

Cyber war

Methods and Practice

Version 3.0 – 12 Jan 2011

Summary

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

Table of Contents

1. Fundamentals	3
1.1 Introduction.....	3
1.2 Background.....	3
1.3 Definition	4
1.4 The general concept of cyber war.....	5
2. Methods.....	7
2.1 General issues	7
2.1.1 Physical damage of computers and communication lines	7
2.1.2 Electromagnetic Pulse EMP	7
2.1.3 The attack on and manipulation of computers and networks	7
2.2 Attack on Computers	7
2.2.1 Strategy	7
2.2.2 Gain access.....	8
2.2.3 Install malware and start manipulation.....	9
2.2.4 Cyber war.....	9
3. The Practice of Cyber war	12
3.1 Introduction.....	12
3.2 Cyber war from 1998-today.....	12
3.2.0 C war: Pipeline explosion in the Soviet Union.....	12
3.2.1 Moonlight Maze 1998-2000	12
3.2.2 Yugoslavian war 1999	12
3.2.3 The Hainan- or EP3-incident 2001	13
3.2.4 Massive attacks on Western government and industry computers	13
3.2.5 The attack on Estonia in 2007.....	14
3.2.6 The attack on Syria 2007	14
3.2.7 The attack on Georgia 2008.....	14
3.2.8 Intrusion into US electricity net 2003-2009.....	15
3.2.9 Intrusion of US drones in Iraq 2009	15
3.2.10 The ‚digital first strike‘ by Stuxnet 2009-2010.....	15
4 The security architecture of the cyberspace.....	18
4.1 Basic principles.....	18
4.2 The Federal Republic of Germany.....	18
4.3 The cyber war strategies of the USA and of China	20
4.4 The cyber policy of the European Union.....	23
4.5 The cyber capabilities of the NATO.....	25
5 Literature references	27
6 Further information	34

1. Fundamentals

1.1 Introduction

Computer and internet security is under discussion due to the increasing relevance of the Internet and of the information and communication technology (ICT). The cyberspace is meanwhile regarded as separate military dimension¹. This paper gives an overview on the methods and practice of cyber war and presents the cyber war activities since 1998 and the security architecture of the cyberspace. Finally, the cyber war strategies of the US and China and the cyber policy of the European Union are discussed.

1.2 Background

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

An increased risk for cyber attacks results in particular from:

- The Next or **New Generation Network NGN** where television, internet and phone submit their data packets via the internet protocol IP (**Triple-Play**)
- In the **Internet of Things IoT**, things (machines and goods) get IP-addresses to localize and track them, to receive status reports and so on. Also machines and devices with **Radiofrequency Identification (RFID)**-chips can communicate with computers and with each other². The car-to-car-communication is another planned feature which may lead to a massive expansion of IoT applications³.
- 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 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 force⁴.
- Further planned extensions of the net are intelligent household appliances and electric meters (**smart grid**) and the use of external computing centers via the Internet instead of using own capacities (**cloud computing**⁵)

¹ USAF 2010a

² The Machine-to-Machine (M2M) communication potentially concerns 50-70 billion 'machines', of which only 1 % are connected today EU 2009a, p.2

³ Quirin 2010, p.2f.

⁴ Grant 2010

- The introduction of mobile phones with internet access (**smartphones**), which integrate the functions of navigation equipment (global Positioning system GPS location data).

These developments and the dependence on information technology massively increase the vulnerability of critical infrastructures (CII)⁶. On the other hand, the execution of an attack is relatively simple⁷.

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

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

1.3 Definition

The term **Cyber war** (also cyber warfare) is a combination of the terms war and cyberspace and designates the military conflict with the means of the information technology. In practice, this is the attack on computers and their data, the computer network and the systems dependent on the computers⁸.

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 conflict⁹.

However, most authors believe that large-scale cyber attacks cannot be done without governmental support due to the required resources and the possible

⁵ Postinett 2008, p.12, Knop 2010, p.14. Risks of cloud computing are e.g. the storage of data on foreign computers that are subject to foreign legislation. Also, this may lead to political influence; refer to FAZ 2010f, p.17. The cloud provider represents an additional entrance gate for attacks, with may be difficult to control by the outsourcing company, Menn 2010, p.H12-H13.

⁶ 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).

⁷ McGill 2005

⁸ Wilson 2008, p.3ff.

⁹ also CSS 2010, Libicki 2009, p. XIV

political consequences. Therefore, some large-scale cyber attacks are presented in literature as cyber war even when the aggressor could not be clearly identified.

Generally attacks on computers, information, networks and computer-dependent systems are called **cyber attacks**. Cyber attacks can also be of private, commercial or criminal nature, but in all types of attack the same technical methods are used, which makes the identification of the aggressor and the motives very difficult or even impossible.

If the attack has a terrorist background, the attack is called **cyber terrorism**, if the primary aim is illegitimate acquisition of information, it is called **cyber espionage**. Cyber terrorism and espionage are both illegal, however the term cyber crime is mostly used for 'normal' crimes like theft of money by abuse of online banking data¹⁰.

