Mateusz Kozłowski (2026)

Humans in the Cyber Loop: Perspectives on Social Cybersecurity

Publisher: Brill
ISBN: 978-90-04-54990-6
Authors: Dorota Domalewska, Aleksandra Gasztold, Agnieszka Wrońska
Number of pages: 284
Year of publication: 2025

About the Publication

The reviewed monograph contributes to the dynamically developing field of research on the social dimensions of cybersecurity, providing an interdisciplinary response to evolving threats in cyberspace. The publication is an interdisciplinary monograph that systematically analyzes the role of the human as an active participant in the digital security ecosystem.

The thematic scope covers four key problem areas: the conceptualization of social cybersecurity, the mechanisms of disinformation's impact on democratic processes, the influence of social media on shaping public opinion, and the socio-ethical implications of algorithmic decision-making. The book is situated at the intersection of security studies, communication sciences, digital sociology, and social informatics, and thus fills a significant gap in the existing literature.

One of the particular strengths of the publication is its departure from the previously dominant technocentric paradigm in cybersecurity. The authors consistently shift the focus from the protection of technological infrastructure to understanding and mitigating the risks associated with the human factor in the digital environment, which constitutes a kind of novum in the approach to the discussed issues.

Main thesis and theoretical assumptions

The main argument of the monograph is the need to shift cybersecurity strategy from a purely technical model to an anthropocentric one. The authors indicate that humans are not merely passive users of digital technologies nor solely the weakest link in the security chain, but active participants who shape the digital ecosystem, which itself requires multidimensional protection.

This fundamental shift in perspective leads to a new conceptualization of cybersecurity as a social phenomenon, in which human actions and vulnerabilities constitute the central element of the security architecture. This

approach does not dismiss the importance of technical safeguards, but rather argues for their integration with a deeper understanding of the human factor in its socio-cultural context.

Scientific value of the publication

The methodological originality of the publication is manifested in the consistent application of a multidisciplinary perspective, integrating knowledge from various fields for a comprehensive understanding of cybersecurity. This approach represents a significant step forward from the traditionally fragmented research in this area. Until now, the main focus regarding cybersecurity issues has been on technical aspects. The approach presented by the authors encourages the reader to expand this perspective to include the human factor.

The theoretical contribution of the monograph lies in the development of the concept of social cybersecurity as a distinct research paradigm. Shifting the focus from technological infrastructure to social behavior opens new research horizons and allows for a more holistic understanding of digital threats. Particularly valuable is the treatment of the human as an entity requiring protection, and not just as a source of threat.

Also of high value is the in-depth analysis of information warfare, which is currently one of the most significant threats we face in an era of tense geopolitical situation. A growing body of research shows that the center of gravity is shifting from common digital attacks, i.e., phishing (which remains the most widespread form of attack), to more advanced threats such as disinformation campaigns.[1]

This shift in focus is significant because, with increasing public awareness and more sophisticated technical security mechanisms, such as cyberattacks have become increasingly difficult to execute, and their scope of impact and damage are shrinking. In contrast, "people's minds" are becoming an increasingly serious threat, as individuals, faced with ever more sophisticated disinformation techniques, become susceptible to adversarial narratives. The authors refer to a series of well-selected case studies and both

[1] Broda, E., & Strömbäck, J. (2024). Misinformation, disinformation, and fake news: lessons from an interdisciplinary, systematic literature review. Annals of the International Communication Association, 48(2), 139–166. https://doi.org/10.1080/23808985.2024.2323736

quantitative and qualitative research, covering, among other examples, disinformation campaigns by the Russian Federation (including interference in electoral processes and actions during the COVID-19 pandemic), armed conflicts, humanitarian crises, and the practices of digital platforms. Such a broad spectrum of examples makes the book not only a theoretical study but also a rich empirical compendium, illustrating the complexity of the social dimensions of cyberthreats.

