From Cyber War to Cyber Peace

7

Thomas Reinhold and Christian Reuter

Abstract

The encompassing trend of digitalisation and widespread dependencies on IT systems also triggers adjustments in the military forces. Besides necessary enhancements of IT security and defensive measures for cyberspace, a growing number of states are establishing offensive military capabilities for this domain. The chapter discusses historical developments and transformations due to advancements in military technologies and the political progress made and tools developed since. Both have contributed to handling challenges and confining threats to international security. With this background, this chapter assesses a possible application of these efforts to developments concerning cyberspace, as well as obstacles that need to be tackled to succeed. The chapter points out political advancements already in progress, the role of social initiatives, such as the cyber peace campaign of the Forum of Computer Scientists for Peace and Societal Responsibility (FIfF), as well as potential consequences of the rising probability of cyber war as opposed to the prospects of cyber peace.

T. Reinhold (✉) · C. Reuter
Science and Technology for Peace and Security (PEASEC),
Technische Universität Darmstadt, Darmstadt, Germany
e-mail: reinhold@peasec.de

C. Reuter
e-mail: reuter@peasec.tu-darmstadt.de

C. Reuter (ed.), *Information Technology for Peace and Security*,
Technology, Peace and Security I Technologie, Frieden und Sicherheit,
https://doi.org/10.1007/978-3-658-44810-3_7

Objectives

- Understanding the ongoing trend of the militarisation of cyberspace, its dynamics and influence on international security politics.
- Gaining insights into the political processes and measures that have been undertaken over the last decades to establish security, stability and peace under the pressure of advances in military technology.
- Identifying the political steps and measures necessary for a peaceful development of cyberspace, as well as the role and possibilities of societal actors within these debates.

7.1 Introduction

In Iran in June 2010, a malicious software (**malware**) had been discovered on specialised industry control computers of a uranium enrichment plant, which had been used to sabotage the facility via centrifuge manipulation. Analyses of the program, deployed by an infected USB flash drive, which is now known as Stuxnet, revealed that the sabotage had already been running for several years, and that the hackers must have possessed remarkable technical skills and detailed knowledge of the plant's construction. Because of the high development costs and effort for such malware capable of attacking an industrial facility disconnected from the internet, a governmental agency was assumed to be the driving force behind Stuxnet. This assumption has been confirmed, and Stuxnet is now known to be a joint project of US and Israeli military and intelligence services (Nakashima & Warrick, 2012; Sanger, 2014).

However, Stuxnet was not the first malware allegedly applied by a state. For example, in 2007, the Israeli military was accused of sabotaging Syrian air defence systems (Fulghum, 2007). In Estonia, servers have been attacked and temporarily disabled, presumably by Kremlin-based activists from Russia (Bright, 2007) – incidents which are said to have occurred during the Caucasian war in 2008 in a similar form (Danchev, 2008). Since 2010, such events have repeatedly been receiving public attention (see Table 7.1) for an extensive list of malicious incidents), like the case in 2015 when the German Federal Parliament's internal communication system Parlakom was spied upon for months, and documents, access details and personal communication by deputies and their employees were presumably stolen. The attack severely impeded the parliament's work and could not be stopped until the system was shut down entirely during the summer break (Reinhold, 2018). Other cases include Phishing attacks against Members of the German Bundestag in 2021 (Jansen, 2021).

A video made by FIfF (2017) motivates the discussion around **cyber war** and **cyber peace** (for a definition of the terms cyber war and cyber peace, see Chapter 2 "*Peace Informatics: Bridging Peace and Conflict Studies with Computer Science*"). Their central argument why cyber war needs to be prevented, and offensive cyber strategies of militaries and secret services stopped, is that cyber weapons are in many ways as dangerous and inhumane as biological and chemical weapons, which the international community

Table 7.1 List of relevant cyber incidents with presumably state or state influenced actors.[1] (Source: Own depiction)

Year	Alleged actor[2]	Description
2007	Russia	The cyber attack on the websites of the government and other institutions, banks and ministries of Estonia that prevented access to them is often considered to be the first significant state-driven cyber attack. Russia denied an official involvement, and the attack was attributed to a patriotic Russian youth organisation
2008	Russia	The cyber attacks against Georgia and South Ossetia websites during the military conflict with Russia prevented public information platforms and media services from working. These incidents are often considered to have been the first attempts to use cyber capabilities as a means in military conflicts
2010	USA / Israel	The malware Stuxnet was used to sabotage the Iranian nuclear program silently. Its presumably long development and deployment time, which involved specific information on the targeted industrial systems, were an international "eye-opener" on how states use cyberspace attack for foreign policy intentions
2012	Iran	A malware named Shamoon/Wiper was used against industrial oil companies in Saudi Arabia. The malware had been explicitly developed to spread quickly within infected networks and render the targeted computers useless by deleting relevant operating system files. It affected up to 30,000 IT systems
2012	USA / Israel	The malware Flame was used in the Middle East for espionage and intelligence purposes, especially in Iran, Israel, Palestine, Lebanon and Saudi Arabia. It was considered to be the most versatile malware development so far, with a vast variety of modules to infect different IT systems and perform multiple tasks on them. Therefore, Flame is seen as the first state-developed "cyber attack multi-purpose framework"
2013	China	A US-based IT security company Mandiant report analysed several long-term cyber attacks and revealed a military cyber force in China, based on IT forensic analysis. The Unit "PLA 61,389" had been accused of espionage attacks with custom-tailored cyber weapons
2014	Israel	The malware campaign Duqu 2.0 was used for espionage purposes with particularly versatile cloaking mechanisms. It is presumably a further development and extension of earlier versions that had been detected 2011

(continued)

[1] Source for all: https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/

[2] The alleged actor is mostly based on information published by intelligence or law-enforcement agencies. The underlying evidence had been seldomly revealed and it had to be considered that such charges can have political motivation, too. Also, it is important to note, that the distinction between hacking activities by a state and its institutions and non-state groups that are not directly connected to a state but under its indirect control is hard to make.

Table 7.1 (continued)

Year	Alleged actor[2]	Description
2014	Palestine	XtremeRAT was a spear-phishing malware campaign in the context of the Middle East conflicts that a Palestinian activist group had used for espionage and data theft
2015	USA	The Equation Group is the name of a malware campaign with a highly complex infrastructure and technological basis. The campaign had been active for several years, with the earliest indications from 1996. Its highly developed tools and malware frameworks had been developed and extended over years and share similarities with incidents like Stuxnet and Flame
2015	Russia	In the context of the Western Ukraine conflict, Russia was accused of attacks against Ukrainian energy companies that stopped the power supply for around 700,000 residents for several hours. The malware BlackEnergy and Killdisk were used to gain access and shut down IT systems
2016	Russia	In preparations for the US presidential elections 2016, cyber attacks were performed against the Democratic National Committee that led to a severe data breach. Some of the documents were subsequently leaked. The cyber attack is seen as part of severe and long-lasting interference within the democratic election process of the USA. As for the end of 2018, the investigations are still ongoing
2016	United States/ Great Britain	Israel revealed that US and UK intelligence services covertly intercepted real-time video feeds from Israeli military drones and fighter jets. Their surveillance efforts were focused on monitoring military activities in Gaza, anticipating any potential Israeli actions against Iran, and tracking the global export of Israeli drone technology
2017	Iran	A malware that targeted specific industrial control systems (SCADA) was deployed against Saudi-Arabian petrochemical companies. It had been specifically designed to trigger physical harm and destruction in these facilities, although this never happened due to programming errors
2017	North-Korea	After the leak of the fatal zero-day exploit EternalBlue, which had been stolen from the NSA and affected Microsoft Windows systems, a malware called WannaCry was deployed that used this exploit. It spread massively around the world and held affected users to ransom by encrypting their hard drives
2018	Russia	In spring 2018, a hacking attack against German governmental IT systems and networks was published. The attack had been active but cloaked for more than a year and had been performed very carefully—without automatic replication or infection of IT systems. Its primary goal presumably had been espionage
2018	Iran	The US Departments of Justice and Treasury have charged Iran in an indictment, alleging the theft of intellectual property from over 300 universities, in addition to government agencies and financial services firms

