Teaching Peace Informatics: Reflections from Lectures and Exercises

21

Christian Reuter, Thea Riebe, Jasmin Haunschild, Thomas Reinhold and Stefka Schmid

Abstract

Conflicts in cyberspace do not longer constitute a fictional scenario of the future. To gain a better understanding of how such conflicts are carried out, interdisciplinary research and teaching building on both computer science and peace and security studies is indispensable. Even though numerous established courses and textbooks exist in some disciplines, this does not apply to their intersection. This chapter (This chapter has been published as a paper (in German): Reuter et al. (2022)) reflects on the introduction of the interdisciplinary course "*Information Technology for Peace and Security*" for students of Computer Science, IT Security and Information Systems at the Technical University of Darmstadt and Peace and Conflict Research at the TU Darmstadt in cooperation with Goethe University Frankfurt. The challenges and solutions of interdisciplinary teaching are presented while the importance of this type of teaching is assessed.

C. Reuter (✉) · T. Riebe · J. Haunschild · T. Reinhold · S. Schmid
Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt, Darmstadt, Germany
e-mail: reuter@peasec.tu-darmstadt.de

T. Riebe
e-mail: riebe@peasec.tu-darmstadt.de

J. Haunschild
e-mail: haunschild@peasec.de

T. Reinhold
e-mail: reinhold@peasec.de
S. Schmid e-mail: schmid@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_21

Objectives

- Gaining an overview of promising teaching methods and best practices in interdisciplinary teaching and their evaluation.
- Fostering a collaborative learning environment that encourages students of computer science and peace and security studies to engage in joint research projects.
- Equipping educators with the capability to facilitate the synthesis of diverse academic disciplines; enabling students to cultivate a holistic understanding of phenomena.

21.1 Introduction: Interdisciplinary Research and Teaching Between Technology and Peace

Political conflicts conducted in cyberspace are gaining increasing significance, presenting a complex empirical challenge for peace and conflict research. The first cyber attacks in the context of armed conflicts occurred approximately 15 years ago (Reinhold & Reuter, 2019): In 2007, the Israeli military is believed to have sabotaged Syrian air defence systems, and, in Estonia, servers were reportedly attacked and temporarily disabled, possibly by pro-Kremlin activists from Russia. Targeted hacking attacks and DDoS attacks, which disrupt internet services through deliberate overloads (e.g. using bots), were observed in the Georgia War in 2008 and during the annexation of Crimea in 2014. Furthermore, German government systems also fell victim to targeted, presumably state-sponsored cyber attacks in 2015 and 2017. Further, the Russian invasion of Ukraine in 2022 highlights that cyber attacks are increasingly being used as preparations for physical attacks and as a disruption tactic against adversaries, potentially affecting international cooperation as other state actors increasingly view cyber attacks as equivalent to physical acts of war (see, e.g. The White House, 2022).

The diverse ways in which digital technologies are used to support new (digital) military attacks, often involving old strategies with new means, have so far been discussed either in peace and conflict research or in computer science. Building on disciplinary perspectives, research analyses have remained selective: On the one hand, discussions have primarily revolved around arms control and the concept of cyber wars (Werkner & Schörnig, 2019). On the other hand, research has focused on classifying different attacks and forensic attribution capabilities (Nisioti et al., 2018). To strengthen an interdisciplinary perspective that integrates peace-related and technical aspects, the field of scientific and technical peace research (Altmann et al., 2017) has been focusing on conflict dynamics and cooperation potential, particularly regarding state-sponsored activities in cyberspace. Through interdisciplinary collaboration, valuable knowledge about threat scenarios and technological capabilities can be integrated into increasingly pressing peace efforts.

