhioGovernor's website hacked with pro-ISIS propaganda 25 Jun 17

Fox Business 2019: Russian 'Evil Corp' hackers charged with $100M in cyber theft 05 Dec 2019

Franke, U.E. (2019): Not smart enough: The poverty of European military thinking on artificial intelligence – ECFR/311 December 2019

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

Freidel, M. (2018): Pjöngjangs digitale Raubzüge. Frankfurter Allgemeine Zeitung 05 Feb 2018, p.3

Fritz, J. (2008): "How China will use cyber warfare to leapfrog in military competitiveness," Culture Mandala: The Bulletin of the Centre for East-West Culture and Economic Studies, Bond University, Vol. 8, 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

Fuest, B. (2018): Leben mit einem Geist. Welt am Sonntag 07 Jan 2018, p.42

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

Gartmann, F., Jahn, T. (2013): Die Geheim-Dienstleister. Handelsblatt 26 Jun 2013, p.24

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

Gebauer, M. et al. (2016): Kühler Krieg. Der Spiegel 39/2016, pp.14-20

Gebauer, M., Wolfangel, E. (2017): Wer war das? Die Zeit 01 Jun 2017, p.31-32

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

Gerden, E. (2015): Russia to ramp up spending on military science. Chemistry World online 02 Sep 2015

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

Gettinger, D. (2019): The Drone Databook. The Center for the Study of The Drone at Bard College, 353 pages

GGE (2021): Report of the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security - Letter of transmittal 28 May 2021

Gibney, E. (2022): Where is Russia's cyberwar. Researchers decipher its strategy. 17 March 2022 Including correction from 18 March 2022. Nature.com/articles/d41586-022-00753-9

Giles, M. (2019): Trition is the most murderous malware, and its spreading. Technology Review online, article 613054

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

Giesen, C., Mascolo, G. and Tanriverdi, H. (2018): Hört, hört. Süddeutsche Zeitung 14 Dec 2018, p.3

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

Goddins, D. (2020): Machine-learning clusters in Azure hijacked to mine cryptocurrency. Ars Technica, 11 June 2020

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

Goetz, J., Steinke, R. (2017): Geheimnisse aus Tresor Nummer 7. Süddeutsche Zeitung No. 58/2017, p.7

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

Gollmer, F. (2019): Eine andere soziale Welt. Neu Zürcher Zeitung 04 Sep 2019, p.7

Gollmer, P. (2022a): Erneut ein Hacker-Großangriff auf Kryptowährungen. Neue Zürcher Zeitung 02 April 2022, p.14

Gollmer, P. (2022b): Russische U-Boote interessieren sich für das Nervensystem des Internets. Neue Zürcher Zeitung 29. April 2022, p.4

Goodin, D. (2017): Advanced CIA firmware has infected Wi-Fi routers for years. Ars Technica 16 Jun 2017

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

Gräfe, D., Link, C. und Schulzki-Haddouti, C. (2018): Das ist über den Hackerangriff bekannt. Stuttgarter Nachrichten online 01 Mar 2018

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

GReAT (2018): OlympicDestroyer is here to trick the industry. 08 March 2018

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

Gruber, A., Reinhold, F. (2017): Was die Whistleblowerin Reality Winner enthüllte. Spiegel online 06 Jun 2017

Grüner, S. (2019): ME-Hacker finden Logikanalysator in Intel-CPUs. Golem.de 01 April 2019

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

Gyr, M. (2016): Geheime Daten aus dem Innersten des Nachrichtendiensts entwendet. Neue Zürcher Zeitung 11 Nov 2016, p.29

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

Hacquebord, F. (2017): Zwei Jahre Pawn Storm. Analyse einer mehr in den Mittelpunkt rückenden Bedrohung. Forward-Looking Threat Research (FTR) Team, TrendLabs Forschungspapier 2017, 37 pages

Häuptli, L. (2018): Chinesen spionieren in der Schweiz. Neue Zürcher Zeitung 08 Jan 2018, p.1

Harris, S., McMillan, R. (2017): Authorities Question CIA Contractors in Connection with Wikileaks Dump. Wall Street Journal 11 Mar 2017

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

HCSEC (2019): Official Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. Annual Report 2019. A report to the National Security Adviser of the United Kingdom March 2019

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

Heide, M., Huttner W.B. and Mora-Bermudez, F. (2018): Brain organoid models for neocortex development and evolution. Current Opinion in Cell Biology 2018, 55:8–1

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

Heighton, L. (2016): Second referendum petition: Inquire removes at least 77,000 fake signatures, as hacker claim responsibility for ‚prank'. The Telegrapah 27 Jun 2016 online

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

Hermann, J. (2020): Brisante Fragen zu den Crypto-Leaks Neue Zürcher Zeitung, 27 Feb 2020, p.5

Hern, A., Gibbs, S. (2017): What is WanaCryptOR 2.0 ransomware and why it is attacking the NHS? The Guardian 12 May 2017

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

Herwig, S. (2021): Operation Russland. Frankfurter Allgemeine Zeitung 04 March 2022, p. 15

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

Hlavica, L.K. (2021): Hacker-Attacks Against Satellites. An Evaluation of Space Law in Regard to the Nature of Hacker-Attacks. Master thesis at the Vrije Universiteit Amsterdam, August 2021

Hoadley D.S., Sayler, K.M. (2019): Artificial Intelligence and National Security Congressional Research Service R45178 Version 6 Updated November 21, 2019

Hoehn, J. (2021a): Defense Primer: Military Use of the Electromagnetic Spectrum. Updated September 27, 2021. Congressional Research Service CRS, Document IF 11155, Version 12

Hoehn, J. (2021b): Defense Primer: Electronic Warfare. Updated September 29, 2021. Congressional Research Service CRS, Document IF 11118

Hoehn, J. (2021c): Defense Primer: Directed-Energy Weapons. Updated September 29, 2021. Congressional Research Service CRS, Document IF 11882