(continued)

Table 7.1 (continued)

Year	Alleged actor[2]	Description
2019	North Korea	In February 2019, the North Korean Bureau 121 attacked the Bank of Valletta, Malta trying to steal $14.5 Million through Phishing attacks
2019	China	The European aerospace corporation Airbus disclosed that it had been the victim of Chinese cyber attacks that led to the theft of personal and IT identification data belonging to several of its European staff members
2020	Iran	During the COVID-19 pandemic, hackers supported by the Iranian government made efforts to infiltrate the accounts of personnel working for the World Health Organisation (WHO)
2020	China	US authorities have alleged that hackers associated with the Chinese government made attempts to pilfer American research related to a coronavirus vaccine
2021	North Korea	North Korean government hackers engaged in a complex social engineering campaign against cyber security researchers, utilising fake Twitter (renamed to X) accounts and a phony blog to lure targets into visiting infected websites or opening compromised email attachments. They approached their targets under the pretence of collaborating on a research project, with the campaign focusing on individuals associated with the Center for Strategic and International Studies (CSIS, 2023) in Washington, D.C
2021	China	Norway pointed to China as the source of a cyber attack on its parliamentary email system in March 2021
2022	Iran	Hackers supported by the Iranian government infiltrated the US Merit Systems Protection Board, exploiting the log4shell vulnerability as early as February 2022. Following the breach, these hackers installed cryptocurrency-mining software and deployed malware to acquire sensitive data
2022	Iran	Hackers supported by the Iranian government infiltrated the US Merit Systems Protection Board, taking advantage of the log4shell vulnerability as early as February 2022. Following the breach, these hackers installed cryptocurrency-mining software and deployed malware to extract sensitive data
2023	China	Authorities of the US and Japan have issued warnings, asserting that Chinese state-sponsored hackers have inserted tampering software into routers to target government agencies, industries, and companies in both nations. These hackers employ firmware implants to maintain a covert presence and navigate within the networks of their targets. China has denied these allegations
2023	Russia	Russian is stepping up cyber attacks against Ukrainian law enforcement agencies, specifically units collecting and analysing evidence of Russian war crimes, according to Ukrainian officials. Russian cyber attacks have primarily targeted Ukrainian infrastructure for most of the war

has already outlawed. Accordingly, **cyber weapons** are malware (such as viruses, worms and Trojans), which work only when based on loopholes in the security of alien systems. Therefore, cyber armament consists mainly of searching alien networks, institutions and devices for potential vulnerabilities or creating them. Of course, as there is a market for everything, access to and knowledge of security gaps can also be bought, predominantly in the Darknet (see Chapter 6, "*Darknets and Civil Security*"). In cyber war, aggressors use their control over systems to harm or spy on the opposing party. In practice, this means that anything containing a computer can be attacked. Thus, every PC, every router and telephone, and every control system, be it small or large, become potential targets. If our **critical infrastructure** (e.g. transportation systems, waterworks, hospitals and power plants) were switched off or even used against us, the consequences and especially the knock-on effects would be just as devastating as in an attack with conventional weapons when supply chains or the transportation system would break down.

Nonetheless, governments around the globe are arming for offensive cyber war, including Germany that establish a dedicated military cyber force, called Kommando Cyber- und Informationsraum (CIR). A broad societal discussion about the legality of turning our devices into weapons that can be used against us at any time has yet to materialise. However, FIfF names several reasons cyber weapons should be outlawed, and money spent on keeping critical infrastructure vulnerable used to close security gaps instead.

1. Cyber weapons can be used anonymously. In global virtual networks such as the internet, it is hard to identify the real perpetrator, as they mostly use several devices to execute the attack to make backtracking impossible. Furthermore, attacks are often committed at a time that suggests a different origin. And even if traces of the attack can be found, they do not prove anything because they are digital, and it is therefore impossible to tell whether they were left intentionally or accidentally (see Chapter 12 "*Attribution of Cyber Attacks*").
2. Cyber weapons cannot be controlled. Malware is often programmed to have an independent existence. It cannot be accounted for if it is intentionally used as a weapon or simply activated by accident. Weapons of this sort can lie dormant in systems for years before causing any harm. What distinguishes cyber weapons from conventional weapons, such as small arms, is that they can easily be stolen, infinitely reproduced and spread simply by copying and pasting them.
3. Cyber weapons are expensive. Militaries and secret services spend vast amounts of money on analysing systems and buying security gaps. As only open loopholes can be used as weapons, buyers of information on them are interested in keeping them open as long as possible. Consequently, vast quantities of money are being spent globally to keep our critical infrastructure insecure and vulnerable deliberately. Naturally, these weaknesses can be (and are) found and exploited daily by criminals and terrorists (FIfF, 2017).

This chapter first illustrates the relevance of cyber war as a realistic part of future warfare and goes on to identify current challenges that the militarisation of cyberspace poses. A central difficulty consists of applying international law to cyberspace, partly due to the characteristics of cyberspace, mainly characterised by the attribution problem and partly due to the lack of international norms and definitions concerning cyberspace. These problems also make arms control in cyberspace more difficult than controlling conventional weapon types. We further present measures that could be taken towards achieving cyber peace and some campaigns that try to raise public awareness of the necessity to act in this direction.

7.2 Current Challenges of Cyber War[3]

7.2.1 Militarisation of Cyberspace

Since the discovery of Stuxnet, the term cyber war – derived from the war as a military-fought conflict between states and the term cyberspace – has been coined in connection to incidents of this kind. However, it neglects a vital distinction which has to be considered when handling and interpreting such events: If the initiators of a cyber attack have not been ordered directly by a government, the attack in question is a "normal" criminal offence, which is a matter of national and international criminal prosecution and police cooperation. These multilateral agreements already exist, such as the *Budapest Convention on Cybercrime* issued in 2001 (Council of Europe, 2001). Only once a government is the assumed attacker the interpretation of the incident concerns the political level and become relevant in international law.

Here, a critical distinction has to be made regarding an appropriate reaction: Are we dealing with an intelligence service **espionage**, mainly targeting a system's confidentiality, (see Chapter 5 "*Cyber Espionage and Cyber Defence*"), **sabotage**, with the goal of eakening a system or military activities directed towards clear strategic goals? For this purpose, we need to look at the damage already inflicted. Depending on the attacker's intention and applied malware, the range can reach from simple theft to temporary shutdown of an IT service to specific damage of IT and subordinated systems (Brown & Tullos, 2012).

