The International Library of Ethics, Law and Technology 21

Markus Christen
Bert Gordijn
Michele Loi *Editors*

The Ethics of Cybersecurity

Springer Open

The International Library of Ethics, Law and Technology

Volume 21

Technologies are developing faster and their impact is bigger than ever before. Synergies emerge between formerly independent technologies that trigger accelerated and unpredicted effects. Alongside these technological advances new ethical ideas and powerful moral ideologies have appeared which force us to consider the application of these emerging technologies. In attempting to navigate utopian and dystopian visions of the future, it becomes clear that technological progress and its moral quandaries call for new policies and legislative responses. Against this backdrop this new book series from Springer provides a forum for interdisciplinary discussion and normative analysis of emerging technologies that are likely to have a significant impact on the environment, society and/or humanity. These will include, but be no means limited to nanotechnology, neurotechnology, information technology, biotechnology, weapons and security technology, energy technology, and space-based technologies.

More information about this series at http://www.springer.com/series/7761

Markus Christen • Bert Gordijn • Michele Loi
Editors

The Ethics of Cybersecurity

Springer Open

Editors
Markus Christen
UZH Digital Society Initiative
Zürich, Switzerland

Bert Gordijn
Dublin City University
Dublin, Ireland

Michele Loi
Digital Society Initiative
University of Zurich
Zürich, Switzerland

ISSN 1875-0044 ISSN 1875-0036 (electronic)
The International Library of Ethics, Law and Technology
ISBN 978-3-030-29052-8 ISBN 978-3-030-29053-5 (eBook)
https://doi.org/10.1007/978-3-030-29053-5

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

1 **Introduction** 1
Markus Christen, Bert Gordijn, and Michele Loi

Part I Foundations

2 **Basic Concepts and Models of Cybersecurity** 11
Dominik Herrmann and Henning Pridöhl

3 **Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security** 45
Ibo van de Poel

4 **Ethical Frameworks for Cybersecurity** 73
Michele Loi and Markus Christen

5 **Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights** 97
Gloria González Fuster and Lina Jasmontaite

Part II Problems

6 **A Care-Based Stakeholder Approach to Ethics of Cybersecurity in Business** 119
Gwenyth Morgan and Bert Gordijn

7 **Cybersecurity in Health Care** 139
Karsten Weber and Nadine Kleine

8 **Cybersecurity of Critical Infrastructure** 157
Eleonora Viganò, Michele Loi, and Emad Yaghmaei

9 **Ethical and Unethical Hacking** 179
David-Olivier Jaquet-Chiffelle and Michele Loi

10 Cybersecurity and the State 205
Eva Schlehahn

11 Freedom of Political Communication, Propaganda and the Role of Epistemic Institutions in Cyberspace 227
Seumas Miller

12 Cybersecurity and Cyber Warfare: The Ethical Paradox of 'Universal Diffidence' 245
George Lucas

13 Cyber Peace: And How It Can Be Achieved 259
Reto Inversini

Part III Recommendations

14 Privacy-Preserving Technologies 279
Josep Domingo-Ferrer and Alberto Blanco-Justicia

15 Best Practices and Recommendations for Cybersecurity Service Providers 299
Alexey Kirichenko, Markus Christen, Florian Grunow, and Dominik Herrmann

16 A Framework for Ethical Cyber-Defence for Companies 317
Salome Stevens

17 Towards Guidelines for Medical Professionals to Ensure Cybersecurity in Digital Health Care 331
David Koeppe

18 Norms of Responsible State Behaviour in Cyberspace 347
Paul Meyer

Appendix 361

Index 377

About the Contributors

Alberto Blanco-Justicia is a Postdoctoral Researcher at Universitat Rovira i Virgili. He obtained his MSc in Computer Security in 2013 from Universitat Rovira i Virgili, and his PhD in Computer Engineering and Mathematics of Security from the same university in 2017, with a thesis focused on the reconciliation of privacy, security and functionality in e-commerce applications. His research interests include data privacy, data security and cryptographic protocols. He has been involved in several European and national Spanish research projects, as well as technology transfer contracts.

Markus Christen is a Research Group Leader at the Institute of Biomedical Ethics and History of Medicine and Managing Director of the UZH Digital Society Initiative. He received his MSc in Philosophy, Physics, Mathematics and Biology from the University of Berne, his PhD in Neuroinformatics from the Federal Institute of Technology in Zurich and his Habilitation in Bioethics from the University of Zurich. His research interests include empirical ethics, neuroethics, ICT ethics and data analysis methodologies.