Hoehn, J.R., Sayler, K.M., Gallagher, J. (2021): Overview of Department of Defense Use of the Electromagnetic Spectrum. Updated August 10 ,2021 R46564

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

Holland, M. (2018): Fitnesstracker: Strava-Aktivitätenkarte legt Militärbasen und Soldateninfos in aller Welt offen. Heise online 29 Jan 2018

Hoppe, T., Osman, Y. (2015): Cybersturm auf Berlin, Handelsblatt 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

Hunt, A. Gentzkow, M. (2017): Social Media and Fake News in the 2016 election Paper of Stanford and New York University 40 pages

Hyslop, W.D. et al. (2020): Indictment by the United States District Court for the Eastern District of Washington from 07 Jul 2020

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

Insikt group (2018): Chinese Threat Actor TEMP.Periscope targets UK-based engineering company using Russian APT techniques. Recorded Future Blog 13 November 2018

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

Jansen, J. (2016): Der Feind in meinem Herzschrittmacher. Frankfurter Allgemeine Zeitung 09 Oct 2016, p.22

Jansen, J. (2017): Hunderte Millionen Smartphones ausspioniert. Frankfurter Allgemeine Zeitung 28 Aug 2017, p.22

JAR (2016): Grizzly Steppe –Russian Malicious Cyber Activity. JAR-16-20296, December 29, 2016, 13 pages

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

Johnson, A. et al. (2013): Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. US Naval Research Laboratory.

Johnson, RF (2016): Experts: The US has fallen dangerously behind Russia in cyber warfare capabilities The Washington Free Beacon 27 Jul 2016

Johnson, J.S. (2020): Artificial Intelligence: A Threat to Strategic Stability. Strategic Studies Quarterly Spring 2020, p.16-39

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

Jung, A. (2020): Ära der Cobots. Der Spiegel 25/2020, 13 Jun 2020, p.70-71

Jung, J. (2020): Iranische Hacker attackieren Netzwerke. 01 Sep 2020

Jung, M., Jansen, J. (2017): Telekom-Hacker bereut seineTat vor Gericht. Frankfurter Allgemeine Zeitung 22 Jul 2017, p.24

Kant, A. (2018): Nordkoreanische Hacker nutzen Zero-Day-Lücke aus. Netzwelt 05 Feb 2018

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

Kant, A. (2018): Nordkoreanische Hacker nutzen Zero-Day-Lücke aus. Netzwelt 05 Feb 2018

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

Karabasz, I. (2013): Gemeinsame Spionageabwehr im Netz. Handelsblatt 29 May 2013, 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 (2013): “Winnti” Just more than a game. April 2013, 80 pages plus appendix

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

Kaspersky (2016): The Project Sauron APT August 2016, 14 pages

Kaspersky (2017a): Securelist BlueNoroff/Lazarus watering hole attack was detected in Poland on 03 Feb 2017

Kaspersky (2017b): Securelist blog on 27 June 2017

Kaspersky (2018a): The Slingshot APT Version 1.0 06 March 2018

Kaspersky (2018b): An overview of the Lamberts. Securelist.com

Kaspersky Lab (2017): Investigation Report for the September 2014 Equation malware detection incident in the US. 16 Nov 2017

Kastilan, S. (2010): Vier Flaschen für ein Heureka. Frankfurter Allgemeine Zeitung 21 May 2010, p.33

Kaufmann, W. (2021): Kooperation mit Hackern. Preußische Allgemeine Zeitung, 05 Aug 2022, p. 4

Kaufmann, W. (2022a): Der Ukrainekrieg findet auch im Cyberspace statt. Preußische Allgemeine Zeitung 18 March 2022, p.4

Kaufmann, W. (2022b): Kooperation mit Hackern. Preußische Allgemeine Zeitung, 05 Aug 2022, p. 4

Kaufmann, W. (2022c): Datenklau und Blackoutvorbereitung. Preußische Allgemeine Zeitung, 12 Aug 2022, p.7

Kim, C. (2017): North Korea hacking increasingly focused on making money more than espionage: South Korea study. Reuters 28 Jul 2017

Kirchner, T., Mühlauer, A. und Steinke, R. (2017): Hacken und doch nicht gehackt werden. Süddeutsche Zeitung No. 213, 15 Sep 2017, p.5

Kirschbaum, L. (2022): Alle Abteilungen zum Kampf. Frankfurter Allgemeine Zeitung No. 150, 01 Jul 2022, p.15

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

Kling, B. (2017a): NSA Exploits: Eternal Rocks nutzt mehr Schwachstellen als WannaCry. 23 May 2017 ZDNet

Kling, B. (2017b): Malware Amnesia bildet IoT/Linux Botnet. ZDNet 07 Apr 2017

Kling, B. (2017c): NSA-Leak: Kaspersky veröffentlicht Untersuchungsergebnis. ZDNet 16 Nov 2017

Kloiber, M., Welchering, P. (2011): Militärs suchen Strategien gegen Cyberattacken. Frankfurter Allgemeine Zeitung 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

Kolokhytas, P: (2017): CIA Malware Athena kann alle Windows-PCs ausspionieren. PCWelt 22 May 2017

Kormann, J. Kelen, J. (2020): Ein beliebtes Repressionsinstrument mit zweifelhafter Wirkung. Neue Zürcher Zeitung 10 Juli 2020, p.4

Kramer, A. (2016): How Russia Recruited Elite Hackers for Cyberwar. New York Times 29 Dec 2016

Kramer, A. (2017): Hacker-Gruppe Shadow Brokers veröffentlicht NSA-Tools. Heise online 09 April 2017

KrebsonSecurity (2016): Carbanak Gang Tied to Russian Security Firm? Official Security Blog of Brian Krebs 2016

KrebsonSecurity (2017): Who is Anna Sempai, the Mirai Worm author? Official Security Blog of Brian Krebs 20 Jan 2017

Krebs on Security (2020): US Treasury, Commerce Depts hacked Through SolarWinds Compromise. 14 Dec 2020

Krebs on Security (2021a): At least 30,000 US Organizations Newly Hacked via Holes in Microsoft's Email Software 05 May 2021

Krebs on Security (2021b): Try This One Weird Trick Russian Hackers Hate 17 May 2021

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

Krupovic, M et al. (2016): A classification system for virophages and satellite viruses. Arch Virol (2016) 161:233–247

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

Kundalia, D. (2020): State-backed group using crypto-mining malware to evade detection and monetize compromised networks. Computing.co.uk online

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

Kurz, C. (2017): Jetzt ist es an der Zeit, die Lücken zu schließen. Frankfurter Allgemeine Zeitung No. 31, 06 Feb 2017, p.13

Lachance J.C., Rodrigue S., Palsson B.O. (2019): Minimal cells, maximal knowledge. Elife. 2019 Mar 12;8. pii: e45379. doi: 10.7554/eLife.45379.