Questions concerning cyber war exceed the purely technical aspect of IT system maintenance or attacks on such systems. Apart from the aspects of defence and offence and the necessary tools, states' security-political and military-strategical doctrines play a significant role. These determine to which degree a state identifies cyberspace as a military domain and how it treats it according measures by other states.

[3] This section is based on a previous version that has been published in German (Reinhold, 2015).

For a few years, since the discovery of Stuxnet at the latest, governments have been increasingly perceiving cyberspace as a military domain. According to a study by the United Nations Institute for Disarmament Research (UNIDIR), at least 47 states operated military cyber programs in 2013, of which ten nations had a nominally offensive intention (UNIDIR, 2013)—a situation that presumably will have changed since then. Documents from Edward Snowden's collection give further evidence. We find that in 2012 Barack Obama, being US president at the time, instructed his military and secret service leaders to create a list of the most critical potential military targets in cyberspace and to develop solutions for the disturbance of these targets up to their destruction (The Guardian, 2013). The consequence of this presidential directive became evident regarding the cyber espionage and manipulation opportunities revealed in 2013, which the National Security Agency (NSA) had been developing in the US. It partially distributed as hidden digital sleeper agents in commercial products. Traditionally, the NSA is subordinated to the US cyber command leader, i.e. the offensive cyber forces of the US armed forces, who therefore have direct access to NSA technologies. Since 2016, these have been officially used for the first time in the war against the Islamic State (US White House, 2016). In the Warsaw Summit Communiqué in 2016, NATO has integrated defence in cyberspace into collective defence according to Article 5 of the North Atlantic Treaty. It is therefore also evaluating cyber attacks and the aspect of military aggression.

Germany's which consisted of approximately 60 members. The CNO forces are assigned to the organisational unit of the strategic reconnaissance command. This unit's task is the offensive access to foreign IT systems. However, they are currently training in enclosed training networks and have not yet been utilised, according to official announcements (German Federal Parliament Defense Committee, 2016). At the end of 2017, the Federal Defence Ministry has officially integrated the Federal Armed Forces' organisational units dealing with IT and cyberspace into a separate organisational unit. "Cyber and information space" consists of 16.000 personnel and shares an organisational level with the military service branches of Army, Marine, Air Force, and the Medical Service (German Federal Ministry of Defense, 2016). Furthermore, the CNO unit has been enhanced to a Centre for Network Operations and expanded by 20 posts. Due to the necessary intelligence information on relevant targets in cyberspace, it is presumably cooperating more closely with the Federal intelligence service. The strategic guidelines of the White Paper show that these restructuring measures are linked to improved defence possibilities, as well as an enforced strategically offensive orientation of the Federal Armed Forces in cyberspace: "The capability of the Federal Armed Forces' common action in all dimensions is the superior benchmark" and an "impact superiority has to be reached across all intensity levels" (German Federal Government, 2016, translations by author). To reach this goal, the Federal Ministry of Defence in cooperation with the Federal Ministry of the Interior, Building and Homeland, founded a new agency for innovations in IT security that should take an example in the US Defense Advanced Research Projects Agency (DARPA). The task of this agency is to initiate, promote and finance research and innovation projects in the field of cyber security, especially "tomorrow's

IT security solutions" (German Federal Ministry of Defence, 2016). For the period from 2019 to 2022, the agency could spend a total of around 200 million euros.[4]

The increasing militarisation of cyberspace holds several challenges in the domains of international law and security policy for the international society and individual states, which will be referred to in the following sections.

The Russian war against Ukraine, which began in February 2022, showed for the first time an open military conflict that was also accompanied by strong activities in cyberspace (Reinhold & Reuter, 2023). Beside this, as shown in Table 7.1 below, there have been quite a few malicious incidents- with different objectives and magnitudes. This hints at possible scopes and consequences of future cyber warfare, and therefore the (growing) relevance of the topic.

7.2.2 International Law in Cyberspace

With regard to the established rules of international operation, the question arises of how they can be applied to cyberspace. The difficulty of this debate already becomes evident with the discussions on a common definition of cyberspace: While technical standards guide the US and Western European understanding and covers the number of IT systems and their network infrastructure so that security primarily refers to the integrity of these systems, other countries like Russia or China consider the information which is saved, transmitted and published therein as part of cyberspace. As a result, security, especially on a national level, exceeds the integrity of technical systems and becomes an issue of control of and access to this information – a point of view which is difficult to reconcile with human-rights principles (UN General Assembly, 2011).

7.2.2.1 Tallinn Manual

Experts convened by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) first attempted to solve this problem in 2013 with the so-called **Tallinn Manual**, a handbook including 95 guidelines for nations in case of a cyber war. Even though it is not binding, it points out the specific characteristics of cyberspace in which international law applies (NATO CCDCOE, 2013), and indicates how international law can be interpreted for military conflicts in this new domain. In 2017, the CCDCOE published a second version of the manual called the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" (NATO CCDCOE, 2017) that continues this evaluation, especially of state behaviour, as well as rules and norms in peacetime.

[4] In comparison, the 2018 DARPA budget had been $3.17 billion. Although it is necessary to mention that the DARPA has a much wider research variety. See https://www.darpa.mil/about-us/budget.

7.2.2.2 Virtuality of Cyberspace

The central challenge lies within the virtuality of cyberspace, which undermines approaches and regulations based on territorial borders or the localisation of military means. Equally problematic are the immateriality of malware as well as the unlimited possibility to reproduce it. Furthermore, due to cyberspace's structure and data transmission principles, it is easy to act secretly or cover up the actual origin of an attack by using proxy servers or other hacked and exploited foreign IT systems resulting in the attribution problem. In addition, IT systems are often highly interconnected and directly or indirectly control processes of so-called critical infrastructures, such as electricity or water supply, communication or traffic (German Federal Ministry of the Interior, 2009). The impairment of a nation's IT system can, therefore, have potentially incalculable consequences with serious impacts on originally not intended targets. Because concealed access to IT systems with the aim of espionage or military situation assessment is often linked to the application of malware and manipulation of the IT system functions, the threshold for such threats is shallow.

Regarding central concepts of international law, these characteristics of cyberspace raise a range of issues. For example, this concerns the international agreement on nonviolence and the right of self-defence according to article 2, paragraph 4, and article 51 of the UN Charter, as well as the **principles of adequacy** and proportionality of military reactions: What does "use of force" mean in cyberspace? When are malware and various cyber attack tools and methods considered "weapons"? When do we speak of an "armed attack"?

Previous approaches to applying these concepts to cyberspace usually refer to the consequences of classical, kinetic weapons to evaluate specific cyber incidents and possible reactions legitimised by international law. Thus, the Tallinn Manual defines armed attacks in cyberspace as "cyber activities that proximately result in death, injury, or significant destruction" (NATO CCDCOE, 2013).