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 attack¹¹. However, large-scale cyber espionage can lead to significant computer and network problems and is then often assigned to cyber war by literature, too.

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

1.4 The general concept of cyber war

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)**¹².

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

¹⁰ also Mehan 2008, CSS 2010

¹¹ Libicki 2009, p.23

¹² Neuneck/Alwardt 2008

- the use of **drones** (Unmanned Aerial Vehicles UAV) or bomb defusers (PackBots¹³)
- and the **integrated warfare**.

Drones are not only used for reconnaissance, but also for active fighting against terrorists as already done in Afghanistan and Pakistan¹⁴. The practical effect of the drones has led to an increased demand that cannot be covered by the current production capacities anymore¹⁵¹⁶.

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 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.¹⁷ 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)** operations¹⁸
- to mislead the enemy by **military deception MILDEC**, e.g. as the Iraqi air defense systems in the Gulf war¹⁹
- 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)**²⁰, **computer network exploitation (CNE)** and the countermeasures as **computer network defense (CND)**²¹
- the conventional **electronic warfare (EW)** where the electronic signals of the enemy are e.g. disturbed by jamming.

¹³ Hürther 2010, p.33-34

¹⁴ Rüb 2010, p.5

¹⁵ FAZ 2010b, p.6

¹⁶ The trend is to reduce size, as the drone type Rabe, that looks like a toy, refer to Singer 2010

¹⁷ Wilson 2007

¹⁸ USAF 2010b, p.5

¹⁹ USAF 2010b, p.32

²⁰ Wilson 2008

²¹ CSS 2010

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**).²²

2.1.1 **Physical damage of computers and communication lines**

This can be done by destruction and sabotage of hardware, cables, aeriels 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 can be caused by a nuclear explosion. The EMP protection is technically possible, but expensive and can only be done for selected systems.

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

Computers and networks can be 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.

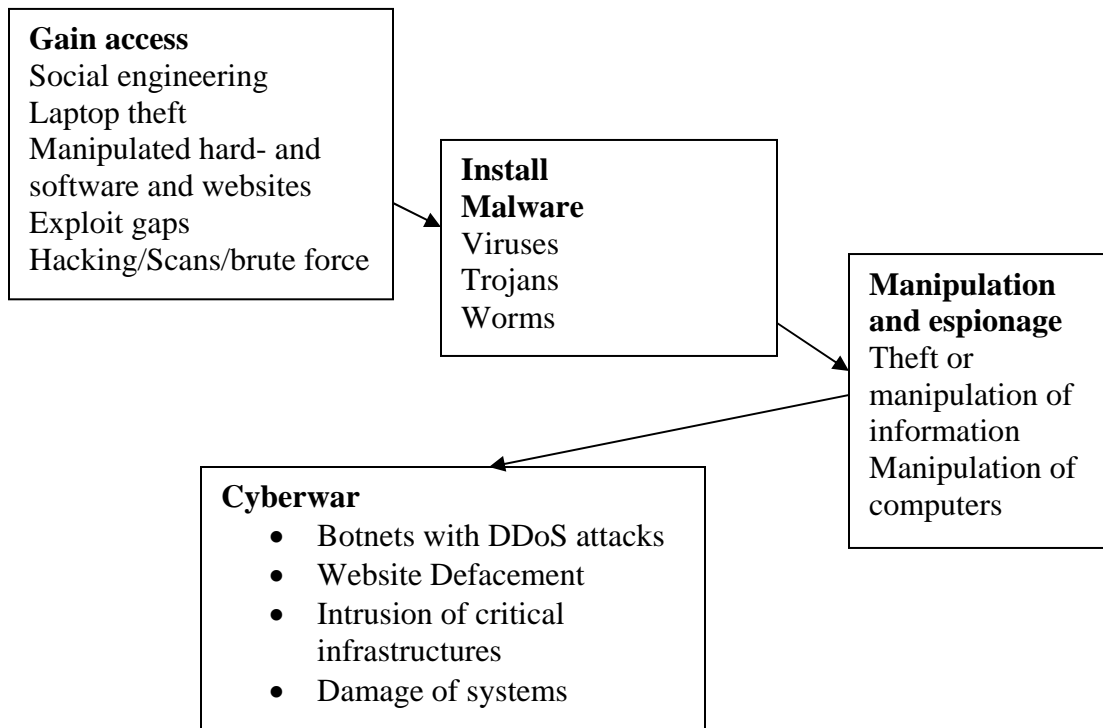
2.2 *Attack on Computers*

2.2.1 **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 below²³.

²² Wilson 2008, p.11

²³ Northrop Grumman TASC 2004



2.2.2 Gain access

The following methods are common to gain access:

- the exploitation of security gaps in software programs and operation systems (e.g. Adobe and Windows) that is also known as **exploit problem**. The probing of computers can also be done by port scans²⁴
- **Hacking** of passwords which is increasingly done automatically (**brute force**)
- Intentional misleading of users by **social engineering**, where e.g. wrong ‘administrators’ ask users for passwords
- Also, manipulated emails with malicious attachments and links to malware-containing websites are increasingly used. **Phishing** is a method where users are misled to a malicious website by masquerading as a trustworthy entity to acquire sensitive information such as usernames, passwords and credit card details. **Spoofing** is a situation where a person or program masquerades as another by falsifying data (in particular wrong Internet IP addresses) while **Cross-site-scripting** is a method where computers are infected while being on another website. **Drive-by download** is the unintended download of malware from the Internet during a website visit.

