EDITORIAL PREFACE: NAVIGATING THE DIGITAL TURN: SECURITY, ETHICS, AND TRANSFORMATION

Dear Readers

We are proud to present to you the 19th issue of the *Cyberpolitik Journal*. It is a great honor for all of us to continue our journey that we started nine years ago without interruption. As the digital world grows every day and every second, new developments and new technologies emerge, we are trying to read and understand this domain within our limitations.

In an era dominated by the omnipresence of technology and interconnected digital ecosystems, the role of digital citizenship education cannot be overstated. The articles featured in the volüme 9th and 17th issue of the *Cyberpolitik Journal* bring forth a compelling narrative, shedding light on diverse facets of cyber landscapes, from ethical considerations for academic writing brought abut by generative AI to Data protection and from ethical dilemma of Transhumanism to the freedom of expression in social media.

In recent decades, the rapid evolution of digital technology has fundamentally transformed the way we live, work, and communicate. As the digital domain continues to expand, it brings with it a myriad of opportunities that promise to enhance our global connectedness, increase access to information, and democratize knowledge. However, alongside these benefits, the digital age also presents significant ethical dilemmas that challenge our moral frameworks and societal norms. As the contributors to this issue of *Cyberpolitik Journal* explore, the ethics of the digital domain are multifaceted and require careful consideration from scholars, policymakers, and practitioners alike.[1]

As organizations, individuals, and governments become increasingly dependent on digital ecosystems, the complex nature of cyber threats and the diversity of attack vectors highlight the inadequacy of traditional security approaches. This is because traditional security systems are inadequate against sophisticated attacks such as zero-day vulnerabilities, advanced persistent threats, and polymorphic malware, further increasing the need for preventative and adaptive security approaches.

The integration of AI technologies, particularly machine learning, deep learning, and natural language processing algorithms, in the cybersecurity domain appears poised to transform

[1] This editorial preface has been predominantly produced by AI, especially ChatGPT.

existing paradigms in this field radically. AI algorithms enhance the capabilities of human analysts in anomaly detection, behavioural analysis, automated threat hunting, and incident response processes, while also significantly improving operational efficiency by reducing false positive rates.

However, the applications of AI technologies in cybersecurity can be used not only for defence but also for developing attack vectors. Adversarial machine learning, AI-enabled phishing campaigns, fake image technologies, and automated vulnerability discovery tools constitute the next-generation threat categories targeted by cybercriminals. This makes it crucial to simultaneously consider both defensive and offensive perspectives in the development of AI-enabled cybersecurity solutions.

This issue of our academic research offers an interdisciplinary perspective on these crucial topics. From the economic impacts of cybersecurity to the philosophical depths of the digital divide, and from the transformative potential of big language models in governance to the evolving structures of cyber alliances, each article offers a critical analysis grounded in current developments. These scholarly works are accompanied by thought-provoking commentary on AI and its growing influence on cybersecurity, as well as comprehensive book reviews exploring the ethical dimensions of AI and cybersecurity applications.

To complement these intellectual contributions, the visual identity of this issue was carefully designed by gen-AI. The magazine cover design features a modern, cyber-inspired aesthetic that integrates elements such as digital grids, data streams, cybersecurity symbols, and AI iconography.

In this context, the first article of the new issue is handled by Gül Ünver and Şerife Deniz Kolat with the title "*The Enhancement of Cybersecurity and Economic Growth: Panel Data Analysis"* Changes in the perception of productivity and efficiency have been reflected in economic life through total factor productivity with the advent of digitalization in daily lives. This study aims to investigate the relationship between cybersecurity and economic growth. The effects of economic growth on cybersecurity have been examined for all countries included in the ICT Development Index for the years 2023-2024 using the multi-dimensional panel data method. Besides the time dimension, using multi-dimensional nested panel data analysis, helps to evaluate how economic growth and cybersecurity are connected at both regional and country levels. Additionally, the existing literature that examines these two phenomena independently often reduces cybersecurity to the national level, while economic growth is primarily addressed within a macroeconomic framework. The fact that the phenomenon of cybersecurity and economic growth was addressed together within the scope of the study, and that all countries covered in the IDI were included in the analysis, allows the study to differentiate itself more originally and comprehensively from the existing literature.

Emre Arslantaş's study, " *Dijital Bölünmenin Tarihsel Materyalizm Yaklaşimi Çerçevesinde Değerlendirilmesi," (The Evaluation of The Digital Divide within the Approach of Historical Materialism)* examines the material elements that continually reproduce the digital divide within the framework of a historical materialist approach. The growing importance of cyberspace has led to discussions about differences in access and technology among users, in other words, the digital divide. While the literature on the digital divide focuses on the consequences of these access and technology differences, it has overlooked the reasons that perpetuate them. The author argues that cyberspace's reliance on material relations is the fundamental element that creates the digital divide. In the capitalist mode of production, cyberspace has become a significant productive force, encompassing elements such as data, algorithms, e-commerce, and artificial intelligence.

