ISSN: 2587-1218

CYBERPOLITIK JOURNAL
Siber Politikalar Dergisi

A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights

www.cyberpolitikjournal.org

Summer 2025

ISSN: 2587-1218

ABOUT THE JOURNAL

Owner/Sahibi

On behalf of Association for Human Rights Education / İnsan Hakları Eğitimi Derneği adına
Prof. Dr. Nezir Akyeşilmen

Peer Review

All articles in this journal have undergone meticulos peer review, based on refereeing by anonymous referees. All peer review is double blind and submission is online. All submitted papers (other than book and article reviews) are peer reviewed.

The Journal

The languages of the Journal are both Turkish and English.

ISSN 2587-1218

Cyberpolitik (CP) aims to publish peer-reviewed scholarly articles and reviews as well as significant developments regarding cyber world, cybersecurity, cyberpolitics and human rights.

Indexing/Endeksler

Cyberpolitik Journal is being indexed by;

* Academia Social Science Index (ASOS),
* Scientific Indexing Services (SIS),
* Eurasian Scientific Journal Index (ESJIndex),
* Index Copernicus International (ICI), (ICV 2017=64.65)
* Directory of Research Journal Indexing (DRJI).
* JournalITOCs.
* Open-Web.info.
* Google Scholars

ISSN: 2587-1218

Issue Referees / Sayı Hakemleri

Prof. Dr. Bilal Sambur

Prof. Dr. Nezir Akyeşilmen

Assoc. Prof. Dr. Mehmet Emin Erendor

Assoc. Prof. Dr. Ali Burak Darıcılı

Assoc. Prof. Dr. Mahyuddin Bin Daud

Asst. Prof. Dr. Fikriye Üstüner

Asst. Prof. Dr. Julide Andiç

Asst. Prof. Dr. Yavuz Akdağ

Dr. Kamil Tarhan

Cyberpolitik consists of the following sections:

Research Articles: Each Volume would publish a selection of Articles covering aspects of cyber politics and human rights with a broad universal focus.

Comments: This section would cover recent developments in the field of cybersecurity, cyber politics and human rights.

Book/Article Reviews: Each Volume aims to review books on cyber politics, cybersecurity and human rights.

Cyberpolitik Award: Each year one '*Cyberpolitik*' prize will be awarded, for the best article from material published in the previous year.

ISSN: 2587-1218

CONTENTS / İÇİNDEKİLER

ISSN: 2587-1218

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

RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ

THE ENHANCEMENT OF CYBERSECURITY AND ECONOMIC GROWTH: PANEL DATA ANALYSIS

Gül Nazik ÜNVER[*]
ORCID ID: 0009-0005-5003-1555

Şerife Deniz KOLAT[*]
ORCID ID: 0000-0002-7831-7150

Declaration[*]

Abstract

This study aims to comprehensively analyze how economic growth influences cybersecurity investments and policies in contemporary economies where digitalization is spreading at an accelerated pace. In an era characterized by mounting direct and indirect expenses stemming from cyber threats to the global economy, there is a pressing need to elucidate the correlation between cybersecurity and macroeconomic performance quantitatively. The present study examines the relationship between cybersecurity capacity and economic growth using a multidimensional nested panel data analysis method, which utilizes annual data for 171 countries in the IDI. The study also reveals that cybersecurity isn't just a technical issue but one of the main determinants of macroeconomic stability. In nations undergoing digital transformation, cybersecurity infrastructure is as strategically significant as traditional infrastructure investments. This study examines the relationship between economic growth and cybersecurity. The findings suggest that there is a statistically significant and positive relationship between cybersecurity and economic growth. The objective of this study is to provide policymakers with strategic recommendations by highlighting the critical role of economic growth in cybersecurity, supported by quantitative data.

Keywords: Cybersecurity, economic growth, panel data analysis, digital economy, macroeconomic effects.

[*] Lecturer Dr., Batman University, Career Development Application and Research Center, Batman, Türkiye, gul.unver@batman.edu.tr
[*] Assistant Professor, Batman University, Social Science Vocational Schools, Batman, Türkiye, serifedeniz.us@batman.edu.tr
[*] This article has been prepared without the use of any Artificial Intelligence (AI) tools or assistance.

Introduction

In the contemporary era, characterized by the accelerated adoption of digital technologies, the drivers of economic growth are undergoing a profound transformation. In addition to factors such as physical capital, human capital, and technological development, which are prominent in traditional growth models, a new one has now been added: cybersecurity. In the contemporary era of increasing digitalization, economic activities have become increasingly dependent on information and communication technologies. This paradigm shift has transformed cybersecurity from a purely technical issue to a strategic element that has a direct impact on economic performance. In this context, systematic analysis of the effects of cybersecurity on economic growth is of great importance at both academic and political levels (Rudnev et al., 2024; Ünver, 2024; Ahmed, 2021, pp. 413, 416-417).