²⁴ A port scanner is a software application that checks a server or host for open ports, i.e which services a system offers.

- **Infected data storage media** (such as floppy and hard discs, DVDs and now USB-Sticks) are more ‘physical’ ways to be infected
- Also there is a debate on ‘**backdoors**’, 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 backdoors²⁵. Also, Microsoft has initiated the Government Security Program GSP where governments get insight into 90% of the source code. However, the USA is also afraid of backdoors, in particular in hardware, thus the use of Asian chips is avoided for security-relevant technologies. For the same reason, the US State Department avoids use of Chinese computers within their networks²⁶. 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. The global supply chain of such products is also a potential source of vulnerabilities²⁷.

2.2.3 Install malware and start manipulation

Cyber espionage may be done for private, commercial, criminal or political reasons and attempts to get sensitive information such as passwords, PIN numbers etc. while cyber war tries to manipulate computer systems actively.

In general, three types of **malware** are most relevant: **viruses** (programs that infect computers), **Trojans** or Trojan horses (programs that report information to other computers) and **worms** (programs that are able to spread actively to other systems). Typically, a malware program consists of two parts, an infection part, that installs the program on a computer and other parts that contain the instructions of the attacker.

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 passwords²⁸ and **rootkits**, which are tools that allow logins and manipulations by the attacker without knowledge of the legitimate user.

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

²⁵ Die Welt 10 January 2007

²⁶ USA and India suspected in 2010 the Chinese provider Huawei and its competitor ZTE to have pre-installed espionage software (spyware) in their products. Huawei opened the source code and allowed inspections and this convinced Indian government that Huawei products are secure, Mayer-Kuckuck/Hauschild 2010, p.28

²⁷ USAF 2010a, p.5

²⁸ Stark 2009, Schmitt 2009, p.83

users by concerted attacks of other computers. 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 capacities²⁹ (**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 today³⁰.

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

1. botnets are often not located in the country of the attacker which makes localization and attribution of an attack difficult and an immediate counterstrike almost impossible³¹
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 attack³².

Other really used methods are:

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

New technologies may change the scenario and strategies suddenly and completely so the history of cyber war may not allow to predict the future

²⁹ 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.

³⁰ 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.

³¹ 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 cyberattack makes attribution (identification of attacker) even more difficult than DDoS.

³² WhiteWolfSecurity 2007

developments here³³. However, it can be expected that botnets will be used in future as core tool for large-scale attacks.

³³ Gaycken 2009

3. The Practice of Cyber war

3.1 Introduction

In reality, cyber war is defined in literature as *cyber 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 C 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 pipeline pressure above maximum range. A three kilotons explosion resulted which equaled 20% of the nuclear bomb of Hiroshima³⁴. 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 involvement³⁵.

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 1999³⁶. Following the accidental bombing of the Chinese embassy in Belgrade, Chinese hackers attacked US government websites such as the website of the White House³⁷.

³⁴ Falliere 2010, Herwig 2010

³⁵ Vistica 1999

³⁶ Hegmann 2010

³⁷ 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“³⁸.

3.2.4 Massive attacks on Western government and industry computers

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 ongoing³⁹. 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 US⁴⁰. Also the German Federal Government reported attacks on their computer systems at a similar.

The analysis of Titan Rain revealed an attack pattern similar to the following: a team of 6-30 hackers takes control of computers, copies everything on the hard drive within 30 minutes, and then send that via a botnet to computers in the Chinese province of Guangdong, however, this could not be definitely proven⁴¹.

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 2008⁴². Moreover, they 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 region⁴³.

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

³⁸ Fritz 2008 and Nazario 2009, who gives in his paper an overview on politically motivated relevant DoS attacks.

³⁹ 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

⁴⁰ Fischermann/Hamann 2010

⁴¹ Fritz 2008, p.55 and also Stokes 2005

⁴² ArcSight 2008, p.2

⁴³ Glenny 2010, p.23

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 and Adobe) and from high-tech companies of the security and defense sector in 2009⁴⁴.

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 repression⁴⁵. Estonia's networks were flooded by data from Russia, however probably not by the state, but by patriotic organizations^{46,47}. Some computers had an increase from 1,000 requests *per day* to 2,000 requests *per second* and the attack went on for weeks⁴⁸.

3.2.6 The attack on Syria 2007

On 06 September 2007, a suspected nuclear plant in Eastern Syria was destroyed by Israeli air attacks. Such an attack required a long route through the Syrian air space. Israel was technically able to simulate a free heaven to Syrian air defense systems and could thus conduct this attack without disturbance. This is a very good example how cyber war can be used as an additional tool within conventional attacks⁴⁹.

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 sectors⁵⁰. 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.