Likewise, teaching frequently occurs within disciplinary silos, which is why a comprehensive compilation of relevant concepts and themes that is equally understandable

for students from various disciplines can make a significant contribution. In the following, we consider the course "*Information Technology for Peace and Security*" as an example of an interdisciplinary course in terms of subject matter and audience. This highlights potentials that need further exploration but also draws attention to the limitations that practical implementation of interdisciplinary exchange entails. It has been offered since the winter semester of 2018/2019 as an integrated course with lecture and tutorial components (exercise), totalling four hours per week every other semester. The thematic exploration of cyber warfare, conflicts, and peace from an interdisciplinary perspective is still relatively uncommon in teaching and provides the participating students with access to mutually complementary knowledge.

While there are already numerous established textbooks in the fields of peace and conflict studies (Gießmann & Rinke, 2019; Imbusch & Zoll, 2010; Schlotter & Wisotzki, 2011; Werkner, 2020) and computer science with its diverse subfields such as cyber security (Rashid et al., 2021), human–computer interaction (Dix et al., 2013) or computer science and society (Quinn, 2018), there are only a few publications that address the intersection of computer science and peace and security research. We have perceived this as a gap, especially considering the significance of the entire field of scientific and technical peace research (Altmann et al., 2017), which, precariously, is now represented in Germany by very few professorships (Reuter et al., 2020), and in terms of the importance of peace informatics as a field of study.

The interdisciplinary orientation, reflected in research literature and offered courses, was institutionalised in 2017 with the establishment of the Chair of Science and Technology for Peace and Security (PEASEC) at the TU Darmstadt. Here, computer science is combined with peace and security research, with a primary affiliation in the Department of Computer Science and a secondary affiliation in the Department of Social Sciences and History. Within the intersection of disciplines such as cyber security and privacy, peace and conflict studies, and human–computer interaction, PEASEC addresses fundamental questions related to peace and war in cyberspace and arms control (Reinhold & Reuter, 2022), dual-use challenges in computer science (Riebe et al., 2021), as well as peace-promoting, security-enhancing, and conflictual interactions on social media (Reuter & Kaufhold, 2018). These topics are covered through the teaching activities of the chair in both, the Department of Computer Science, especially in the bachelor and master programs in computer science, IT security, and business informatics (all integrated as elective modules) as well as in the Department of Social Sciences and History, particularly in the master program in International Studies/Peace and Conflict Research. In general, attendance in the course is open to all those interested in choosing the interdisciplinary study focus of Science and Technology Studies at TU Darmstadt. This contribution introduces the course and discusses the challenges of an interdisciplinary course with a highly diverse audience, as well as best practices from the teaching activities.

21.2 The Course: Information Technology for Peace and Security

In the following, we will initially reflect on our experiences with the course "*Information Technology for Peace and Security*" during the four winter semesters from 2018/2019 to 2021/2022. We will begin by presenting the concept of the lecture and exercise offered on a weekly basis, alternating between them, with a total duration of approximately three hours per week. We will also discuss the digital teaching activities during the COVID-19 pandemic as well as the results and evaluations of the courses. Finally, we will delve into identified challenges and key observations.

21.2.1 Course Concept: Preparation and Knowledge Transfer

Based on the experiences gained from our 2018 published textbook, "*Security-Critical Human–Computer Interaction: Interactive Technologies and Social Media in Crisis and Security Management*" (Reuter, 2018), the textbook "*Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*" (Reuter, 2019) was developed in 2019 as a fundamental introduction to issues and perspectives on the intersections of computer science and peace and conflict studies. This textbook delves into conflicts, war, and peace in cyberspace, cyber arms control, cyber attribution, and infrastructures as well as culture and interaction before providing a final outlook. The introductory course structure closely follows the book's organisation. By involving authors from various disciplines (e.g. security studies or cyber security) and subsequent reflection on the presented contributions, an inherently interdisciplinary foundation was established. Starting with the introduction of more abstract political science concepts and theoretical frameworks (e.g. war, conflict, security dilemma), the textbook gradually leads to a further concretisation of conflictual and cooperative scenarios by illustrating socio-technical issues and possibilities. This allows for bridging the gap between the scientific aim of better understanding (e.g. what are the different dimensions of violence that can prevail?) and problem-solving-oriented thinking (e.g. how can systematically defence mechanisms against cyber attacks be developed?). These concerns are not always strictly separated in their approach. For instance, arms control measures, including the development of technical tools, are discussed in the context of analysing state behaviour in international relations. Additionally, interpreting the darknet as a security concern for computer scientists provides the opportunity to comprehend various attribution (and law enforcement) efforts as embedded in a political context.