It is becoming increasingly evident that global cyberattacks represent a threat not only to digital systems but also to entire economic cycles (Kırtıllı, 2019). Attacks in strategic areas, such as finance, healthcare, energy, and critical infrastructure, can lead to the cessation of production, disruption of services, a decline in consumer confidence, and an increased risk perception among international investors. A prime example of this phenomenon is the WannaCry ransomware attack of 2017, which not only disrupted information systems but also public health services, production facilities, and transportation systems, resulting in economic losses amounting to billions of dollars. According to McAfee, the global cost of cybercrime has exceeded $1.5 trillion. This compelling data unveils the direct impacts of cybersecurity on economic stability (Zaiats & Kytsyuk, 2024; Miliefsky, 13.03.2025; ISACA, 2022).

It is essential to adopt a nuanced perspective on cybersecurity, one that transcends the conventional defence-based approach. Instead, it should be conceptualized as a proactive investment domain that fosters growth and development. In this context, three fundamental mechanisms have been identified as explanatory of the relationship between cybersecurity and growth. These measures have been shown to enhance the investment environment, ensure uninterrupted production processes, and safeguard innovation capacity (Akyeşilmen, 2022). The presence of secure digital infrastructures has been demonstrated to be a contributing factor to the observed increase in foreign direct investments, particularly within the technology and finance sectors. The 30% increase in investments in the technology sector following Israel's national cybersecurity strategy implementation in 2018 provides concrete support for this situation (Benaichouba et al., 2024, pp. 3-7; Falevich, 2018). Conversely,

IBM Security (2023) data indicates that the average cyberattack results in approximately 200 hours of operational downtime and losses exceeding $3.5 million for businesses, directly impacting total factor productivity. Furthermore, the preponderance of digital infrastructure in R&D underscores the indispensability of cybersecurity for sustaining innovation processes (IBM Security, 2023). The primary objective of this study is to ascertain the ways and the extent to which an augmentation in cybersecurity capacity affects economic growth, employing panel data analysis as a methodological framework. The main questions of the study are shaped within the following framework: (1) Do cybersecurity investments significantly and positively affect economic growth? (2) How does this effect differ between developed and developing countries? The analyses conducted in line with these questions are also supported by heterogeneity tests, and the behavioral patterns of different country groups in the cybersecurity-growth relationship are comparatively evaluated. The contribution of the study to the existing literature can be summarized as follows. This study, which encompasses 171 countries based on IDI data, has developed a comprehensive cybersecurity index. In addition, it has empirically tested how the structural differences between developed and developing country groups modify the effect of cybersecurity on economic growth.

Literature Review

The relationship between cybersecurity and economic growth has emerged as an interdisciplinary field of research with the transformation created by digitalization in global economies. In the extant literature, three fundamental theoretical approaches have been advanced to elucidate this relationship, namely, endogenous growth theory, institutional economics and network effects, and the systemic risk approach. The extant literature on this subject posits that cybersecurity exerts a dual effect on economic growth, both direct and indirect. However, studies examining the relationship between ICT and economic growth emphasize the critical role of cybersecurity in this process (Albimana & Sulongb, 2018).

The theory of endogenous growth posits that technological progress is the primary catalyst for economic growth. In this context, cybersecurity is a vital element in terms of protecting the stock of knowledge and sustaining innovation processes. The Estonian case demonstrates that investments in cybersecurity can yield an annual growth rate of 1.2% in the digital economy (Skierka, 2022). Furthermore, studies examining the contribution of ICT to economic growth (Dewan & Kraemer, 2000; Ahmed & Ridzuan, 2013) have revealed that technological infrastructure increases efficiency, but the lack of cybersecurity measures can reduce this

effect. Albiman and Sulong (2018) and Suzuki (2024) have asserted that, within the paradigm of network effects theory, the proliferation engendered by digitalization can only be perpetuated through the implementation of security measures.

Institutional economics theory (North, 1987) posits that the presence of secure digital infrastructure is conducive to economic growth by virtue of the manner in which it protects property rights and serves to reduce transaction costs. Regulations such as the Cybersecurity Information Sharing Act (CISA) in the United States have aimed to reduce the potential impact of cyberattacks and strengthen overall market confidence by increasing the sharing of cyber threat information between the public and private sectors (Yang et al., 2020). A body of research has been conducted that examines the impact of ICT infrastructure on growth (Pradhan et al., 2022). The findings of these studies have emphasized the critical role of institutional regulations on financial stability and investment climate. As posited by Singh and Alshammari (2020), the absence of adequate digital security policies in developing countries serves to curtail the potential for ICT to exert its impact on growth.