⁴⁴ Markoff/Barbosa, 18 Feb 2010

⁴⁵ Busse 2007

⁴⁶ Later on the patriotic Youth Organization **Naschi** ('our people') said that they conducted the attack, Frankfurter Allgemeine Zeitung 11 Mar 2009

⁴⁷ Koenen/Hottelet 2007, p.2

⁴⁸ Wilson 2008, p.7ff.

⁴⁹ Herwig 2010, p.60

⁵⁰ refer to official statement of government of Georgia 2008

3.2.8 Intrusion into US electricity net 2003-2009

Also during the power failure of 2003 it was discussed whether this was caused by a computer virus⁵¹. 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 time⁵². Since 2006 nuclear power plants were shut down two times after cyber attacks⁵³. In April 2009, hackers successfully intruded the US electricity net control⁵⁴ and installed programs that allowed manipulation and turn-off. China was suspected, that denied and also Russia.

3.2.9 Intrusion of US drones in Iraq 2009

Iraq insurgents were able to use commercially available software to intrude U.S. drones which allowed them to view the videos of these drones⁵⁵.

3.2.10 The ‚digital first strike‘ by Stuxnet 2009-2010

Industrial Control Systems ICS such as Supervisory Control and Data Acquisition SCADA⁵⁶) 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 particular⁵⁷.

Stuxnet is a **worm**, i.e. a program that is able to spread actively to other systems⁵⁸. The infection was started via an infected USB-stick and Stuxnet exploits security gaps in Windows LNK-files to intrude systems⁵⁹. 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 Edition⁶⁰.

The Simatic S7-system of Siemens is running under a Windows environment, also the WinCC software for parameter control and visualization⁶¹. 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 Stuxnet⁶². In case of success, Stuxnet starts to send information to external servers, thereof two servers in

⁵¹ Gaycken 2009 with picture of power failure in Northeast USA 2003

⁵² Wilson 2008, p.22

⁵³ ArcSight 2009

⁵⁴ Goetz/Rosenbach 2009, Fischermann 2010, p.26

⁵⁵ Ladurner/Pham 2010, p.12

⁵⁶ Shea 2003

⁵⁷ Welt online 2010b. Consequently, Siemens expands its cyber war research capacities, Werner 2010, p.7

⁵⁸ As Stuxnet has dozens of functions and tools, it sometimes also described as Trojan horse or virus, FAZ2010a.

⁵⁹ On 13Oct 2010 Microsoft released 16 Updates to cover 49 security gaps, Handelsblatt 2010, p.27

⁶⁰ Rieger 2010, p.33, who invented the term ‚digitaler Ersts Schlag‘ (‚digital first strike‘).

⁶¹ Krüger/Martin-Jung/Richter 2010, p.9

⁶² Schultz 2010, p.2

Malaysia and Denmark. Stuxnet also contains rootkits, i.e. tools for control of computers⁶³.

Stuxnet is also searching for other applicable systems by exploiting the *autorun*-function of Windows. After a certain number of successful infections, Stuxnet deactivates itself⁶⁴. It was assumed that uranium gas centrifuges needed for construction of nuclear bombs were damaged in Iran, as the number of centrifuges declined in 2009 and the International Atomic Energy Agency (IAEA) reported downtime also in 2010⁶⁵, which was confirmed by Iran⁶⁶⁶⁷.

These issues, the use of several unknown security gaps (**zero-day-exploits**) and the estimated development costs of about 1 Million US-Dollars⁶⁸ resulted in the theory of a new weapon constructed by secret services to damage the Iranian nuclear program⁶⁹.

However, there are some open questions:

- Other states were also affected, in particular Indonesia, India, Azerbaijan and Pakistan, and also many other states such as the USA and Great Britain, even if the Iran may have been the primary target⁷⁰.
- 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 attack⁷¹.
- Finally, 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 and as a consequence, ‘relatives’ of Stuxnet may be created in future and may cause problems⁷².
- The German media reports on Stuxnet show 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

⁶³ Kaspersky 2010

⁶⁴ Falliere 2010

⁶⁵ FAZ2010c, p.6

⁶⁶ refer to FAZ2010d, S.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.

⁶⁷ 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

⁶⁸ Schultz 2010, p.2

⁶⁹ Ladurner/Pham 2010, p.12

⁷⁰ Handelsblatt 2010, p.27, Symantec 2010, p.5-7

⁷¹ 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

⁷² Rosenbach/Schmitz/Schmundt 2010, p.163

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*⁷³. Siemens confirmed that 15 clients were affected, thereof 60% in the Iran. Possible explanations for this gap may be the upcoming assumption of intelligence involvement, a presumed infection of the nuclear plant in Buschehr and the debate of the new NATO strategy⁷⁴.

