Towards IT Peace Research: Challenges at the Intersection of Peace and Conflict Research and Computer Science*

Christian Reuter

Abstract: Advances in science and technology, including information technology (IT), play a crucial role in the context of peace and security. However, research on the intersection of peace and conflict research as well as computer science is not well established yet. This article highlights the need for further work in the area of research "IT peace research", which includes both empirical research on the role of IT in peace and security, as well as technical research to design technologies and applications. Based on the elaboration of the disciplines, central challenges, such as insecurity, actors, attribution and laws, are outlined.

Schlüsselwörter: IT-Friedensforschung; Technische Friedensforschung; Cyberspace; Cyber-Angriffe
Keywords: IT peace research; technical peace research; cyberspace; cyber attacks

1. Introduction

In 2017, numerous cyber attacks have occurred worldwide. In December 2017, an invasion of the German government network which connects federal ministries and responsible authorities was discovered (cf. Reinhold, 2018). Another example that represents one of the major ransomware attacks in the recent past is the "NotPetya" attack from June 2017. After large parts of Europe, especially the Ukraine, were attacked, the ransomware spread to other countries such as Brazil and the US. NotPetya worked by "modifying the Windows´s system´s Master Boot Record which caused the crashing of the system" (Aidan, Verma, & Awasthi, 2018, p. 124). Cyber attacks like WannaCry ransomware and NotPetya have led to the introduction of initiatives such as the Digital Geneva Convention (cf. Brinkel, 2018).

Besides the fact that those cases illustrate a serve IT security problem, they are also discussed as examples for espionage where an unknown group tried to obtain political information for unknown reasons. On this point, it is important to point out that cyber warfare does not know any boundaries, which is why it poses a threat for all countries and for international peace. Incidents such as the ones mentioned above and the current tensions between the US and Iran after the targeted killing of General Suleimani illustrate an increasing relevance of information technology for peace and security (cf. Kanno-Youngs & Perlroth, 2020; cf. Reinhold & Reuter, 2019). US American cybersecurity experts have already observed increases in malicious cyber activities by pro-Iranian hackers in their systems. They believe that the hackers try to destroy US government databases (cf. Kanno-Youngs & Perlroth, 2020). Those frictions evidence that cyber attacks can lead to an escalation on a political, diplomatic, and military level.

Innovations in scientific and technical research have always been used for military purposes and therefore had a strong influence on warfare. In the First World War, chemists, mathematicians, physicists and engineers were systematically involved in the production of war material (cf. Thee, 1988). Further on, telephones, radio, and digital communication were introduced on the battlefields. Transmission Control Protocol/Internet Protocol (TCP/IP) was developed by Vinton Cerf, an American scientist, in order to communicate under nuclear-war conditions, to create a common protocol for inter-network exchange of information and to let tank formations communicate on the battlefield (cf. Restivo & Denton, 2008, p. 262). Ever since, IT, with its extensive developments in crises, conflicts, and wars, has become increasingly important and part of international political agendas. With the aim of maintaining international peace and security, issues such as cyber attacks and cyber weapons have steadily been addressed in the last few years (cf. Bernhardt & Ruhmann, 2017).

This article aims to highlight the role of IT and computer science in peace and conflict studies, and it outlines challenges at their intersection. The research question in this article therefore is: **What are the central challenges for research at the intersection of peace and conflict studies as well as computer science?**

After presenting such a broad question, it should be noted that an answer containing all possible challenges is beyond the scope. However, some central ones will be outlined. As a first step, the disciplines of peace and conflict studies, natural science/technical peace research, computer science and cyber security are presented in this article as the basis of IT peace research. As a second step, central challenges of IT peace research, including insecurity, actors, attribution, verification, transparency, dual-use, proliferation and laws are analysed. The article closes with conclusions.

2. Towards a Definition of IT Peace Research

In the following sections, the author understands IT peace research as a field of research, which includes various other disciplines

* This article has been double blind peer reviewed. Parts of this article are based on the book "Information Technology for Peace and Security" (cf. Reuter, 2019), especially parts of section 1 and 2 (cf. Reuter, Aldehoff, et al., 2019) as well as some parts of section 3 (cf. Reinhold & Reuter, 2019; Riebe & Reuter, 2019a). The original contribution of this article is the outline of challenges on the intersection of the disciplines. The author would like to thank Laura Guntrum for her valuable support, Thea Riebe and Thomas Reinhold for discussions on the topic, as well as the (anonymous) reviewers for their feedback. This research work has been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Centre for Applied Cybersecurity ATHENE as well as the *Deutsche Forschungsgemeinschaft* (DFG, German Research Foundation) – SFB 1119 CROSSING – 236615297.

https://doi.org/10.5771/0175-274X-2020-1-10
DOI: 10.5771/0175-274X-2020-1-10

such as peace and conflict studies and computer science. First, the article will show the relations of computer science and peace and conflict. Second, a definition of IT peace research is given.