Josep Domingo-Ferrer is the Distinguished Professor of Computer Science and an ICREA-Acadèmia Researcher at Universitat Rovira i Virgili, Tarragona, Catalonia, where he holds the UNESCO Chair in Data Privacy and is the founding director of CYBERCAT-Center for Cybersecurity Research of Catalonia. He received his MSc and PhD degrees in Computer Science from the Autonomous University of Barcelona. He also holds an MSc in Mathematics. His research interests include data privacy, data security, statistical disclosure control and cryptographic protocols, with a focus on the conciliation of privacy, security and functionality. He is an IEEE Fellow, an ACM Distinguished Scientist and an elected member of Academia Europaea.

Gloria González Fuster is a Research Professor in the Faculty of Law and Criminology at the Vrije Universiteit Brussel (VUB). She is Co-Director of the Law, Science, Technology and Society (LSTS) Research Group, and a member of

the Brussels Privacy Hub (BPH); she investigates legal issues related to privacy, personal data protection and security, and teaches 'Data Policies in the European Union' at the Data Law option of the Master of Laws in International and European Law (PILC) of VUB's Institute for European Studies (IES). She studied law at the Universidad Nacional de Educación a Distancia (UNED), journalism in the Faculty of Communication Sciences of the Universidad Autónoma de Barcelona (UAB) (including a stay at the Université Paris VIII) and modern languages and literature at the Université Libre de Bruxelles (ULB).

Bert Gordijn has been a Full Professor and Director of the Institute of Ethics at Dublin City University (Ireland) since 2008. He is a Visiting Professor at Lancaster University (UK), Georgetown University (USA), the National University of Singapore, the Fondation Brocher (Switzerland), Yenepoya University (India) and the University of Otago (New Zealand). He has served on advisory panels and expert committees of the European Chemical Industry Council, the European Patent Organisation, the Irish Department of Health and UNESCO. He is currently the Secretary of the European Society for Philosophy of Medicine and Healthcare and President of the International Association of Education in Ethics.

Florian Grunow is a Security Analyst and currently CEO of ERNW GmbH, Heidelberg, Germany. He holds a Master of Science degree in computer science with a focus on software engineering and a Bachelor of Science degree in medical computer sciences. He is committed to practical security education, both internally at ERNW and by giving public talks.

Dominik Herrmann is a Full Professor of Privacy and Security in Information Systems at University of Bamberg (Germany). Prior to this, he was a Temporary Professor at the University of Siegen between October 2015 and March 2017. He holds a PhD in Computer Science (University of Hamburg, 2014) and a Diploma with Honors in Management Information Systems (University of Regensburg, 2008). He has received a series of awards, including the GI-Dissertationspreis 2014 for the best computer science dissertation in Germany. He was also named a Junior Fellow of the German Computer Science Society for his services to the profession.

Reto Inversini studied Geography at the University of Berne and Information Technology at the University of Applied Sciences in Berne. He worked for Amnesty International as a network and systems engineer and for the Swiss Federal Administration as a security architect. He currently works as a malware analyst and security officer for the Swiss Governmental CERT (GovCERT.ch). He is a part-time lecturer at the University of Applied Sciences in Bern in the domains of network engineering and information security. His focus lies on network intrusion detection and malware analysis. It is important to him that core values of our society such as individual responsibility, democracy, freedom of speech and privacy are preserved while increasing the security of the Internet.

David-Olivier Jaquet-Chiffelle is a Full Professor at the School of Criminal Justice, University of Lausanne, Switzerland. He is the head of the Master programme in forensic science, orientation digital investigation and identification. He accomplished his PhD in Mathematics at the University of Neuchâtel, Switzerland. He spent a post-doc at Harvard University (Boston, USA). He then strengthened his experience in cryptology while working for the Swiss government at the Swiss Federal Section of Cryptology. He has a long experience in projects related to identity, security and privacy. His current research includes cybercrime, security and privacy, and new forms of identities in the information society, as well as authentication, anonymisation and identification processes, especially in the digital world.