⁷³ Iran Daily 26 July 2010

⁷⁴ Knop/Schmidt 2010, p.20

4 The security architecture of the cyberspace

4.1 Basic principles

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

4.2 The Federal Republic of Germany

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

The **Federal Office for Information Security BSI** is the government agency in charge of managing computer and communication security for the German government since 1991. The predecessor of the BSI was the cryptographic department of Germany's foreign intelligence agency (BND). With the rise of the Internet and the end of cold war there was a need for an agency for the new technical challenges. Within Germany's foreign intelligence agency, the central service for information security was created in 1989 (Zentralstelle ZSI), and then the new BSI in 1991. The new amendment of the BSI-Act BSIG von 2009 has significantly strengthened the central role of the BSI for information security matters in Germany, in section 5 of the amendment also for the government communication⁷⁵.

Important responsibilities and projects are e.g.⁷⁶:

- member of the German Critical Infrastructure working group (AK KRITIS)⁷⁷
- 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 2009⁷⁸
- document protection within **Government** procedures

⁷⁵ Act to Strengthen the Security of Federal Information Technology dated 14 August 2009

⁷⁶ Refer to Annual reports of the BSI 2005, 2006-2007 and 2008-2009

⁷⁷ 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)

⁷⁸ Steinmann 2010, p.10

- Protection of NATO communication via encryption technology, in particular **Elcrodat 6.2**
- BSI provides the Secure Inter-Network Architecture (SINA) to allow very secure communication via the ordinary internet
- BSI works on communication security (**Comsec**) projects such as shielding of buildings⁷⁹
- Work on **computer resilience**⁸⁰ and on the **micro kernel's architecture** is based on firewalls within the computer sealing off the program segments from each other
- It is under discussion to establish a **National Cyber Defense Center** at the BSI in 2011⁸¹

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. 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 2002⁸² and which has key functions in military intelligence since 2008. In 2010 it had a workforce of 6,000 people⁸³ and was responsible for

- the electronic warfare (Elektronische Kampfführung EloKa),
- since 2007, the KSA has a **computer- and network operation (CNO) unit**⁸⁴ which is also responsible for cyber war issues⁸⁵

⁷⁹ To control problems such as the computer radiation which allows to detect the information that is shown on the computer screen, Schröder 2008

⁸⁰ Resilience means permanent availability. Not only cyber attacks, but physical damage by an **electromagnetic pulse** are relevant issues here.

⁸¹ FAZ 2010g, p.4

⁸² Eberbach 2002

⁸³ Bischoff 2009

⁸⁴ Bischoff 2009

⁸⁵ 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 to provide a centrally coordinated information policy for media and citizens.

- the new military satellites Synthetic Aperture Radar (SAR-Lupe)⁸⁶ 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**. Herkules is still under construction⁸⁷.

4.3 The cyber war strategies of the USA and of China

Presumably more than 100 countries try to establish cyber war capacities and US experts say that approximately 140 foreign intelligence agencies try to get access computers of US government and companies⁸⁸.

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 general⁸⁹.

The primary aim of actors is to achieve and maintain **electromagnetic dominance** and **cyberspace superiority**⁹⁰ in particular, that is to control the cyberspace during a conflict.

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

The USA has systematically developed their cyber war capacities in the last 2 decades⁹¹.

In 1988, the Department of Defence DoD established a Computer Emergency Response Team CERT at the Carnegie-Mellon University⁹².

In 1992, the Defensive Information Warfare Program was established that was accompanied by a Management Plan in 1995.

⁸⁶ Bischoff 2009. 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.

⁸⁷ Scheidges 2010a, p.2-3

⁸⁸ Wilson 2008, p.12

⁸⁹ Kanwal 2009

⁹⁰ USAF 2010a, p.2

⁹¹ Hiltbrand 1999

⁹² Porteuos 2010, S.3

According to Hiltbrand, the Air Force established the Air Force Information Warfare Center (I.W.C.) in 1996. That same year, the Navy established the Fleet Information Warfare Center (F.I.W.C.) and the Army established the Land Information Warfare Activity (L.I.W.A.). In 1998, the Pentagon established the Joint Task Force for Computer Network Defense.

Thereafter, Cyber Commands were established within the military branches⁹³ and consequently, a central **Cyber Command** (US CYBERCOM) was established in May 2010 with an estimated staff of 1,000 people and which is led by the director of the National Security Agency NSA, General Keith Alexander⁹⁴. US CYBERCOM is subordinated to the Strategic Command US STRATCOM that plans and executes Cyberspace Operations⁹⁵.

The CYBERCOM is responsible for the protection of the domain '.mil' that is exclusively used by the US military, while the Department of Homeland Security DHS is responsible for the civil US government domain 'gov'⁹⁶.

The NSA plans to handle Chinese cyber war issues in a more offensive way⁹⁷.

A first large cyber exercise was the so-called **electronic Pearl Harbour** of the US Navy in 2002, where a massive attack on critical infrastructures was simulated. Since that time, the term 'electronic Pearl Harbour' is often used as figure of speech for the consequences of cyber attacks.

Regular exercises are the **Cyber Storm** exercises; Cyber Storm I-III were organized in the years 2006, 2008 und 2010 by the Department of Homeland Security (DHS) and again, the capability to defend against massive attacks was tested.

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.

Also the Chinese government is working on cyber war issues and is building cyber war capacities like many other states, too.