2.1 Peace and Conflict Studies

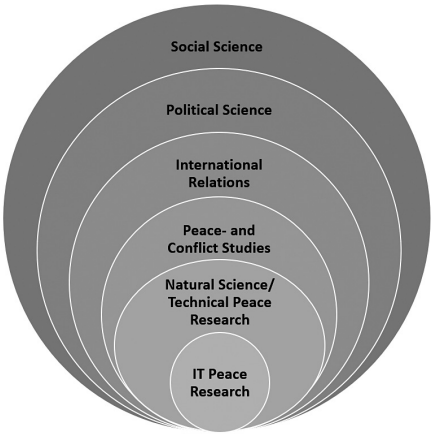
This section provides an overview of peace and conflict studies and classifies IT peace research within it. IT peace research is, amongst others, part of peace and conflict studies, which is an interdisciplinary research field in International Relations (IR). Peace research analyzes the causes of peace and war on the basis of scientific methods and theories from several relevant disciplines, as war and conflicts have almost always been present in mankind (cf. Bonacker, 2011). The oldest empirical study on peace can be dated back to the nineteenth century. Already between 1817 and 1819, the Massachusetts Peace Society investigated human losses in wars. Some of the oldest organisations of peace and conflict studies such as the Carnegie Endowment for International Peace (funded in 1910) and the World Peace Foundation (funded in 1911) are still working in the research field of peace and conflict nowadays (cf. Koppe, 2006). Besides peace and conflict studies, "International Security Studies (ISS) grew out of debates over how to protect the state against external and internal threats after the Second World War" (Buzan & Hansen, 2009, p. 8) and still play an important role in IR today.

As the research on wars previously meant the pure empirical investigation of war and the causes of war, the discipline of peace and conflict studies reinvented itself in the 1950s and early 1960s. Instead of seeing war as a necessary, or even inevitable, social phenomenon (cf. Bonacker, 2011), scientists like Boulding (1963), who saw war namely as a social but preventable phenomenon, attempted to radically change the methodology of the discipline and explain war by using existing social science methods (cf. Bonacker, 2011). This perspective was increasingly and step by step accepted and thereby established inter alia the field of peace research (cf. Gleditsch, Nordkvelle, & Strand, 2014; Koppe, 2006).

Peace research was particularly shaped by Johan Galtung who distinguished between negative and positive peace (cf. Galtung, 1998, p. 66f.). Initially, this new discipline understood itself as very normative – as a "research for peace". Although normativity never completely disappeared and is still nowadays more or less subliminally present, the self-conception of the discipline has changed over time. This is evidenced by the description of the discipline via the term "research on peace". This means that peace is the actual object of empirical research and not necessarily a goal that has to be achieved through it (cf. Bonacker, 2011). The understanding of peace research as a disciplinary field has also been controversially discussed: on the one hand, it can be seen as a field of research in IR, and on the other hand, it is often understood as an interdisciplinary field that makes use of methods and theories of various different disciplines (cf. Bonacker, 2011) in order to explain phenomena related to war and peace. Additionally, it addresses conflict management, conflict resolution, and peacebuilding.

The following figure (Figure 1) provides an overview of how IT peace research can be classified from a peace and conflict research and social science perspective.

Figure 1: IT Peace Research embedded in Peace and Conflict Studies and Social Science.



Source: Own illustration.

2.2 Natural Science/Technical Peace Research

In the interdisciplinary field of peace and conflict studies, technology plays a key role for various forms of conflict resolution. According to Reuter et al. (2020), natural science/technical peace research is a broad research field that deals with the role of scientific and technical possibilities in the context of war and peace, armament and disarmament. Technology is based on findings from various natural sciences and technical disciplines such as physics, chemistry, biology, and computer science. Natural science/technical peace research supports the political processes of preventing war, reducing armament and building confidence with technical solutions. This is necessarily based on the inherent ambivalence of technology and the fact that technological developments have changed the dynamics of war and therefore determine the conditions for disarmament and peace processes (cf. Altmann, 2017). Scientists who are aware of potential negative consequences of these technologies are working on technical solutions in order to reduce or even prevent possible damage. Potential examples of approaches include enabling verification (i.e. checking of compliance with disarmament treaties) or the restriction of innovations to peaceful aims (i.e. regulation of intrusion software as dual-use good). The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a good example for this (cf. Reinhold, 2015). Altmann (2019) points out that this research is strongly needed to complement political-scientific peace research.

The emergence of natural science/technical peace research was a consequence of the emergence and spread of nuclear weapons in the East-West conflict since the late 1940s. With the possibility of using nuclear weapons in war, technical innovations also became strategically (war-)relevant. Despite public concerns, deterrence became the choice at the time as the concept of mutually assured destruction (MAD) would imply (Sokolski, 2004). The best-known example for the existing doubts is the "Russell-Einstein Manifesto" from 1955 which calls for nuclear disarmament and the rejection of war in general. The concerns about the dangers posed by nuclear weapons were shared by wider scientific circles. As a consequence of this appeal, the Pugwash Conferences on Science and World Affairs were created. At the first conference in 1957 in Pugwash,

Canada, 22 scientists from ten countries, from both sides of the Iron Curtain, discussed strategies for nuclear disarmament. Ever since, the so-called "Pugwash Movement" has organised workshops and conferences and conducted research on the problems of nuclear weapons. A similar development could also be observed in Germany with the "Declaration of Göttingen" from 1957. Leading physicists and chemists stated their disapproval of the German government's demand for the nuclear armament of the newly founded German Armed Forces. Such activities represented an important basis which enabled and supported subsequent international treaties on arms control (cf. Altmann et al., 2010; Neuneck G., 2011).