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

Langer, M.A. (2018a): Schwerer Hackerangriff auf Marriot Hotel Gruppe Neue Zürcher Zeitung 03 Dec 2018, p.11

Langer, M.A. (2018b): Pekings Hacker unter Verdacht. Neue Zürcher Zeitung 14 Dec 2018, p.3

Langer, M.A. et al. (2021): Großangriff auf Infrastruktur in den USA. Neue Zürcher Zeitung 19 Jun 2021, p.14

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

Lawfare (2019): France's New Offensive Cyber Doctrine – Lawfare lawfareblog.com 26 Feb 2019

Lee, M. et al. (2017): Wanna Cry? TALOS Intelligence Blog May 2017

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

Leyden, J., Williams, C. (2018): Kernel memory-leaking Intel processor design flaw forces Linux, Windows redesign. The Register 02 Jan 2018

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

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

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

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

Limonier, K. (2017): Silicon Moskau, Le Monde Diplomatique Deutsche Ausgabe August 2017, S.1 und 18-19

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

Lindner, M. (2017): Wenn der Hacker mitbehandelt. Neue Zürcher Zeitung 24 May 2017

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

Lohse, E. (2016): Krieg der Sterne. Frankfurter Allgemeine Zeitung 206/2016, p.4

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

Lovelace, DC Jr. (2017): in: The Strategic Studies Institute (SSI) and U.S. Army War College Press. At our own peril: DoD risk assessment in a post-primacy world. Principal Author and Project Director: Nathan P. Freier. June 2017

Lubold, G., Harris, S. (2017): Russian Hackers stole NSA data on US Cyber Defense. The Wall Street Journal online 05 Oct 2017

Ludwig, J. Weimer, S. (2019): Aufruhr um Datendiebstahl. Neue Westfälische 07 Jan 2019, p.2

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

Ma, A. (2019): Russia plans to disconnect the entire country from the internet to simulate an all-out cyberwar . Business Insider online Feb 2019

Mäder, L. (2021a): Ermittler setzen mit Schlag gegen Emotet neue Maßstäbe im Kampf gegen Cyberkriminalität. Neue Zürcher Zeitung 03 Feb 2021, p.18

Mäder, L. (2021b): Russland, China und die USA einigen sich überraschend bei der Cybersicherheit. Neue Zürcher Zeitung 30 March 2021, p.4

Mäder, L. (2022a): Russland übt den Cyberkrieg schon länger in der Ukraine. Neue Zürcher Zeitung 14 Feb 2022, p.3

Mäder, L. (2022b): Russischer Cyberangriff Neue Zürcher Zeitung. 14 April 2022, p.3

Mäder, L. (2022c): Russland führt seit Monaten einen heimlichen Cyberkrieg. Neue Zürcher Zeitung 30 April 2022, p.3

Mäder, L. (2022d): Ukrainische IT-Armee kämpft online gegen Russland. Neue Zürcher Zeitung 25 Jun 2022, p.2

Mäder, L. (2022e): Ziel der Urheber ist die Kapitulation der Ukraine. Neue Zürcher Zeitung 25 Jul 2022, p.3

Mäder, L., Hosp, G. (2022): Cyberangriff zielt auf Mineralölhändler. Neue Zürcher Zeitung 07 Feb 2022

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

Malpedia (2020): Online APT list of the FKIE.

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

Marimov, AE (2017): Ex-NSA contractor pleaded not guilty to spying charges in federal court. Washington Post 14 Feb 2017

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 No. 271, 25 Nov 2014, p. 17

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

Mascolo, G., Steinke, R. (2019): Lizenz zum Löschen. Süddeutsche Zeitung No. 109, 11/12 May 2019, p.9

Masuhr, N. (2019): AI in Military Enabling Applications. CSS Analyses in Security Policy No. 251, October 2019

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

Mazzetti, M. et al. (2017): Killing CIA Informants, China crippled US spying operations. New York Times 20 May 2017

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

Menn, A. (2010): Schutz vor dem Wolkenbruch. Handelsblatt Topic Cloud Computing 02 Dec 2010, p.H12-H13

Menn, J. (2018): China-based campaign breached satellite, defense companies: Symantec. Reuters online 19 June 2018

Merkur (2019): Hackerangriff auf deutsche Politiker LiveBlog. Merkur.de online 04 Jan 2019

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

Mikelionis, L. (2018): Ex-NSA contractor to plead guilty to breathtaking heist of top-secret data. Fox News 04 Jan 2018

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

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

Miller, G. et al. (2017): Obama‘s secret struggle to punish Russia for Putins election assault. The Washington Post online 23 June 2017

Morschhäuser, T. (2014): Heftiger Sonnensturm verfehlt Erde nur knapp. Frankfurter Rundschau online version 25 July 2014, p.1-2

Mozur, P., Metz, C. (2020): A U.S. Secret Weapon in A.I.: Chinese Talent New York Times online 09 June 2020

Mueller, R.S. (2018): Indictment in the United States District Court for The District of Columbia. Received 13 July 2018

Müller, G.V. (2014): Die Schatten-IT wird zum Problem. Neue Zürcher Zeitung 11 April 2014, p.16