7.2.2.3 Characteristics of the Application of Malware

Such an approach, however, falls short since it does not sufficiently consider that the scope, timing and form of damage from cyber attacks are not comparable to conventional weapons in many ways:

- Firstly, it is possible for malware to spread uncontrollably beyond IT networks and affect external systems that were not the attack's target and possibly belong to an uninvolved nation. For example, inactive versions of Stuxnet have been discovered on tens of thousands of systems worldwide (Falliere & Murchu, 2011). The application of malware operating secretly over a longer time frame or using indirect methods of sub-system manipulation, and thus not inflicting directly visible and assignable damage, is equally problematic.
- In addition, the current trend towards cloud technologies further complicates the geographical localisation of IT systems because electronic data is processed and stored not

on a single computer but possibly on various such systems that are often globally distributed. Linked to this is the so-called **attribution problem** (see Chapter 12 "*Attribution of Cyber Attacks*"): Every nation's right of self-defence implies that the origin of an attack to which the nation is forced to react promptly must be clear. In cyberspace, however, as mentioned above, it is common practice to carry out attacks from external systems specifically hijacked for this purpose to cover up the source. As a consequence, the retracing of these attacks through several steps cannot be carried out in a timely and forensically reliable manner. The particular limitation of permitted military use of malware proves to be equally difficult. Usually, IT tools, methods and software used by criminals, IT security experts and military forces to access IT systems are barely distinguishable. Nevertheless, depending on the intention, their usage has very different outcomes: For example, revelation, analysis and remedy of weaknesses (IT security expert), theft of credit card details (criminals) or the disruption or destruction of military system like an air monitoring program (military). Apart from the tools, the identifiability of state or military agents, the term combatants in cyberspace, and their distinction from civilians, are hard to achieve with current technologies. However, such labels are essential for dealing with agents in crisis and war situations.

Expert groups are debating these questions in the United Nations and the Organisation for Security and Co-operation in Europe (OSCE). However, we cannot yet see specific approaches for binding international regulations in cyberspace, especially about the "right to war" (***ius ad bellum***) and the "law of war" (***ius in bello***).

7.2.3 Lacking International Norms and Definitions

7.2.3.1 Cyber War vs. Cybercrime

A fundamental problem when evaluating incidents in cyberspace consists in the distinction between ordinary criminality in cyberspace, so-called **cybercrime**, and governmental actions as well as those directed against other nations, referred to as **cyber war.**[5] Furthermore, the evaluation of a threat caused by a cyber incident and the reaction on the political and legal level, is up to the affected state. Based on already established regulations on cybercrime, international agencies like ICPO-Interpol or Europol are dealing with international criminality in cyberspace. At the same time, the European Network and Information Security Agency (ENISA) is consulting and connecting EU states via cooperation centres.

In contrast to this, it is challenging to apply established norms to cyber incidents which are allegedly traced back to state agents or third parties under governmental order

[5] The term "war" refers to the international law and its regulations. War therefore is always an action of or between states.

since the partaking agents cannot be identified and, therefore, compliance with covenants cannot be verified, and because of a lack of internationally binding agreements. It is controversial whether international humanitarian law can be applied to cyberspace because of national sovereignty and the right of self-defence, but also with regard to nations' responsibilities in cyberspace. Another question concerns the scope of damage caused by a cyber attack, which would correspond to an armed attack and legitimise national self-defence, according to Art. 51 of the UN Charter.

The NATO CCDCOE, among others, has been mainly contributing to the answer to these questions with the two Tallinn Manual publications (NATO CCDCOE, 2013, 2017), along with the UN Group of Governmental Experts with their reports (Tikk-Ringar, 2012) and the Organisation for Economic Co-operation and Development (OECD). All are dealing with the application and extension of established norms of international law to cyberspace, difficulties and limitations resulting from this, and discussing different solution approaches. While the groups agree on the fact that cyber attacks, under certain circumstances, can violate national sovereignty, there are significant differences concerning clear definitions for cyber attacks. Especially so, when it comes to their comparability to armed attacks and the issue of appropriate reaction to a cyber attack, such as the use of conventional weapons. The underlying differences between states on these issues still strongly inhibit the development of internationally binding agreements (Tikk & Kerttunen, 2017).

7.2.3.2 Binding Norms

Apart from questions concerning the motivation for a cyber attack, establishing binding norms is further complicated by differentiating between cyber activities without the intention of damage (espionage) and those attacks which are actively carried out with the aim of disrupting external IT systems (sabotage). Both kinds of access correspond to similar principles and use similar tools. They notably differ in terms of the malware installed and controlled by the attacker, which performs the desired damaging function on the target system (**payload**). The latter can consist of copying and stealing information, and completely shutting down thousands of afflicted PCs, as demonstrated in the attack on the Saudi company Aramco (Bronk & Tikk-Ringas, 2013).

7.2.3.3 Attribution Problem

Another problem for applying international law lies within the attribution problem of attacks in cyberspace mentioned above, i.e. timely identification of an attack source. This is much harder in cyberspace than with conventional weapons, since the attackers possess many options to cover up their identity. Even though debates often refer to the practical impossibility of attribution, authors like Herb Lin (2011) argue that under certain circumstances, the identification of the origin network is sufficient to gain details about the offender so that the same source computer does not necessarily have to be identified. Apart from this, the planning and operation of specific access to complex systems take a particular time, where transmission data can be collected, forensically analysed and used for attribution under consideration of the current international political situation (Clark & Landau, 2010). Using this approach, in spring 2013, the US IT forensic company Mandiant identified a cyber unit of the Chinese People's Liberation Army (PLA Unit 61,398) as the initiators of several attacks against US-American organisations and institutions carried out over many years. They published their insights (Mandiant Corporation, 2013) at a time of high-level meetings between the US and Chinese presidents and state secretaries on security in cyberspace.

Methods of cyber attribution consist of metadata analysis such as IP-tracking, analysing re-used cryptographing keys, attacking servers used in the malware (command and control servers), looking for language specific hints, or even recognising patterns in the code with the help of artificial intelligence to link a software to a single person (see Chapter 12 "*Attribution of Cyber Attacks*").

7.2.3.4 Elaboration of International Norms and Cyber Weapons

Furthermore, the elaboration of international norms for cyberspace becomes difficult due to the definition above of cyber weapons. As explained above, the hardware and software tools for accessing external systems do not reveal many details on the specific intention. The OECD analysed this question about characteristics of conventional weapons:

> There is an important distinction between something that causes unpleasant or even deadly effects and a weapon. A weapon is 'directed force' – its release can be controlled, there is a reasonable forecast of the effects it will have, and it will not damage the user, his friends or innocent third parties. (Sommer & Brown, 2011)

Based on these criteria, the authors of this OECD study identified essential reference points for evaluating specific malware, taking into account technical details, the political situation of the national agents, and their presumed intention. They suggest a classification of all malware in a continuum between "low-level cyber weapons" (the manipulation of websites or purposefully sent emails inflicted with malware for espionage purposes) and "high-level cyber weapons" (attacks with direct and lasting disturbing or destructive effects). A sufficient distinction between malware and the decision of whether it is a weapon according to international law can, therefore only be made in the context of individual cases.

7.2.4 Difficulties for Arms Control in Cyberspace

The presented difficulties and ambiguities which the international community is facing concerning militarisation of cyberspace also raise issues of security policy. On the one hand, considering the increasing cyber threats and the higher awareness of risk around critical infrastructures, it is important to protect IT systems more effectively and sustainably. On the other hand, improvement of defence know-how, analysis of attack scenarios and identification of weak points also implies an increase in the potential ability for offensive actions in IT systems. A sensible technical distinction is not possible at this point, while limitations to purely defensive activities by military forces are declarative only.