Meanwhile, digital labour has given rise to new production relations, particularly in terms of surplus value creation. The dominance of developed states in the physical, logical, and content layers, as well as that of private companies headquartered in these states, leads to the emergence of class relations in cyberspace. These class relations lead to the development of capitalist states and private corporations playing a leading role in determining the content of elements that constitute the superstructure of cyberspace, such as culture, law, and politics. Based on these elements, Arslantaş argues that the digital divide should be understood as a phenomenon created by the material elements of the capitalist mode of production and should be examined through a historical materialist approach.

The study titled "*The Rise of LLMs in Bureaucracy and Military Decision-Making and the Cybersecurity Imperative*", written by Gloria Shkurti Özdemir, focuses on a critical but relatively novel topic: the adaptation of LLMs in bureaucracy and military decision-making processes. Considering the increasing application of these models in various states, Shkurti Özdemir analyses how these models are implemented, while also addressing the risks associated with their application, especially given the sensitive areas and subjects involved. The author examines the cybersecurity and geopolitical risks they pose and frames their adoption within broader debates on technological sovereignty, the power of big tech companies, and data colonialism.

The study, titled "*The Evolution of the Alliance Concept in Cyberspace,"* written by Onur Yılmaz, draws attention to the growing significance of cyberspace within the field of International Relations, particularly in the context of security studies, and examines the structural specificities that define this domain. The anarchic nature of cyberspace, its multi-actor composition, and the absence of a sovereign authority or binding legal framework have resulted in a fragmented and normatively underdeveloped environment. These conditions highlight the limitations of unilateral state responses to cyber threats and underscore the necessity of cooperative security arrangements. In this context, the study aims to explore whether "cyber alliances" can emerge as viable and functional mechanisms for enhancing security in cyberspace. In addressing this question, the research seeks to provide a conceptual clarification of the cyber alliance phenomenon by examining its relationship with the traditional notion of alliances. Through a comparative approach, the study identifies both similarities and divergences between classical and cyber alliances, thereby offering a theoretical framework that delineates the structural characteristics and scope of this new form of security cooperation.

The article "*Consumer Protection in the Malaysian Digital Marketplace: From Risks and Concerns to A Law Reform"* by Sonny Zulhuda that the transformation of today's marketplace into a digital version is neither mere technical nor peripheral. Instead, it necessitates a reform of the whole processes including the enabling legal and regulatory framework. This paper analyses the dynamic of that reform in Malaysia by assessing the Consumer Protection (Electronic Trade Transaction) Regulation 2024 and the potential effect it brings about

In addition to academic articles, this study presents the reader with two fascinating and insightful commentaries on the relationships between AI and cybersecurity, as well as between AI and religion. Amirudin Abdul Wahab offers insightful insights into the changes in the cyber ecosystem resulting from the increased use of AI in recent years, as well as the complex relationship between *AI and Cybersecurity.* The author evaluates the ethical implications of AI use and the latest developments in defence and cyberattacks. In the second commentary, Bilal Sambur offers fascinating insights with his commentary titled *"Artificial Intelligence and Institutional Religion."* He argues that AI is reshaping humanity's relationship with religion. The author states that the significant changes in people's social lives brought about by AI are beginning to erode the concept of religion.

Finally, two important book reviews provide valuable insights into ethics. Mehmet Şencan reviews the book "*The Ethics of Cybersecurity*" (Edited by Markus Christen, Bert Gordijn, and Michele Loi) (2020). This study offers a comprehensive overview of the concept of ethics in cybersecurity. The final study is "*Ethics of Artificial Intelligence: Case Studies and Options for Addressing Ethical Challenges*" (By Bernd Carsten Stahl, Doris Schroeder, and Rowena Rodrigues) (2023) by Merve Ayşe Kızılaslan. Like the previous study, Kızılaslan also examines the ethical dimensions of AI. The interdisciplinary dimension of this study provides the reader with a compelling assessment of the new ideas it has introduced to the literature.

In summary, the articles, commentaries, and book reviews in this issue contribute to our better understanding of the opportunities and risks presented by the digital age. These contents, prepared with academic depth and visual integrity, aim to open doors to interdisciplinary thought and new areas of discussion. We hope they inspire our readers and open new horizons.

Kamil Tarhan, Ph. D

Issue Editor