In accordance with Metcalfe's Law, the proliferation of digital networks has been demonstrated to engender economic value, whilst concomitantly giving rise to an augmentation in cyber risks. A notable example of this phenomenon is the 2018 Aadhaar data breach in India, which compromised the personal data of approximately 1.1 billion individuals. This incident has been categorized as one of the most significant data breaches ever documented, yet the precise total of the confirmed economic loss resulting from this breach remains ambiguous (Pimenta et al., 2023). A body of research has been conducted on the impact of ICT on growth (Niebel, 2018; Appiah-Otoo & Song, 2021). The findings of these studies indicate that cybersecurity investments have a beneficial effect on macroeconomic stability in developed countries. However, the effect is limited in developing countries due to a lack of infrastructure. Convergence Theory (Barro & Sala-i-Martin, 1992) posits that digital infrastructure and cybersecurity levels will converge across countries over time. However, subsequent theories (Stephens et al., 2008) contend that cyber threats necessitate a continuous adaptation process due to their dynamic nature.

The impact of investments in cybersecurity on economic growth is subject to variation depending on factors such as the development level of countries, their digital infrastructure, and their institutional capacity. A body of research has been conducted on the relationship between ICT and growth (Saba et al., 2024). The findings of this research indicate that the

impact of cybersecurity investments in developing countries can only be observed after a certain digital infrastructure threshold is exceeded. Despite the confirmation provided by extant literature that cybersecurity supports economic growth, the effects of such measures are considered to be inadequate, particularly in the context of developing countries. A number of studies examining the relationship between ICT and growth (Shiu & Lam, 2008; Pradhan et al., 2016) have argued that the causality relationship is unclear, whereas others (Fernández-Portillo et al., 2020) have emphasized that ICT triggers growth and that the effect of this is strengthened by cybersecurity measures. Consequently, comparative studies that will be conducted by taking into account the digital infrastructure and institutional capacities of countries with panel data analyses will reveal the effect of cybersecurity on growth more clearly.

Method

This study examines the relationship between economic growth and IDI. 171 nations that are part of the ICT Development Index (IDI) are covered in this study for the period of 2023-2024. The focus on these years stems from the fact that the IDI, which was published between 2009 and 2017 by ITU, underwent significant changes in 2017. As a result of these changes, data limitations forced the index computation to be done for all countries as of 2023.

Some of the countries, namely Bhutan, Liberia, Liechtenstein, Monaco, Palestine, San Marino, Sierra Leone, the Syrian Arab Republic, Tonga, Venezuela, and Yemen, are excluded from the sample due to data limitations. In some of the mentioned countries, there are no data for GDP per capita, while in others, there are no available data for IDI**.** Predictions are made by using the multidimensional panel data analysis method. Table 1 presents the dataset used in this study.

Table 1. Data Set

Variables	Dimensions	Representation	Source
IDI	Country	μi	ITU Reports
GDP per capita			World bank
Europe, Asia- Pacific, Arab States, Africa, Common Wealth of Independent States, America	Region	γj	ITU Reports
	Time	λt	

The countries included in IDI are classified according to their geographic region. Unit dimensions presented in the table represent country, region, and time unit dimensions. Therefore, the overall trend of the groups created based on their geographic regions may be seen in addition to country effects. Yerdelen Tatoğlu (2016) used all of the specifications for unnested multidimensional panel data models proposed by different academics to build fixed and random effect estimators for nested multidimensional panel data models. The three-dimensional and two-effect panel data specification is shown in equation (1).

$$Y_{ijt} = \alpha + \beta X_{ijt} + \mu i + \gamma j + \lambda t + u_{ijt} \quad i=1,\ldots..,N,\ j=1,\ldots M,\ t=1,\ldots.T \qquad (1)$$

Here, Y_{ijt} represents the dependent variable, α represents the model fixed term, β represents the independent variable coefficient, X_{ijt} represents the independent variable, u_{ijt} represents the error term, and μi, γj, and λt represent country, region, and time unit effects, respectively.

Two distinct methods are used under the assumption of fixed effects: the within-group estimator and the least squares dummy variable estimator (LSDV). Because of multicollinearity, the findings of the LSDV estimator are biased and unable to reveal information about nested units within one another. In this study, the fixed-effects within-group estimators were used under the assumption of fixed effects. Equation (2) displays the within-group transformation for equation (1).

$$\left(Y_{ijt} - \bar{Y}_i - \bar{Y}_j - \bar{Y}_t + 2\bar{Y}\right) = \beta\left(X_{ijt} - \bar{X}_i - \bar{X}_j - \bar{X}_t + 2\bar{X}\right) + \left(u_{ijt} - \bar{u}_i - \bar{u}_j - \bar{u}_t - 2\bar{u}\right) \quad (2)$$

Here, $\bar{X}$ represents the overall average, $\bar{X}_i$ represents the average according to unit i, $\bar{X}_j$ represents the average according to unit j, $\bar{X}_t$ represents the average according to unit t, and similar representations are valid for the error term as well. The model loses all effects and fixed parameters due to the transformation. Using pooled ordinary least squares (OLS) to estimate equation (2) yields the fixed-effect within-group estimator for three-dimensional panel data models.

