Outlook: The Future of IT in Peace and Security

22

Christian Reuter, Konstantin Aal, Jürgen Altmann, Ute Bernhardt, Kai Denker, Jonas Franken, Anja-Liisa Gonsior, Laura Guntrum, Dominik Herrmann, Matthias Hollick, Stefan Katzenbeisser, Marc-André Kaufhold, Thomas Reinhold, Thea Riebe, Ingo Ruhmann, Klaus-Peter Saalbach, Lisa Schirch, Stefka Schmid, Niklas Schörnig, Ali Sunyaev and Volker Wulf

Abstract

Not only today, but also in the future, information technology and advances in the field of computer science will have a high relevance for peace and security. Of course, a textbook like this can only cover a selective part of research and a certain point in time. Nonetheless, it can be attempted to identify trends, challenges and offer an outlook into the future. In this chapter, we want to formulate a basis for anticipating future developments and correct classification. These considerations were made both by the editor and the involved authors. Thus, an outlook based on fundamentals, cyber conflicts and war, cyber peace, cyber arms control, infrastructures as well as social interaction is given.

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

J. Franken
e-mail: franken@peasec.tu-darmstadt.de

A.-L Gonsior
e-mail: gonsior@peasec.tu-darmstadt.de

L. Guntrum
e-mail: guntrum@peasec.tu-darmstadt.de

M.-A Kaufhold
e-mail: kaufhold@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_22

Objectives

- Learning about current trends and ideas on future developments.
- Being able to judge in which directions the field of research is developing.
- Gaining the ability to make seminal decisions with regard to probable developments.

T. Reinhold
e-mail: reinhold@peasec.de

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

S. Schmid
e-mail: schmid@peasec.tu-darmstadt.de

K. Aal · V. Wulf
Information Systems and New Media, University of Siegen, Siegen, Germany
e-mail: konstantin.aal@uni-siegen.de

V. Wulf
e-mail: Volker.Wulf@uni-siegen.de

J. Altmann
Physics and Disarmament, TU Dortmund, Dortmund, Germany
e-mail: juergen.altmann@tu-dortmund.de

U. Bernhardt
Forum of Computer Scientists for Peace and Social Responsibility (FIfF) E.V, Berlin, Germany
e-mail: ute@kriton.org

K. Denker
Institut Für Philosophie, Technische Universität Darmstadt, Darmstadt, Germany
e-mail: kai.denker@tu-darmstadt.de

D. Herrmann
Privacy and Security in Information Systems Group, University of Bamberg,
Bamberg, Germany
e-mail: dominik.herrmann@uni-bamberg.de

M. Hollick
Secure Mobile Networking Lab (SEEMOO), Technische Universität Darmstadt,
Darmstadt, Germanye-mail: matthias.hollick@seemoo.tu-darmstadt.de

S. Katzenbeisser
Chair of Computer Engineering, Universität Passau, Passau, Germany
e-mail: Stefan.Katzenbeisser@uni-passau.de

I. Ruhmann
TH Brandenburg, Berlin, Germany
e-mail: ingo@ruhmann.digital

K.-P. Saalbach
Institute for Political Science, University Osnabrück, Osnabrück, Germany
e-mail: ksaalbac@uni-osnabrueck.de

22.1 Motivation

Of course, predicting the future in an area of research is not an easy task. Also, any prediction will certainly be faulty in many ways. Nonetheless, we shall dare an outlook into the future of information technology for peace and security. In some cases, where the future depends on scientific modelling or when political decisions that cannot be predicted at all, we instead propose what should be done.

This was not an effort by the editor alone, but in cooperation with several authors of this book. The authors were invited to contribute an outlook from the perspective of their respective chapter on the future in 5 to 15 years and possible trends. The outcomes are intriguing and will be presented on the following pages.

22.2 Introduction and Fundamentals (Part I)

Chapter 2 "*Peace Informatics: Bridging Peace and Conflict Studies with Computer Science*" introduces the field of peace informatics. The chapter emphasises the escalating potential of cyber attacks, leading to increasing international insecurity caused by IT tools. It highlights the need to investigate technical solutions and stresses the importance of establishing fundamental definitions to facilitate international agreements on the use of IT tools for military and intelligence purposes. Simultaneously, the peace-building impact of ICT needs to be considered for technology development. Overcoming these challenges requires an interdisciplinary research approach and suitable research funding.