Based on such initiatives, scientific research groups were founded at renowned U.S. universities in the 1960s. During the continuous East-West conflict they investigated nuclear disarmament, arms control, proliferation, and international security. In Germany, Carl Friedrich von Weizsäcker established a working group at the Federation of German Scientists and can therefore be seen as the founding father of natural science and technical peace research in the country. Further working groups such as IANUS at TU Darmstadt, were formed in the 1980s and have ever since deepened their institutionalisation. However, it is agreed that the weak structural establishment and support of this area of research is in big contrast to its importance (cf. FONAS, 2015; Wissenschaftsrat, 2019). Only universities in Hamburg and Darmstadt have full professorships with such a denomination. Furthermore, there is an assistant professorship in Aachen and further positions at peace research institutes that often focus mostly on political science peace research.

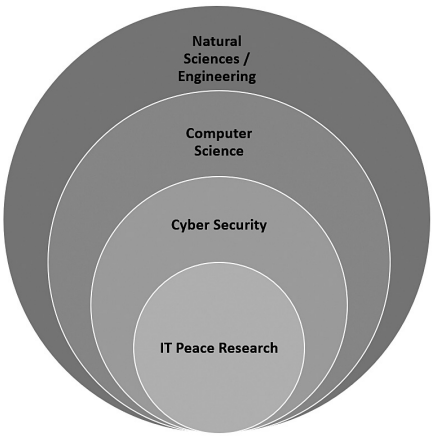
2.3 Computer Science

IT peace research is not only peace research, but also computer science research. Computer science is "the study of computers and the major phenomena that surround them" (Newell, Perlis, & Simon, 1967) or "the systematic study of algorithmic processes that describe and transform information: their theory, analysis, design, efficiency, implementation, and application" (Denning et al., 1989, p. 12).

According to French dictionaries, the origin of the academic use of *Informatique* goes back to 1962, when Dreyfus used the term as an artificial word, consisting of the words "Information" and "*Automatique*" or "*Electronique*". It was understood as the science of the rational processing of information, in particular information by automatic machines (in Coy, 2001, p. 4). This definition assumes that computer science was understood as science even before it became institutionalised. In the German language, the French term was established very quickly, whereby the comprehensive definition was replaced by an American-influenced interpretation. However, automatic machines are still regarded as a central aspect of computer science and computer engineering. Some argue(d) that technical problems and their theoretical-mathematical basics play an important role, whereby economic and social effects are dealt with in other areas. In contrast to the U.S., for example, where computer science and information science are covered under the definition from the *Académie* (and computer engineering is neglected), in Germany computer science is regarded as a link between the understandings of (more theoretical) computer science and (more practical) computer engineering (cf. Coy, 2001).

The following figure (Figure 2) provides an overview of how IT peace research can be classified from a natural sciences/ engineering perspective.

Figure 2: IT Peace Research embedded in Computer Science and Cyber Security



Source: Own illustration

2.4 Cyber Security

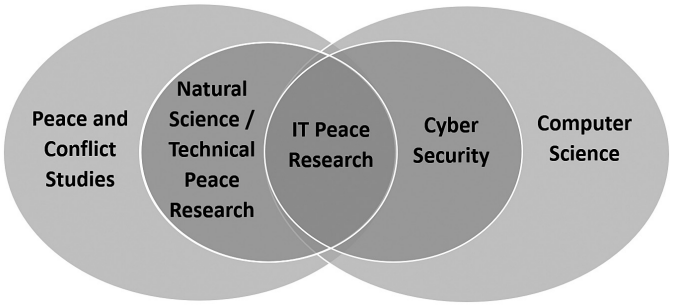
Nowadays, cyber security research can be seen as an important part of computer science, as well as of IT peace research. Initially coming from the Latin word "*securitas*", the term security stands for "without concern". In contrast to the German language, where the word security is only known as "*Sicherheit*", the term can be differentiated between safety and security in English. According to Storey (1996, p.2.), safety can be understood as a protection against unintended events such as natural occurrences or incidents induced through errors or malfunction. Security, on the other hand, means the protection against external or malicious actors like terrorists, perpetrators, or armed forces.

According to ISO/IEC 27001, IT security is defined as "preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved" (ISO, 2013). The term cyber security is often used interchangeably with the term information security. However, as von Solms and van Niekerk (2013, p. 97) state, "cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him- / herself. In information security, reference to the human factor usually relates to the role(s) of humans in the security process."

2.5 IT Peace Research

The above described areas of peace and conflict studies, in particular natural science/technical peace research and computer science, above all cyber security, form the basis for IT peace research (see Figure 3). IT peace research is in particular necessary to restrict the dangers of a cyber arms race and to offer better tools for verification and disarmament (cf. Altmann, 2019).

Figure 3: IT peace research as the intersection of peace and conflict studies and computer science.



Source: Reuter, 2019, p. 24.

