Chapter 1
Introduction

Markus Christen, Bert Gordijn, and Michele Loi

Abstract This introduction provides a short overview on the book "The Ethics of Cybersecurity". The volume explains the foundations of cybersecurity, ethics and law, outlines various problems of the domain such as ethical hacking and cyberwar, and it lists recommendations and best practices for cybersecurity professionals working in various application areas. Furthermore, the introduction outlines the background of the European CANVAS project, from which this volume emerged.

Keywords Cybersecurity · Ethics · Law · Trust · Values

The increasing use of information and communication technology (ICT) in all spheres of modern life makes the world a richer, more efficient and interactive place. However, it also increases its fragility, as it reinforces our dependence on ICT systems that can never be completely safe or secure. Therefore, cybersecurity has become a matter of global interest and importance. Accordingly, we can observe in today's cybersecurity discourse an almost constant emphasis on an ever-increasing and diverse set of threats, ranging from basic computer viruses to sophisticated kinds of cybercrime and cyberespionage activities, as well as cyber-terror and cyberwar. This growing complexity of the digital ecosystem in combination with increasing glo bal risks has created the following dilemma. Overemphasising cybersecurity may violate fundamental values such as equality, fairness, freedom or

M. Christen (✉)
UZH Digital Society Initiative, Zürich, Switzerland
e-mail: christen@ethik.uzh.ch

B. Gordijn
Dublin City University, Dublin, Ireland
e-mail: bert.gordijn@dcu.ie

M. Loi
Digital Society Initiative, University of Zurich, Zurich, Switzerland

Institute of Biomedical Ethics and History of Medicine, Zurich, Switzerland
e-mail: michele.loi@uzh.ch

M. Christen et al. (eds.), *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology 21,
https://doi.org/10.1007/978-3-030-29053-5_1

privacy. However, neglecting cybersecurity could undermine citizens' trust and confidence in the digital infrastructure, in policy makers and in state authorities. Thus, cybersecurity supports the protection of values such as nonmaleficence, privacy and trust, and therefore imposes a complex relationship among values: some may be supportive and others conflicting, depending on context. For example, whereas cybersecurity is in most cases a precondition to protect data and thus the privacy of people, it may also make private information more accessible to cybersecurity experts, in order to detect malicious activities.

Understanding this and other value dilemmas has become imperative, yet cybersecurity is still an under-developed topic in technology ethics. Although there are numerous papers discussing issues such as 'big data' and privacy, cybersecurity is—if at all—only discussed as a tool to protect (or undermine) privacy. Nevertheless, cybersecurity raises a plethora of ethical issues such as 'ethical hacking', dilemmas of holding back 'zero day' exploits, weighting data access and data privacy in sensitive health data, or value conflicts in law enforcement raised by encryption algorithms. For example, a governmental computer emergency response team (CERT) may fight a ransomware attack by turning off the payment servers and destroying the business model of the attackers to prevent future attacks—but this means that people whose data already has been encrypted would never retrieve it. A medical implants producer may want to protect the data transfer between implant and receiver server by means of suitable cryptology—but this significantly increases the energy consumption of the implant and frequently requires more surgeries for battery exchange. Finally, a white hat hacker may discover a dangerous vulnerability in an IoT device and inform the manufacturer—but the company does not attempt to correct the error and the hacker considers how to generate public attention for the case. Such issues are usually discussed in an isolated manner, whereas a coherent and integrative view on the ethics of cybersecurity is missing. Only a few authors such as Kenneth Einar Himma (2005, 2008) have worked systematically on the ethical issues of cybersecurity for a longer time, and recent authors on this topic have focused on more specific issues such as cyberwar (Lucas 2017; Taddeo and Glorioso 2017). A rare example of broader coverage of the topic is Manjikian (2017).