With respect to the role, relevance and tasks of Chapter 3 "*Natural Science/Technical Peace Research"* it is necessary to consider the fundamental structure of the international system where there is no overarching authority with a monopoly of legitimate violence that guarantees the security of the states. To be prepared for attacks by others the states maintain armed forces which in turn, due to their offensive potential, increase mutual threats. This security dilemma is aggravated by fast technological advance. Arms races and military destabilisation should be limited by (preventive) arms control. For states to have trust in limitation of weapons and armed forces, arms control agreements require

L. Schirch
University of Notre Dame, Notre Dame, USA
e-mail: lschirch@nd.edu

N. Schörnig
Peace Research Institute Frankfurt (PRIF), Frankfurt Am Main, Germany

A. Sunyaev
Institute of Applied Informatics and Formal Description Methods (AIFB),
Karlsruher Institut Für Technologie, Karlsruhe, Germany
e-mail: sunyaev@kit.edu

adequate verification of compliance. In order to limit and reduce dangers from new military technologies, natural science/technical peace research is needed in several respects: analysis of properties of military systems, their dangers, options to reduce them, and methods to verify compliance. While such research has a considerable tradition regarding weapons and carriers based on physics, chemistry and biology, with results reflected in many arms control treaties, there is a big gap in the emerging field of preparations for cyber warfare scenarios. IT-based peace research should be done in several important areas. With regard to the risk of cyber war such research should follow up military developments, analyse their dangers, investigate how civilian IT security measures could be extended to the military, and develop concepts for confidence and security building measures (CSBMs), for limitations and for their verification. In other fields of peace and international security research is needed on the trend toward autonomous weapons and the use of artificial intelligence (AI) on the battlefield, but also on the positive contributions that AI can bring for monitoring and verification. IT-based peace research can prepare CSBMs and arms control in cyberspace and will hopefully help to convince states and publics that transparency as well as limitations are needed as well as feasible.

22.3 Cyber Conflict and War (Part II)

A major trend in the context of Chapter 4 "*Information Warfare: From Doctrine to Permanent Conflict*" is that digital technology has created new opportunities to wage Information War; its pervasiveness will widen the scope of actors and reduce the threshold for using any means available. The major players see information warfare as a permanent form of conflict, eroding the distinction between war and peace. The digital arms race accelerates, its resources dwarfing the investments in secure IT systems. If reason will not surprisingly prevail, instability and conflict will increase around the globe.

Of "*Cyber Espionage and Cyber Defence*", covered in Chapter 5, particularly the former is unlikely to go away very soon because of its clandestine nature. Nation states are confronted with a prisoner's dilemma: Everyone would be better off by shutting down all state-sponsored hacking initiatives on a global scale; however, it is easy to cheat on such a policy. The fact that more and more countries are interested in stockpiling zero-day vulnerabilities will create a strong demand on the vulnerability market. Finally, we will see more state-sponsored attempts at introducing backdoors into hardware components. The fear of such supply-chain attacks might even create an incentive for European nation states to build up their own ecosystem of hardware manufacturers.

Also related to the previous chapter, "*Darknets and Civil*", the topic of Chapter 6, continues to be highly relevant. First, means of anonymous, even obfuscated communication are important to diverse actors in a conflict-ridden world. Second, Darknets allow for trading hacking services and exploits, which serve as building blocks for cyber weapons. Finally, Darknets offer the possibility to disseminate information unfiltered – be it disinformation and propaganda, be it reports from authoritarian countries by activist

groups. Still, delineating the role of Darknets to civil security through the identification of threats highlights the problem of securitisation: they reciprocally serve as discursive reservoirs for deliberately constructing threat scenarios on unclear empirical grounds.

22.4 Cyber Peace (Part III)

There are also some trends with regard to cyber peace: The struggle to make the step "*From Cyber War to Cyber Peace*" (as discussed in Chapter 7) can only be resolved on a global scale, where the current global players meet, discuss and support such efforts. Nevertheless, the actual political and military situation does not provide much hope that these things will happen soon. However, IT security can be regarded as the "lowest common denominator" of all states that economically depend on the invulnerability of the cyberspace as infrastructure. Furthermore, IT services tend to spread around the world. Especially cloud applications do not regard borders. This "digital globalisation" could be an important force that can be used by civil societies to foster the ideal of a peaceful development of the cyberspace. The potential impact of such efforts will strongly depend on the question if cyber peace campaigns can be coordinated globally.

Looking at Chapter 8 "*Dual-Use Information Technology: Research, Development and Governance*" we expect that dual-use assessment will gain more importance, in particular due to the increasing potential to misuse IT (e.g. assistant systems) and their access to personal, business or governmental data. Another development we might see is the increasing risk of misusing robots and robot assistants to harm people. IT development will thus face the challenge to find ways to mitigate the risks of manipulation of IT and thus necessitates awareness-raising and evaluation methods during the R&D process.