There are two alternative estimators in terms of random-effects, namely generalized OLS and the maximum likelihood estimator. Under the assumption of random effects, the maximum likelihood estimator has been employed in this study.

GDP per capita, which is the model's independent variable, is derived from World Bank data, while the IDI data, which is the dependent variable, is derived from ITU reports (ITU, 2023; ITU, 2024). The dimensions of the region consist of six groups: Europe, Asia-Pacific, Arab

States, Africa, the Commonwealth of Independent States, and the Americas. All variables are included in the model in the form of natural logarithms. The LR test is used to examine the existence of unit effects.

Table 2. Results of the LR Test

Null Hypothesis	LR Statistic	P Value
H0= μi=γj=λt=0	414.56	0.000
id(i)	333.69	0.000
region(j)	54.27	0.000
year (t)	0.17	0.3381

The LR test results are shown in Table 2. According to the results, the joint significance of each unit effect on the null hypothesis was rejected. To ascertain which effect is significant, each effect was investigated separately under the alternative hypothesis, which states that at least one unit effect is significant. The unit effects of country and region are statistically significant, whereas the unit effect of time is not, in terms of LR test results, which examine the separate significance of unit effects. In light of this information, the time unit effect was removed from the model in equation (1) in order to obtain the three-dimensional two-unit effect panel data model employed in this study and shown in equation (3).

$$\mathrm{LIDI}_{ijt} = \alpha + \beta\, \mathrm{LGDP}_{ijt} + \mu i + \gamma j + u_{ijt} \quad (3)$$

i=1,…..,N, j=1,…M , t=1,….T

In this case, all variable explanations are the same as above. The within-group transformation for the model in equation (3) is shown in equations (4) and (5).

$$\widetilde{\mathrm{LIDI}_{ijt}} = \mathrm{LIDI}_{ijt} - \overline{\mathrm{LIDI}_{i}} - \overline{\mathrm{YLIDI}_{j}} + \overline{LIDI} \quad (4)$$

$$\widetilde{\mathrm{LGDP}_{ijt}} = \mathrm{LGDP}_{ijt} - \overline{\mathrm{LGDP}_{i}} - \overline{\mathrm{LGDP}_{j}} + \overline{LGDP} \quad (5)$$

Under the assumption of fixed effects, the within-group estimators are generated by these transformations. $\overline{LIDI}$ represents the overall average, $\overline{\mathrm{LIDI}_{j}}$ represents the average according to unit j, $\overline{\mathrm{LIDI}_{i}}$ represents the average according to unit i, and $\widetilde{\mathrm{LIDI}_{ijt}}$ represent the within-group estimators. The transformation process and explanation for variable GDP are the same as IDI.

Findings

Fixed and random effects model estimations were performed following the selection of the panel data model to be employed in the analysis.

Table 3. Fixed Effects and Random Effects Estimator Results

	Fixed Effects – Within Group Estimator	F statistic	Random Effects - Maximum Likelihood Estimator	Wald Statistic
LGDP	0.2383***	2344.17***	0.1568***	217.58***
AIC	-667.2633		-557.1812	
BIC	-663.5013		-534.6089	

Note: ***, **, and * represent statistical significance at the 1%, 5%, and 10% levels, respectively.

The results of the fixed and random effects estimators for the multidimensional panel data model are shown in Table 3. The Wald and F tests have been used to evaluate the models' overall significance for random-effect and fixed-effect estimators, respectively. Both the fixed effect within-group estimator and the random effect maximum likelihood estimator clearly show that GDP per capita has a positive and statistically significant impact on IDI. The findings indicate that economic development has a statistically significant and positive effect on IDI, with an increase in per capita GDP leading to an increase in IDI. A 1% increase in economic growth leads to approximately a 0.24% and 0.16% increase in the IDI according to fixed-effect and random-effect, respectively.

Table 4. Test of homoscedasticity, parameter heterogeneity and model selection.