The author suggests the following as descriptions:

- Motivated by the relevance of IT for peace and security, **IT peace research** is an interdiciplinary discipline that addresses the role of IT in peace and security from a theoretical, empirical and technical perspective.
- IT peace research is both part of **peace and conflict studies** (especially natural science/technical peace research) as well as of **computer science** (especially cyber security). This is the case because peace and security are either the aim or the object of investigation. Moreover, cyber activities nowadays play a crucial role in war, which is why research on cyber conflicts is becoming increasingly important (cf. Bonacker, 2011). Further, algorithmic processes and IT with reference to security have been important for peace research (Denning et al., 1988; cf. Newell et al., 1967). In summary, IT peace research can be seen as a part of both social and technical research.
- From the **social science perspective**, the aim of the discipline is to (empirically research and) understand the role of IT and computers in peace and security. IT has revolutionised peoples´ lives and has therefore become more important in, for example, organizing protest movements all over the world. Further, IT applications can be used in order to prevent and manage conflicts, crises and disasters.
- From the **technical (natural science/engineering) research perspective**, the aim of the discipline is to design and develop technical possibilities (normative) for preventing war and escalation of cyber conflicts and attacks, avert international security threats and to develop damage control from intergovernmental (and in some cases interpersonal) insecurity. In addition, the discipline helps with the verification in other areas in arms control, such as the processing of big data and satellite images.

3. Research Challenges for IT Peace Research

Cyber attacks often have a transnational component, as the above-mentioned examples of the incident in the German government network and NotPetya show. This is why they are becoming increasingly relevant for IR and international security. In-depth research is necessary in order to find adequate social, political and legal approaches in addition to just technical ones. This type of research has to integrate computer science just as much as approaches from peace and conflict studies and can therefore be described as IT peace research. In the following, some characteristics and exemplary challenges of IT peace research will be outlined.

3.1 Uncertainty regarding Cyber Forces

Challenge 1: Uncertainty about the targets and aims of emerging cyber forces and the probability of targeting civilian infrastructures unintentionally.

One big challenge is the uncertainty, which exists, inter alia, in the recognition of targets, the intentions of cyber attacks and involved key figures. More and more national defence ministries include the cyber domain as a field of its own. For instance, the US Department of Defense defines the cyberspace as an operational domain apart from land, air, water and space (cf. United States Department of Defense, 2011). In 2016, all NATO member states recognised cyberspace as a military domain in order to identify cyber operations as an attack, to adapt to the cyber threat scenarios or to take military actions themselves (cf. NATO, 2016). Furthermore, the NATO decided that cyberspace is an essential domain that needs to be covered by the collective defence strategies and that attacks over cyberspace can invoke the alliance case of Article V of the Charter (cf. NATO, 2019). "The enduring challenge of cyber threats requires that the alliance continuously evaluates whether it is adapting and responding appropriately" (Brent, 2019).

All of this affects military organisational structures: E.g., since 2017, cyber and information space is a separate military organisational area in the German Federal Armed Forces, besides Army, Navy and Air Force, which implements the forces' defensive and offensive capabilities in cyberspace (cf. Bundesministerium der Verteidigung 2016). Often, both capabilities and activities are not obvious, which is why a targeted pursuit and the attribution of the cyber attacks is quite difficult. To date, neither the size of armed forces nor the offensive and defensive distribution of resources can be determined in a targeted manner because many attacks remain hidden and do not occur under a particular, official force. Thus, there are risks of escalation and destabilisation as well as a certain risk that civilian infrastructures could be unintentionally attacked as unintended collateral damage, which could lead to complications or risks for the public sphere. To sum up, we have little information about cyber forces because much of it remains secret and because "normal" hacker groups also carry out cyber attacks without being part of a superior group. This increases the uncertainty between two or more opponents, because the intentions can hardly be gauged.

3.2 Variety of Actors

Challenge 2: Variety of (state and non-state) potential assailants.

A second challenge is the difficult distinction between state and non-state actors, which is not obvious, based on the possibilities of handling cyber weapons – in contrast to nuclear weapons – also by non-state actors. It is also often unclear whether the actors pursue military-strategic or commercial objectives and whether they have no political, but maybe commercial interests maybe on behalf of the private sector or on behalf of a state or group with political intents.

Moreover, cyber activities are more intransparent, since it is more difficult to identify involved actors in the operational domain. The role and responsibilities of state actors in cyber conflicts such as in *defensive* protection procedures need to be strengthened. Further *active* cyber defensive measures (especially counter-attacks) by companies should be forbidden. Offensive operations by non-state actors (e.g. commercial) and the influence of foreign states on democratic processes, such as elections, should be reduced.

3.3 Difficulty of Attribution

Challenge 3: Attribution of security-threatening or even offensive activities.

In order to implement a security strategy, the cyber attack has to be attributed to a person, a state or other unit, such as an organisation. In the case of safety-endangering and offensive-aggressive activities where the perpetrator cannot be identified, it is quite difficult to apply the security strategy in a targeted manner (cf. Rid & Buchanan, 2014). For Wheeler and Larsen (2003, p. 1), attribution is "determining the identity or location of an attacker or an attacker's intermediary". In contrast, Rid and Buchanan (2014, p. 4) state that "attribution is the art of answering a question as old as crime and punishment: who did it?". Despite these different perceptions, the common intent is to identify the attacker responsible for a malicious activity. The process of attribution not only helps to identify the motivation behind an attack but to learn about the technology involved in executing the attack.