This book aims to provide the first systematic collection of the full plethora of ethical aspects of cybersecurity. It results from the research activities of the CANVAS Consortium—Constructing an Alliance for Value-driven Cybersecurity—that unified technology developers with legal and ethical scholar and social scientists to approach the challenge of how cybersecurity can be aligned with European values and fundamental rights. The project was funded by the European Commission and aimed to bring together stakeholders from key areas of the European Digital Agenda—business/finance, the health system and law enforcement/national security—in order to discuss challenges and solutions when aligning cybersecurity with ethics. A special focus of CANVAS was on raising the awareness of the ethics of cybersecurity through teaching in academia and industry.

In a series of four White Papers, the CANVAS consortium provides an extensive overview of the discourse of ethical, legal and social aspects of cybersecurity. The first White Paper 'Cybersecurity and Ethics' outlines how the ethical discourse on cybersecurity has developed in the scientific literature, which ethical issues have

gained interest, which value conflicts are being discussed, and where the 'blind spots' are in the current ethical discourse on cybersecurity (Yaghmaei et al. 2017). Here, an important observation is that the ethics of cybersecurity is not yet an established subject. In all domains, cybersecurity is recognised as being an instrumental value, not an end in itself, which opens up the possibility of trade-offs with different values in different spheres. The most prominent common theme is the existence of trade-offs and even conflicts between reasonable goals, for example between usability and security, accessibility and security, and privacy and convenience. Other prominent common themes are the importance of cybersecurity to sustain trust (in institutions) and the harmful effect of any loss of control over data.

The second White Paper 'Cybersecurity and Law' explores the legal dimensions of the European Union's value-driven cybersecurity policy (Jasmontaite et al. 2017). It identifies the main critical challenges in this area and discusses specific controversies concerning cybersecurity regulation. The White Paper recognises that legislative and policy measures within the cybersecurity domain challenge EU fundamental rights and principles, stemming from EU values. Annexes provide a review of EU soft-law measures, EU legislative measures, cybersecurity and criminal justice affairs, the relationship of cybersecurity to privacy and data protection, cybersecurity definitions in national cybersecurity strategies, and brief descriptions of EU values.

The third White Paper 'Attitudes and Opinions regarding Cybersecurity' summarises the currently available empirical data regarding the attitudes and opinions of citizens and state actors regarding cybersecurity (Wenger et al. 2017). The data emerges from the reports of EU projects, Eurobarometer surveys, policy documents of state actors and additional scientific papers. It describes what these stakeholders generally think, what they feel and what they do about cyber threats and security (counter)measures.

Finally, the fourth White Paper 'Technological Challenges in Cybersecurity' summarises the current state of discussion regarding the main technological challenges in cybersecurity and their impact, including ways and approaches to address them, on key fundamental values (Domingo-Ferrer et al. 2017).

These White Papers serve as a baseline for this volume, which involves the contributions of CANVAS researchers as well as those of external experts. The first part of the volume outlines the general problems associated with the ethics of cybersecurity. This involves defining the basic technical concepts of cybersecurity, the values affected by cybersecurity, and the ethical and legislative framework, with a particular focus on Europe. The second part of the volume introduces a variety of ethical questions raised in the context of cybersecurity. The contributions are mostly structured along the major domains of interest that were investigated in the CANVAS project: business/finance, the health system, and law enforcement/national security. The last part of the volume is dedicated to recommendations in order to tackle some of the ethical challenges of cybersecurity. Overall, given the broad scope of the topics addressed in this book, it will not only be relevant for scholars focusing on philosophy and the ethics of technology. Many practitioners in cybersecurity—providers of security software, CERTs or Chief Security Officers in companies—are increasingly aware of the ethical dimensions of their work. We therefore hope that the practical focus of this book will also help those experts to not only gain awareness

of the ethics of cybersecurity but also provide them with the concepts and tools to tackle them.[1]