Name of test	Test Statistics	p-value
Hausman test	218.85	0.000
Breush-Pagan/Cook-Weisberg test	265.28	0.000
S test (Swamy, 1970)	1892.62	0.000

The results of the parameter heterogeneity test, the model selection criteria, and the existence of heteroscedasticity are shown in Table 4. The Breusch-Pagan/Cook-Weisberg (1980-1983) test was used to determine the presence of heteroscedasticity. The parameter heterogeneity was tested by Swamy's (1970) S test. The null hypothesis was rejected, which demonstrated that the parameters are not homogeneous. The Hausman test is used for model selection. The alternative hypothesis, which states that the fixed effects model is consistent and the random effect model is inconsistent, was accepted based on the results of the Hausman test. A 1% rise in per capita income is roughly associated with a 0.24% increase in IDI, in terms of the results of the fixed effects estimator.

The results of the LR test demonstrate the impact of both the country and the region of the country. In addition, the results of the S test (Swamy, 1970) indicate parameter heterogeneity.

A two-dimensional panel data model estimation based on regions is made due to this heterogeneity. Europe (region 1), Africa (region 4), America (region 6), Arab countries (region 3), Asia and the Pacific (region 3), and the Commonwealth of Independent States (CIS) (region 5) are the six dimensions of the regional distinction.

Table 5. Two-Dimensional Panel - Fixed Effects and Random Effects Estimation Results According to Geographic Region

	Variables	Fixed Effects	Random Effects	Hausman Test Statistic	F Test Statistic	Wald Statistic
Region 1 (Europe)	LGDP	-0.1006	**0.0421*****	2.76*	1.37	45.82***
	constant	5.4993	**4.0656*****			
Region 2 (Asia-Pacific)	LGDP	0.0622	**0.1641*****	2.01	0.69	61.95***
	constant	3.7551***	**2.8547*****			
Region 3(Arab Countries)	LGDP	0.2947	**0.2125*****	0.03	0.33	41.00***
	constant	1.7133	**2.4245*****			
Region 4 (Africa)	LGDP	**1.4338*****	0.3416***	4.97**	8.52***	108.11***
	constant	**-6.7133***	1.3162***			
Region 5 (Commonwealth of Independent States)	LGDP	**0.4922*****	0.0339	13.03***	14.07***	1.05
	constant	**0.2499**	4.1635***			
Region 6 (America)	LGDP	0.0885**	**0.1328*****	1.72	5.56**	66.85***
	constant	3.5137***	**3.1053*****			

Note: The models shown in dark colour are the ones recommended according to the Hausman test statistics. ***, **, and * represent statistical significance at the 1%, 5%, and 10% levels, respectively.

The fixed effects and random effects estimators for the groups according to the region of countries are shown in Table 5. The fixed effect estimators have a negative sign for Europe and are statistically insignificant for the European region, Asia-Pacific, and Arab states. In addition, the random effects model estimators are statistically significant and have a positive sign for all regions. The model selection for each group was made by using the Hausman test statistic. The fixed effects estimations are consistent for the regions of Africa and the Commonwealth of Independent States, while the random effects estimator is effective for Europe, Asia-Pacific, Arab States, and the Americas regions, according to the Hausman test results. A one per cent increase in per capita income raises the ICT Development Index by 1.43% for African region countries and by 0.49% for the Commonwealth of Independent States region countries, depending on the country's geographic region. A 1% increase in per capita income causes the ICT Development Index to rise by 0.21% for Arab nations, 0.16% for the Asia-Pacific region, and 0.13% for American countries, respectively. The lower amount of increase is observed in European countries, where a 1% increase in GDP leads to only a 0.04% increase in IDI for this region's countries. The reason for this issue might be

that the European region generally consists of developed countries, and compared to regions with developing and relatively less developed countries, financial development and stability have been achieved.

Conclusion

The present study aims to reconceptualize the multi-layered relationship between cybersecurity and economic growth in today's world, where digitalization is accelerating, by analyzing it theoretically and empirically. Cybersecurity, a factor that has thus far been overlooked by traditional growth theories, is considered a fundamental production factor. This is due to the fact that it both protects the fragile infrastructure of the information society and secures macroeconomic stability.

This study addresses cybersecurity from three different perspectives. Firstly, it is evident that cybersecurity investments have a significant impact on total factor productivity. This is due to the fact that such investments serve to preserve the integrity of digital infrastructure. Secondly, within the context of the institutional regulatory framework, the implementation of effective cybersecurity regulations has been demonstrated to reinforce investor confidence and to reduce market failures, thereby ensuring efficiency in resource allocation. Thirdly, with regard to systemic risk management, cybersecurity provides resilience against macroeconomic shocks and strengthens financial stability. In developing countries, the simultaneous development of these three dimensions is a critical requirement for the sustainability of the digital economy. The findings indicate that economic growth has a statistically significant and positive effect on cybersecurity, as expected theoretically.