7.2.4.1 Active Defence

Similar problems emerge from the **active defence** concept considered by NATO CCD-COE (2014) and the German Federal Armed Forces (German Federal Parliament Defense Committee, 2016). The essence of this idea lies within preventing cyber threats not only by purely defensive measures like disconnecting network connections but also via hack-back, i.e. the intrusion into and disruption of the offender's IT systems. Apart from the problem that the perceived source of an attack does not necessarily lead back to the actual attacker, offensive capabilities must be established here. Furthermore, a detailed knowledge of the domain is required, i.e. understanding of the goals, their state and technical details, as well as the used software and its version, to be able to use cyber weapons effectively and purposefully so that, if necessary, intelligence service activities can be initiated in the potential attackers' IT systems before an attack.

Apart from this, knowledge of security gaps in the target systems is necessary for specific access. In many past incidents, security gaps in popular and widely used software such as email programs, browsers or Office applications have been used. An increase in offensive military activities does not benefit an open approach to security gaps and their closure – instead, the trade with such knowledge has been flourishing, be it on the black market or by companies that seek, buy and commercially exploit such security gaps (Reinhold, 2014).

7.2.4.2 Dual-Use

Along with the militarisation of cyberspace, considering the current uncertainties on the international evaluation of the new military potential, there is a risk of an arms race between states that try to excel each other with military cyber capabilities. About the established international arms control measures and disarmament initiatives, new questions arise in this context. IT assets as well as software security gaps with potential military value, are commonly used by civilians. While this so-called **dual-use** character (see Chapter 8 "*Dual-Use Information Technology: Research, Development and Governance*") creates the necessity for a thorough export examination, the software characteristics mentioned above make it difficult to comprehend the proliferation and use, cases of exports and to verify the commitments of importers and purchasers of these systems.

As a first step for monitoring trade with IT systems of value for intelligence service or military, the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies*, established in 1995, has been extended to include so-called intrusion software in 2013 (Wassenaar Arrangement Secretariat, 2017). Even though this multilateral arrangement currently consists of 42 states should be regarded critically (Holtom & Bromley, 2010), it is an essential starting point for establishing regulations and the future of arms control in cyberspace. Furthermore, export control of high-tech hardware systems with enough computational power to possibly break cryptographic systems has been introduced (Supercomputer und Exportkontrolle, Bundesministerium für Bildung und Forschung, 2021).

In order to prevent an arms race, further confidence-building measures between states are crucial. These should allow states to discuss their ideas of security, perceived threats and those addressed in the context of security strategies, as well as initiated measures. The goal is "to reduce and even eliminate the causes of mistrust, fear, misunderstanding and miscalculations with regard to relevant military activities and intentions of other states" (UN General Assembly, 1988) and to establish communication channels for further conversations or crises.

First, bilateral agreements on a common interest in security of civil IT systems, as well as limitation of potentially threatening intelligence service espionage already exist. Especially the US and China have been leading high-level discussions in the past years under the Obama presidency, establishing the first bilateral contract specifically referring to IT security in 2015, where both states addressed critical potential cyber threats (Nakashima & Mufson, 2015). This process has been accompanied by bi- and multilateral military crisis training for cyber incidents (Hopkins, 2012).

7.2.4.3 Computer Emergency Response Teams

Another important step towards confidence-building measures consists in the development and establishment of collective incident reporting systems, i.e. structured and hierarchical warning and reporting systems for critical cyber incidents, such as already existing **Computer Emergency Response Teams** (CERT) on a national level, or for partial networks like academic research associations. The European Union is moving towards transnational protection of IT infrastructure stability by introducing a national obligation to report such incidents and an interconnected exchange network crossing national borders.

All this contributes to reducing irrational fear of the cyber doomsday often spread through media. The cyber incidents of the past years have shown that cyber attacks by state agents rarely result in open war-like conflicts carried out over the internet, but rather become a matter for foreign policy, as is the case with classical espionage incidents. For example, the US government used a data theft in the context of a cyber attack on a company affiliated with Sony located in the US in 2013 as an opportunity to impose sanctions on North-Korean citizens and companies, even though there was no sufficient evidence.

7.3 Measures for Cyber Peace

The militarisation of cyberspace also concerns its civil, individual use. The NSA affair of 2014 and 2015 has demonstrated the wide range of surveillance and control options in cyberspace – from an aggregation of various data by IT services and social networks to total surveillance or a well-aimed hardware manipulation (Appelbaum et al., 2013) – and the degree to which their military use in the context of international competition for dominance in cyberspace affects universal human rights. The destructive and economically disastrous malware campaigns WannaCry and NotPetya from 2017 (Ehrenfeld, 2017; Fayi, 2018; Fruhlinger, 2017b, 2017a), both based on zero-day exploits which had been stolen from the NSA, demonstrated once again the risks of the non-disclosure of vulnerabilities for intelligence or military purposes.

At the same time, cyberspace resembles commons regarding its broad impact and social dependencies as defined by Elinor Ostrom's theories (1990). Constant intelligence service activities in cyberspace as well as the purposeful weakening of IT systems, or the conscious manipulation of IT infrastructures in favour of military strategies are hence impairing a commonly used asset.

Therefore, the international state community must face the numerous challenges on the way to peaceful use of cyberspace. Apart from the questions as mentioned above referring to arms control and confidence-building measures, these challenges also concern the structures behind cyberspace itself: The discussions around increased participation by international organisations such as the International Telecommunication Union of the United Nations in decisions concerning the development and technological expansion of cyberspace are still ongoing. For quite some time, emerging nations like Brazil have been demanding an end to the dominance of the US-American Internet Corporation for Assigned Names and Numbers, which is coordinating the domain name system and the assignment of IP addresses, as well as a broad participation of all nations in designing cyberspace. Moreover, even economic actors that often provide the technical infrastructures or essential services demand multi-stakeholder debates on the future embodiment of cyberspace and binding rules for the actors in this domain.[6]

As a domain defined and entirely controlled by humans, cyberspace offers prerequisites for a peaceful formation on the one hand. On the other hand, the all-destructive cyber war will probably never happen due to increasing international dependencies, but they risk spilling over to conventional wars. Cyber weapons will rather be included in the military strategic planning arsenal and primarily used along with conventional methods (Hybrid Warfare). However, this is a relatively weak reassurance and should not satisfy peace activists.

Due to the different characteristics of problems cyber war and cyber peace pose, as well as the multitude of stakeholders involved and their interests, various possibilities to influence and shape the process are offered. To do this successfully, measures must be targeted at the respective bargaining level and context of the discussion. In this context, Götz Neuneck (2001) proposes differentiating between three areas of measures:

[6] As an example, see the proposal for a "Digital Geneva Convention" by Microsoft (https://blogs.microsoft.com/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf) or Google's proposal for a new law framework (https://www.blog.google/topics/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/).

1. **cooperative** and **declaratory approaches**
2. **informational approaches** and
3. **technical approaches**

In the following, these areas will be presented. As cyberspace provides the unique chance of perfect human control and design, the focus of information scientists should lie on questions regarding the possible realisation of peace-building measures, such as **confidence building**, **arms control** and **verification** by technical means. To be more precise, they should consider how cyberspace's technical foundations and operating principles can contribute to this goal. Although findings from past decades concerning similar lines of questioning in different technological areas (e.g. nuclear armament, biological and chemical weapons, as well as the *Outer Space Treaty*) are not necessarily transferable, the experiences of these long-standing endeavours can provide essential indications and impulses for the upcoming international debates on the peaceful usage of cyberspace between states or at UN level.