As cybersecurity is a quickly evolving domain, this book will not provide a complete overview of all relevant topics. Emerging issues concern, for example, cybercurrencies or the role of artificial intelligence (AI) in cybersecurity. The latter will become important both as a tool to complement the toolset for defending against attacks (e.g., for supervising large networks) as well as for more efficient attacks. AI may also become a dangerous tool for very new kinds of attacks (e.g. for learning instabilities in electronic stock markets and providing buy/sell 'signals' that destabilise the stock market). Furthermore, 'hacking' AI systems—which in the future may play important roles such as in autonomous driving—through compromised data may also become an increasingly relevant issue for cybersecurity. In addition, as processes and interactions in many social spheres increasingly rely on ICT systems, traditional security issues interfere with cybersecurity issues in domains such as food-security or migration and security. In this book, we only cover a few of these emerging issues, such as the danger of 'hacking democracy' through ICT-mediated means such as deep fakes and botnets (see Chaps. 11 and 12) and partly AI threads related to critical infrastructure (Chap. 8). Others should become topics of a new book, perhaps with more emphasis on autonomous decision-making systems and machine learning.

1.1 Explaining the Foundations

In the first chapter, *Dominik Herrmann* and *Henning Pridöhl* provide a technical introduction to the topic of this book. In this chapter, they review the fundamental concepts of cybersecurity by explaining common threats to information and systems to illustrate how matters of security can be addressed with methods from risk management. They also describe typical attack strategies and principles for defence. They review cryptographic techniques, malware and two common weaknesses in software: buffer overflows and SQL injections. This is followed by selected topics from network security, namely reconnaissance, firewalls, Denial of Service attacks and Network Intrusion Detection Systems. Finally, they review techniques for continuous testing, stressing the need for a free distribution of dual-use tools.

Ibo van de Poel then provides an introduction into the core values and value conflicts in cybersecurity. He does so by distinguishing four important value clusters that should be considered by deciding about cybersecurity measures: security, privacy, fairness and accountability. Each cluster consists of a range of further values that may be seen as articulating specific moral reasons relevant in devising cybersecurity measures. Following this introduction, potential value conflicts and value tensions are discussed as well as possible methods for dealing with these conflicts.

The next chapter by *Michele Loi* and *Markus Christen* provides an in-depth discussion of ethical frameworks for cybersecurity. These include the principlist frame-

[1] For doing this, the CANVAS project has also created a whole spectrum of practical tools such as briefing material, a reference curriculum on the ethics of cybersecurity including teaching material, and a Massive Open Online Course. This material is available on the CANVAS website www.canvas-project.eu.

work employed in the Menlo Report on cybersecurity research and the rights-based principle that is influential in the law, in particular EU law. The authors show that since the harms and benefits caused by cybersecurity operations and policies are of a probabilistic nature, both approaches cannot avoid dealing with risk and probability. Therefore, the ethics of risk is introduced in several variants as a necessary complement to such approaches. They propose a revised version of this framework for identifying and ethically assessing changes brought about by cybersecurity measures and policies, not only in relation to privacy but more generally to the key expectations concerning human interactions within the practice.

Finally, *Gloria González Fuster* and *Lina Jasmontaite* introduce the legislative framework for cybersecurity. The authors provide an overview of the current and changing legal framework for regulating cybersecurity with a particular focus on the new EU Data Protection Regulation. By invoking a historical perspective, the chapter analyses the policy developments that have shaped the cybersecurity domain in the EU. It reviews the mobilisation of multiple domains (such as the regulation of electronic communications, critical infrastructures and cybercrime) in the name of cybersecurity imperatives, and explores how their operationalisation surfaced in the EU cybersecurity strategy. It highlights how the perception of cybersecurity's relation with (national) security play a determinant role in EU legislative and policy debates, whereas fundamental rights considerations are only considered to a limited extent.

1.2 Outlining the Problems

The chapter by *Gwenyth Morgan* and *Bert Gordijn* provides a care-based stakeholder approach to the ethics of cybersecurity in business. After sketching the main ethical issues discussed in the academic literature, the chapter aims to identify some important topics that have not yet received the attention they deserve. The chapter then focuses on one of those topics, namely ransomware attacks, one of the most prevalent cybersecurity threats to businesses today. Using Daniel Engster's care-based stakeholder approach, the responsibilities that businesses have to their stakeholders are analysed—in particular with respect to patching identified vulnerabilities and paying the ransom.