The most fundamental contribution of this study is that it addresses the relationship between cybersecurity and economic growth as a multidimensional, reciprocal, and dynamic interaction network, rather than a unidirectional causality. This approach provides structural contributions to academic literature and national and international policy-making processes. This is particularly evident in economies undergoing digital transformation, where cybersecurity investments have become as important as traditional infrastructure investments. In some contexts, these investments have even assumed a more strategic role.

In the future, as digital technologies become more central to economic systems, we anticipate that the macroeconomic effects of cybersecurity will become more apparent. Consequently, there is an imperative for both academia and public policy to adopt interdisciplinary, data-

based and forward-looking approaches. The objective of this study is to establish a theoretical, empirical, and methodological foundation that will contribute to this transformation and to the establishment of a new paradigm in this field.

References

Ahmed, E. M. (2021). Modelling Information and Communications Technology Cyber Security Externalities Spillover Effects on Sustainable Economic Growth, *Journal of the Knowledge Economy*, (12), 412-430, https://doi.org/10.1007/s13132-020-00627-3.

Ahmed, E. M., & Ridzuan, R. (2013). The Impact of ICT on East Asian Economic Growth: Panel Estimation Approach, *Journal of the Knowledge Economy*, 4(4), 540-555.

Akyeşilmen, N. (2022). Cyber (In)Security in Metaverse: New Threats Old Measures?, *Cyberpolitik Journal*, 7 (13), 98-107.

Albiman, M. M. & Sulong, Z. (2018). Information and Communication Technology, Production and Economic Growth: A Theoretical Nexus, *International Journal of Academic Research in Business and Social Sciences*, 8(12), 642–657.

Appiah-Otoo, I., & Song, N. (2021). The Impact of ICT on Economic Growth-Comparing Rich

and Poor Countries, *Telecommunications Policy*, 45(2).

Barro, R. J., & Sala-i-Martin, X. (1992). Convergence, *Journal of Political Economy*, 100(2),

223-251.

Benaichouba, R., Brahmi, M. & Adala, L. (2024). Economics of Cyber-Security and Society Databases: Protecting the Digital Ecosystem from Cyber-Attacks, *International Journal of Professional Business Review*, pp. 1-26.

Cook, R. D., Weisberg, S. (1983), "Diagnostics for Heteroscedasticity in Regression", *Biometrika*, 70(1), 1-10.

Dewan, S., & Kraemer, K. L. (2000). Information Technology and Productivity: Evidence from Country-level Data, *Management Science*, 46(4), 548–562.

Falevich, N. (2018). Start-Up Nation Central: Finder Insights Series Israel's Cybersecurity Industry in 2018, Start-Up Nation Central.

Fernández-Portillo, A., Almodóvar-González, M., & Hernández-Mogollón, R. (2020). Impact of ICT Development on Economic Growth, A study of OECD European Union Countries, *Technology in Society*, (63), https://doi.org/10.1016/j.techsoc.2020.101420.

Hausman, J. (1978) Specification Tests in Econometrics, *Econometrica*, (46), 1251-1271, https://doi.org/10.2307/1913827.

IBM Security (2023). *Cost of a data breach report 2023,* https://www.ibm.com/reports/data-breach.

ITU (2023). Measuring digital development - ICT Development Index 2023, https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-2/.

ITU (2024). Measuring digital development - ICT Development Index 2024, https://www.itu.int/itu-d/reports/statistics/idi2024/.

ISACA (2022). The Human Consequences of Ransomware Attacks, https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/the-human-consequences-of-ransomware-attacks.

Kırtıllı, S. (2019). Cybersecurity and Economic Development: Comparing Developed, Developing and Emerging Economies, *Cyberpolitik Journal*, 4 (7), 43-69.

Miliefsky, G. (13.03.2025). The True Cost of Cybercrime: Why Global Damages Could Reach $1.2 - $1.5 Trillion by End of Year 2025, *Cyber Defense Magazine*, https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/.

Niebel, T. (2018). ICT and Economic Growth-Comparing Developing, Emerging and Developed Countries, *World Development*, (104), 197-211.

North, D.C. (1987). Institutions, Transaction Costs and Economic Growth, *Economic Inquiry*, 25, 419-428.

Pradhan, R. P., Arvin, M. B., Mittal, J., & Bahmani, S. (2016). Relationships Between Telecommunications Infrastructure, Capital Formation, and Economic Growth, *International Journal of Technology Management*, 70(2-3), 157-176.

Pradhan, R. P. (et al.) (2022). Institutional Development in an Information-Driven Economy: Can ICTs Enhance Economic Growth for Low- and Lower Middle-Income Countries?, *Information Technology for Development*, 28(3), 468-487.

