An Overview and Introduction to Information Technology for Peace and Security

1

Christian Reuter, Jonas Franken, Anja-Liisa Gonsior, Laura Guntrum and Stefka Schmid

Abstract

Technological and scientific progress, especially the rapid development in information technology (IT), plays a crucial role regarding questions of peace and security. This textbook addresses the significance, potential, and challenges of IT for peace and security. For this purpose, the book offers an introduction to peace, conflict, and security research, thereby focusing on natural science, technical, and computer science perspectives. In the following, it first sheds light on fundamentals (e.g. peace informatics, natural science/technical peace research). Then, cyber conflicts and war (e.g. information warfare, cyber espionage, cyber defence, darknet), cyber peace (e.g. dual-use, confidence and security building measures) and cyber arms control (e.g. arms control in the cyberspace, verification, attribution) are covered. It then covers cyber infrastructures (e.g. secure critical

C. Reuter (✉) · J. Franken · A.-L. Gonsior · L. Guntrum · 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

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_1

infrastructures, resilient infrastructures, critical information infrastructures), artificial intelligence (cyber weapons, unmanned systems) as well ICT in peace and conflict (e.g. cultural violence, social media, digital peacebuilding), before concluding with an outlook. This chapter provides an overview of all the chapters in this book.

Objectives

- Gaining a basic understanding of information technologies in the domain of peace and security.
- Receiving an overview of selected methods of information techniques in peace, conflict, and security research.
- Gaining the ability to orient oneself in the application domains and fields.

1.1 Introduction

Technological and scientific progress, especially the rapid development of information technology (IT), plays a crucial role regarding questions of peace and security. This chapter aims to introduce the content of the book. Part I introduces central concepts and highlights fundamentals (e.g. IT in peace, conflict, and security, natural science/technical peace research). Part II focuses on cyber conflicts and war (e.g. information warfare, cyber espionage, cyber defence, darknet), followed by Part III on cyber peace (e.g. from cyber war to cyber peace, dual-use and other dilemmas for cyber security, technology assessment, confidence, and security building measures). Afterwards, Part IV covers cyber arms control (e.g. arms control in cyberspace, verification in and attribution of cyberspace), Part V on cyber infrastructures (e.g. critical infrastructures, resilient critical infrastructures, secure information infrastructures), and Part VI on artificial intelligence (e.g. artificial intelligence and cyber weapons, unmanned systems). In Part VII on Information and Communication Technology (ICT) in Peace and Conflict (e.g. cultural violence in social media, ICT usage in conflict areas, digital peacebuilding) various aspects are presented, before an outlook is provided in Part VIII.

1.2 Introduction and Fundamentals (Part I)

Chapter 2 "*Peace Informatics: Bridging Peace and Conflict Studies with Computer Science*" by Christian Reuter, Anja-Liisa Gonsior, Thea Riebe and Marc-André Kaufhold (TU Darmstadt), presents an introduction and the fundamentals of this textbook as it deals with the role of information technology in war and peace. Examining the impact of IT on peace and security, the chapter emphasises the resilience of IT infrastructures as targets in conflicts and outlines how IT can prevent conflicts, crises, and disasters. Additionally, groundwork for the field of peace informatics is presented, offering an interdisciplinary overview of concepts in peace, conflict, and security.

Chapter 3 "*Natural Science/Technical Peace Research*" by Jürgen Altmann (TU Dortmund University) argues that building up national armed forces and, in particular, the quest for military-technological advances results in an arms race and deteriorates the security of the countries, requiring mutual limitations. It explains why natural science/technical research is needed for peace and international security and how it can be carried out as well as how the risks of war can be reduced by arms control with adequate verification of compliance. This chapter highlights the importance of natural science/technical peace research.

1.3 Cyber Conflicts and War (Part II)

Chapter 4 "*Information Warfare: From Doctrine to Permanent Conflict*" by Ingo Ruhmann and Ute Bernhardt (TH Brandenburg and Forum of Computer Scientists for Peace and Social Responsibility), draws its relevance from the increasing importance of information technology for militaries and secret services. It deals with the evolvement of information warfare by first exploring the establishment of doctrines and then elaborates on the tactics and targets of information warfare. The chapter concludes with threats of cyber warfare and the necessity of a new security architecture.

Chapter 5 "*Cyber Espionage and Cyber Defence*" by Dominik Herrmann (University of Bamberg), deals with cyber espionage, its superiority over traditional espionage, its characteristics, and its drawbacks for citizens and businesses. The author presents the fundamental security design principles and the primary protection goals of information security and describes typical attack vectors. Elaborating on the higher costs of defensive versus offensive tactics leads him to explore the relevance of security vulnerabilities for attacks, which cause the lack of security for end users.

Chapter 6 "*Darknets and Civil Security*" by Kai Denker, Marcel Schäfer, and Martin Steinebach (TU Darmstadt, Fraunhofer USA and Fraunhofer SIT), looks sat Darknets as platforms of both lawful activities, such as journalism, and illicit trade with narcotics, forged documents, weaponry, cyber arms, and their building blocks, among others. Moreover, the characteristic of providing anonymity to users and offering obfuscated services makes them an essential tool for cybercrime and violence and thus a significant concern of national and international security. The chapter discusses their technology, provides an overview of common Darknet phenomena, and puts these into the context of civil security and critical securitisation studies.