While students in the social sciences tend to be familiar with handling these fundamental concepts, technical background knowledge helps computer science students in transferring peace-related questions to empirical cases of IT use in the context of peace and security. Concluding questions at appropriate points in each chapter allow for the recapitulation of newly acquired knowledge. The lecture and exercises are also oriented

towards this iterative approach, which places the (self-)examination of what has been learned at the forefront. Furthermore, to create a common learning space, practices from the respective disciplinary cultures were adopted, so that familiar procedures can provide a reference framework for the communication of an unfamiliar subject matter to student groups. For example, the orientation toward the textbook is familiar to students in peace and conflict studies, while the required foundational reading often represents a new routine for computer science students. Likewise, the applied orientation of the course, which includes exercises focused on concrete case studies of socio-technical interaction, is a largely unfamiliar field for students in the social sciences.

21.2.2 Lecture for Knowledge Transfer and Discussion of Topics

The lecture, which was offered alternately with the exercise on a weekly basis, is divided into seven parts. In Part I: Introduction and Fundamentals, an introduction to scientific and technical peace research, especially IT in peace, conflict, and security research, is provided. Part II deals with cyber conflicts and warfare, including components such as information warfare, cyber espionage, and cyber attacks, as well as Darknets as instruments of cyber warfare. Part III, Cyber Peace, aims to outline the transition from cyber warfare to cyber peace, dual-use and dilemmas in cyber security, and trust- and security-building measures. Part IV, Cyber Arms Control, addresses arms control, its applicability, and new concepts for cyber weapons, unmanned systems, and cyber verification. Part V: Cyber Attribution and Infrastructures focuses on the attribution of cyber attacks, as well as resilient and secure critical infrastructures. Part VI: Social Interaction addresses the division of safety and security, cultural violence, as well as the use of social media and information and communication technology in crisis areas. Part VII: Outlook ventures into a prognosis for the future of IT in peace and security.

For the second edition of the book the parts have been restructured: Part I: Introduction and Fundamentals, Part II: Cyber Conflicts and War, Part III: Cyber Peace, Part IV: Cyber Arms Control, Part V: Cyber Infrastructures, Part VI: Artificial Intelligence, Part VII: ICT in Peace and Conflict, Part VIII: Outlook. Part V and Part VI are combined in one lecture.

The lecture, attended by 50 to 150 students, included the transfer of content oriented towards the textbook but often also involved active discussions with students. While verbal discussions worked excellently during in-person semesters, with either computer science students (contributing more to technical aspects) or peace and conflict studies students (contributing to security policy aspects) making valuable contributions depending on the question, this changed somewhat during the COVID-19 pandemic. In the live online lecture, there was greater reluctance towards verbal discussion, so regular quizzes or open questions for chat-based responses supplemented the discussion.

Video recordings of live events are bundled with learning materials from exercises and external events in the Moodle course, and communication with students is

channelled. In addition, further (non-exam-relevant) materials are provided via the university's E-Learning platform. These materials include lectures or interviews in which experts discuss their research in a practical context. Students could access relevant information and explore further topics, emphasising the exploratory nature of interdisciplinary debate. The topicality of the subject of IT in the context of war and peace also came to the fore in spontaneous additional events related to the Russian invasion of Ukraine. Here, open, extraordinary information and discussion events were offered via Zoom, allowing participants to discuss relevant developments and reflect on their role as (future) peace and conflict researchers or computer scientists.