Müller, G.V. (2016): Der Verpächter des Internets. Neue Zürcher Zeitung, 01 Nov 2016, p.7

Müller, M. (2016): Die chinesische Datenkrake wächst. Neue Zürcher Zeitung 09 Nov 2016, p.3

Müller, G. (2019): Firmen gehen beim Cloud-Computing unkalkulierbare Risiken ein. Neue Zürcher Zeitung, 18 May 2019, p.14

Müller, M. (2019): Die Sanktionen der USA gefährden den weiteren Aufstieg Huaweis. Neue Zürcher Zeitung 22 May 2019, p.9

Muth, M. (2022): Gut geölte Cyber-Abwehr. Süddeutsche Zeitung No. 137, 17 June 2022, page 19

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. et al. (2017): NSA officials worried about the day its potent hacking tool would get loose. Then it did. Washington Post 16 May 2017

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

Nakashima, E. et al. (2017): NSA officials worried about the day its potent hacking tool would get loose. Then it did. Washington Post 16 May 2017

Nakashima, E. (2018): National Security - Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. Washington Post online, 12 Jan 2018

Nakashima, E., Timberg, C. (2020): Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce. Washington Post. 14 Dec 2020

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

NATO (2019): Artificial Intelligence: Implications for NATO's Armed Forces. Science and Technology Committee (STC) - Sub-Committee on Technology Trends and Security (STCTTS) Rapporteur: Matej Tonin (Slovenia) 149 STCTTS 19 E rev. 1 fin Original: English 13 October 2019

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)

NCSC (2020): National Cyber Security Centre (NCSC) Advisory: APT29 targets COVID-19 vaccine development Version 1.1 16 July 2020

NDAA (2019): National Defense Authorization Act (NDAA) United States of America 2019

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

Neuroth, O. (2017): Appetit auf Plastiktüten. Tagesschau online 24 Apr 2017

New York Times (2020): Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks. https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html

New York Times online (2021): Cyberattack Forces a Shutdown of a Top US Pipeline. 09 May 2021

Niewald, L.V. (2018): Alexa, wie gefährlich bist Du? Neue Westfälische 26 Oct 2018

Nligf (2012): Structure of Iran's Cyber Warfare (Source: the BBC Persian). PDF-file on nligf.nl 7 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

NSCAI (2020): National Security Commission on Artificial Intelligence First quarter Recommendations March 20202, 131 pages

NSTC (2020): Artificial Intelligence and Cybersecurity: Opportunities and Challenges Technical Workshop Summary Report - A report by the Networking & Information Technology Research and Development Subcommittee and the Machine Learning & Artificial Intelligence Subcommittee of the National Science & Technology Council March 2020

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

NZZ (2016): Malware knackt Android Handys. Neue Zürcher Zeitung 03 Dec 2016, p.20

NZZ (2017a): Überschätzte Fake-News. Neue Zürcher Zeitung 24 Jan 2017, p.32

NZZ (2017b): Die USA klagen chinesische Hacker an. NZZ 30 Nov 2017, p.3

NZZ (2021): Polen beschuldigt Russland der Cyberspionage. Neue Zürcher Zeitung 28 Juni 2021, p. 3

NZZ online (2021): Darkside-eine Gruppe russischer Cyberkrimineller presst den amerikanischen Energiesektor aus. 10 May 2021

Orcutt, M. (2019): Once hailed as unhackable, blockchains are now getting hacked. MIT Technology Review online 19 Feb 2019

ODNI (2017): Intelligence Community Assessement Assessing Russian Activities in Recent US Elections, 14 pages

O'Leary, J. et al. (2017): Insights into Iranian Cyber espionage: APT 33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware. FireEye Blog 20 Sep 2017

O'Neill, PH and Bing, C. (2017): WannaCry ransomware shares code with North Korean malware. Cyberscoop 15 May 2017

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)

Osborne, C. (2018): Shamoon data-wiping malware believed to be the work of Iranian hackers. ZDNet 20 Dec 2018

Osterloh, F. (2017): Schützenswerter Kernbereich festgelegt. Deutsches Ärzteblatt Nr.24 16 Juni 2017, S.B795

OSTP (2020): American Artificial Intelligence Initiative: Year One Annual Report. Prepared by The White House Office of Science and Technology Policy February 2020

RAND (2019): The Department of Defense Posture for Artificial Intelligence. Rand Corporation Document RR4229 Santa Monica, USA

Osterloh, F. (2017): Schützenswerter Kernbereich festgelegt. Deutsches Ärzteblatt No.24 16 Jun 2017, p.B795

Paganini, P. (2015): Turla APT Group Abusing Satellite Internet Links. September 10, 2015 https://securityaffairs.co/wordpress/40008/cyber-crime/turla-apt-abusing-satellite.html

Paganini, P. (2018a): The Dutch Intelligence AIVD ‚hacked' Russian Cozy Bears for years. Securityaffairs.co from 26 Jan 2018 Securelist.com

Paganini, P. (2018b): Experts from Kaspersky highlighted a shift focus in the Sofacy's APT group's interest, from NATO member countries and Ukraine to towards the Middle East and Central Asia. Securityaffairs.co from 21 Feb 2018 Securelist.com

Paganini, P. (2019): Russian-APT Turla group Hijacked C2 of the Iranian OilRig. Securityaffairs online, 21 Jun 2019

Paletta, D.Ä, Schwartz, F. (2016): Pentagon deploys cyberweapons against Islamic State. Wall Street Journal online 29 Feb 2016, article 1456768428, 4 pages

Palo Alto (2018): Shamoon 3 Targets Oil and Gas Organization. Dec 2018 ttps://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/

PandaSecurity (2017): Adylkuzz, the malware that steals virtual money from thousands of computers. 22 May 2017

Park, S.J. et al. (2016): Phototactic guidance of a tissue-engineered soft-robotic ray. Science 08 Jul 2016: Vol. 353, Issue 6295, pp. 158-162