Karsten Weber and *Nadine Kleine* investigate in their chapter the specific ethical issues of cybersecurity in health care. Using the approach of principlism, enhanced with additional values, they demonstrate how value conflicts can emerge in that domain and they provide possible solutions. With the help of implantable medical devices and the electronic Health Card as case studies, they show that these conflicts cannot be eliminated but must be reconsidered on a case-by-case basis.

The cybersecurity of critical infrastructures is analysed in the chapter of *Eleonora Viganò*, *Michele Loi* and *Emad Yaghmaei*. They provide a political and philosophical analysis of the values at stake in ensuring cybersecurity for national infrastructure. Based on a review on the boundaries of national security and cybersecurity with a focus on the ethics of surveillance for protecting critical infrastructure and the use of AI, they apply a bibliographic analysis of the literature until 2016 to identify and discuss the cybersecurity value conflicts and ethical issues in national security. This

is integrated with an analysis of the most recent literature on cyber-threats to national infrastructure and the role of AI. They show that the increased connectedness of digital and non-digital infrastructure enhances the trade-offs between values identified in the literature of the past years.

In the next chapter *David-Olivier Jaquet-Chiffelle* and *Michele Loi* discuss an inherent ethical issue of cybersecurity: ethical and unethical hacking. They provide a conceptual analysis of ethical hacking, including its history, in order to provide a systematic classification of hacking. They conclude by suggesting a pragmatic best-practice approach for characterising ethical hacking, which reaches beyond business-friendly values and helps with taking decisions respectful of the hackers' individual ethics in morally debatable, grey zones.

The interrelation of cybersecurity and the state is then investigated in the chapter by *Eva Schlehahn*. The author provides an overview of state actor's opinions and strategies relating to cybersecurity matters, with a particular focus on the EU. Furthermore, the role of the new European data protection framework is addressed, while it is explained why data protection also has a close relationship to cybersecurity matters. The main tensions and conflicts in relation to IT and cybersecurity are depicted, which evolve primarily around the frequently negative effect on the rights of data subjects that IT and cybersecurity measures have. In particular, the issue of governmental surveillance is addressed, with its implications for the fundamental rights of European citizens.

Seumas Miller then approaches this political dimension by analysing the tricky balance between freedom of communication and security in the cyber domain. The author provides definitions of fake news, hate speech and propaganda, and shows how these phenomena are corruptive for epistemic norms. He elaborates on the right to freedom of communication and its relation both to censoring propaganda and to the role of epistemic institutions, such as a free and independent press and universities. Finally, he discusses the general problem of countering political propaganda in cyberspace.

The contribution of *George Lucas* goes in a similar direction, but he particularly discusses the case that increasingly, state actors undermine cybersecurity, broadly construed by both propaganda and other types of cyber operations. He presents the current cyber domain as a Hobbesian state of nature, a domain of unrestricted conflict constituting a "war of all against all". The fundamental ethical dilemma in Hobbes's original account of this 'original situation' was how to establish a more stable political arrangement, comprising a rule of law under which the interests of the various inhabitants in life, property and security would be more readily guaranteed. The author discusses how to achieve an acceptance of general norms of responsible individual and state behaviour within the cyber domain, arising from experience and consequent enlightened self-interest.

Finally, *Reto Inversini* proposes focusing on 'cyberpeace' as a guiding principle in cybersecurity. He analyses elements of cyber conflicts and attacks, defines the term cyber peace and identifies the components that make such a state possible. The chapter closes with an assessment of the different roles and responsibilities of stakeholders to reach and preserve a state of peace in the digital sphere.

1.3 Presenting Recommendations

The first chapter of the final part is dedicated to technological means. *Josep Domingo-Ferrer* and *Alberto Blanco-Justicia* review the entire spectrum of privacy-enhancing techniques (PET). They first enumerate design strategies and then move to privacy-enhancing techniques that directly address the *hide* strategy but also aid in implementing the *separate*, *control* and *enforce* strategies. Specifically, they consider PETs for: (1) identification, authentication and anonymity; (2) private communications; (3) privacy-preserving computations; (4) privacy in databases; and (5) discrimination prevention in data mining.