The main trend in context of Chapter 9 "*Confidence and Security Building Measures for Cyber Forces*" is that many states are preparing military action in cyberspace, not only for defence, but also for offence, resulting in increasing mutual threats. An arms race has begun. International security is in danger, particular urgency will ensue if cyber operations will be automated. Destabilisation of the military situation has to be feared – because the real originator of an attack can be concealed, because cyber operations are integrated with general warfighting, and because military and civilian IT infrastructure are strongly coupled. These prospects call for limitations and prohibitions, but cyber arms control and its verification meet very high hurdles: Weapons can be duplicated easily, their properties can be kept secret before use and there is no clear separation between espionage and attack. Thus, as a first step, confidence and security building measures (CSBMs) are advisable. States have begun to discuss and recommend confidence building measures for the civilian cyber sphere. However, these measures are voluntary and do not focus on military preparations. What is lacking are measures that are obligatory and focus on cyber armed forces directly. A role model exists in the CSBMs that hold for the conventional armed forces in Europe in the context of the Organisation for Security and Co-operation in Europe (OSCE). Not all these CSBMs can be transferred to cyber

forces because some would be unacceptably intrusive or difficult to define and verify. For example, this holds true for exchanges on the characteristics of cyber weapons or for limits on large-scale military activities and for their observation. But information exchanges on organisation and person power of cyber forces, on policy, doctrine and budgets, as well as consultations and, to some extent, visits and military contacts should be possible. International security would greatly improve if states will introduce such binding CSBMs for cyber forces. One can hope that with growing experiences cyber CSBMs could be expanded over time and would pave the way, together with research, to actual limitations, that is cyber arms control with adequate verification of compliance.

22.5 Cyber Arms Control (Part IV)

In context of Chapter 10 "*Arms Control and its Applicability to Cyberspace*", the examples of international and national approaches to the development of binding rules and norms for state behaviour have highlighted the increasing acceptance of the importance of cyberspace and the growing commitment of the international community to ensuring its stability. However, assessments, such as the 2013 Cyber Security Index (UNIDIR, 2013), can only be the first step towards binding rules that limit, reduce, or even prohibit the development, proliferation and usage of offensive cyber tools for military purposes. Besides the political will of states, many technical issues need to be analysed to develop solutions to these challenges. Measures need to be developed that allow controlling compliance of treaty parties, the practical monitoring of military facilities, or the tracking of cyber weapon material like software vulnerability exploits. The history of arms control shows that this is a long way to go but a necessary step towards the peaceful development of a global domain.

In the context of Chapter 11 "*Verification in Cyberspace*", we expect a trend of further militarisation of cyberspace and increasing numbers of military forces that establish offensive capabilities for cyber warfare. Simultaneously, the asymmetry of cyber powers will rise. Cyber operations will become a normal part of military conflicts with the disruption and even the destruction of critical infrastructures as part of strategic military planning. The pressure of the international state community on the leading cyber power countries to negotiate and agree to a dedicated binding regulation of the usage of cyber weapons and the protection of civilian infrastructures will rise. The impact of cyber weapons on military systems that is hard to contain may optimally lead to cyber weapon treaties and the establishment of initiatives on verification.

Looking at the context of Chapter 12 "*Attribution of Cyber Attacks*", this will remain a major challenge for cyber security in all its technical, legal and political dimensions. Attackers will probably always be one step ahead, because hackers will continue to find new vulnerabilities and unexpected ways to attack computers and devices. However, attack attribution efforts have made substantial progress in recent years. The trend is shifting from a more analytical approach of malware and tactics, techniques and programs to an active use of cyber and conventional intelligence. Artificial Intelligence tools can systematically

collect, consolidate and analyse threat intelligence data from multiple sources. Nonetheless, the development of cyber weapons is also in progress and their proliferation is difficult to control, so attackers will still have multiple options to mislead investigations. Cooperation between organisations by combination of resources, experience and knowledge remains a key element for future success in attributing of cyber attacks.

22.6 Cyber Infrastructures (Part V)

Concerning Chapter 13 "*Secure Critical Infrastructures*", it is worth noting the recent rise in the usage of infrastructure as a concept and its application to ever more objects of interest. With upcoming national legislation implementing EU directives, there will be a considerable increase in the number of critical infrastructures. Also, while digital tools are included in virtually any CI, the potential impact of cyber attacks by private and state actors targeting infrastructures or components further increases. Additionally, ongoing climate change increases the likelihood of extreme weather phenomena impacting critical infrastructures. Therefore, raising the physical and digital resiliency is paramount and will require academic foundation and scrutiny by CI researchers.

