19 The Future of IT in Peace and Security

Christian Reuter · Konstantin Aal · Larissa Aldehoff · Jürgen Altmann · Ute Bernhardt · Johannes Buchmann · Kai Denker · Dominik Herrmann · Matthias Hollick · Stefan Katzenbeisser · Marc-André Kaufhold · Alfred Nordmann Thomas Reinhold · Thea Riebe · Annette Ripper · Ingo Ruhmann · Klaus-Peter Saalbach · Niklas Schörnig · Ali Sunyaev · Volker Wulf

Abstract

Not only today, but also in the future information technology and the advances in the field of computer science will have a high relevance for peace and security. Naturally, 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 venture an outlook into the future. That is exactly what we want to achieve in this chapter: To predict future developments and try to classify them correctly. These considerations were made both by the editor and the authors involved alike. Therefore, an outlook based on fundamentals, cyber conflicts and war, cyber peace, cyber arms control, infrastructures as well as social interaction is given.

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.

C. Reuter (Ed.), *Information Technology for Peace and Security*,
https://doi.org/10.1007/978-3-658-25652-4_19

19.1 Motivation

Surely, 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 science-planning as well as political decisions that cannot be predicted, we rather explain what should be done.

This was tried not 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.

19.2 Introduction and Fundamentals (Part I)

Chapter 2 *"IT in Peace, Conflict, and Security Research"* introduces the field of IT peace research. The potential for escalation of cyber attacks and therefore the interstate (and in some cases interpersonal) insecurity caused by IT tools is increasing. It becomes more and more important to investigate and develop technical solutions for prevention. Moreover, fundamental definitions have to be developed to enable international agreements on the use of IT tools for military and intelligence purposes. At the same time the peace-building impact of ICT needs to be considered for technology development. An interdisciplinary research approach as well as suitable research funding is necessary to overcome these challenges.

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 the mutual threats. This security dilemma is aggravated by fast technological advance. Arms races and military destabilisation should be limited by (preventive) arms control. In order that states have trust in limitation of weapons and armed forces, arms-control agreements require 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 new field of preparations for cyber war. IT-based peace research should be done in several areas. With respect to 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.

19.3 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 markedly 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 as Tools for Cyber Warfare"*, the topic of Chapter 6, will gain importance for many forms of cyber warfare in future years. First, undoubtedly important for cold and hot conflicts are means of anonymous, even obfuscated communication. 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. Still, delineating the role of Darknets as tools for cyber warfare highlights the problem of securitisation: they reciprocally serve as discursive reservoirs for deliberately constructing threat scenarios on unclear empirical grounds.

19.4 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 at least 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 and Dilemmas for Cybersecurity, Peace and Technology Assessment"*, we are convinced, that in 5 to 15 years, dual-use assessment will gain more importance. Especially so due to the increasing potential to misuse IT in 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 will therefore have to develop awareness-raising and evaluation methods during the research and development 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 general, 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 Organization 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. This holds e.g. for exchanges on the characteristics of cyber weapons or for limits on large military activities and for their observation. But information exchanges on organisation and manpower 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.

19.5 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.

Looking at the topic of Chapter 11 "*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.

In the context of Chapter 12 *"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 13 "*Attribution of Cyber Attacks*" will remain a major challenge for cyber security in all its technical, legal and political dimensions. The 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, attribution efforts have made substantial progress in the last 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. In combination with the ongoing accumulation of data and experience by security actors the time between an attack and a sufficient attribution will become shorter. 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 on the wrong track. The cooperation between organisations by combination of resources, experience and knowledge is and will be a key element for future success in attribution of cyber attacks.

19.6 Critical Infrastructures (Part V)

Chapter 14 *"Resilient Critical Infrastructures"* argue 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.

In context of Chapter 15 *"Security of Critical Information Infrastructures",* Critical information infrastructures (CII) exhibit unique characteristics that makes their management and protection challenging. CII emerge and evolve over time and are opaque systems due to the complex interconnections and interdependences 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 evolved to a CII; 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 a CII. Future research is required that provides guidance on identifying and modelling CII.

Currently, critical infrastructure operators often host their own IT infrastructure or, at most, share resources with organisations with similar demands. However, critical (information) infrastructure operators 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, security, and data protection and leads to a high dependency of critical infrastructure operation on the cloud service. Future research is required to understand resulting challenges and minimum requirements that cloud services must fulfil to prevent ripple effects and to ensure reliable operation of CII.

The current CII landscape faces unclear legislation and requires further regulations. Although, for example, in Germany, the 'IT-Sicherheitsgesetz' provides first minimum requirements that critical (information) infrastructures have to fulfil, 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.

"*Safety and Security – Their Relation and Transformation*", as discussed in Chapter 16, calls for an assessment, critique, perhaps transformation of a new technopolitical challenge – reflecting the insight that the safe and secure operation of any technology requires legal frameworks and trustworthy institutions and thus involves politics as it operates beyond the technological sphere. While engineers maintain the physical integrity of a system, public authorities and concerned citizens need to provide and monitor the safety of the environment for safe operation. If the convergence of technologies and their complex integration through IT continues, it will be ever more difficult to maintain the traditional division

of labour between safety and security, between technical and political problems. This undermines what C.P. Snow famously called the two cultures with humanities and social science on the one side, science and engineering on the other. And yet, the integrative notion of an all-encompassing "safety culture" places a considerable burden of responsibility especially on engineers who require a cross-disciplinary education encompassing computer science, humanities and the social sciences – as exemplified by this book. It is not clear, however, that the diagnosed trend and the shift from the traditional sphere of politics to the sphere of technology can and should continue. A critical assessment of this trend has to consider strategies for bringing politics back in with its emphasis on law, contractual obligation, the creation and maintenance of relations of trust.

19.7 Social Interaction (Part VI)

Looking at Chapter 17 *"Cultural Violence and Peace in Social Media"*, it is likely that the number of social media platforms will further increase, extending the opportunities to disseminate cultural violence in manual or semi-automatic manner 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. Especially social bots are capable of publishing significant amounts of manipulative content. Nonetheless, researchers will work on more sophisticated bot detection algorithms, bot developers will improve the bots' imitation of human behaviour, leading to an arms race between concealment and detection. Since this chapter focuses on three specific topics, namely fake news, cyber terrorism and social bots, further domains or phenomena prone to cultural violence, such as (socio-political) diversity, have to be examined in order to achieve a more comprehensive view on the field. Furthermore, even though countermeasures and positive interventions are outlined as well as the development of social media guidelines and the application of social media analytics are envisioned in that chapter, their actual contribution to cultural peace must be researched in a more systematic and thorough manner to draw robust conclusions.

Trends in the context of the Chapter 18 *"Social Media and ICT Usage in Conflicts Areas"* depend on the development of internet penetration in the Arab world and Eastern parts of Europe, as well as the Southern Hemisphere 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 take into account 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.

19.8 Outlook (Part VII)

We can draw from the different perspectives of all chapters that the development around information technology for peace and security by far is not completed at all developments. This promises many fascinating and highly relevant tasks and hopefully solutions that can be addressed in future research, in order to make the world a slightly better and more secure and peaceful place.