21.2.3 Exercise for Application, Group Work, and Presentation

The focus of the exercise was on the application and discussion of content, including the assessment of empirical cases and the merit of various concepts. As is common in computer science, accompanying exercises are offered for many lectures. In addition to the recapitulative questions from the textbook, questions were developed for students to prepare and present in the exercise. These questions are designed to address current debates, introduce important organisations in technical peace and conflict research, and explore significant historical cases. Tasks included, for example: "What is meant by the militarisation of cyberspace and what societal and international risks arise from it? Explain using a real example" or "Describe the differences between the 'walled fortress' and 'defence in depth' approaches and explain their respective relationship with resilience." This does not involve the application of programming skills but is primarily about the classification of different cyber activities, which is intended to provide insights into conflict dynamics in terms of costs, complexity, and invasiveness.

During the pandemic, new tasks were developed, which were worked collaboratively in breakout rooms for about 60–80 min during the exercise. Afterwards, two groups presented their results, which were then discussed and complemented in the plenum. At the beginning of the exercise, past content is recapitulated with a quiz. This serves to promote active participation and self-assessment of all students, both in-person and online. Simultaneously, the recapitulation serves as a reminder of course syllabus, and thus can be used as a transition from issues of the proceeding session to current session topics. In addition to consolidating knowledge from the lecture, the exercise is intended to teach its application to current and real cases and to identify important relationships among different issues. A central learning outcome is to identify how the use of new technologies changes peace and conflicts, but also how, in certain scenarios, they represent an extension of long-used strategies and developments and therefore serve as a means for a political purpose. Another goal is to consider challenges and potentials for peace-promoting measures in a differentiated manner, and despite all adversities, to develop constructive approaches and provide examples of successful regulation and trust-building between

states based on historical cases. Engaging with the role of technology in national and international security policy helps students critically reflect on their role in future activities. International organisations and career fields are also introduced (e.g. the NGO ICT-4Peace or working with **Computer Emergency Response Teams** (CERT)), opening perspectives for professional fields that are committed to peace and security.

While concepts like hybrid wars or traditional International Relations theories are usually completely new to computer science students, course participants from peace and conflict studies gain, for example, new insights when it comes to the technical implementation of attacks and their prevention. Students from various disciplines often choose exercise questions that correspond to their knowledge, allowing them to act as experts to students from other disciplines. This leads to both a greater understanding and greater appreciation of the other discipline.

21.2.4 Assessment

The learning objectives of the course are assessed through a written examination. The focus here is on discussing the content based on several case study-like tasks from various topic areas and categorising them, using technical terminology and referencing real historical cases, agreements, or technical methods. This corresponds to the task of the exercise, which specifically works towards the learning objectives and prepares for the exam. To encourage active participation during the semester, there is the opportunity to receive an exam bonus. This is achieved by presenting a task solution in the plenum twice. In in-person semesters, tasks were mainly worked on and presented individually, while answers in online semesters were worked on and presented by the entire group. Groups were initially drawn to promote active work in all small groups and enable social interaction. Throughout the semester, groups that had not yet presented were given preference. The PowerPoint slides prepared were commented on by the instructors and made available online. Bonus points can also be earned by creating a quiz with review questions on the most important content from the previous session or by providing a presentation on a non-exam-relevant topic as a video in Moodle. Depending on the program of study, students could earn 6 (for computer science programs) or 3 or 8 ECTS (peace and conflict studies, with or without module final exam) in the course.