7.3.1 Cooperative and Declaratory Approaches

Cooperative approaches pursue coordination and confidence building at a low level amongst relevant actors of the different states and their military organisations. In practice, this implies promoting the interaction of representatives at conferences and in workshops. While doing so, there is opportunity to discuss and explain threat scenarios, cyber doctrines and security concepts, to gain a mutual and common understanding of the problems, as well as develop a uniform language regarding the issues at hand. Moreover, joint military training in cyber scenarios can help establish communication channels and reduce worries about armament and mistrust. Examples for such cooperative exercises are Cyber Europe 2010 and 2012 (ENISA, 2011, 2012) and the China-US-Wargames 2012 (Hopkins, 2012), the latter of which was organised by NGOs in cooperation with armed forces.

Another possible approach consists of establishing platforms to exchange information on the details of defensive and offensive measures the respective actors are conducting or planning in cyberspace. Such information can compensate for perceptions of opposing parties' potential for aggression and destruction and their technological abilities. Emergency communication could also be conducted over such channels, which can serve as an early warning system in the way of the red telephone, metaphorically direct contact between political leaders of different states for crises, or an emergency broadcast system designed for cyber incidents.

Further cooperative approaches are mutual support (capacity building) in establishing national measures of protection against cyber attacks, linkage of national reporting and emergency teams for cyber incidents (computer emergency response teams (CERTs)), the development of collective cyberspace treaties, and in the long run, measures of arms control and verification. Particularly for the latter, however, there is an apparent lack of willingness to cooperate as well as a lack of convincing concepts.

Next to these cooperative approaches are declaratory ones that states can unilaterally self-commit to as a **policy of détente**. Among these are the defensive orientation of armed forces as well as their security and defence doctrines and limitations in establishing cyber forces. This can be reflected in the total personnel strength of cyber forces, their drills and training scenarios, their technical equipment and organisational embedment in military operations. Renunciation of the “first use” of cyber weapons also belongs into this category.

A large fraction of these measures is regulative. It is like rules that they are, among other things, declared out of political rationales and can be broken. Nonetheless, they are suited to counteract distrust, misjudgement of opposing parties’ potentials and motivations, and rash reactions.

7.3.2 Informatory Approaches

A substantial part of states’ security concepts comprises collecting, central notification and analysing security incidents in state-owned and commercial institutions. In cyberspace, the concept of CERTs has existed for several decades. These central, intra-organisational registration offices collect incidents and report them to affiliated CERT organisations, to warn and inform partners about security problems. This concept has been picked up by states for some years now, and extended, linked and hierarchically organised in whole economic branches up to government agencies. Especially the European Network and Information Security Agency (ENISA) (2018) promotes such linkage inside and between EU states and develops concepts for the categorisation of cyber security incidents, as well as the classification and definition of security warning levels.

A further measure in this area is the creation and harmonisation of statutory reporting obligations of relevant security incidents in the commercial and private sector, in order to identify cyber threats in good time and share this information over CERT infrastructures.

7.3.3 Technical Approaches

As mentioned above, developing technical options for the establishment and the preservation of peace is an important part of necessary research. Such measures are currently barely being discussed on an international level. However, the technology of cyberspace is firstly designable. Secondly, computer systems already generate and save many relevant data and information that are suited for interchange and transparency building. The spectrum of technical measures that can be analysed encompasses short-term approaches from the field of classical cyber security, such as the exchange and analysis of communication and log data of computer systems and networks, as well as more research-intensive questions, such as the improvement of the detectability of cyber attacks and their origin, or questions of mapping the concept of borders with state responsibility and accountability into cyberspace. Further aspects concern the idea of neutral territory and objects defined by the *Geneva Convention* that should not be used by military forces or the development of sensor-based measures of verifying cyberspace disarmament treaties (Reinhold, 2018).

7.3.4 Cyber Peace Campaign

In their campaign Cyberpeace (Forum of Computer Scientists for Peace and Societal Responsibility, 2014) (see Fig. 7.1), the Forum calls for an end to all military operations on the internet by raising awareness of such dangers for, among others, individual privacy and human rights.

According to the Forum, the greatest threat lies in (unreported) flaws and loopholes inside IT systems used for cyber attacks. Because such attacks can hardly be controlled, they might affect civilian parties and critical infrastructures providing energy, water, communication and health, and other IT systems with potential security gaps. Especially governmental cyber attacks, which can use most resources and influence, can weaken these systems and threaten society's functioning and even human lives.

The Forum demands that all cyber weapons be abolished by creating binding international arrangements on arms control, disarmament and the renunciation of developing and using cyber weapons for offensive actions on a governmental level. At the same time, the internet should function as a civil and peaceful resource without being misused for spying on civilians. Connected to this, the concept of general suspicion should be abandoned and replaced by achieving reliable evidence. The detailed demands can be found in Table 7.2.

The threshold for military activities is lower on the cyber level as it does not create the impression of an actual war, which makes the abolishment of all cyber weapons necessary (see Table 7.2, demands 1, 2 and 3). This involves extending existing agreements like the *Geneva Convention* to cyberspace (5). Especially when it comes to critical infra-

Fig. 7.1 Logo of the Cyberpeace campaign

Table 7.2 Detailed demands of the Cyberpeace campaign (FIfF, 2023)

Demand	Details
1. No Pre-emptive or Offensive Strikes in Cyberspace	Nations should oblige themselves not to make offensive moves against others in cyberspace, while international agreements and cooperation on the prosecution of cybercrime should be extended to military and secret service activities
2. Purely Defensive Security Policy	Instead of developing and using cyber weapons for offensive purposes, nations should apply a defensive strategy of protecting IT systems against cyber attacks
3. Disarmament	Regulated by international agreements, nations should completely disarm on the cyber level. This does not concern (hacker) tools for defending against cyber attacks and exposing existing security gaps
4. No Conventional Response to Cyber attacks	Because of the attribution problem, the source of a cyber attack cannot be clearly identified. Therefore, conventional weapons should not be used to respond to such an offence to prevent a military escalation without valid evidence
5. Geneva Convention in Cyberspace	All applicable requirements of the Geneva Convention should be extended to cyberspace, and their disregard should be treated as a war crime. This especially concerns critical infrastructures for supplying existential goods and services, whose failure can threaten human lives
6. Government-Level Cyberpeace Initiative	Governments should establish an internationally binding cyberspace initiative to protect the internet as critical infrastructure and support the research and development of peace strategies
7. Democratic Internet Governance and Democratic Control over Cyber Security Strategies	Instead of being the domain of secret services and military consulting companies, cyber security strategies and attacks should be transparent, officially confirmed and openly discussed, to include them in the democratic decision process
8. Online Protest is not a Crime	As freedom of speech and assembly are basic human rights, they should be respected in cyberspace and not justify criminal prosecution or military activities
9. Clearly Defined and Demilitarised Political Language	Terms in the context of cyberspace should be officially defined and not used to mislead and fuel conflicts, as it currently is the practice in politics and media
10. Obligatory Disclosure of Vulnerabilities	By officially reporting security gaps, especially for public and corporate IT systems, it should be ensured that these are closed before they can be exploited instead of leaving them open for intelligence services or armed forces. Consequently, public awareness of and trust in defensive cyber strategies will grow
11. Protection of Critical Infrastructures	All operators of critical infrastructures should be obliged to independently and transparently secure and protect their systems from attacks and, if possible, detach them from the internet to prevent access for offenders