Park, J., Pearson J. (2017): Exclusive: North Koreas Unit 180, the cyber warfare cell that worries the West. Reuters 21 May 2017

Pekkanen, S.M. (2019): Introduction to the Symposium on the New Space Race. Governing the New Space Race. Ajil Unbound. doi:10.1017/aju.2019.16

Perez J.A., Deligianni, F., Ravi D. and Yan G.Z. (2019): Artificial Intelligence and Robotics. The UK-RAS Network

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

Perloth, N. (2017a): Russian hackers who targeted Clinton appear to attack France's Macron. New York Times 24 Apr 2017

Perloth, N. (2017b): Hackers are targeting Nculear Facilities, Homeland Security Dept and FBI say. New York Times 06 Jul 2017

Perloth, N., Sanger, D. (2017): In Computer Attacks, Clues Point to a Frequent Culprit: North Korea New York Times 15 May 2017

Perloth, N., Shane, S. (2017): How Israel caught Russian hackers scouring the world for US Secrets New York Times online, 10 Oct 2017

Perragin, C and Renouard, G. (2021): Verkabelter Ozean – Geopolitik der Datenströme. Le Monde Diplomatique, p.1 and 14

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

Pinkert, H., Tanriverdi, H., Von Bullion, C. (2018): Schläfer im Datennetz. Süddeutsche Zeitung 03/04 Mar 2018, p.8

Plan, F. et al. (2019): APT 40: Examining a China-Nexus Espionage Actor FireEye 04 Mar 2019

Poddebniak, D. et al. (2018): Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels (draft 0.9.0) Universities of Bochum/Muenster/Leuven 17 May 2018

Pofalla, B. (2013): Datenfüchse von morgen. Frankfurter Allgemeine 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

Proofpoint (2020): A Comprehensive Look at Emotet's Summer 2020 Return 28 Aug 2020

Puhl, J. (2013): Im Silicon Savannah. Der Spiegel 48/2013, p.118-122.

PwC/BAE Systems (2017): Operation Cloud Hopper PWC in collaboration with BAE Systems Report 25 pages April 2017

Quirin, I. (2010): Vorfahrt fürs Netz. FTD Dossier Intelligente Netze 15 Oct 2010, p.2-7

RadioFreeEurope (2016): Hacking Group from Russia, China Claims Credit for a Massive Cyberattack. 13 Oct 2016

Radsan, A.J. (2007): The Unresolved Equation of Espionage and International Law. Michigan Journal of International Law Volume 28, Issue 3, pp.596-623

Ragan, S. (2016): Salted Hash – Top Security News. Hackers say leaked NSA tools came from a contractor at Red Seal. CSO online article 3109936, 6 pages

Raiu, C., Baumgartner, K., Kamluk, V. (2013): The MiniDuke Mystery. PDF 0-day Government Spy Assembler 0x29A MicroBackdoor, 20 pages

Rajagopalan, R.P. (2015): Japans Shift in Space Policy Reflects New Asian Realities. 23 Feb 2015

Rajagopalan, R.P. (2019): Electronic and Cyber Warfare in Outer Space. UNIDIR May 2019 — Space Dossier 3, May 2019

Raman, R.S., Shenoy, P, Kohls, K., Ensafi, R. (2020): Censored Planet: An Internet-wide, Longitudinal Censorship Observatory. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communication Security (CCS' 20), pages 49-65.

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

Reuters (2017a): German parliament foiled cyber attack by hackers via Isreali website 29 Mar 2017

Reuters (2017b): Under pressure, Western tech firms bow to Russian demands to share cyber secrets. 23 Jun 2017

Reuters (2017c): Russian firm provides new internet connection to North Korea. 03 Oct 2017

Reuters World News (2017): China's economic cyber espionage plummets in US: cyber experts.

Reuters (2022): Exclusive: US spy Agency probes sabotage satellite internet during Russian attack Reuters online 11 March 2022

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

Robertson, J., Riley, M. (2018): How China used a tiny chip to infiltrate America's top companies. Bloomberg Businessweek 04 Oct 2018

Rößler, C. (2016): Ab in den Süden. Frankfurter Allgemeine Zeitung 02 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

Rötzer, F. (2018): Wer wird zuerst eine EMP-Waffe einsetzen? Heise online 01.01.2018

Rogers, J. (2009): From Suez to Shanghai: the European Union and Eurasian maritime security. Occasional Paper - n°77, March 2009

Rogers, F. and Oesch, J. (2022): Das Ende der Anonymität. Neue Zürcher Zeitung 17 Sep 2022, p.22-23

Rohde, D. (2016): Is the CIA ready for the age of Cyberwar? The Atlantic online 02 Nov 2016

Rõigas, H., Minárik, T. (2015): 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law. Incyder news, 31 August 2015

Rolfs, O. (2021): Der Krieg um die Untersee-Datenkabel. Neue Zürcher Zeitung 29 July 2021

Ross, M. (2016): Global Government Forum - UK Defence Intelligence to establish new cyber warfare unit. 24 Feb 2016

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

Rosenbach, M. (2016): Hacker aus dem Staatsdienst. Der Spiegel 40/2016, p.78-79

Rosenbach, M. (2019): Zugriff aus Fernost. Der Spiegel 21/2019, S.74-76

RP online (2018): Forscher hacken sich selbst und entdecken Meltdown. 05 Jan 2018

Rüb, M. (2010): Jenseits der Partnerschaftsrhetorik. Frankfurter Allgemeine Zeitung No. 129/2010, p.5

Rüesch, A. (2018): Die Jagd nach Putins Agenten. Neue Zürcher Zeitung, 19 Oct 2018, p.4-5

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

Russia Today (RT Deutsch) online (2017): Russland: FSB und Kaspersky Lab in Erklärungsnot – Landesverrat im Bereich Cybersicherheit vermutet. 27 Jan 2017

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

Sanger, D.E. and Broad, W.J. (2017): Trump inherits a Secret Cyberwar Against North Korean Missiles. NY Times 04 Mar 2017 online

Sanger, D.E., Perlroth, N. (2019): U.S. escalates online attacks on Russia's power grid. New York Times 15 Jun 2019

Sanger, D.E., Wong, E. and Horowitz, J. (2020): The Vatican is said to be hacked from China before talks with Beijing. New York Times, 28 July 2020

Sattar, M., Löwenstein, M., Carstens, P. (2010): Vertrauliches, Geheimes und streng Geheimes. Frankfurter Allgemeine Zeitung No.279/2010, p.3

Satter, R., Stubbs, J. and Bing, C. (2020): Reuters Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike 23 March 2020

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

Schäfer, J. (2019): Virulente Erdäpfel. Frankfurter Allgmeine Zeitung, No.166/2019, p.14

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.