Lina Jasmontaite is a PhD candidate at the Vrije Universiteit Brussel. She joined the Law, Science, Technology and Society (LSTS) Research Group in September 2016. Currently, she works on the awareness raising project under the Rights, Equality and Citizenship Programme 2014–2020 titled 'Support Small and Medium Enterprises on the Data Protection Reform II' (STARII). Under the supervision of Professor Gloria González Fuster, she contributed to the Horizon 2020 project titled 'Constructing an Alliance for Value-driven Cybersecurity' (CANVAS). She is also a Contributing Fellow at the Brussels Privacy Hub, where she explores the legal implications of new technologies that are being operationalised in humanitarian practice. Her PhD research concerns primarily the interaction between data breach notification obligations foreseen in the General Data Protection Regulation and the Network and Information Security Directive.

Alexey Kirichenko received his MSc in Mathematics from Leningrad (St. Petersburg) State University, Russia, and completed his PhD in Theoretical Computer Science at Aalto University, Finland. He joined F-Secure in 1997 and was for a long time leading the development of the company's cryptographic modules and authorisation infrastructure. Since 2007, he has been working as Research Collaboration Manager, coordinating F-Secure's participation in European and Finnish national research collaboration projects. He represents F-Secure in WG6 of European Cyber Security Organisation (ECSO) and significantly contributed in the ECSO SRIA preparation. Prior to joining F-Secure, he worked in the Computer Graphics area at Altsys Corp., and prior to this he lectured in mathematical courses at St. Petersburg Electro-Technical University. He is actively involved in training the Finnish national team for the International Mathematical Olympiad.

Nadine Kleine studied sociology and political science at the University of Potsdam, Germany, as well as cultural sciences with a focus on technology at the BTU Cottbus-Senftenberg, Germany. She was a Research Associate at the Institute for Social Research and Technology Assessment (IST), Regensburg University of Applied Studies, where she worked on the H2020 project "Constructing an Alliance for Value-driven Cybersecurity" (CANVAS) concerning issues of cyber security and ethics in healthcare. Currently, she researches worker's autonomy and

acceptance of digital technologies in the work environment as a member of the doctoral research group "Trust and Acceptance in Augmented and Virtual Working Environments" (va-eva) and is involved in the project "Teamwork 4.0" at the Department of Economic and Industrial Sociology, both at the University of Osnabrueck.

David Koeppe studied economics at the Free University of Berlin (Diplom-Kaufmann) and has worked in various positions in hospitals since 1995. As Privacy Officer of the Vivantes Group (Netzwerk für Gesundheit GmbH), he is intensively involved with all facets of data protection in the health care sector. Within the framework of the society 'Gesellschaft für Datenschutz und Datensicherheit e.V.' (Society for Data Protection and Data Security), he is leading the working group 'Data Protection and Data Security in Health and Social Services' and the regional experience exchange group in Berlin. He is the co-editor of the *Handbuch Datenschutz und Datensicherheit im Gesundheits und Sozialwesen* (Datakontext, 2016) and co-author of a number of published data protection tools.

Michele Loi (PhD, Luiss Guido Carli) is an applied philosopher working at the intersection between digital ethics and bioethics. Besides researching the ethics of cybersecurity, he is also interested in fairness and transparency in machine learning and in the regulation access and use to big data in health. Currently, he is affiliated as Postdoctoral Researcher with the Digital Ethics Lab, Digital Society Initiative and with the Institute of Biomedical Ethics and the History of Medicine (both University of Zurich). His research on the ethics of cybersecurity has been funded by the CANVAS project, the same H2020 project funding the project of this book.

George Lucas is retired as Distinguished Chair of Ethics at the US Naval Academy (Annapolis, Maryland). He is a Senior Fellow at the Stockdale Center for Leadership and Ethics at US Naval Academy. His most recent book is *Ethics and Military Strategy in the 21st-Century: Moving Beyond Clausewitz* (Routledge, 2019).

Paul Meyer is Fellow in International Security and Adjunct Professor of International Studies at Simon Fraser University and a Senior Fellow with The Simons Foundation in Vancouver, Canada. He is also a Senior Advisor with ICT4Peace, an NGO devoted to preserving a peaceful cyberspace. Previously, he had a 35-year career with the Canadian Foreign Service, including serving as Canada's Ambassador to the United Nations and to the Conference on Disarmament in Geneva (2003–2007). He writes on issues of nuclear non-proliferation and disarmament, space security and the diplomacy of international cyber security.