Compared to conventional war, cyber war is relatively cheap and allows to get to close the gap to other states much quicker than with massive expenses for conventional weapons („leapfrog strategy“). Cyber war cannot replace conventional capabilities, but helps to expand the own options quickly and also fits well with the concept of '**active defense**', where the early and quick elimination of possible retaliation of the enemy is an essential aim⁹⁸.

⁹³ USAF: 24th Air Force, Army Forces Cyber Command (ARFORCYBER), Fleet Cyber Command (FLTCYBERCOM) and Marine Forces Cyber Command (MARFORCYBER)

⁹⁴ Hegmann 2010, p.5, The Economist 2010, p.9/22-24, Glennly 2010, p.23

⁹⁵ USAF 2010, p.21-22

⁹⁶ Porteuos 2010, p.7.

⁹⁷ Barnford 2010

⁹⁸ Kanwal 2009, p.14

Also China is surrounded by states which have critical relations with China or are even allies of the USA⁹⁹, such as Japan, Taiwan and South Korea, so that China may currently not be able to apply major physical damage to the USA in case of serious conflict (e.g. in an escalating Taiwan conflict scenario). The cyber war can be done without distance problems, it allows making an asymmetric war and the cyber war training brings a lot of useful information, because intrusion can be used for cyber espionage also.

Analysis of Chinese cyber war-strategy by Northrop Grumman showed the critical points. There are three security levels, the normal civil net, the secured **Secret Internet Protocol Router Network SIPRNET** for critical infrastructure and government and close-to-military institutions and the third maximum security level for military operations¹⁰⁰. The cyber war would be mainly directed against level 2 and would affect networked based warfare operations significantly¹⁰¹¹⁰². Meanwhile, the WikiLeaks disclosure of confidential SIPRNET data from 28 Nov 2010 showed that too many people also of low ranks had access to SIPRNET¹⁰³, as discussed in the debates after the incident¹⁰⁴.

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 incidents¹⁰⁵. As a first step, the number of people with SIPRNET access was reduced¹⁰⁶.

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 possible¹⁰⁷. 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

⁹⁹ Rogers 2009

¹⁰⁰ In the USA, these are the Non-classified Internet Protocol Router Network NIPRNET, the Secret Internet Protocol Router Network SIPRNET and the Joint Worldwide Intelligence Communication System JWICS; in Germany the Herkules platform is similar to SIPRNET and the JASMIN database to JWICS.

¹⁰¹ Krekel et al. 2009

¹⁰² The Internet worm **Conficker** damaged in 2008 German army and French Marine, also military jets could not start for 2 days, Leppegrad 2009.

¹⁰³ About 2.5 million persons had basic access and 280.000 persons access to higher classified documents; Schneider 2011, p.9

¹⁰⁴ Schaaf 2010, p.9

¹⁰⁵ Sattar et al. 2010, p.3

¹⁰⁶ vgl. Schneider 2011, S.9

¹⁰⁷ Krekel et al. 2009

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 time¹⁰⁸

However, other issues may be even more relevant for the future of computer and internet industry. China has 97% market share¹⁰⁹ for rare industry metals which cannot yet be recycled in an efficient manner and China is reducing the export volume to satisfy the needs of their domestic industry¹¹⁰. 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 is now restarted with highest priority¹¹¹.

4.4 The cyber policy of the European Union

In contrast to USA and China the European Union consists of 27 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. As encrypted communication could be used for terrorist activities also, it is essential for intelligence agencies to get access to keys or to the source code of encryption software to have the option to decode encrypted information based on the applicable legal provisions. In Germany, this access is guaranteed by the telecommunication surveillance regulation **Telekommunikations-Überwachungsverordnung (TKÜV)** since 2002. Similar regulations exist worldwide in almost all states, e.g. in the USA, where the **National Security Agency NSA** has access to the source codes of encryption software¹¹². The access of national intelligence agencies means that a foreign or international IT platform can be technically accessed by foreign agencies¹¹³. IT and cyber attacks are global matters, but IT security structure paradoxically promotes national solutions.

In most states so-called **Computer Emergency Response Teams (CERTs)** or Computer Security Incident Response Teams (CSIRTs) are established for detection and reporting of security incidents and for countermeasures. However, the **European Government CERT Group EGC** still has only 10 member states

¹⁰⁸ Tinner et al. 2002.

¹⁰⁹ Büschemann/Uhlmann 2010, p.19

¹¹⁰ 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

¹¹¹ FAZ 2010d, p.12, Bierach 2010, p.11

¹¹² Scheidges 2010b, p.12-13

¹¹³ Scheidges 2010b, p.12-13

(Finland, France, Germany¹¹⁴, Netherlands, Norway, Hungary, Spain, Sweden, United Kingdom, and Switzerland)¹¹⁵.

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.*)”¹¹⁶

The focus is now on the **ENISA (European Network and Information Security Agency)**, that was founded in 2004 with regulation 460/2004 with a budget of 33 Mio. Euros and 50 employees. ENISA became operational in 2005 and is located in Heraklion/Iraklion, the capital of Crete, at the Southern EU border, which is perceived as a suboptimal solution¹¹⁷.

