THE ETHICS OF CYBERSECURITY

Mehmet ŞENCAN[*]
ORCID ID: 0000-0002-4445-8924

Edited by Markus Christen, Bert Gordijn, and Michele Loi. (2020). The International Library of Ethics, Law and Technology, Volume 21.

Declaration[*]

In the current age where cyber and digital technologies have started to be embedded in the international security framework, the book with the title "*The Ethics of Cybersecurity*" suggests a well-settled and comprehensive examination of both the moral and legal contradictions accompanying these kinds of changes. Edited by Markus Christen, Bert Gordijn, and Michele Loi, the study introduces a multi-disciplinary overlook to the pressing need for the ethical phenomenon of the cybersecurity policy and implementations. This study, based on the findings and insights generated through the EU-supported CANVAS initiative, is organised into three thematically interconnected parts: conceptual groundwork as the title "*Foundations*", key challenges as "*Problems*", and proposed solutions as "*Recommendations*". This threefold evaluation offers advantages to challenge intricate theoretical perspectives of cybersecurity, real-world deviations and searching for an evolving cyber/digital framework.

The opening part of the study introduces cybersecurity as an evolving ethical space, shaped by the growing range of digital threats and the varied ways societies are generating responsive initiatives to them. The authors of this part prefer to present a broader frame of coincident arguments, such as equality, credibility, and fairness, instead of an oversimplified binary of privacy and security. Of course, it can be clearly said that these arguments are not complementary; more precisely, they have discord in the case of ethical trade-offs. A notable case is seen in how authorities handle ransomware incidents, especially while blocking payment systems may serve the broader public good, it can also mean that victims lose their data forever (p. 2). In the same way, opting to strengthen encryption for medical implants may improve the protection of sensitive data, but it could also lead to reduced battery longevity

[*] Phd Candidate in International Relations at Ankara Social Science University, Ticaret Bakanlığı, mhmdsencan34@gmail.com

[*] In this study, ChatGPT and Deepseek were used as generative AI tools. These were primarily used for language correction and sentence structure. In addition, translation assistance was occasionally utilized to improve understanding of the study. Finally, they were used for research purposes, including commentary, literature review, and critiques of the reviewed book.

and more frequent surgeries as a result (p. 2). These citations clearly explain that cybersecurity policies contain complicated ethical implications, particularly when enacted at the level of policy or corporate governance.

The foundational section of the book paves the way for a framework of the ethics of cybersecurity in a way that is both theoretically robust and applicable to real-world situations. This section not only contains technical arguments, such as network vulnerabilities, malware, and cryptographic tools, but also examines how technological systems embody moral axioms. The discussion highlights those certain defensive technologies, though designed to enhance security, can unintentionally introduce fresh vulnerabilities or reinforce imbalances in power. As illustrated in the article by Dominik Herrmann and Henning Pridöhl, tools like network intrusion detection systems may blur the line between protection and surveillance, especially when there are no well-defined mechanisms to ensure accountability or transparency in data handling (p. 15). The authors emphasise that security is not an objective state but a normative orientation, one that depends on context, institutional norms, and societal expectations.

Further explanations of the foundational aspects deeply focus on how security, fairness, accountability and privacy coexist in sometimes responsive or sometimes contentious ways. Instead of viewing these values as autonomous moral ideals, the authors emphasise their fluid and interconnected nature, shaped by how institutions are structured and what users expect from them. They carefully assess existing ethical models by noting that both principles and rights-based aspects fall short when used in isolation. To address this gap, they suggest integrating "risk ethics", which offers a more flexible and probability-based way of thinking about ethical challenges. In addition, this shift underlines the impact of uncertainty and contingency that shape the cybersecurity strategies in particularly complicated socio-technical systems (p. 84). This part of the discussion takes a close look at the European Union's legal structure, especially the GDPR, acknowledging its valuable contributions while also pointing out its shortcomings. Although the EU promotes core human rights, inconsistencies in how laws are applied across member states hinder the creation of a coherent and unified ethical stance on cybersecurity policy (p. 104). This analysis underscores the tension between supranational regulation and national sovereignty within the EU. Without greater legal harmonisation, efforts to establish a common ethical foundation for cybersecurity will likely remain uneven and fragmented.

In the second part of the book, with the title "*Problems*", the focus of the exploration shifts to the practical challenges and domain-based problems. Evidently, it can be clearly said that the field of cybersecurity is not monolithic, particularly since it represents a web of interconnected issues, each one carrying its distinct ethical implications. In the business sector, for example, the ethics of corporate responsibility are interrogated through the lens of care theory (p. 121). The investigation in this part highlights that business facilities can not be described as only technical actors but also moral ones for the sake of responsibilities transcending the shareholders, including consumers, employees and society. Failing to properly address vulnerabilities or respond to security breaches isn't just a technical oversight; it's also a violation of the moral trust placed in those responsible for safeguarding digital systems.