Seumas Miller holds research positions at Charles Sturt University, Technical University Delft and the University of Oxford. He is the author or co-author of 20 books, including *Social Action* (CUP, 2001), *Moral Foundations of Social Institutions* (CUP, 2010), *Terrorism and Counter-terrorism* (Blackwell, 2009), *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force* (OUP, 2016)

and *Institutional Corruption* (CUP, 2017), and of over 200 academic articles. He is currently working on a co-authored book on the ethics of cybersecurity with a computer scientist, Terry Bossomaier.

Gwenyth Morgan is a PhD candidate at the ADAPT Centre for Digital Content Technologies and at the Institute of Ethics in All Hallows Drumcondra. She is conducting her research on the topic of ethically appropriate business responses to ransomware attacks and data breaches. Her work encompasses ethics and cybersecurity, ranging from ethical issues in cybersecurity relating to dataveillance, hacking back and the use of AI, to the dynamic and ambiguous relationship between businesses and security researchers, i.e., white hats, grey hats and black hats. She aims to open up the field of ethics and cybersecurity research in such a way that business ethics theories such as stakeholder theory can be used to practically establish how businesses can ethically manage and respond to issues that arise in cybersecurity. She teaches bachelor's and master's students at the Dublin City University on the topics of applied ethics, ethics of technology and health care ethics.

Henning Pridöhl is a Research and Teaching Assistant in the Privacy and Security in Information Systems Group at University of Bamberg. Prior to this, he was a Research Assistant in the Security in Distributed Systems Group at University of Hamburg. He holds an MSc in Computer Science from the University of Hamburg, where he graduated in 2016. He enjoys playing Capture The Flag security competitions and mentors young hackers in programming and IT security.

Eva Schlehahn is a Senior Legal Researcher and Consultant employed at Unabhängiges Landeszentrum für Datenschutz (ULD) in the German federal state of Schleswig-Holstein. Her work focuses on the requirements of the European General Data Protection Regulation (GDPR) and Privacy Enhancing Technologies (PETs). Since 2010, she has been working in various EC-funded FP7 and H2020 R&D projects focused on a multitude of data protection relevant topics. In her work, she has obtained a variety of know-how and experience related to topics such as cloud computing, identity and consent management, accessibility, UI design and usability, IT security, data privacy vocabularies and ontologies, data policy enforcement, surveillance technologies, requirements analysis and conceptualisation. Her research interests include interdisciplinary requirements analysis, balancing and evaluation, specifically considering Privacy by Design solutions.

Salome Stevens is a Teaching and Research Fellow at the Department of Criminal Law of the University of Zurich. She is pursuing her PhD on the subject of cybersecurity. Before joining the university, she worked as a Legal and Political Advisor for the Federal Department of Foreign Affairs and the Police Force, as well as for the private sector and the United Nations. She also supported several NGOs in their mandate to prevent international crime and fight impunity. Throughout her professional development, she has lived in Switzerland, Italy, Israel and the United Arab Emirates.

Ibo van de Poel is Anthoni van Leeuwenhoek Professor in Ethics and Technology and head of the Department of Values, Technology and Innovation at the Faculty of Technology, Policy and Management at the Technical University Delft in the Netherlands. He has published on engineering ethics, the moral acceptability of technological risks, design for values, responsible innovation, moral responsibility in research networks, ethics of newly emerging technologies and the idea of new technology as a social experiment. He has recently received an ERC Advanced grant for 'Design for changing values: a theory of value change in sociotechnical systems'.

Eleonora Viganò is a Postdoctoral Researcher at the Institute of Biomedical Ethics and History of Medicine and at the Digital Society Initiative of the University of Zurich. Her research is funded by the Cogito Foundation and the CANVAS project. She is a Moral Philosopher with a strong interest in the neuroscience of ethics. Her research interests include intrapersonal conflicts of values, the morality of prudence, and the implications for ethics of the neuroscientific discoveries on decision making. She has recently started working on ethical trade-offs in cybersecurity and on trust and transparency in machine learning algorithms.

Karsten Weber studied philosophy, informatics and sociology at University Karlsruhe (TH), Germany, and from 1996 to 1999 worked there as a Junior Researcher. After his doctorate in 1999, from 1999 to 2008 he was a Senior Researcher at European University Viadrina in Frankfurt (Oder), Germany. From 2006 to 2012, he worked as a Professor of Philosophy at University Opole, Poland. Since 2007, he has held an honorary professorship for Culture and Technology at BTU Cottbus-Senftenberg, Germany. At TU Berlin from 2008 to 2009, he was a Professor for Information Ethics and Data Protection and from 2009 to 2011 Professor for Computer Science and Society. From 2011 to 2016, he was Chair for General Science of Technology at BTU Cottbus-Senftenberg. Since 2013, Prof. Weber has taught technology assessment at OTH Regensburg, Germany and is co-head of the Institute for Social Research and Technology Assessment (IST) and one of the three directors of the Regensburg Center of Health Sciences and Technology (RCHST).