Scherschel, F. (2017a): Industroyer: Fortgeschrittene Malware soll Energieversorgung in der Ukraine gekappt haben. Heise 12 Jun 2017

Scherschel, F. (2017b): Alles, was wir bisher über den Petya/NotPetya-Ausbruch wissen. 28 Jun 2017

Scherschel, F. (2018): MeltdownPrime and SpectrePrime: Neue Software automatisiert CPU-Angriffe. Heise Security 15 Feb 2018

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

Schmidt, J. (2017): Hardware Fuzzing: Hintertüren und Fehler in CPUs aufspüren. Heise online 23.08.2017

Schmidt, H., Mäder, L. (2022): Ein 19-Jähriger hackt Teslas – wie sicher sind vernetzte Autos? Neue Zürcher Zeitung 03 Feb 2022, p.20-21

Schmiechen, F. (2019): Deutschland ist ein leichtes Opfer Bild 05 Jan 2019, p.2

Schmieder, J. (2017): Bizarro und die Cyberattacken. Süddeutsche Zeitung 29 Mar 2017, p.74

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.

SC Magazine (2015): Research Squadrons to raise IT capability of Russian army. 09 Dec 2015

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

Schneier, R. (2022): Wie lange braucht es uns noch? NZZ Folio September 2022, p.9-23.

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

Scholl-Trautmann, A. (2017): Kaspersky Lab identifiziert 8 auf Ransomware spezialisierte Gruppen, u.a. PetrWrap, Mamba und sechs weitere Gruppen ZDNet

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

Schubert, K. (2019): Als Martin Schulz Nachrichten von Fremden bekommt. Heute.de 04 Jan 2019

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

Securelist (2019a): OperationShadowhammer 25 March 2019

Securelist (2019b): Recent Cloud Atlas activity https://securelist.com/recent-cloud-atlas-activity/92016/

SecurityWeek online (2017): Poland Banks attack part of a bigger campaign targeting over 100 organizations.

Seliger, M. (2018): Datenstaubsauger mit Anleitung. Frankfurter Allgemeine Zeitung, 20 Jun 2018, p.4

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

Shane, S., Mazetti, M., Rosenberg, M. (2017): Wikileaks releases trove of alleged CIA Documents Washington Post 07 Mar 2017

Shane, S., Perloth, N., Sanger, D.E. (2017): Security Breach and Spilled Secrets have shaken the NSA to its core. New York Times online 12 Nov 2017

Shalal, A. (2016): IAEA chief: Nuclear power plant was disrupted by cyber attack. Reuters 10 Oct 2016

Sharma, D. (2011): China's Cyber Warfare Capability and India's Concerns. Journal of Defence Studies 2011, p.62-76

Shekhar, S. (2017): The India-Pakistan cyber war intensifies as retaliatory ransomware attack crippled websites of Islamabad, Multan and Karachi airports. Mail online India 02 Jan 2017

Shields, N.P. (2018): Criminal Complaint United States vs. Park Jun Hyok at the United States District Court for The District of Columbia. Received 08 Jun 2018, 179 pages

Shuster, S. (2016): Hacker Kremlin Emails could signal a turn in the U.S.-Russia Cyberwar. Time Magazine online 07 Nov 2016

Siegel, J. (2018a): Verschlüsselte emails nicht mehr sicher. Neue Zürcher Zeitung 16 May2018, p.20

Siegel, J. (2018b): Mehr Sicherheit für das Internet der Dinge. Neue Zürcher Zeitung, 29 Oct 2018, p. 18

Singer, P.W. (2010): Der ferngesteuerte Krieg. Spektrum der Wissenschaft December 2010, p.70-79

Skinner, B., Oesch, J. (2020): Diese Länder bestellten Schweizer Krypto-Technik für 500 Millionen Franken. Neue Zürcher Zeitung, 24 Feb 2020, p.21

Sokolov, D. (2017): USA - Cybersoldaten an die Front. Heise online 14 Dec 17

Solon, O. (2016): Hacking group auctions 'cyber weapons' stolen from NSA. The Guardian online, 16 August 2016, 2 pages

South Africa (2010): Note of Intention to make national cyber security policy for South Africa. In Government Gazette Vol. 536, No. 32963, 16 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

Spehr, M. (2017): Jeder Schritt zählt. Frankfurter Allgemeine Zeitung 25 Oct 2016, p. T1

Spetalnick, M. (2019): Russian deployment in Venezuela includes 'cybersecurity personnel', U.S. official Reuters.com 26 Mar 2019

Spiegel online (2011): Deutschland probt den Cyber-Ernstfall http://www.spiegel.de/netzwelt/netzpolitik/0,1518,801114,00.html

Spiegel (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 (2016a): Gruppe "Shadow Brokers" Hacker erbeuteten offenbar NSA-Software. 17 Aug 2016, 1 page

Spiegel online (2016b): Hackergruppe Shadow Brokers: NSA soll Uniserver für Angriffe genutzt haben. 01 Nov 2016

Spiegel (2018): Chinesische Hacker stehlen geheime US-Pläne für U-Boot-Waffensystem. Spiegel online 09 Jun 2018

Stabenow, M. (2017): Warnung in roten Lettern. Frankfurter Allgemeine Zeitung 25 Jan 2017, p.3

Stamoulis, C. and Richardson, AG. (2010): Encoding of brain state changes in local field potentials modulated by motor behaviors. J Comput Neurosci. 2010 December ; 29(3): 475–483. doi:10.1007/s10827-010-0219-6.