(continued)

Table 7.2 (continued)

Demand	Details
12. Cyber Security Centres	Independent and democratically regulated centres should be established to prevent cyber attacks, protect human rights and work towards cyber peace
13. Promotion of (rookie) IT Experts	Education around IT skills and their significance for society should be promoted to increase the number of qualified experts, improve the security and quality of IT systems, and raise discussion on ethical and political issues around technology
14. Promotion of FLOSS (Free and Libre Open Source Systems)	By officially promoting independent and transparent development, examination and risk analysis of software, loopholes can be openly identified and prevented, increasing security, especially for critical infrastructures

structures which guarantee the supply of existential goods and services, whose failure can threaten human lives, their disruption from outside should be treated as a war crime (5). All operators of critical infrastructures should be obliged to independently and transparently secure and protect their systems from attacks and, if possible, detach them from the internet to prevent access for offenders (11). At the same time, governments should establish an internationally binding cyberspace initiative to protect the internet as a critical infrastructure and support the research and development of peace strategies (6).

The employment of conventional weapons as a reaction to a cyber attack equally contradicts the Forum's peaceful policy. Because of the attribution problem, the source of a cyber attack cannot be identified. Therefore, conventional weapons could cause a military escalation without a good body of evidence (4).

Nonetheless, nations are urged to pursue a defensive strategy to protect their IT systems against cyber attacks and therefore be allowed to use (hacker) tools for defence and exposure of existing security gaps (2 and 10). Such security gaps, once identified, should be officially reported, especially for public and corporate IT systems, and closed before they can be exploited, instead of leaving them open for intelligence services or armed forces (10). Consequently, public awareness of and trust in defensive cyber strategies will grow. Furthermore, to prevent such weaknesses from emerging in the first place, security should be a central aspect for the architecture of computers, operating systems, infrastructures and networks (6, 11 and 14). The educational systems should promote education around IT skills and their significance for society to increase the number of qualified experts, improve the security and quality of IT systems, and invigorate discussion on ethical and political issues around technology (13).

Transparency and democracy are further central aspects of the campaign. By officially promoting independent and transparent development, examination and risk analysis of software, loopholes can be openly identified and prevented, increasing security, especially for critical infrastructures (14). Furthermore, instead of being the domain of secret services and military consulting companies, cyber security strategies and attacks should be officially confirmed and openly discussed to include them in the democratic decision process (7). As freedom of speech and assembly are fundamental human rights, they should be equally respected in cyberspace and not justify criminal prosecution or military activities (8). To further help protect human rights, independent and democratically regulated cyber security centres should be established to prevent cyber attacks and establish cyber peace (12).

As an essential tool for the formation of public opinion, discussion of cyberspace in media and politics should follow defined terms and not be used to mislead and fuel conflict (9). Therefore, the Forum also offers definitions for a better understanding of cyberspace-related terms.

7.4 Conclusions

The answer to the initial question crucially depends on the underlying concepts of cyber war and cyber peace. These are open to discussion, as the disputes on definitions of crucial terms, such as cyber weapons or cyberspace, are unresolved. Consequently, in times of increasing militarisation of cyberspace, applying international law to it is still challenging. At the same time, more and more activists try to frame cyber peace. Among them is the Forum of Computer Scientists for Peace and Social Responsibility, which advocates international disarmament, purely defensive cyber military capabilities, and an increasing formalisation of organisation and international law in cyberspace.

To recapitulate, the central challenges cyber arms pose are:

- The militarisation of cyberspace.
- Necessitated by its militarisation, the application of international law in cyberspace. Difficulties result from the characteristics of cyberspace and malware (which lead to problems of attribution and therefore problems distinguishing cybercrime from cyber attacks), as well as the lack of international norms and definitions.
- Arms control in cyberspace is complicated by the problems mentioned above. The offensive usefulness of defensive cyber capabilities and the dual-use character of civil IT systems further impede efforts made.

Measures to overcome these problems and achieve cyber peace include:

- Cooperative and declaratory approaches, i.e. promoting interaction and the exchange of information on the one hand, and unilateral commitments to arms control on the other hand;
- Informational approaches, i.e. increasing cooperation when it comes to the collection of information; and
- Technical approaches, i.e. increasing cyber security by technical means, especially by intensifying research.

Or, more programmatically put (by FIfF):

- Allowing purely defensive cyber policies only. The focus should lie on protecting IT systems; all other capacities should be disarmed.
- Illegalising conventional responses to cyber attacks. As the source of a cyber attack cannot be identified, conventional weapons should not be used in response.
- The extension of the *Geneva Convention* to cyberspace to make states legally liable for their actions in cyberspace.

7.5 Exercises

Exercise 7-1: How are military forces dependent on IT systems and how does the trend of digitalisation affect these organisations?
Exercise 7-2: What are the threats of a militarisation of cyberspace in terms of societal and international security?
Exercise 7-3: Which "lessons learned" could be taken from historical developments and how can they be applied to current challenges of cyber war and cyber peace?
Exercise 7-4: How can other tools (like social networks, open source or collaborative knowledge platforms) that also emerged from the digitalisation trend be used to empower civil campaigns and movements for the peaceful development of this domain?
Exercise 7-5: Which measures towards cyber peace do you think most promising in terms of their realistic capacity of achieving arms control and/or making cyberspace a solely peaceful domain? Can you think of alternative ways to achieve cyber peace (in light of your knowledge of International Relations theory)?
Exercise 7-6: Do you think solving the problems of applying international law to cyberspace is possible? If so, what would be appropriate measures towards your solution?

References

Recommended Reading

Neuneck, G. (2001). Präventive Rüstungskontrolle und Information Warfare. In Rüstungskontrolle im Cyberspace. Perspektiven der Friedenspolitik im Zeitalter von Computerattacken (pp. 47–53). Berlin: Dokumentation einer Internationalen Konferenz der Heinrich-Böll-Stiftung am 29./30. Juni 2001.

UNIDIR. (2013). The Cyber Index——International Security Trends and Realities. Geneva, Switzerland.

Forum of Computer Scientists for Peace and Societal Responsibility. (2014). No military operations in the Internet! Retrieved from https://cyberpeace.fiff.de/Kampagne/WirFordernEn.

Bibliography

Appelbaum, J., Horchert, J., Reißmann, O., Rosenbach, M., Schindler, J., & Stöcker, C. (2013, December 30). Neue Dokumente: Der geheime Werkzeugkasten der NSA. *Spiegel Online*. www.spiegel.de

Bright, A. (2007, May). Estonia Accuses Russia of „Cyber Attack". *Christian Science Monitor.*

Bronk, C., & Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. *Survival*, *55*(2), 81–96. https://doi.org/10.1080/00396338.2013.784468

Brown, G. D & Tullos, O. W. (2012, December). On the Spectrum of Cyberspace Operations. *Small Wars Journal*.