The ENISA works on network security studies, encryption tools, etc. Cryptography is also part of the current EU research program¹¹⁸. In 2008, the mandate of the ENISA was prolonged until 2012.

The new director of the ENISA, Dr. Udo Helmbrecht, was the former president of the German BSI and was appointed in 2009. Since that year, the following actions were started to strengthen the key role of ENISA in European cyber policy:

- the ENISA should strengthen the cooperation between National/Governmental CERTs, also by leveraging and expanding existing cooperation mechanisms like the EGC¹¹⁹,
- 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 ENISA¹²⁰.

¹¹⁴ The German group CERT-Bund is presented on the BSI Website

¹¹⁵ ECG 2008, ECG Website Nov 2010. Other CERT cooperations where CERT-Bund is involved are FIRST (Forum of Incident Response and Security Teams) and TI (Trusted Introducer).

¹¹⁶ EU 2010b. The European Council released already in 2006 a cooperation plan for Critical Information Infrastructure Protection, it took some time after attack on Estonia 2007 before further steps were implemented

¹¹⁷ EU-ISS 2007

¹¹⁸ ENISA 2007

¹¹⁹ EU 2007, EU 2009b

¹²⁰ ENISA 2009

- In line with the European Commission Communication on Critical Information Infrastructure Protection 2009,¹²¹ 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 tests¹²². However, the exercise showed the uneven and uncoordinated national approaches and insufficient preparedness of smaller member states¹²³. After analysis and lessons learned sessions, the next exercise will also include private actors.

The European Commission plans to establish a **European Public Private Partnership for Resilience (EP3R)** and a European Information Sharing and Alert System (EISAS), which is also accessible for citizens and small and medium-size enterprises (SMEs). Moreover, it is planned to develop in cooperation with Member States and all relevant stakeholders the criteria for identifying European critical infrastructures for the information and communication technology (ICT) sector¹²⁴.

The United Kingdom and France agreed upon a general military cooperation in November 2010, which also should include cyber war issues¹²⁵.

4.5 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 issues¹²⁶.

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-infrastructure¹²⁷.

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).

¹²¹ EU 2009b

¹²² ENISA 2010a, ENISA2010b

¹²³ 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.”

¹²⁴ EU2009b, also EU 2010b

¹²⁵ Thibaut/Alich 2010, p.15

¹²⁶ Schuller 2010, p.6

¹²⁷ NCSA 2009a-c

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.

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 Tallinn¹²⁸, Estonia with a staff of 30 people, which is supported by Estonia, Lithuania, Latvia, Italy, Spain, Slovakia and Germany, i.e. it is supported by a few member states only¹²⁹, Poland plans to join in 2011.

NATO Cyber Defense exercises were **Digital Storm** and **Cyber Coalition** 2008, 2009 and 2010 and were managed by the CCD CoE together with the NCIRC and other NATO bodies¹³⁰. Together with Sweden, the CCDCoE conducted the **Baltic Cyber Shield** exercise in May 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*“) ¹³¹.

¹²⁸ In reality, the CCD CoE became operational already in 2006 after an Estonian initiative in 2004; CCDCoE 2010a

¹²⁹ The NATO plans to rely on consultations after a cyber attack; von Kittlitz 2010, p.33

¹³⁰ vgl. Wildstacke 2009, S.28/29, CCDCoE 2010b

¹³¹ NATO 2010

5 Literature references

- ArcSight (2009): Cyberwar: Sabotaging the System. Managing Network-Centric Risks and Regulations. ArcSight White Paper Research 021-111609-03
- BBC News (2009): Major cyber spy network uncovered. 29 March 2009
- Bierach, B. (2010): Australien will Seltenerdmetalle fördern. Neue Zürcher Zeitung 18 Dec 2010, S.11
- Bischoff, M. (2009): Kommando Strategische Aufklärung (Kdo StratAufkl) -Stand July 2009, <http://www.manfred-bischoff.de/KSA.htm>
- Büschemann, K.-H., Uhlmann, S. (2010): Deutschland braucht eine Rohstoffstrategie. Süddeutsche Zeitung 15 Oct 2010, p.19
- Busse, N. (2007): Krieg im Cyberspace. Frankfurter Allgemeine Zeitung 22 Nov 07, p.10.
- 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>
- DHS (2008): The Cyber-Terror Threat. New Jersey Office of Homeland Security and Preparedness 7 pages
- Die Welt (2007): US-Geheimdienst kontrolliert Windows Vista. http://www.welt.de/wirtschaft/webwelt/article707809/US_Geheimdienst_kontrolliert_Windows_Vista.html
- Eberbach, H.E. (2002): Neuorientierung des Militärischen Nachrichtenwesens der Bundeswehr <http://www.europaeische-sicherheit.de/alt/ausgaben/10oktober2002/1002,04.html>
- ENISA (2009): Analysis of Member States' Policies and Regulations. Policy Recommendations, 112 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'.
- 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-ISS (2007): Chaillot Paper No. 76 of the European Institute for Security Studies EU-ISS