Emad Yaghmaei is a Senior Researcher at the Faculty of Technology, Policy and Management at the Technical University Delft. His research interests include the innovation management issues arising from the intersections of science, technology and society. The emphasis of his research and consulting is on innovation and technology management of emerging technologies such as ICT, the Internet of Things, nanotechnology and so on to identify and work on the social impacts of these technologies. He has been working on monitoring industry business innovation across non-financial values. He is currently focusing on Responsible Research and Innovation (RRI) principles in an industrial context to demonstrate how industry can work productively together with societal actors and integrate methodologies of RRI into research and innovation processes.

Acronyms and Abbreviations

ACM	Association for Computing Machinery
AI	Artificial Intelligence
APT	Advanced Persistent Threat
ASLR	Address Space Layout Randomization
AV	Anti Virus
C&C	Command and Control
CA	Certification Authority
CANVAS	Constructing an Alliance for Value-driven Cybersecurity
CCC	Convention on Cyber Crime
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
CFI	Control-Flow Integrity
CFSP	Common Foreign and Security Policy
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés
CoE	Council of Europe
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DNS	Domain Name System
DPI	Deep Packet Inspection
DPIA	Data Protection Impact Assessment
EC	European Commission
ECHR	European Convention of Human Rights
ECSO	European Cyber Security Organisation
ECHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EFF	Electronic Frontier Foundation
eHC	electronic Health Card
ENISA	European Network and Information Security Agency
EU	European Union
FRS	Face Recognition System

GAFAM	Google, Apple, Facebook, Amazon and Microsoft
GDPR	General Data Protection Regulation
GGE	Group of Governmental Experts
HTTP	Hypertext Transfer Protocol
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
IMD	Implantable Medical Device
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISP	Internet Service Providers
ITU	International Telecommunication Union
LEA	Law Enforcement Agency
MAC	Message Authentication Code
MDR	Medical Device Regulation
MitM	Man in the Middle
NATO	North Atlantic Treaty Organization
NER	Named Entity Recognition
NIDS	Network Intrusion Detection Systems
NIS	Network and Information Security
NSA	National Security Agency (USA)
OJ	Official Journal of the European Communities
OSCE	Organization for Security and Cooperation in Europe
PGP	Pretty Good Privacy
PPDM	Privacy-Preserving Data Mining
QC	Quantum Computing
ROP	Return-Oriented Programming
SDC	Statistical Disclosure Control
SDM	Standard Data Protection Model
SME	Small and Medium Enterprises
SOST	Surveillance-Oriented Security Technology
SQL	Structured Query Language
TAO	Tailored Access Operations
T-CY	Cybercrime Convention Committee
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TLS	Transport Layer Security

List of Figures

Fig. 2.1 Safety versus security 15
Fig. 2.2 Relationship between vulnerability and risk 16
Fig. 2.3 Example of a C program with a buffer overflow vulnerability 29
Fig. 2.4 Login source code fragment of a PHP program that is vulnerable to SQL injections 31
Fig. 2.5 PHP code with a prepared statement to protect against SQL injection attacks 32

Fig. 3.1 Value tensions in cybersecurity. (Reproduced from Christen et al. 2017) 61

Fig. 7.1 Technical aims mapping to ethical principles 144

Fig. 9.1 Word cloud around 'hackers' 181
Fig. 9.2 Shift in the hackers' incentives 182
Fig. 9.3 White hats, black hats, grey hats and script kiddies 183
Fig. 9.4 A third dimension to represent true hackers and hacktivists 184
Fig. 9.5 A societal dimension in hackers' incentives 185
Fig. 9.6 Crackers, pen testers and social engineering experts 190
Fig. 9.7 Ethical hackers 193
Fig. 9.8 Potential conflicts between collections of possibly competing ethical values 200

Fig. 10.1 Simplified overview of cybersecurity issues 217
Fig. 10.2 Data protection goals (darker grey) integrating the IT security goals (lighter grey) that require balancing 220

List of Tables

Table 2.1 A table in an SQL database that is used by an application vulnerable to SQL injections 30