Clark, D. D., & Landau, S. (2010). The problem isn't attribution: It's multi-stage attacks. *Proceedings of the Re-Architecting the Internet Workshop*, 1–6. https://doi.org/10.1145/1921233.1921247

Council of Europe. (2001). *Convention on Cybercrimes*. https://rm.coe.int/1680081561

CSIS (Center for Strategic & International Studies). (2023). *Significant Cyber Incidents Since 2006*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Danchev, D. (2008, August). Coordinated Russia vs Georgia Cyberattack in Progress. *Zero Day*.

Ehrenfeld, J. M. (2017). WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *Journal of Medical Systems*, *41*(7), 104, s10916–017–0752–1. https://doi.org/10.1007/s10916-017-0752-1

ENISA. (2012). *Cyber Europe 2012—Key Findings Report*. https://www.enisa.europa.eu/publications/cyber-europe-2012-key-findings-report?v2=1

ENISA. (2017). *Cyber Europe 2016*. Publications Office. https://data.europa.eu/doi/https://doi.org/10.2824/218244

ENISA. (2018). *Cyber Europe 2018—After Action Report*. https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report?v2=1

Falliere, N. & Murchu, L. O. (2011). W32. *Stuxnet Dossier*. https://symantec-enterprise-blogs.security.com/threat-intelligence/stuxnet-dossier-espionage

Fayi, S. Y. A. (2018). What Petya/NotPetya Ransomware Is and What Its Remidiations Are. In S. Latifi (Ed.), *Information Technology – New Generations* (Vol. 738, pp. 93–100). Springer International Publishing. https://doi.org/10.1007/978-3-319-77028-4_15

FIfF (Director). (2017). *Cyberpeace statt Cyberwar!* https://www.youtube.com/watch?v=St955HBD-7k

FIfF. (2023, December). Eine Kampagne Des Forum InformatikerInnen Für Frieden Und Gesellschaftliche Verantwortung e.V. https://cyberpeace.fiff.de/Kampagne/Home/

FIfF. (2014). *No military operations in the Internet!* https://cyberpeace.fiff.de/Kampagne/WirFordernEn/.

Fruhlinger, J. (2017a). What is WannaCry ransomware, how does it infect, and who was responsible? *CSO*.

Fruhlinger, J. (2017b, October). Petya ransomware and NotPetya malware: What you need to know now. *CSO*. https://www.csoonline.com/article/563255/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

Fulghum, D. A. (2007, October). Why Syria's Air Defenses Failed to Detect Israelis. *Aviation Week & Space Technology*.

German Federal Government. (2016). *Weißbuch 2016—Zur Sicherheitspolitik und zur Zukunft der Bundeswehr.* https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf

German Federal Ministry of Defense. (2016). *Abschlussbericht Aufbaustab Cyber- und Informationsraum.* http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf

German Federal Ministry of the Interior. (2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie).* https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3

German Federal Parliament Defense Committee. (2016). *Wortprotokoll der 61. Sitzung*. Berlin, Germany.

Holtom, P. & Bromley, M. (2010). The International Arms Trade: Difficult to Define, Measure, and Control. *Arms Control Association*.

Hopkins, N. (2012, April). US and China Engage in Cyber War Games. *The Guardian*.

Jansen, F. (2021). Cyberattacke auf Bundestagsabgeordnete: Russische Hacker schicken deutschen Politikern Phishing-Mails. *Tagesspiegel*. https://www.tagesspiegel.de/politik/russische-hacker-schicken-deutschen-politikern-phishing-mails-6858718.html

Lin, H. (2011). *On Attribution and Defense. International Conference on Challenges in Cybersecurity – Risks, Strategies, and Confidence-Building.*

Mandiant Corporation. (2013). *APT1—Exposing One of China's Cyber Espionage Units.*

Nakashima, E., & Mufson, S. (2015, September). The U.S. and China Agree not to Conduct Economic Espionage in Cyberspace. *Washington Post*.

Nakashima, E. & Warrick, J. (2012, June). Stuxnet Was Work of U.S. and Israeli Experts, Officials Say. *Washington Post*.

NATO CCDCOE. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press. https://assets.cambridge.org/97811070/24434/frontmatter/9781107024434_frontmatter.pdf

NATO CCDCOE. (2014). *Responsive Cyber Defence: Technical and Legal Analysis*.

NATO CCDCOE. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (M. N. Schmitt & L. Vihul, Hrsg.)*. Cambridge Univeristy Press. https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

Neuneck, G. (2001). *Präventive Rüstungskontrolle und Information Warfare. Rüstungskontrolle im Cyberspace. Perspektiven der Friedenspolitik im Zeitalter von Computerattacken, (p. 47–53).* Dokumentation einer Internationalen Konferenz der Heinrich-Böll-Stiftung am 29./30. Juni 2001, Berlin.

Ostrom, E. (1990). *Governing the Commons. The Evolution of Institutions for Collective Action.* Cambridge Univeristy Press.

Reinhold, T. (2015). Militarisierung des Cyberspace—Friedens- und sicherheitspolitische Fragen. *Wissenschaft & Frieden*, *2*, 31–34.

Reinhold, T. (2014). *Die neuen digitalen Waffenhändler?* https://cyber-peace.org/2014/04/22/die-neuen-digitalen-waffenhaendler/.

Reinhold, T. (2018). *Maßnahmen für den Cyberpeace*. https://cyber-peace.org/cyberpeace- cyberwar/masnahmen-fur-den-cyberpeace/.

Reinhold, T., & Reuter, C. (2019). From Cyber War to Cyber Peace. In C. Reuter (Ed.), *Information Technology for Peace and Security* (pp. 139–164). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4_7

Reinhold, T., & Reuter, C. (2023). Zur Debatte über die Einhegung eines Cyberwars: Analyse militärischer Cyberaktivitäten im Krieg Russlands gegen die Ukraine. *Zeitschrift für Friedens- und Konfliktforschung*, *12*(1), 135–149. https://doi.org/10.1007/s42597-023-00094-y

Sanger D. E. (2014). Syria War Stirs New U.S. Debate on Cyberattacks. *New York Times*.

Sommer, P. & Brown, I. (2011). Reducing Systemic Cybersecurity Risk. OECD/IFP Project on »Future Global Shocks«. *OECD document* IFP/WKP/FGS (2011)3.

The Guardian. (2013, June). Obama Tells Intelligence Chiefs to Draw up Cyber Target List – Full Document Text. *The Guardian*.

Tikk, E. & Kerttunen, M. (2017). The Alleged Demise of the UN GGE: An Autopsy and Eulogy. *Cyber Police Institute.* https://cyber-peace.org/wp-content/uploads/2018/11/Tikk-Kerttunen-2017-The-Alleged-Demise-of-the-UN-GGE-An-Autopsy-and-Eulogy.pdf

Tikk-Ringar, E. (2012). Developments in the field of information and telecommunication in the context of international security: Work of the UN first Committee 1998—2012. ICT4Peace Publishing.

UN General Assembly. (1988). Special Report of the Disarmament Commission to the General Assembly at Its Third Special Session Devoted to Disarmament.

UN General Assembly. (2011). Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.

UNIDIR. (2013). *The Cyber Index—International Security Trends and Realities.*

US White House. (2016). Statement by the President on Progress in the Fight Against ISIL.

Wassenaar Arrangement Secretariat. (2017). The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies—List of dual-use goods and technologies and munitions list. *Wassenaar Arrangement Secretariat.*