Standard (2015): Sicherheitslücke: Hacker kapern Jeep während Fahrt auf Autobahn derStandard.at 22 July 2015, 2 pages

Stark, H. (2009): Digitale Spionage. Der Spiegel 11/2009, p.33

State Department (2020): The Clean Network - United States Department of State https://www.state.gov/the-clean-network/ August 2020

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

Steier, H. (2017): Cyber-Angriff verursacht Chaos. Neue Zürcher Zeitung 15 May 2017, p.1

Steinitz, D. (2014): Großes Drama. Süddeutsche Zeitung No. 296 from 19 Dec 2014, p.11

Steinke, R. (2017): Die dunkle Seite des Netzes. Süddeutsche Zeitung No. 155/2017, p.6

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

Strout, N. (2021): National Geospatial Agency (NGA) boss reveals strategy. C4ISRnet.com 06 Oct 2021

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 (2016a): The Waterbug attack group. Security Response Version 1.02 Symantec, 14 Jan 2016, 44 pages

Symantec (2016b): Strider: Cyberespionage group turns eye of Sauron on targets, Symantec Official Blog, 07 Aug 2016

Symantec (2016c): Odinaff: New Trojan used in high level financial attacks, Symantec Official Blog, 11 Oct 2016

Symantec (2017): Longhorn: Tools used by cyberespionage group linked to Vault 7. 10 Apr 2017

SZ (2013): Wie CIA und Co. heikle Aufträge zivilen Firmen überlassen. Süddeutsche Zeitung No. 265, 16/17 Nov 2013, p.8-9

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 (2020): Angriff auf die Kampagne. Süddeutsche Zeitung No.129, p.9

SZ online (2013a): Über den Dächern von Berlin. Report on 12 Nov 2013

SZ online (2013b): Fernseher schaut zurück. Report on 21 Nov 2013

SZ online (2016): Lücke bei Facebook. Zugriff auf die Welt. Article 1.2901048 10 March 2016

SZ online (2017): Verunglückter Tesla-Fahrer ignorierte Hinweise des Autopiloten. 20 June 2017

T-online (2015): Apple löscht über 250 Spionage-Apps aus App-Store, 2 pages. Artikel id_75824954

T-online exklusiv (2019): So begründet der Hacker seine Aktion. T-online Exklusivinterview mit Tomasz Niemiec. 04 Jan 2019, 2 p.m. local time

T-online (2019): Medien: Polizei durchsucht Wohnung in Heilbronn. 07 Jan 2019

Tagesschau (2015): Umbaupläne vorgestellt: Bei der CIA soll vieles anders werden. Tagesschau.de 07 Mar 2015, 1 page.

Tagesschau (2018): Microsoft wehrt Hackerangriff ab. Tagesschau online 21 Aug 2018

Tagesschau online (2019): Spionage im Steakhaus? Tagesschau online 09 Feb 2019

Tagesschau online (2020): Hacker Angriff auf Politiker-Fahrdienst. Tagesschau online 15 Aug 2020

Tagesschau (2021): Schadsoftware „Emotet“ zerschlagen. Tagesschau online 27 Jan 2021

Talos Cooperation (2012): Transportable Autonomous Patrol for Land Border Surveillance D.10.3 4th Workshop 25 May 2012

Talos (2018): VPN Filter. Talos Threat Intelligence Blog 23 May 2018

Tanriverdi, H. (2017): Hackerangriff auf den Bundestag. Süddeutsche Zeitung, 29. Mar 2017, p.5

TAZ online (2013): China testet das “scharfe Schwert”. 23 Nov 2013, 4 pages

Technology review (2018): Russian hackers are accused of infecting three Eastern European companies with malware. Technology review.com 18 Oct 2018

Technology review (2020): American Cyber Command hamstrung Iran's paramilitary force 19 May 2020

Tellenbach, B. (2017): Darknet macht keinen neuen Kriminellen. Neue Zürcher Zeitung 17 Feb 2017, p.31

The Australian (2017): US move to boost cyber war capacity. 17 July 2017

The Economist (2013): War on terabytes. The Economist 02 February 2013, p.59

The Next Web (2020): North Korean Hacker Group Lazarus is using Telegram to steal cryptocurrency. 09 Jan 2020

The SecurityLedger online (2014): New Clues in Sony Hack point to insiders, away from DPRK, page 1 18 Dec 2014

The Telegraph (2017): The Football Association disappointed as Fancy Bears leak anti-doping records 22 August 2017

Thibaut, M., Alich, H. (2010): Paris und London besiegeln Militärkooperation. Handelsblatt No.213/2010, p.15

Thiel, T. (2012): Auf der sicheren Seite. Frankfurter Allgemeine Zeitung No. 281/2012, p.Z1-Z2

Threat Connect (2016): ThreatConnect discovers Chinese APT activity in Europe 17 Oct 2016

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

Trump, D.J. (2019): Donald J. Trump, Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence, Washington, D.C.: The White House, February 11, 2019.