Table 5.1 Definitions of cybersecurity in national cybersecurity strategies of EU Member States 105

Table 6.1 Ethical issues in cybersecurity in business 121

Table 8.1 The main ethical issues and value conflicts in the literature on national cybersecurity strategies 159

Table 8.2 Types of attacks on critical infrastructure 165

Table 9.1 A first classification based on expertise and legal goals 187

Table 9.2 Analogy between authentication technologies and criteria to classify hackers 188

Table 9.3 Similarities between authentication technologies and ethical evaluation parameters 200

Table 16.1 Application of a second layer of categorisation to cyber-defence 319

Table 17.1 Example of a protection needs matrix 337

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

Part I
Foundations

Chapter 2
Basic Concepts and Models of Cybersecurity

Dominik Herrmann and Henning Pridöhl

Abstract This introductory chapter reviews the fundamental concepts of cybersecurity. It begins with common threats to information and systems to illustrate how matters of security can be addressed with methods from risk management. In the following, typical attack strategies and principles for defence are reviewed, followed by cryptographic techniques, malware and two common weaknesses in software: buffer overflows and SQL injections. Subsequently, selected topics from network security, namely reconnaissance, firewalls, Denial of Service attacks, and Network Intrusion Detection Systems, are analysed. Finally, the chapter reviews techniques for continuous testing, stressing the need for a free distribution of dual-use tools. Although introductory in nature, this chapter already addresses a number of ethical issues. For instance, well-intended security mechanisms may have undesired side effects such as leaking sensitive information to attackers. As asymmetries and externalities are at the core of many security problems, devising effective security solutions that are adopted in practice is a challenge.

Keywords Advanced persistent threat · Availability · Black hats · Certificates · Confidentiality · Cryptography · Integrity · Malware · Supply-chain attack · Vulnerabilities · White hats

2.1 Introduction

Honesty was never a given in human history. In the physical world, we can rely on decades of experience to defend against malicious actors. We have devised sophisticated laws that govern what is acceptable and what is illegal. In addition, we have a number of technical means at our disposal to secure our property and our secrets.

D. Herrmann (✉) · H. Pridöhl
Privacy and Security in Information Systems Group (PSI), University of Bamberg, Bamberg, Germany
e-mail: dominik.herrmann@uni-bamberg.de; henning.pridoehl@uni-bamberg.de

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_2

However, we are still in the process of learning how to secure cyberspace. Cyberspace has become the handle of choice to refer to the virtual world created by networked computer systems that affect large parts of our lives; securing it is challenging. According to Bruce Schneier "complexity is the enemy of security" (Chan 2012). There are not only more devices hooked up to the Internet, but also more manufacturers building them, which increases both the size and diversity of the systems forming the cyberspace and thus the probability of failures.

Moreover, cybersecurity is subject to significant asymmetries. Attackers can choose from a large variety of approaches, while defenders have to pay attention to every detail and be prepared for anything at any time. Therefore, successful attacks are not necessarily the result of negligence. Sometimes security controls are in place but are not used properly, for instance, because they conflict with the needs of users. Given these difficulties, there is now much interest in reactive security, which embraces the insight that we cannot prevent all attacks.

In this chapter, we introduce the basic concepts of cybersecurity. We start by defining common threats in Sect. 2.2 and reviewing typical attack and defence techniques in Sect. 2.3. Subsequently, we present security fundamentals in various domains, namely cryptography for data security in Sect. 2.4, malware in Sect. 2.5, software security in Sect. 2.6 and network security in Sect. 2.7. Finally, we stress the importance of continuous testing in Sect. 2.8 before we conclude the chapter in Sect. 2.9.

2.2 Threats

Before we can discuss attacks and defences in cyberspace, we must clarify what is at stake. In the following, we review the fundamental protection goals that help us gain a comprehensive picture of all aspects of security.

Before the term 'cybersecurity' became fashionable, discussions focused on computer security. The goal of computer security is to protect assets. Valuable assets can be hardware (e.g. computers and smartphones), software and data. These assets are subject to threats that may result in loss or harm.

Computer security consists of information security and systems security. It is instructive to consider the foundations of these two fields, which laid the ground for cybersecurity. Information security is concerned with the protection of data (potentially processed by computers) and any information derived from its interpretation. In systems security, we aim to ensure that (computer) systems operate as designed; i.e. attackers cannot tamper with them.