Pimenta R.G.A. et al. (2023). Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review, *Data*, 9 (27), https://doi.org/10.3390/data9020027.

Rudnev, S.G., Zolkin, A.L., Artemyev, N.V., & Tychkov, A.S. (2024). The Economic Importance of Cybersecurity for Enterprises in The Context of Digital Transformation, *Economika I Upravlenie: Problemy, Resheniya.*

Saba, C. S. (et al.) (2024). Information and Communication Technology (ICT), Growth and Development in Developing Regions: Evidence from a Comparative Analysis and a New Approach, *Journal of Knowledge Economy*, (15), 14700-14748.

Shiu, A., & Lam, P. L. (2008). Causal Relationship Between Telecommunications and Economic Growth: A Study of 105 Countries, In the 17th Biennial Conference of the International Telecommunications Society, Montreal, 24-27.

Singh, H.P. & Alshammari T. S. (2020). An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia*, Beijing Law Review*, 11(3), 637-650, https://doi.org/https://doi.org/10.4236/blr.2020.113039.

Skierka, I. (2022). When Shutdown is no Option: Identifying the Notion of the Digital Government Continuity Paradox in Estonia's eID Crisis, Gov. Inf. Q., 40, 101781.

Stephens, K. K. (et al.) (2008). Discrete, Sequential, and Follow-Up Use of Information and Communication Technology by Experienced ICT Users, *Management Communication Quarterly*, 22(2), 197-231. https://doi.org/10.1177/0893318908323149.

Suzuki, R. (2024). Impact of 5GTechnology on Mobile Internet Usage in Japan, *International Journal of Technology and Systems*, No. 2, 9(4), 12-22.

Swamy, P. A. (1970), "Efficient Inference in a Random Coefficient Regression Model", *Econometrica: Journal of the Econometric Society*, 38(2), 311-323.

Tatoğlu Yerdelen, F. (2016), "Various Approaches for the Estimation of the Three-Dimensional Fixed and Random Effect Models", Eurasian Academy of Sciences Eurasian Econometrics, *Statistics&Emprical Economics Journal*, (5), 60-70.

Ünver, G. N. (2024). Comparison Of Cyber Security Policies of Türkiye And England, *Cyberpolitik Journal*, 8 (16), 49-84.

Yang, S., Kwon, Y., & Lee, S.T. (2020). The Impact of Information Sharing Legislation on Cybersecurity Industry, *Ind. Manag. Data Syst.*, (120), 1777-1794.

Zaiats, D., & Kytsyuk, I. (2024). The Role of Cybersecurity in International Economic Relations, *Herald UNU, International Economic Relations and World Economy*, DOI: 10.32782/2413-9971/2024-53-2.

Annex 1: List of the Group of Countries Based on Geographical Region.

Europe (EUR)	Asia-Pacific (ASP)	Arab States (ARB)	Africa (AFR)	Commonwealth of Independent States (CIS)	America (AMS)
Albania	Afghanistan	Algeria	Angola	Armenia	Antigua and Barbuda
Andorra	Bangladesh	Bahrain	Benin	Azerbaijan	Argentina
Austria	Bhutan	Comoros	Botswana	Belarus	Australia
Belgium	Brunei Darussalam	Djibouti	Burkina Faso	Kazakhstan	Bahamas
Bosnia and Herzegovina	Cambodia	Egypt	Burundi	Kyrgyzstan	Barbados
Bulgaria	China	Iraq	Cabo Verde	Russian Federation	Bolivia (Plurinational State of)
Croatia	Hong Kong, China	Jordan	Cameroon	Uzbekistan	Brazil
Cyprus	Indonesia	Lebanon	Chad		Canada
Czech Republic	Iran (Islamic Republic of)	Libya	Congo (Rep. of the)		Chile
Denmark	Japan	Mauritania	Côte d'Ivoire		Colombia
Estonia	Kiribati	Morocco	Dem. Rep. of the Congo		Costa Rica
Finland	Korea (Rep. of)	Oman	Equatorial Guinea		Cuba
France	Kuwait	Palestine	Eswatini		Dominica
Georgia	Lao P.D.R	Qatar	Ethiopia		Dominican Rep.