Chapter 14 "*Resilient Critical Infrastructures*" argues that information and communication technology (ICT) used within critical infrastructures should be designed with resilience as a guiding principle. Furthermore, the chapter also offers suggestions on how resilience can be achieved. However, mapping the suggestions to concrete architectural designs can be challenging due to a number of reasons. First, multiple security controls will raise the cost of the complete system. Second, resilience may be hard to achieve in systems that need to support legacy devices or protocols. Finally, the division into more or less independent sub-systems, which continue to operate under attacks, is challenging. We can conclude that further fundamental research is required in the domain of resilient ICT systems. Subsequently, the transfer of this fundamental research into concrete security architectures and solutions for critical infrastructures as well as the derivation of best practices to integrate the solutions into existing systems is required. Finally, it is important to note that besides technology, processes need to be in place so that an organisation can react to security incidents in a timely fashion, thus ensuring the continuity of its critical operations. Chapter 15 "*Security of Critical Information Infrastructures*" focuses on how critical information infrastructures (CII) exhibit unique characteristics that make their management and protection challenging. CII emerge and evolve over time and are opaque systems due to the complex interconnections and interdependencies of their parts. On the one hand, operators of an infrastructure (and their respective customers) might not be aware that over time their IT infrastructure has become critical; thus, they may not implement required CII security-protection mechanisms. On the other hand, we are currently lacking clear definitions and classifications of CII that help infrastructure operators to decide whether they are operating CII. Future research is required that provides guidance on identifying and modelling CII. Operators of CII often host their own

IT infrastructure or, at most, share resources with organisations with similar demands. However, operators of CII are increasingly migrating their IT services to cloud environments to achieve manifold benefits, such as scalability, flexibility, and cost reduction. Nevertheless, outsourcing critical IT systems poses high risks, for example, with respect to system availability, confidentiality, integrity, and data protection and leads to a high dependency of CII on employed cloud services. Future research is required to understand resulting challenges and minimum requirements that cloud service providers must fulfil to prevent ripple effects and to ensure reliable operation of CII. The current CII landscape faces unclear legislation and requires further regulations. For example, in Germany, the *IT-Sicherheitsgesetz 2.0* and the *BSI-Kritisverordnung* provide first minimum requirements that critical (information) infrastructures have to fulfil. Yet, standards, certifications, and best practices on how to protect critical (information) infrastructures are still lacking, specifically, for sectors with strict requirements for data protection and security, such as finance or health. In addition, there is a need for continuous assurance that the determined standards and regulations are enforced, for example, by applying appropriate (continuous) certification methods.

22.7 Artificial Intelligence (Part VI)

Chapter 16 "*Artificial Intelligence and Cyber Weapons*" illustrates that, contrary to the negative trends of increasing automation of offensive cyber tools and the arising challenges for arms control, AI methods can also support the task of arms control itself. In particular, the task of verification – the meticulous process of collecting information, comparing data or analysing combined sources to control and monitor the compliance of treaty members with signed agreements – is usually a task of detecting the needle in the haystack. Given the increasing processing capacity and capabilities of AI, these challenges could be alleviated. However, as this is uncharted territory, a lot of research still needs to be done and the long-term results are questionable.

Looking at the topic of Chapter 17 "*Unmanned Systems: The Robotic Revolution as a Challenge for Arms Control*" more and more functions of military systems will see automation in the future - as it is the case in the civilian sector - and the human role will shift towards observation and oversight rather than direct control. In this context, manned-unmanned teaming (MUM-T) will increase significantly and more complex systems will allow the human to oversee more and more unmanned systems working independently or as a swarm. Weapon systems with a huge variety of autonomous functions are already in the testing phase, yet facing technical teething troubles. These systems, including unmanned jetfighters and tanks, will reach readiness status in the years to come. More and smaller systems will be integrated into a network, constantly exchanging data and adopting to new situations instantly. Whether an international treaty, a norm or a (weaker) Code of Conduct can be agreed upon by the international community to ban or regulate lethal autonomous weapon systems is yet to be seen.