2.2.1 Information Security

We begin our discussion of threats with information security. There are three protection goals in information security: confidentiality, integrity and availability (Anderson 1972; Voydock and Kent 1983), commonly referred to as the 'CIA triad' (the origin of this abbreviation is unknown). Security measures have the purpose of addressing one or more of these objectives, as follows:

- Confidentiality: prevent unauthorised information gain.
- Integrity: prevent or detect unauthorised modification of data.
- Availability: prevent unauthorised deletion or disruption.

These protection goals apply both to data at rest, i.e. stored on a computer or on paper, and to data in transit, i.e. when data is sent over a network. The definitions refer to 'unauthorised' activities, which implies that there is an understanding about which actors are supposed to be allowed to interact with the data.

In some scenarios, there is only one authorised actor. An example in the context of the protection goal confidentiality is a smartphone or a computer with encrypted storage (sometimes called 'full-disk encryption'). In this case, only the owner of the device is authorised. An example for the goal availability is to backup data so that it remains accessible when a machine fails.

Most of the time, there are several authorised actors; often there are precisely two. For instance, the protection goal confidentiality may be relevant when a sender sends an e-mail to a particular recipient. Confidentiality is also essential during online banking. Here, we also want integrity protection for the exchanged messages to avoid transactions being modified.

The three fundamental protection goals of confidentiality, integrity and availability refer to the content. Besides content, we may also be concerned with the identity of other actors. For instance, we would like to know when the sender of an e-mail message has been forged. The protection goal *authenticity* prevents actors from impersonating someone else, usually by providing others with a means to verify a claimed identity. A related and even stronger protection goal is *non-repudiation*, which prevents actors from denying that they carried out a particular act, for instance, sending a message. Authenticity and non-repudiation are necessary to hold actors accountable (Gollmann 2011: 38).

2.2.2 Systems Security

How should we design systems so that they provide security for data stored on them? This question is at the centre of systems security. Consequently, the protection goals that are pursued in systems security are the same ones as in information security.

Often there are multiple ways to achieve the desired goal. For instance, confidentiality can be achieved by encrypting data or by a combination of authentication (e.g. by requiring users to enter a password) and access control (rules that govern which user is allowed to access which particular files). Designing systems that use a suitable combination of security measures is a non-trivial task.

However, systems security is not limited to achieving information security. Some systems hold no particularly interesting data at all. However, we rely on them and their functionality, i.e. the proper flow of a process. For instance, if an authentication system component of an operating system contains a bug, attackers may be able to shut it down (preventing authorised users from controlling the server) or bypass it (allowing unauthorised users to control the server). Integrity and availability are common protection goals in systems security. Keeping a particular procedure confidential may be a goal to secure intellectual property. However, it is considered bad practice to hide how a system works for reasons of security (cf. Sect. 2.3.2).

Of particular interest in systems security are so-called *cyber-physical systems* that affect the real world, such as traffic lights, autopilots, industrial robots, and control systems for chemical processes or power plants. Some of these systems are considered critical infrastructures; i.e. failures may have a significant impact on society. Policy makers are concerned that future wars might be fought by attacking critical infrastructures to cause chaos—without having to use physical force (Wheeler 2018). Well-known attacks on cyber-physical systems include the Stuxnet malware, which was used to sabotage an Iranian uranium enrichment facility at Natanz in 2010 (Langner 2013) and an attack on a Ukrainian power plant in 2015 (Zetter 2016).

2.2.3 Security Versus Safety

The cybersecurity community differentiates between security and safety (cf. Fig. 2.1). Harm can be caused by humans or by nonhuman events (Pfleeger et al. 2015). Examples of nonhuman events are natural disasters such as earthquakes, fires, floods, loss of electrical power, faults of hard disks and so on. Human threats are either benign or malicious. Benign threats are the result of accidents and inadvertent human errors such as mistyping a command, whereas malicious acts result from bad intentions.

Ensuring that a system remains operational during natural disasters and when faced with human errors (i.e. benign threats) is a matter of *safety*. Safety is crucial in cyber-physical systems, where the failure of a system may harm humans. Safety has a long tradition in engineering, for instance, in cars and airplanes that contain many critical systems designed for maximum dependability.

In contrast, matters of *security* focus on malicious acts of humans, which are called attacks. There are random attacks and directed attacks. In random attacks, attackers do not care who they attack as long as there is something to gain from the victim (cf. pickpockets in the physical world). In the electronic domain, phishing