Cybersecurity in healthcare comes with its unique difficulties, largely because of the highly sensitive nature of patient data and the critical condition of those receiving care. Making ethical choices in this setting involves carefully weighing the need to keep data secure while ensuring it remains accessible. The authors, Karsten Weber and Nadine Kleine, stress the importance of tailoring decisions to specific contexts, which draws on the core principles of biomedical ethics. Instead of relying on one-size-fits-all solutions, healthcare institutions must consider how technical choices affect patient rights, organisational practices, and the everyday challenges faced by medical staff (p. 145).

Further, a comparable complicated landscape exists in the context of public health policies in the national infrastructure. The increasing popularity of the use of artificial intelligence in supervising and administering critical systems unearths profound challenges in terms of surveillance and privacy. There comes one of the basic argumentations about that, as Vigano, Loi and Yaghmaei mention in their article with the title "*Cybersecurity of Critical Infrastructure*", the ethical deductions of cybersecurity strategies are usually undertheorized while these national strategies illustrate the technical and digital power of the nations (p. 159). The section underlines that developing infrastructure is not solely a technical endeavour; it requires ethical clarity and public transparency to ensure that the trade-offs made in the name of security do not undermine democratic norms (p. 163).

Another central subject addressed in this section is the ethical complexity of hacking. Rather than treating it only as a matter of legal compliance, the authors adopt a layered moral perspective. They assess hacking based on the hacker's purpose, the techniques used, and the

resulting consequences, drawing clear distinctions between morally supportable actions like whistleblowing or responsible disclosure and those that cause direct harm. By doing so, Jaquet-Chiffelle and Loi foster a deeper, more thoughtful discussion about how cybersecurity policies can account for and legitimise ethical forms of hacking (p. 185).

Political interaction and state actions in the field of cybersecurity are also evaluated crucially in this section. From propaganda activities to manipulative actions through deep fakes, the weaponisation of information disseminating clashes with the democratic universal norms. In that manner, Seumas Miller raises epistemic concerns about an escalating crisis of knowledge infrastructure, in which the breakdown of shared truths and declining trust in institutions threaten to undermine both constructive political discourse and the fabric of social unity (p. 230). In addition, Lucas stresses the Hobbsean thought about the state of nature for the sake of the orientation of the anarchic environment of cyberspace (p. 246). Inspired by Hobbesian thought, the part depicts cyberspace as drifting toward a chaotic environment with the origins of the state of nature. It is like an arena where authority is dictated by strength rather than ethics. This escalating disorder, amplified by the advanced capabilities of state-sponsored cyber activities, underscores the urgent necessity for a common set of guiding norms and values.

The final part of the book shifts its pillar focus to practical advice, which presents value-driven recommendations specifically designed to address the needs of various actors involved in the anarchic nature of cyberspace. Privacy-preserving technologies are searched and evaluated, not only in terms of their technical performance but also their ethical adequacy (p. 288). The book also outlines ethical guidelines for cybersecurity service providers, addressing a wide range of responsibilities from how they report security vulnerabilities to the ways they manage client data and cooperate within the industry.

One of the most intriguing discussions in the part of the book is situated at the contentious practice of “hacking back.” The authors in this section warn against reactionary tactics that can escalate conflicts or breach legal norms. On the other hand, the articles suggest a decision-making model built around core principles like fairness in response, openness in actions, and a clear sense of responsibility for outcomes. These principles are intended to discourage agents from resorting to overly aggressive, military-style approaches in their cybersecurity strategies, particularly when there’s no well-defined legal basis for such actions.

What truly sets *The Ethics of Cybersecurity* apart from others centers on the ground with its comprehensive and integrative approach. Blending solid theoretical foundations with real-world analysis and ethical recommendations, the book moves beyond the limits of any one-sided field. While its primary lens is Europe, its insights resonate well beyond. For nations like Türkiye, where the lines between digital governance and national security are growing ever closer, it provides a vital blueprint for developing policy rooted in ethical principles.

On a deeper level, the book encourages readers to rethink cybersecurity as more than just a technical challenge; it frames it as a shared ethical and social responsibility. It pushes the readers to reflect on the digital future it has been building: Who defines safety in cyberspace? Whose interests are protected, and whose are left out? And how can we avoid turning protective technologies into tools of domination or exclusion? In an era marked by rising cyber risks and moral ambiguity, the book stands as both a thoughtful guide and a timely caution. It reminds the readers that the true foundation of cybersecurity isn't just in algorithms but in the values people choose to uphold.