1.4 Cyber Peace (Part III)

Chapter 7 "*From Cyber War to Cyber Peace*" by Thomas Reinhold and Christian Reuter (TU Darmstadt), looks at the changes militaries have made to adapt to the widespread use of IT systems for civil and military purposes. Building on this, it analyses possible benefits in cyberspace for tools and policies developed to confine threats to international

security. The chapter further points out political advancements already in progress, the role of social initiatives, and the potential consequences of the rising probability of cyber war as opposed to the prospects of cyber peace.

Chapter 8 "*Dual-Use Information Technology: Research, Development and Governance*" by Thea Riebe, Stefka Schmid and Christian Reuter (TU Darmstadt), illustrates the history and definitions of dual-use, as well as highlights three examples of dual-use IT. Furthermore, methods for technology assessment and ethical design are introduced, while it provides insight into the implementation of dual-use assessment guidelines at TU Darmstadt, the so-called Civil Clause.

Based on the preparation of cyber armed forces by many states, Chapter 9 "*Confidence and Security Building Measures for Cyber Forces*" by Jürgen Altmann (TU Dortmund University), discusses the possibility of applying established procedures such as arms control and confidence (and security) building measures (C(S)BMs) in cyberspace. Due to difficulties with the former, the latter can act as the first step, creating transparency and reducing misperceptions and suspicions. There is a particular need for inclusive and binding agreements focusing on cyber forces. These could include exchanging information on force structures, policies, and doctrines.

1.5 Cyber Arms Control (Part IV)

Chapter 10 "*Arms Control and its Applicability to Cyberspace*" by Thomas Reinhold and Christian Reuter (TU Darmstadt), focuses on arms control as a means to preventing conflicts and fostering stability in inter-state relations by either reducing the probability of the usage of specific weapons or regulating their use and thus reducing the costs of armament. Extrapolating from historical examples and existing measures, the general architecture of arms control regimes and the complex topic of establishing and controlling the agreements will be discussed. The chapter will then discuss the challenges of applying these established approaches to cyberspace. Finally, building on these theoretical considerations, the chapter will present important treaties and first approaches.

Chapter 11 "*Verification in Cyberspace*" by Thomas Reinhold and Christian Reuter (TU Darmstadt), analyses the problems of applying traditional verification measures in cyberspace. In particular, it deals with distinguishing problems in relation to selected established verification measures for nuclear, biological, and chemical weapons technology. It further elaborates on possibilities to adjust technical settings, rules, and principles to reduce the threat of militarisation and presents some potentially useful verification approaches.

In Chapter 12 "*Attribution of Cyber Attacks*" Klaus-Peter Saalbach (Osnabrück University), begins by defining attribution as the allocation of a cyber attack to a particular attacker or a group of attackers in a first step and unveiling the real-world identity of the attacker in a second step. He then elaborates on the progress methods of attacker

allocation have made in recent years and the continuing problems digital technologies face providing definite evidence for the real-world identity of an attacker. He also stresses that digital forensics can be combined with evidence from the physical world and that gaps can also be filled by conventional espionage and the systematic collection, consolidation and analysis of threat intelligence data. He also provides real-world examples of current methods and practices of cyber attribution.

1.6 Cyber Infrastructures (Part V)

Chapter 13 "*Secure Critical Infrastructures*" by Jonas Franken and Christian Reuter (TU Darmstadt), gives a broad introduction to the essential knowledge and standard concepts of critical infrastructure research. Supported by multiple examples from all sectors, it nuances out what makes infrastructures critical, how they are sectorized but interdependent, who governs them in what way, and what actors are shaping them. Here, the German critical infrastructure governance serves as an example of a multi-level approach to critical infrastructure protection. A specific focus is put on the current role of information and communication technology, which is increasingly integrated into critical infrastructures of all sectors.

Chapter 14 "*Resilient Critical Infrastructures*" by Matthias Hollick (TU Darmstadt) and Stefan Katzenbeisser (University of Passau), deals with the risks of vulnerable critical infrastructure by giving insight into their nature and past attacks. It further introduces the proposal of making critical infrastructures resilient by enabling them to function even under attack, which requires adopting a "defence in depth" concept, i.e. deploying multiple layers of security controls. The chapter concludes with some recommendations which can make safety–critical transportation infrastructures more resilient.

Chapter 15 "*Security of Critical Information Infrastructures*" by Tobias Dehling, Sebastian Lins, and Ali Sunyaev (Karlsruhe Institute of Technology), clarifies the concept of critical information infrastructures. After a brief introduction to their salient characteristics and main functions, the chapter discusses threats and risks critical information infrastructures are confronted with and presents approaches to master these challenges.