21.3 Evaluation and Reflection

The course was evaluated each semester using standardised evaluation forms for courses at the TU Darmstadt (EvaSys), which provide insights from the students' perspective (NL = 87, NE = 98). Overall, the course was rated very good to good in its entirety (Overall grade Lecture = 1.67–1.89, average grade for the instructor: 1.2–1.47; Overall

grade E = 1.88–2.23). In addition to the "substantive discussion", the "pleasant and respectful atmosphere," and the encouragement to participate, the repetition of content was considered positive: through the "combination of the book, lecture, and exercise […] you automatically repeat it three times and retain it immediately". The digital teaching format was also addressed: "The lecture in digital form is very successful, enjoyable, and highly encourages one to engage more with the topic" and "I really liked the many surveys", and it is "a shining example of the use of digital teaching resources". The combination of various tools was also highlighted: "In the lecture, various digital tools were used sensibly to liven up the course and engage the students".

Some responses address the interdisciplinary nature of the course: The content is "made understandable even for those who do not have/need technical backgrounds in their study program." In this regard, the course's objective is achieved. However, computer science students often note over the years that it is the first course where there is no "right or wrong". This indicates a learning effect that encompasses a broadening of perspectives regarding different scientific and real-world approaches. At the same time, due to its introductory nature, it was usually not entirely possible to convey that there are different understandings of truth even within the humanities and social sciences and that the claim of a systematic approach can be common to various disciplines regardless of the specific method and research subject. Some students also wished for a "lesser societal and greater technical focus", although this aspect was certainly more or less pronounced depending on the study background and personal interests. It was also noted that it is "almost impossible to follow the lecture if you haven't read the book beforehand", which puts emphasis on the importance of pre-required reading. Handling English literature is also less practiced in computer science. Perhaps for this reason, the use of the English language in the textbook is suggested as a potential change in a lecture held in German. Students of International Studies/Peace and Conflict Research, based on the regular consumption of required readings, tended to be more experienced in preparing for the exam and answering essay questions. At the same time, it was also about reducing resistance to technical topics ("please […] less cyber"). This can often be countered with a pleasant learning atmosphere that allows students to ask questions ("helpful", "attention to students").

Open-text responses provide insights into the students' motives for participating in the course. One person emphasised: "The topic of the lecture is very important and is unfortunately neglected in computer science studies". Interest in dealing with political conditions was evident in the last digitally conducted reflection round, especially regarding the military use of IT and cyber espionage in the context of international relations. In addition, computer science students showed interest in updating theoretical concepts with reference to empirical objects in cyberspace. Awareness of current societal conflicts was also heightened, which students considered important in their role as future computer scientists.

21.4 Conclusion: Core Observations

In conclusion, based on four iterations of the course, including evaluations, four core observations can be made. Focused on a problem-solving-oriented science, we first recognise a high empirical relevance of engaging from the perspective of scientific and technical peace and conflict research, which is also reflected in university teaching (see (1) Peace and Security Policy Necessity). In terms of the systematic processing of the topic areas, the course reveals limitations of the scientific environment and attempts to capture potential for research in this context (see (2) Disciplinary Boundaries of Natural, Engineering, or Social Sciences, (3) Complementary Knowledge and Competence Acquisition). This leads to the question of the substantial gain that results from the interdisciplinary approach, especially concerning changing real-world phenomena (see (4) Concept Transfer and Sustainable Applicability).

21.4.1 Peace and Security Policy Necessity

Events such as the invasion of Ukraine in 2022 highlight the importance of well-founded knowledge in peace and conflict research, but especially in scientific and technical peace research with connections to physics, biology, chemistry, computer science, electrical engineering, mechanical engineering, and other technical disciplines, for the critical assessment of technologies in conflicts. This underscores the urgent recommendation of the *Wissenschaftsrat* (German Council of Science and Humanities) to strengthen this field even further (Wissenschaftsrat, 2019). For aspiring peace and conflict researchers, such a course allows them to connect with relevant subject matters or evaluate theoretical debates regarding their impact. For computer science students, who will play a significant role in shaping the future, the course provides a meaningful space for reflection on the societal impacts of IT, which can also be incorporated into the design of artifacts. Feedback from technical disciplines clearly indicates a continued need to inform and mobilise students, helping them understand technology as an integral part of societies and shapers of societal processes. Reflecting on the social, ethical, and, in this case, security-policy consequences of technical products and processes and one's own involvement in them is an ongoing necessity in technical fields. At the same time, discussions with students have shown that the approach of communicating not only personal responsibility but also opportunities to shape realities through technical skills is well-received and often met with great enthusiasm.