The next chapter outlines some concrete best practices and recommendations for cybersecurity service providers. Based on a brief outline of dilemma that cybersecurity service providers may experience in their daily operations, *Alexey Kirichenko*, *Markus Christen*, *Florian Grunow* and *Dominik Herrmann* discuss data handling policies and practices of cybersecurity vendors along the following five topics: customer data handling, information about breaches, threat intelligence, vulnerability-related information and data involved when collaborating with peers, CERTs, cybersecurity research groups, etc. They also include a discussion of specific issues of penetration testing such as customer recruitment and execution as well as the supervision and governance of penetration testing. The chapter closes with some general recommendations regarding improving the ethical decision-making procedures of private cybersecurity service providers.

Salome Stevens then analyses a highly debated strategy of businesses to counteract cyber threats: hacking back. Several security experts call for a more active cyber-defence of companies, including offensive actions in cyberspace taken with defensive purposes in mind. The lack of legal regulations, however, raises insecurities over the legal scope of action of private companies. The authors investigate questions such as: When is a private company allowed to act? When by such an act could it itself be implicated into committing illegal actions? The chapter concludes by giving recommendations for companies on how to define ethical cyber-defence within their security strategy.

How the awareness for cybersecurity can be enhanced in health care is then discussed by *David Koeppe*. Given that the medical domain is characterised by special processing situations and, in particular, by the very high protection requirements of data and processes, cybersecurity is a must and requires the setup of proper information security management systems. The authors discuss the key requirements of such management systems—also given the requirements of the new EU data protection regulation.

Finally, *Paul Meyer* discusses norms of responsible state behaviour in cyberspace. The chapter sketches the increasing 'militarisation' of cyberspace as well as the diplomatic efforts undertaken to provide this unique environment with some 'rules of the road'. The primary mechanism for discussing possible norms of responsible state behaviour has been a series of UN Groups of Governmental Experts which have produced three consensus reports over the last decade. The author calls for renewed efforts to promote responsible state behaviour that will require greater

engagement on the part of the private sector and civil society, both of which have a huge stake in sustaining cyber peace.

In conclusion, it is our sincere hope that this book enables the reader to gain a broad understanding of the various ethical issues associated with cybersecurity. We close by expressing our gratitude to the two anonymous reviewers of this manuscript, who provided helpful comments, and to Edward Crocker, proof reader of Cambridge Proofreading & Editing LLC. This book has been supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540 and the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. We are thankful to our funding institutions.

References

Domingo-Ferrer J, Blanco A, Arnau P et al (2017) Canvas White Paper 4 – Technological Challenges in Cybersecurity SSRN. https://ssrn.com/abstract=3091942 or https://doi.org/10.2139/ssrn.3091942. Last access 7 July 2019

Himma KE (2005) Internet security: hacking, counterhacking, and society. Jones and Bartlett Publishers, Inc., Missisauga

Himma KE, Tavani HT (eds) (2008) The handbook of information and computer ethics. Wiley, Hoboken

Jasmontaite L, González FG, Gutwirth S et al (2017) Canvas White Paper 2 – Cybersecurity and Law. SSRN. https://ssrn.com/abstract=3091939 or https://doi.org/10.2139/ssrn.3091939. Last access 7 July 2019

Lucas G (2017) Ethics and cyber warfare: the quest for responsible security in the age of digital warfare. Oxford University Press, New York, p 187

Manjikian M (2017) Cybersecurity ethics: an introduction. Routledge, London/New York

Taddeo M, Glorioso L (eds) (2017) Ethics and policies for cyber operations. Springer, Cham

Wenger F, Jaquet-Chiffelle DO, Kleine N et al (2017) Canvas, White Paper 3 – Attitudes and Opinions Regarding Cybersecurity. SSRN. https://ssrn.com/abstract=3091920 or https://doi.org/10.2139/ssrn.3091920. Last access 7 July 2019

Yaghmaei E, van de Poel I, Christen M et al (2017) Canvas White Paper 1 – Cybersecurity and Ethics. SSRN. https://doi.org/10.2139/ssrn.3091909. Last access 7 July 2019