1.7 Artificial Intelligence (Part VI)

Chapter 16, "*Artificial Intelligence and Cyber Weapons*" by Thomas Reinhold and Christian Reuter (TU Darmstadt) analyses the trend of implementing methods and algorithms of Artificial Intelligence and Machine Learning into cyber weapons to mitigate the imminent challenge of processing, filtering and aggregating vast amounts of digital data into decisions and actions in real time. It highlights the increasing tendency towards AI enabled autonomous decisions in both defensive and offensive cyber weapons, the

resulting additional challenges in attributing cyber attacks and the problems in developing arms control measures for this technology fusion.

Chapter 17 "*Unmanned Systems: The Robotic Revolution as a Challenge for Arms Control*", by Niklas Schörnig (Peace Research Institute Frankfurt), looks at the nexus of armament and technology in general and autonomous weapons and the increasing reliance on information technology in the military in particular. It argues that these developments necessitate new methods and techniques of arms control, as measures of arms control have fallen behind the development of IT, automation, and autonomy. These may offer military advantages at first glance; however, a more detailed analysis reveals that they will most likely have a destabilising effect on the international realm.

1.8 ICT in Peace and Conflict (Part VII)

Chapter 18 "*Cultural Violence and Peace Interventions in Social Media*" by Marc-André Kaufhold, Jasmin Haunschild and Christian Reuter (TU Darmstadt), deals with the positive and negative role that social media services play in influencing discourse and conflicts. Based on the notions of cultural violence and cultural peace, it first presents human cultural interventions in social media and respective countermeasures. Secondly, it discusses automatic cultural interventions realised via social bots and possible countermeasures. It does so by looking at the cases of fake news, hate speech, and online terrorist recruitment.

Chapter 19 "*Political Activism on Social Media in Conflict and War*", by Konstantin Aal, Sarah Rüller, Maximilian Krüger, Markus Rohde, Borislav Tadic and Volker Wulf (University of Siegen and 1&1), illuminates the role social media and ICT continue to play in a multitude of conflicts around the globe. It goes on to discuss how and what kind of tools and methods different actors use in their struggle. It mainly focuses on how actors appropriate the available tools to suit the specific conditions they find themselves in and discusses the importance of an embedded perspective on using ICTs in conflict to understand these practices of appropriation.

Chapter 20, titled "*Digital Peacebuilding and PeaceTech*" by Lisa Schirch, explains the concept of digital peacebuilding and peacetech, providing a comprehensive analysis of how ICT is employed to foster social cohesion, advocate for social justice, and fortify human security. It further defines the parameters of digital peacebuilding, emphasising the transformative potential inherent in the integration of ICT within these spheres. The chapter presents instances wherein ICT manifests its efficacy, specifically in areas such as violence prevention and inclusive governance, substantiating the versatility of its application across diverse domains. While the narrative predominantly accentuates positive outcomes associated with the deployment of ICT in peacebuilding efforts, it is not devoid of a critical appraisal of existing challenges. The chapter undertakes a discerning examination of the current landscape, proffering pragmatic insights aimed at improving both the developmental trajectory and the use of peacetech.

1.9 Outlook (Part VII)

Chapter 21 "*Teaching Peace Informatics: Reflections from Lectures and Exercises*" by Christian Reuter, Thea Riebe, Jasmin Haunschild, Thomas Reinhold and Stefka Schmid (TU Darmstadt) highlights the need for interdisciplinary education given the looming threats in cyberspace. It delves into the course "*Information Technology for Peace and Security"*, a joint initiative between TU Darmstadt and Goethe University Frankfurt. The chapter presents insights from student evaluations and direct feedback, providing a holistic assessment of the teaching experience.

Chapter 22 "*Outlook: The Future of IT in Peace and Security*", by all coreesponding authors of this book, anticipates developments in the field for the next 5–15 years and resulting challenges. It is structured by chapters, with each author contributing their estimation for the field on which they wrote a chapter on. Overall, it can be said that the authors paint a lively picture of future developments in the field of information technology for peace and security that will offer enough interdisciplinary challenges to researchers and policy makers alike.

1.10 Didactical Information

The structure of this book envisages its use as an accompanying read for lectures.

- The chapters offer an **introduction** and provide a good **overview** of the topic.
- While being introductory and understandable for students, they still outline the state of research. In length, they are confined to approximately 20-25 pages.
- Every chapter is designed to cover a **lecture** and accompanying **tutorial**.
- At the end of every chapter, **exercises** are listed which can accompany a tutorial. These include both questions for revision and questions for further analysis.
- The book thus comprises a **course** of overall four hours per week for 15 weeks.
- As every chapter is comprehensible on its own, it is possible to put together a class individually and employ different chapters to this end.
- **Material for lecturers** can be found at www.peace-book.chreu.de.
- Experiences from teaching this subject can be found Chapter 21 "*Teaching Peace Informatics: Reflections from Lectures and Exercises*".

1.11 Exercises

Exercise 1–1: Name the fields of applications for information technology for peace and security.
Exercise 1–2: Indicate central players, methods, and technical systems in the field of this book.

Exercise 1–3: Looking at the outlines above, and drawing on your knowledge of International Relations, think of the central overarching problems in the field of IT peace research.
Exercise 1–4: Of the topics presented above, which are the two you are most interested in and why? Come up with three questions you expect this chapter to answer.