The attribution of cyber attacks consists of technical, legal, and political processes. While the methods of attacker allocation have made significant progress in recent years, digital technologies often still do not provide sufficient evidence for the real-world identity of an attacker (cf. Saalbach, 2019). Research distinguishes two types of cyber attribution challenges (cf. Davis et al., 2017). First, there is the challenge of "accessing, interpreting, and comparing technical and other evidence in an effort to reach a high-confidence attribution finding in a timely manner. Second, there is an additional challenge of persuasively communicating an attribution finding to a target audience or the general public" (Davis et al., 2017, p. 9). Related to that, further research on the development of parameters that allow attribution without disturbing the privacy aspect of the entire internet is needed.

3.4 Verification and Transparency in Cyber Space

Challenge 4: Measures for verification need to be adapted to emerging technologies, and rules for transparency need to be established.

Verification is one of the pillars for treaties and regimes that facilitate members or entitled institutions to verify each other's compliance. Originally, verification has been introduced as a tool for weapons systems that have been utilised for military purposes. Now, its usage on cyberspace is impeded by specific features of this new domain. On this basis, new approaches will have to be developed (cf. Reinhold & Reuter, 2019). This includes, for instance possibilities to measure and verify the total power supply, the available supply of cooling systems, available network bandwidth capacities, the number of connections of monitored networks, and the number of required staff as some of the measurable parameters in the cyberspace.

Further research is necessary in order to tackle two existing issues: 1) How can measures be developed or strengthened to prevent the circumvention or manipulation of monitoring? 2) How can verification of cyber arms control itself work adequately? To sum up, all verification measures are used for specific purposes and use cases (cf. Reinhold & Reuter, 2019). For new or emerging technologies, standards and measurement units are needed. These enable control of the particular measurable parameters in cyberspace (cf. ibid). One sub-question is how transparent cyberspace can be and who has to be transparent to whom about what? One possibility would be an independent, international organisation for attribution that possesses secret service reconnaissance tools and could communicate its results reliably (cf. Davis et al., 2017).

As in other military areas, confidence- (and security-) building measures (C(S)BMs) can act as first steps towards creating transparency and reducing misperceptions and suspicions. Concepts for voluntary CBMs have been developed in the United Nations and are being implemented in the Organisation for Security and Cooperation in Europe (OSCE). Such activities should be improved by explicitly including cyber activities of armed forces and making agreements politically binding, as with the OSCE CSBMs for conventional forces (Altmann 2019, p. 185). In spite of existing differences, many actors try to reduce the existing uncertainties on different technical levels.

3.5 Dual-Use of IT

Challenge 5: How can military/civilian and use/misuse be differentiated?

The use of IT in peace, conflict and for security raises some questions, i.e. whether the use of IT can be limited exclusively to so-called beneficial purposes and whether improper use can be prevented. This ambivalence is called a dual-use dilemma, meaning that objects, knowledge and technology can find both useful and harmful applications. Dual-use questions have been addressed in various disciplines, e.g. in nuclear technology, chemistry, and biology. The importance of dual-use differs slightly, depending on the technology and its risks, as well as its distribution and application (cf. Riebe & Reuter, 2019).

Encryption hard- and software can be seen as dual-use products. Since only strong encryption guarantees tap-proof and confidential communication, cryptography plays a key role in security issues (cf. Vella, 2017). Further, the dual-use debate has led to the proliferation of spyware through additions to the Wassenaar Arrangement in 2013 and 2016 (cf. Herr, 2016). Although software dual-use is becoming a constant problem as part of weapons modernisation (cf. Bernhardt & Ruhmann, 2017; Reuter & Kaufhold, 2018), empirical case studies on dual-use IT are lacking (cf. Leng, 2013; Lin, 2016). On the one hand, modern software development is characterised by agile process models such as "Scrum", in which developers can react flexibly to changes in (customer) requirements (cf. Dingsøyr, Nerur, Balijepally, & Moe, 2012). Therefore, it is obvious that dual-use potentials need to be checked not only in the initial planning of software, but also during the programming itself. On the other

hand, the flexibility of using software in different application contexts is the essential challenge for dual-use impact assessment and must fundamentally differ from the situation in the life sciences (cf. Lin, 2016). The aim is both to minimize risks by non-state actors and to anticipate the risk of uncontrolled distribution of malware between states. It needs to be possible to distinguish between civilian and military use and to prevent applications from being misused. This requires a clear line between legitimate and illegitimate deployments and an appropriate reconnaissance and enforcement mechanism (cf. Riebe & Reuter, 2019).

3.6 Proliferation

Challenge 6: A code can hardly be restricted in its distribution or duplication. Furthermore, the dissemination of (dual-use) technologies within and between countries is proving to be a challenge.