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>

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 Nr. 283/2010, p.17

FAZ (2010g): Bundesregierung plant „Cyber-Abwehr-Zentrum“. Frankfurter Allgemeine Zeitung Nr. 302/2010, p.14

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

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

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

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

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

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

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

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

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

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

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

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

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

Hunker, J. (2010): Cyber war and cyber power. Issues for NATO doctrine. Research Paper No. 62 - November 2010 of the NATO Research College, Rome

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

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

Kaspersky (2010): Stuxnet-Trojaner öffnet Zero-Day-Lücke in Windows. Meldung des Kaspersky Lab ZAO 19 Jul 2010

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

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

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

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

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

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

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

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

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

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

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

Menn, A. (2010): Schutz vor dem Wolkenbruch. Handelsblatt Topic Cloud Computing vom 02 Dec 2010, p.H12-H13

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

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

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

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)
- 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
- Northrop Grumman TASC (2004): Cyber Warrior Hacker Methodology. Presentation, 44 pages
- 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
- Quirin, I. (2010): Vorfahrt fürs Netz. FTD Dossier Intelligente Netze 15 Oct 2010, p.2-7
- Rieger, F. (2010): Du kannst Dich nicht mehr verstecken. Frankfurter Allgemeine Zeitung No.43/2010, p.5
- Rogers, J. (2009): From Suez to Shanghai: the European Union and Eurasian maritime security. Occasional Paper - n°77, March 2009
- Rosenbach, M., Schmitz, G.P., Schmundt, H. (2010): Mord ohne Leiche. Spiegel 39/2010, p.163
- Rüb, M. (2010): Jenseits der Partnerschaftsrhetorik. Frankfurter Allgemeine Zeitung No. 129/2010, p.5
- Sattar, M., Löwenstein, M., Carstens, P. (2010): Vertrauliches, Geheimes und streng Geheimes. Frankfurter Allgemeine Zeitung No.279/2010, p.3
- Schaaf, S. (2010): Wikileaks verstreut massenhaft schmutzige Wäsche. Financial Times Deutschland 29 Nov 2010, p.9
- Schäder, B., Fend, R. (2010): Peking macht seltene Erden noch rarer. Financial Times Deutschland 30 Dec 2010, p.3
- Scheidges, R. (2010a): „Herkules“ versagt im Praxistest. Handelsblatt April 2010, p.2-3
- Scheidges, R. (2010b): Bundesamt misstraut US-Firmen. Handelsblatt 02 Dec 2010, p.12-13
- Schmitt, J. (2009): Virtuelle Spürhunde. Der Spiegel 10/2009, p.83

Schneider, W. (2011): Das Unheimliche am Internet. Neue Zürcher Zeitung NZZ Folio January 2011, p.9

Schröder, T. (2008): Was Du siehst, sehe ich auch. Frankfurter Allgemeine Sonntagszeitung No.3, p.58

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>

Singer, P.W. (2010): Der ferngesteuerte Krieg. Spektrum der Wissenschaft December 2010, p.70-79

Stark, H. (2009): Digitale Spionage. Der Spiegel 11/2009, p.33

Steinmann, T. (2010): Deutschland im Visier der Cyberkrieger. Financial Times Deutschland 29 Dec 2010, p.10

Stokes, G. (2005): Cyber Security Fundamentals: What You Should Know About Protecting Data & Systems Orus Group LLC, Orus Group Cyberwar Institute

Symantec (2010): W32.Stuxnet Dossier by Nicolas Falliere, Liam O Murchu, and Eric Chien. Version 1.3. November 2010, 64 pages

Thibaut, M., Alich, H. (2010): Paris und London besiegeln Militärkooperation. Handelsblatt No.213/2010, p.15.

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

Uhlmann, P. (2010): Informationsprofis arbeiten enger zusammen. Truppe für Operative Information - Übergabe InfoOp. Stand vom: 01 Jul 2010 http://www.opinfo.bundeswehr.de/portal/a/opinfo/unsere_l/zopinfo/infoop/uebergabe

USAF (2010a): US Air Force Doctrine Document (AFDD) 3-12, Cyberspace Operations 15 July 2010, 55 p.

USAF (2010b): US Air Force Doctrine Document (AFDD) 3-13, Information Operations 17 September 2010, 54 p.

Vistica, G. (1999): We're in the Middle of a Cyberwar. Newsweek 13 Sep 1999

Werner, K. (2010): Siemens zieht in den Cyberkrieg. Financial Times Deutschland 21 Dec 2010, p.7

White Wolf Security (2007): Estonia and Cyberwar – Lessons Learned and Preparing for the Future By White Wolf Security, 3 pages, 6 April 2007

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 p.

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

6 Further information

Would you like to know more?

The **Kompendium der Sicherheitspolitik** (in German language) provides comprehensive and current information on security policy matters.

Kompendium der Sicherheitspolitik

440 Pages

EUR 29.80

Verlag Dirk Koentopp, Osnabrueck, Germany

2nd, extended edition

ISBN 978-3-938342-26-8

www.dirk-koentopp.com