22.8 ICT in Peace and Conflict (Part VII)

Chapter 18 "*Cultural Violence and Peace Interventions in Social Media*" shows that social media platforms play an important role and will likely continue to evolve, and change based on technological trends and increasing government regulation. This will also affect the dissemination of cultural violence in manual or semi-automatic manners across social media. Although a variety of countermeasures exist, such as gatekeeping, laws, media literacy, or detection algorithms, these must be adopted to the characteristics of new social media and, with regard to existing social media, malintent actors will likely find new or still exploit established ways of disseminating cultural violence. While social bots are capable of identifying vulnerable users and of publishing significant amounts of manipulative content, researchers work on more sophisticated bot detection algorithms and bot developers improve bots' abilities to identify people prone to radicalisation, leading to an arms race between concealment and detection. Since this chapter focuses on three specific topics, namely fake news, cyber abuse and cyber terrorism recruitment, further domains or phenomena prone to cultural violence, such as partisanship, have to be examined in order to achieve a more comprehensive view of the phenomenon. Furthermore, even though countermeasures and positive interventions are outlined, including the development of social media guidelines and the application of social media analytics, their actual contribution to cultural peace must be researched in a more systematic and thorough manner to draw robust conclusions and to keep pace with technological changes.

Trends in the context of the Chapter 19 "*Political Activism on Social Media in Conflict and War*" depend on the development of internet penetration in the Arab world and Eastern parts of Europe, as well as the Southern Hemisphere such as Columbia as a whole. Also, more politicians and other government actors are joining social media and becoming quite apt and active users, such as Narendra Modi in India. This is likely to influence how future conflicts play out online, and how digital tools are used. The power asymmetries discussed in the chapter potentially shift further towards an imbalance in favour of state actors in control of infrastructure and larger financial resources. But the increased awareness about the importance of social media and associated risks also leads activists and support groups such as Amnesty International or Tactical Tech to improve their practices. Current research on the use of social media in conflict situations presents the platforms as simply passive stages of the actions of others instead of actors with their own intentions. Future research needs to consider the platforms themselves, their technological structures as well as the tools and services they provide as deliberate and purposeful actors in political conflicts. The spread of misinformation on Facebook and Twitter around the 2016 presidential election in the USA, and Facebook's current reaction to this are examples of such interactions. Furthermore, the development and adaptation of future technologies in those fields can result in novel possibilities for "citizen journalists" to create news content (e.g. live streams). However, new technological developments and an increased awareness of the power and importance of social media

in political situations also leads to advanced mechanisms for online surveillance, as well as attempts to avoid such surveillance.

Chapter 20 "*Digital Peacebuilding*" discusses the current state and potential future trends of digital peacebuilding, emphasising its reliance on evolving technologies. Overall, four key trends for the future are presented. Firstly, efforts are underway to make peacetech and digital peacebuilding more desirable, affordable, and actionable, with the Council on Technology and Social Cohesion advocating for public policy and funding support. Secondly, the chapter underscores the potential dangers of technology, citing disparities in digital access, privacy concerns, and the misuse of technology e.g. by authoritarian governments. Thirdly, it advocates for peace engineering, defined as the application of science and engineering principles to promote peace, emphasising the need for ethical and humane design in technological development. Lastly, the importance of digital media literacy is highlighted, with a focus on countering online disinformation and ensuring that governments, businesses, and civil society can effectively use technology for human security, social cohesion, and social justice.

22.9 Outlook (Part VII)

In Chapter 21 "Teaching Peace Informatics: Reflections", the importance of interdisciplinary research and teaching at the intersection of computer science and peace and security studies is highlighted. The chapter discusses the collaborative introduction of the course "*Information Technology for Peace and Security*" at TU Darmstadt, involving students from various disciplines. Four key observations emerge from course iterations and evaluations. Rooted in problem solving-oriented science, the course underscores empirical relevance in peace and conflict research, revealing disciplinary limitations and emphasising substantial gains through an interdisciplinary approach to address real-world phenomena.

Considering the different perspectives that are reflected across book sections, it becomes clear that there is still a need for interdisciplinary research on information technology and its relationship to security and peace, both in a more general way regarding these broader concepts as well as with respect to concrete applications. With its focus on information technology, we offer a contribution to peace and conflict studies as we introduce fundamental concepts such as structural violence or negative peace to existing debates of cyber security. This regularly necessitates a sociotechnical perspective on problems and phenomena. Thus, across specific topics, the contingent, non-linear nature of social processes becomes clear and demands iterative research processes. Building on technical, systematic problem-solving approaches, it is possible to identify potentials as well as limitations of real-life artefacts. If we continue to exchange such perspectives and insights, research could help in creating win–win scenarios for decision-making actors. These are urgently needed in times of multiple, long-term crises and reconfiguration of global structures.