It is extremely difficult to stop or restrict the distribution or duplication of codes. Furthermore, the spread of (dual-use) technologies within and across countries increases the risk of military actions as a tool of preventive action. Assessments like the cyber security index from 2013 (cf. UNIDIR, 2013) solely represent the first step towards binding regulations that restrict, reduce or even forbid the development, dissemination and use of offensive cyber tools for military purposes. Not only does the political will of a state count, there are numerous technical questions that must be analysed in order to develop solutions for existing challenges. IT peace research can help in finding relevant solution strategies. Measures need to be developed that make it possible to monitor compliance with contractual partners, practically monitor military installations or track cyber weapon components such as software vulnerability attacks. As the history of arms control shows, it is a long way to go but an indispensable step towards peaceful development of a global domain (cf. Reuter, Aal, et al., 2019).

3.7 Laws

Challenge 7: The permanent adaption of international and national laws to new technologies seems to be a challenge; e.g. there is no agreement on the technological artefacts of cyber weapons, their quality and quantity that should be monitored.

An existing challenge is the adaption and implementation of (inter-)national laws in the sector of new technologies. So far, there is still no universally valid definition of the term "cyber weapon" and it remains unclear how they can be characterised. Thus, an unhindered upgrading is possible, like with many other weapons as well, but with cyber weapons even easier (cf. Reinhold & Reuter, 2020). Therefore, a control of cyber weapons in quality and quantity turns out to be challenging (cf. Rid & McBurney, 2012). Currently existing approaches to classify and define cyber weapons are mostly user-driven or actor-centred. Furthermore, they focus on the purpose and the application of vicious IT tools. Although all these terms such as "cyber weapon" are unclear, they are currently used for political arrangements, formulating norms for state behaviour and entering into documents (cf. Reuter & Reinhold, 2020). The aforementioned terms are therefore not capable to define and limit the subset of potential cyber weapons within the broad spectrum of malware prior to deployment. Essentially, this poses the most important challenge for the restriction and monitoring of particular military cyber technologies and their evolution, and for a limitation of inventory on cyber weapons. This aims to slow down and reduce the current militarisation of cyberspace.

Regarding espionage, there is uncertainty, too. Some scholars argue "that cyber espionage is more intrusive than traditional espionage, because it allows adversaries to repeatedly exfiltrate large amounts of information clandestinely", and it therefore "should be treated as (threat of) use of force or as an armed attack under the United Nations Charter in some situations" (Melnitzky 2012, p. 537), while other scholars "have suggested to create new laws to govern cyber espionage in particular" (in Herrmann, 2019, p. 85). As discussed, attribution and verification continue to pose problems, although they are indispensable for the enforcement of international law. Cyber defence faces legal dilemmas, not least because of lack of norms regarding pre-emption, prevention and counter-operations.

4. Discussion and Conclusion

This article highlights that information technology has a significant influence on warfare and military strategies (cf. Reuter, Riebe, Aldehoff, Kaufhold, & Reinhold, 2019). This makes clear that IT peace research should be expanded in the future. On the one hand, military forces are increasingly relying on cyberspace, creating capacities for offensive action in this domain and even, as in the case of the U.S., placing it in the centre of prospective warfare. On the other hand, there are still no adequate answers for the international regulation of cyber conflicts and the current dynamics of armament. This circumstance is owed to the permanent ambiguity in cyberspace, concerning its actors and the operations carried out: There are neither dividing lines between internal and external security nor can it be clearly determined which cyber resources can be assigned to defensive or offensive purposes. Even though espionage and even cyber attacks are regularly not seen as an act of war, some cyber incidents might cause serious tensions between two or more actors. According to Rid (2013) "cyber war will not take place" – for him, cyber war is a mythos, because war contains targeted violence against people, which has not existed in previous digital attacks. Nevertheless, the number of cyber attacks is constantly increasing worldwide. The particularities of cyberspace in the context of peace and security make it necessary to consider espionage and attacks separately in order to satisfy the complexity and ambiguity of the field.

This article suggested a definition of IT peace research, which might be considered as a (sub-)discipline, a field of research or an interdisciplinary research area. It is based on peace and conflict studies as well as computer science; furthermore, it is inspired by many other disciplines nearby. Central challenges, that have been elaborated in this article, include the insecurity, the variety of actors, the difficulty of attribution, verification and transparency, dual use, proliferation, and laws. Now, further steps and research are necessary in order to address at least some of them soon. To achieve this, a strong connection to both communities, peace and conflict research, as well as computer science is

needed, in order to combine the state of the art of both disciplines as a strong basis, and then to combine methods and research approaches from both areas to solve the complex problems at hand. Interdisciplinary research making contributions to the challenges described in this article, but also contributions to the individual disciplines, have to be fostered.

Christian Reuter is Full Professor for Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at the Technische Universität Darmstadt with a secondary appointment in the Department of History and Social Sciences. His research focuses on interactive and collaborative technologies in the context of crises, security, safety, and peace.

5. Bibliography

Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2018). Comprehensive survey on petya ransomware attack. *Proceedings – 2017 International Conference on Next Generation Computing and Information Systems, ICNGCIS 2017*, 131–136. https://doi.org/10.1109/ICNGCIS.2017.30.