21.4.2 Disciplinary Boundaries of Natural, Engineering, or Social Sciences

In an interdisciplinary event like this, depending on the topic and audience's interdisciplinary nature, there is always the risk that it may be perceived as too technical or

too social science-oriented. It has been essential for us to break down potential barriers or obstacles to attending this event (e.g. "I have no knowledge of computer science; can I still participate?") and encourage everyone to contribute. Furthermore, seminars, research internships, or thesis work building on this foundation offer opportunities for targeted deepening. The integration of familiar practices from the involved study programs provides reference points that facilitate engagement with the subject matter. The diverse teaching formats (lecture, exercise, book, e-learning) also facilitate accessibility for students with different routines and learning competencies. Maintaining social interaction, even in times of digital teaching, is essential for substantive discussions on topics where not everyone always feels "at home", and an iterative nature of the course can provide additional security. As specialisation in specific areas occurs within the respective disciplines during study, the lack of focus on areas that require disciplinary background knowledge is not always positive. In interdisciplinary courses, it is therefore important to make sensible use of the different scientific cultures and to promote an open culture of error to initiate dialogue.

21.4.3 Complementary Knowledge and Competence Acquisition

It is relatively likely that students from different study programs need to learn different things. While for some, concepts like DDoS attacks, encryption algorithms, vulnerabilities, exploits, and backdoors are already technically comprehensible, others may have extensive knowledge of the concepts of positive and negative peace, securitisation, or the mechanisms of arms control or verification. Through well-balanced questions, disciplines get the opportunity to act as experts at different times. At the same time, differences between disciplines must also be addressed: the argumentative retrieval of knowledge must already be conveyed in a suitable teaching format, such as the exercise, to ensure equal chances of successful completion in an exam that assesses such skills. In the exercise, the different backgrounds are harnessed for complementary learning, while in the exam, specialisations no longer play a role. Thus, the focus is on transferring a knowledge base that is accessible to all to address problem scenarios.

21.4.4 Concept Transfer and Sustainable Applicability

In addition to the existing textbook on scientific and technical peace research as a whole (Altmann et al., 2017), the transferability of concepts was actively promoted through textbooks such as "*Information Technology for Peace and Security*" (Reuter, 2019). It is worth noting that due to the dynamic nature of technological advancements, further editions are necessary. This is because the knowledge and classifications presented can quickly become outdated if not updated. However, interdisciplinary focus on IT and peace is not about presenting a series of diverse and sometimes (seemingly) unrelated

topics. Rather, sustainable approaches are those that operate on a middle level of abstraction. Just as computer science students cannot readily make use of meta-theories or grand theories of international relations, specialised technical knowledge does not significantly advance students in peace and conflict studies in this context. Additionally, applying theoretical concepts to case studies or drawing on middle-range theories allows for the convergence of different epistemological backgrounds, thereby strengthening interdisciplinary discourse in a sustainable way. An important foundation of the textbook and the lecture lies in the interdisciplinary and highly heterogeneous group of authors of the textbook and the composition of the teaching staff. This allows for the in-depth transfer of domain knowledge while also anchoring it broadly and placing it in different contexts. Such transmission could also be facilitated through unconventional teaching formats, such as lecture series and exercises with guest lecturers from various disciplines or with practical relevance to peace and security issues. Especially regarding technical questions and fundamentals, it seems crucial to incorporate technical relationships into social science discourses and potentially involve external expertise. Courses that build on such a textbook and include additional experts on current topics can also be conducted by chairs or individuals who primarily work within their disciplinary boundaries.