Of particular note is the in-depth analysis of the role of algorithms and artificial intelligence in shaping user experiences and reproducing social inequalities. The authors, in an accessible yet critical manner, demonstrate the mechanisms of content allocation, message personalization, the formation of information bubbles, and algorithmic biases, placing them in the broader context of research on algorithmic culture, surveillance capitalism, and discrimination in automated decision-making processes. This type of synthetic overview provides a valuable reference point for further analyses of the ethical and political consequences of AI development.

A great advantage of the monograph is its clear and logical structure, which guides the reader from the fundamentals to complex challenges. First, key terms and theoretical frameworks are defined, then topics such as cybercrime, cyberwarfare, information warfare, and the role of algorithms are analyzed, followed by the social and cultural consequences of the digital transformation. The work concludes with a concise summary and justification of the adopted approach, which makes the book useful both as an introduction and as a starting point for further in-depth research.

The relevance of the subject matter is indisputable in the context of the growing importance of disinformation, manipulation of public opinion through social media, and the ethical dilemmas related to algorithmic decision-making. The authors address urgent contemporary challenges, such as threats to democratic processes or the exploitation of human cognitive weaknesses in disinformation campaigns.

Attention to the practical dimension is also noteworthy. Alongside a critical analysis of threats, the authors present examples of institutional solutions and public policies, including a developed ecosystem of digital services

and AI applications in public administration, which may serve as inspiration for designing systems more resilient to information abuse. Such illustrations make it easier to translate the proposed social paradigm of cybersecurity into actionable recommendations for policymakers.

Finally, it is worth emphasizing the breadth and relevance of the literature base, which draws on work from security sciences, sociology, psychology, political sciences, digital economy, media and communication studies, and research on artificial intelligence. The careful selection of recent scholarly publications makesthe monograph a valuable and reliable guide to contemporary literature on the social dimension of cybersecurity.

Significance for research development

The monograph signals a significant paradigmatic shift in studies on cybersecurity and has thepotential to initiate a new line of research on the social and behavioral aspects of digital security. It can serve as a point of reference for future research projects that combine technical, humanistic, and social perspectives.

Critical remarks

Despite its undeniable merits, the publication is not without limitations that should be pointed out for a fully reliable assessment.

One significant shortcoming is the insufficient problematization of the tension between security and individual freedom. The authors advocate for the protection of humans in cyberspace, but they do not fully explore the potential threats to privacy and autonomy that may arise from increased monitoring of digital behaviors. This problem is particularly relevant in the context of algorithmic decision-making, where the requirement for security can conflict with the right to privacy.
Another noteworthy limitation is the economic dimension of implementing anthropocentric cybersecurity strategies. Organizations and institutions not only need to be convinced of the value of the new approach, but also require a reliable assessment of the costs, resources, and time required to transform existing systems.

Summary and final assessment

Humans in the Cyber Loop: Perspectives on Social Cybersecurity is a valuable and innovative contribution to the developing field of social cybersecurity. The main thesis

emphasizing the need to shift focus the emphasis from technical infrastructure to the human as an active participant and beneficiary of digital security strategies is both convincing and well-argued.

The book stands out for its interdisciplinary approach and its ability to synthesize knowledge from various fields, which makes it relevant to both theory and practice in cybersecurity. Its analyses of disinformation, public opinion manipulation, and the ethical aspects of algorithms address some of the most pressing challenges of our time.

At the same time, the publication does not exhaust all aspects of this complex issue. The limitations mentioned, from insufficient operationalization of concepts to gaps in economic and cultural analysis, create space for further research. However, they do not undermine the fundamental value of the monograph, but rather indicate promising directions for future research.

In the context of dynamically evolving digital threats and the growing complexity of cyberspace, this publication constitutes a significant step towards a more human-centric and socially oriented understanding of cybersecurity. Despite the noted limitations, it deserves recognition as a strong foundation for further discussion and research on the role of the human in the digital security ecosystem.

The practical relevance of the publication is evident in its potential as a reference for a broad range of audiences: academics dealing with cybersecurity, IT professionals, policymakers, and anyone interested in the complex relationships between technology, human behavior, and digital security. The monograph may also serve as a source of inspiration for developers of technical solutions, encouraging them to place greater emphasis on the active involvement of the user in protecting IT systems.