Altmann, J. (2017). Einführung. In J. Altmann, U. Bernhardt, K. Nixdorff, I. Ruhmann, & D. Wöhrle (Eds.), *Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung* (pp. 1–7). Wiesbaden: Springer VS.

Altmann, J. (2019). Natural-Science/Technical Peace Research. In C. Reuter (Ed.), *Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace* (pp. 39–60). Wiesbaden: Springer.

Altmann, J., Kalinowski, M., Kronfeld-Goharani, U., Liebert, W., & Neuneck, G. (2010). Naturwissenschaft, Krieg und Frieden. In P. Schlotter & S. Wisotzki (Eds.), *Friedens- und Konfliktforschung* (pp. 410–445). Baden-Baden: Nomos.

Bernhardt, U., & Ruhmann, I. (2017). Informatik. In P. Imbusch & R. Zoll (Eds.), *Naturwissenschaft – Rüstung – Frieden* (pp. 337–448). https://doi.org/10.1007/978-3-658-01974-7.

Bundesministerium der Verteidigung (2016). *Abschlussbericht Aufbaustab Cyber- und Informationsraum*. Berlin, Germany.

Bonacker, T. (2011). Forschung für oder Forschung über den Frieden? Zum Selbstverständnis der Friedens- und Konfliktforschung. In P. Schlotter & S. Wisotzki (Eds.), *Friedens- und Konfliktforschung* (pp. 46–78). Baden-Baden: Nomos.

Boulding, K. E. (1963). Towards a pure theory of threat systems. *The American Economic Review*, *53*(2), pp. 424–434.

Brent, L. (2019). *NATO's role in cyberspace*. Retrieved from https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

Brinkel, G. (2018). *7 Stimmen zur Digital Geneva Convention*. Retrieved from https://www.microsoft.com/de-de/berlin/artikel/7-stimmen-zur-digital-geneva-convention.aspx.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Coy, W. (2001). Was ist Informatik? In *Das ist Informatik* (pp. 1–22). Berlin, Heidelberg: Springer.

Davis, J. S. I., Boudreaux, B., Welburn, J. W., Ogletree, C., McGovern, G., & Chase, M. S. (2017). *Stateless Attribution: Toward International Accountability in Cyberspace*.

Denning, P. J., Comer, D. E., Gries, D., Mulder, M. C., Tucker, A., Turner, A. J. O. E., & Young, P. R. (1989). *Computing as a discipline*. *32*(I), 9–23.

Denning, P. J., Comer, D. E., Gries, D., Mulder, M. C., Tucker, A., Turner, A. J., & Young, P. R. (1988). *Report of the ACM task force on the core of Computer Science*.

Dingsøyr, T., Nerur, S., Balijepally, V., & Moe, N. B. (2012). A decade of agile methodologies: Towards explaining agile software development. *Journal of Systems and Software*, *85*(6), pp. 1213–1221. https://doi.org/10.1016/j.jss.2012.02.033.

FONAS. (2015). Forschungsmemorandum – Naturwissenschaftliche Friedensforschung in Deutschland – Eine neue Förderinitiative ist dringend nötig. Dortmund, Forschungsverbund Naturwissenschaft, Abrüstung und internationale Sicherheit e.V.

Gleditsch, N. P., Nordkvelle, J., & Strand, H. (2014). Peace research – Just the study of war? *Journal of Peace Research*, *51*(2), pp. 145–158. https://doi.org/10.1177/0022343313514074.

Herr, T. (2016). Malware counter-proliferation and the Wassenaar Arrangement. *International Conference on Cyber Conflict, CYCON*, *2016-Augus*, pp. 175–190. https://doi.org/10.1109/CYCON.2016.7529434.

Herrmann, D. (2019). Cyber Espionage and Cyber Defence. In *Information Technology for Peace and Security* (pp. 83–106). Wiesbaden: Springer vieweg.

ISO. (2013). *ISO/IEC 27001: 2013: Information Technology-Security Techniques--Information Security Management Systems--Requirements*. Retrieved from https://www.iso.org/standard/54534.html.

Koppe, K. (2006). Zur Geschichte der Friedens- und Konfliktforschung im 20. Jahrhundert. In P. Imbusch & R. Zoll (Eds.), *Friedens- und Konfliktforschung. Eine Einführung* (pp. 17–66). Wiesbaden: VS Verlag für Sozialwissenschaften.

Leng, C. (2013). *Die dunkle Seite: Informatik als Dual-Use-Technologie*. Berkeley.

Lin, H. (2016). Governance of Information Technology and Cyber Weapons. In E. D. Harris (Ed.), *Governance of Dual-Use Technologies: Theorie and Practice* (pp. 112–157). American Academy of Arts & Sciences.

Melnitzky, A. (2012). *Defending America against Cyber Espionage Through the Use of Active Defenses*. 20 Cardozo J. Int'l and Comp. L.,

NATO. (2016). *Warsaw Summit Communiqué*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NATO. (2019). Collective defence – Article 5. Retrieved from https://www.nato.int/cps/en/natohq/topics_110496.htm

Neuneck G. (2011). Frieden und Naturwissenschaft. In B. Rinke & H.J. Gießmann (Ed.), *Handbuch Frieden*. Wiesbaden, VS Verlag für Sozialwissenschaften.