References

Recommended Reading

Reuter, C., Riebe, T., Haunschild, J., Reinhold, T., & Schmid, S. (2022): Zur Schnittmenge von Informatik mit Friedens- und Sicherheitsforschung: Erfahrungen aus der interdisziplinären Lehre in der Friedensinformatik. Zeitschrift für Friedens- und Konfliktforschung (ZeFKo);11(2):129–140. https://doi.org/10.1007/s42597-022-00078-4

Bibliography

Altmann, J., Bernhardt, U., Nixdorff, K., Ruhmann, I., & Wöhrle, D. (2017). Naturwissenschaft—*Rüstung—Frieden*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-01974-7

Dix, A., Finlay, J., Abowd, G., & Beale, R. (2013). *Human–Computer Interaction* (1–3). Upper Saddle Rive.

Gießmann, H. J., & Rinke, B. (Hrsg.). (2019). *Handbuch Frieden*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-23644-1

Imbusch, P., & Zoll, R. (Hrsg.). (2010). *Friedens- und Konfliktforschung*. VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-92009-2_4

Nisioti, A., Mylonas, A., Yoo, P. D., & Katos, V. (2018). From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods. *IEEE Communications Surveys & Tutorials*, *20*(4), 3369–3388. https://doi.org/10.1109/COMST.2018.2854724

Quinn, M., J., (2018). *Ethics for the Information Age*. Pearson Education.

Rashid, A., Howard, C., Emil, L., Martin, Andrew, & Schneider, Steve. (2021). *CyBOK: The Cyber Security Body of Knowledge*. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

Reinhold, T., & Reuter, C. (2022). Toward a Cyber Weapons Assessment Model—Assessment of the Technical Features of Malicious Software. *IEEE Transactions on Technology and Society*, *3*(3), 226–239. https://doi.org/10.1109/TTS.2021.3131817

Reinhold, Thomas, & Reuter, Christian. (2019). From Cyber War to Cyber Peace. In *Information Technology for Peace and Security—IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Springer Vieweg.

Reuter, C. (Hrsg.). (2018). *Sicherheitskritische Mensch-Computer-Interaktion*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-19523-6

Reuter, C. (Hrsg.). (2019). Information *Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4

Reuter, C., Altmann, J., Göttsche, M., & Himmel, M. (2020). Zur naturwissenschaftlich-technischen Friedens- und Konfliktforschung: Aktuelle Herausforderungen und Bewertung der Empfehlungen des Wissenschaftsrats. *Zeitschrift für Friedens- und Konfliktforschung*, *9*(1), 143–154. https://doi.org/10.1007/s42597-020-00035-z

Reuter, C., & Kaufhold, M. (2018). Fifteen years of social media in emergencies: A retrospective review and future directions for crisis Informatics. *Journal of Contingencies and Crisis Management*, *26*(1), 41–57. https://doi.org/10.1111/1468-5973.12196

Riebe, T., Schmid, S., & Reuter, C. (2021). Measuring Spillover Effects from Defense to Civilian Sectors –A Quantitative Approach Using LinkedIn. *Defence and Peace Economics*, *32*(7), 773–785. https://doi.org/10.1080/10242694.2020.1755787

Schlotter, Peter & Wisotzki, Simone. (2011). *Friedens- und Konfliktforschung*. Nomos.

The White House. (2022). *Remarks by President Biden Providing an Update on Russia and Ukraine*. https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/15/remarks-by-president-biden-providing-an-update-on-russia-and-ukraine/

Werkner, Ines-Jacqueline. (2020). *Friedens- und Konfliktforschung—Eine Einführung*. utb.

Werkner, Ines-Jacqueline & Schörnig, Niklas. (2019). *Cyberwar – die Digitalisierung der Kriegsführung*. Springer.

Wissenschaftsrat. (2019). *Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung*. https://www.wissenschaftsrat.de/download/2019/7827-19.pdf?__blob=publicationFile&v=2