Truong, T.C., Diep, Q.B. and Zelinka, I: (2020): Artificial Intelligence in the Cyber Domain: Offense and Defense Symmetry 2020, 12, 410; doi:10.3390/sym12030410 www.mdpi.com/journal/symmetry

Uchill, J. (2019): Microsoft: Iranian hacker group homing in on industrial systems. 20 Nov 2019 for AXIOS

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

UK Government (2016): National Cyber Security Strategy 2016

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

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

United States Studies Centre (2019): Townshend A. and Brendan Thomas-Noone with Matilda Steward "Averting crisis: American strategy, military spending and collective defence in the Indo-Pacific," United States Studies Centre at the University of Sydney, August 2019

Urbina, F. et al. (2022): Dual use of artificial-intelligence-powered drug discovery. Nature Machine Intelligence, Vol 4 March 2022, 189-191

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

Van Lijnden, C. (2019): Ein fast perfektes Spiel. Frankfurter Allgemeine Zeitung 07 Jan 2019, p.2

Vasen, T. (2018): Responsive Launch of ISR Satellites - A Key Element of Space Resilience? Joint Air Power Competence Centre (JAPCC) Journal Edition 27/2018, p.17-21

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

Voke, M.R. (2019): Artificial Intelligence for Command and Control of Air Power. Wright Flyer Paper No. 72 Air University Press

Von Petersdorff, W., Finsterbusch, S. (2021): Cyberangriff provoziert Amerika. Frankfurter Allgemeine Zeitung 06 Jul 2021, p.15

von Spreckelsen, M. (2018): Electronic Warfare –The Forgotten Discipline. Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict? Joint Air Power Competence Centre (JAPCC) Journal Edition 27/2018, p.41-45

WADA (2016): WADA statement regarding additional data leak via Russian hacker Fancy Bear 09/2016

Wang F., Zhang W. (2019): Synthetic biology: Recent progress, biosafety and biosecurity concerns, and possible solutions. Journal of Biosafety and Biosecurity 1 (2019) 22–30

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

Weber, S. et al. (2018): Meltdown & Spectre: Details und Benchmarks zu den Sicherheitslücken in CPUs. Computerbase online 04 Jan 18

Wechlin, D. (2016): Auf Orwells Spuren. Neue Zürcher Zeitung 27 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. (2016a): Cyberkrieg. Frankfurter Allgemeine Sonntagszeitung from 07 Aug 2016, p.6

Wehner, M. (2016b): Häck auf Beck. Frankfurter Allgemeine Sonntagszeitung Dec 2016, p.9

Weidemann, A. (2017a): Spion sieht Spion sieht Spion. Frankfurter Allgemeine Zeitung 02 Nov 2017, p.15

Weidemann, A. (2017b): Greift Iran jetzt an? Frankfurter Allgemeine Zeitung 20 Dec 2017, p.15

Weinbaum C., Berner, S. and McClintock, B. (2017): SIGINT for Anyone. The Growing Availability of Signals Intelligence in the Public Domain. RAND Corporation Publication PE273

Welch, C. (2018): Play Station4 reportedly crashing due to malicious message. The Verge online, 13 Oct 2018

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

Welchering, P. (2017): Cyberwar in der Luft - Hacker warnen vor Angriffen. Heute online May 2017

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

Welt online (2019): USA führen Cyberangriffe gegen den Iran aus. 22 Jun 2019

Welter, P. (2018): Hackerangriff trifft japanische Krypto-Börse. Neue Zürcher Zeitung 30 Jan 2018, p.8

Welter, P. (2022): Taiwans digitaler Schutzschild? Frankfurter Allgemeine Zeitung 17 Aug 2022, p.8

Wendt, J. (2014): Geheimdienste - Das Cyber-Konglomerat. Die Zeit online 01 Aug 2014

Werner, K. (2010): Siemens zieht in den Cyberkrieg. Financial Times Deutschland 21 Dec 2010, p.7

Westerheide, F. (2020): China – The First Artificial Intelligence Superpower. Forbes Cognitive World Contributor Group online 14 Jan 2020

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

Whitmore, W. Parham, G. (2020): COVID-19 cyberwar: How to protect your business, IBM Research Insights 2020

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

WinFuture (2017): Immer mehr: Geleakte NSA-Hackersoftware infiziert Windows-PCs 24 April 2017

Winkler, P. (2013): Die Affäre Edward Snowden schreckt Washington auf. Neue Zürcher Zeitung International 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

Winkler, P. (2018): Spionageaffäre verblüfft die USA. Neue Zürcher Zeitung 19 Jan 2018, p.3

Wired (2019): What Israel's Strike on Hamas Hackers means for Cyberwar. Wired online May 2019.

Wittmann, J. (2017): Gesucht: Bond. Jane Bond. Neue Westfälische 11 Feb 2017

Wolfangel, E. (2017): Social Bots Eine Armee virtueller Schläferagenten. Spektrum der Wissenschaft 7/17, p.27-29

Wolff, J. (2020): How to Improve Cybersecurity for Artificial Intelligence. Brookings Report 08 June 2020

Wong, E. (2013): Espionage Suspected in China`s drone bid. New York Times international Weekly 27 Sep 2013, p.1 and p.4

Woolley, SC, Howard, PN. (2017): Computational Propaganda –worldwide– Executive Summary. Working Paper No. 2017.11 University of Oxford, Project on Computational Propaganda 2017, 15 pages

Wright, N.D. (2019): Artificial Intelligence, China, Russia, and the Global Order Technological, Political, Global, and Creative Perspectives. Air University Press in October 2019

Wüllenkemper, C. (2017): Wir haben es mit medialem Krieg zu tun. Frankfurter Allgemeine Zeitung 27 Jan 2017, p.15

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

Zeit online (2016a): Mögliche Cyber-Attacke soll Russland bloßstellen. October 2016, 2 pages

Zeit online (2016b): Atemberaubender Computerschwund in britischem Verteidigungsministerium 22 Dec 2016

Zeit online (2017): Ermittler decken riesiges Netzwerk für Phishing und Betrug auf. 04 Dec 2017

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

Zhang, L. (2012): A Chinese perspective on cyber war. International Review of the Red CrossVolume 94 Number 886 Summer 2012 p.801-807

Zhanga, X. (2012): Structure of Sputnik, a virophage, at 3.5-Å resolution. PNAS, 06 Nov 2012 vol. 109, no. 45, S.18431–18436

Zhou, J. et al. (2012): Diversity of Virophages in Metagenomic Data Sets. J. Virol. 2013, 87(8):4225. DOI: 10.1128/JVI.03398-12. Journal of Virology 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