Kanno-Youngs, Z. & Perlroth, N. (2020). Iran´s Military Response May Be ´Concluded´, but Cyberwarfare *Threat Grown*. Retrieved from https://www.nytimes.com/2020/01/08/us/politics/iran-attack-cyber.html.

Newell, A., Perlis, A. J., & Simon, H. A. (1967). Computer science. *Science*, *157*(3795), 1373–1374.

Reinhold, T. (2015). Möglichkeiten und Grenzen zur Bestimmung von Cyberwaffen. In: Cunningham, D. W., Hofstedt, P., Meer, K. & Schmitt, I. (Hrsg.), INFORMATIK 2015. Bonn: Gesellschaft für Informatik e.V. (pp.587-596).

Reinhold, T. (2018). Hack der deutschen Regierungsnetze. Retrieved from Datenbank Relevante Cybervorfälle website: https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/hack-der-deutschen-regierungsnetze/.

Reinhold, T., & Reuter, C. (2019). Verification in Cyberspace. In C. Reuter (Ed.), *Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden, Germany: Springer Vieweg.

Restivo, S., & Denton, P. H. (2008). *Battleground Science and Technology*. California: Greenwood Press.

Reuter, C., Altmann, J., Göttsche, M., Himmel, M. (2020). Zur naturwissenschaftlich-technischen Friedens- und Konfliktforschung: Aktuelle Herausforderungen und Bewertung der Empfehlungen des Wissenschaftsrats. ZeFko, 9(1), 2020.

Reuter, C. (2019). Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden, Germany: Springer Vieweg. https://link.springer.com/book/10.1007/978-3-658-25652-4

Reuter, C., Aal, K., Aldehoff, L., Altmann, J., Bernhardt, U., Buchmann, J., Katzenbeisser, S., Kaufhold, M.-A., Nordmann, A., Reionhold, T., Riebe, T., Ripper, A., Ruhmann, I., Saalbach, K.-P., Schörnig, N., Sunyaev, A., Wulf, V. (2019). The Future of IT in Peace and Security. In *Information Technology for Peace and Security* (pp. 405–413). Springer.

Reuter, C., Aldehoff, L., Riebe, T., & Kaufhold, M.-A. (2019). IT in Peace, Conflict, and Security Research. In C. Reuter (Ed.), *Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden, Germany: Springer Vieweg.

Reuter, C., & Kaufhold, M.-A. (2018). Informatik für Frieden und Sicherheit. In C. Reuter (Ed.), *Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement* (pp. 577–597). Wiesbaden: Springer Vieweg.

Reuter, C., & Reinhold, T. (2020). On the nature of cyber weapons. In *Information Technology for Peace and Security*. Wiesbaden, Germany: Springer Vieweg.

Reuter, C., Riebe, T., Aldehoff, L., Kaufhold, M.-A., & Reinhold, T. (2019). Cyberwar zwischen Fiktion und Realität – technologische Möglichkeiten. In I.-J. Werkner & N. Schörnig (Eds.), *Cyberwar – die Digitalisierung der Kriegsführung* (pp. 15–38). https://doi.org/10.1007/978-3-658-27713-0.

Rid, T., & Buchanan, B. (2014). Attributing Cyber Attacks. *The Journal of Strategic Studies*, *38*(1–2), pp. 4–37. https://doi.org/10.1080/01402390.2014.977382.

Rid, Thomas (2013). Cyber war will not take place, Oxford University Press.

Rid, T., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal*, *157*(1), pp. 6–13. https://doi.org/10.1080/03071847.2012.664354.

Riebe, T., & Reuter, C. (2019). Dual Use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In C. Reuter (Ed.), *Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace* (p. 165-184). Wiesbaden, Germany: Springer Vieweg.

Saalbach, K.-P. (2019). Attribution of Cyber Attacks. In *Information Technology for Peace and Security* (pp. 279–303). Wiesbaden: Springer Vieweg.

Sokolski, H. D. (2004). Getting Mad: Nuclear Mutual Assured Destruction, Its Origins and Practice. In *Strategic Studies Institute*.

Storey, N. (1996). *Safety Critical Computer Systems*. London: Addison-Wesley Longman.

Thee, M. (1988). Science and Technology for War and Peace. *Bulletin of Peace Proposals*, *19*.

UNIDIR. (2013). *The Cyber Index – International Security Trends and Realities 2013*. Geneva: United Nations Institute for Disarmament Research (UNIDIR).

United States Department of Defense (2011). *Strategy for Operating in Cyberspace*. Retrieved from https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Vella, V. (2017). Is There a Common Understanding of Dual-Use ?: The Case of Cryptography. *Strategic Trade Review*, *3*(4), pp. 103–122.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, pp. 97–102. https://doi.org/10.1016/j.cose.2013.04.004.

Wheeler, D. A., & Larsen, G. N. (2003). *Techniques for Cyber Attack Attribution*. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf.

Wissenschaftsrat. (2019). *Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung, (Drs. 7827-19)*. pp.1–178. Retrieved from https://www.wissenschaftsrat.de/download/2019/7827-19.html.