Germany	Macao, China	Saudi Arabia	Gabon	Ecuador
Greece	Malaysia	Somalia	Ghana	El Salvador
Georgia	Maldives	Syrian Arab Republic	Guinea-Bissau	Fiji
Hungary	Pakistan	Tunisia	Kenya	Guatemala
Iceland	Philippines	United Arab Emirates	Liberia	Grenada
Ireland	Samoa	Yemen	Lesotho	Honduras
Israel	Singapore		Madagascar	Jamaica
Italy	Sri Lanka		Malawi	Mexico
Latvia	Thailand		Mali	Mongolia
Liechtenstein	Timor-Leste		Mauritius	Myanmar
Lithuania	Tonga		Mozambique	New Zealand
Luxembourg	Vanuatu		Namibia	Nicaragua
Malta	Viet Nam		Nigeria	Panama
Moldova			Rwanda	Paraguay
Monaco			São Tomé and Príncipe	Peru
Montenegro			Senegal	Saint Kitts and Nevis
Netherlands (Kingdom of the)			Seychelles	Saint Lucia
North Macedonia			Sierra Leone	Saint Vincent and the Grenadines
Norway			South Africa	Suriname
Poland			Tanzania	Trinidad and Tobago
Portugal			Togo	United States
Romania			Uganda	Uruguay
San Marino			Zambia	Venezuela
Serbia			Zimbabwe	
Slovakia				
Slovenia				
Spain				
Sweden				
Switzerland				
Türkiye				
Ukraine				
United Kingdom				

DİJİTAL BÖLÜNMENİN TARİHSEL MATERYALİZM YAKLAŞIMI ÇERÇEVESİNDE DEĞERLENDİRİLMESİ

Emre ARSLANTAŞ[*]
ORCID ID: 0000-0002-8934-244X

Declaration[*]

Özet

Siber uzay insan hayatını kolaylaştırıcı etkiler yaratmakla birlikte insanlar ve devletler arasındaki mevcut eşitsizliklere yenilerini de eklemektedir. Bahse konu eşitsizliklerden biri olan dijital bölünme, siber uzaya erişim ve siber tekniklerin kullanılmasındaki farklılıkları ifade etmektedir. Dijital bölünmeye ilişkin literatür, kavramın ortaya çıkışına ve farklı seviye ayrımlar çerçevesinde eşitsizlik yaratan sonuçlarına odaklanmıştır. Ancak bu çalışma, siber uzayın maddi bir temele sahip olmasının dijital bölünmeyi sürekli olarak yeniden ürettiğini ileri sürmektedir. Siber tekniklerin günümüzde önemli bir üretici güç haline gelmesi ile dijital alandaki üretim ilişkileri, alt-yapının üst-yapıyı belirlemesi ve sınıf kategorizasyonun varlığı dijital bölünmeyi oluşturan temel nedenleri belirtmektedir. Başka bir anlatımla, dijital bölünme maddi ilişkilere dayanan yapısal bir olgu olarak kavranmalıdır. Dolayısıyla çalışmada tarihsel materyalizm yaklaşımı çerçevesinde dijital bölünme analiz edilmiş ve mevcut düzenin değişim potansiyeli tartışılmıştır.

Anahtar Kelimeler: Siber uzay, tarihsel materyalizm, dijital bölünme

THE EVALUATION OF THE DIGITAL DIVIDE WITHIN THE APPROACH OF HISTORICAL MATERIALISM

Abstract

Cyberspace creates facilitating effects on human life but also adds new ones to the existing inequalities between people and states. One of the inequalities in question, the digital divide, refers to the differences in access to cyberspace and the use of cyber techniques. The literature on the digital divide has focused on the emergence of the concept and its consequences, which

[*] Öğr. Gör. Dr., Selçuk Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, emre.arslantas@selcuk.edu.tr
[*] This article has been prepared without the use of any Artificial Intelligence (AI) tools or assistance.

create inequality within the framework of different levels of distinctions. However, this study asserts that the material basis of cyberspace continuously reproduces the digital divide. The fact that cyber techniques are becoming an important productive force today, production of relations in the digital field, the determination of the base over the superstructure and the existence of class categorisation indicate the fundamental reasons that create the digital divide. In other words, the digital divide should be understood as a structural phenomenon based on material relations. Therefore, in this study, the digital divide is analysed within the framework of the historical materialism approach and the potential for change in the current order is discussed.

Keywords: Cyberspace, historical materialism, digital divide

Giriş

1990'lı yıllarla birlikte bilgi teknolojilerinin kullanımının yaygınlaşması, bireyler ve devletler arasındaki eşitsizliklerin azalacağı yönünde güçlü bir beklenti yaratmıştır. Siber uzaya erişim maliyetinin düşük olması ve her yerden erişim; bahse konu beklentinin temelini oluşturmuştur. Ancak günümüzde gelinen nokta söz konusu beklentinin gerçekleşmemesi ve siber uzayın dijital bölünme olarak kavramsallaştırılan yeni bir eşitsizlik türü yaratmasıdır. Dijital bölünme, bireyler ve devletler arasında siber uzaya erişim ve siber tekniklerin kullanılmasında ortaya çıkan eşitsizlik olarak belirtilebilir (Hargatti, 2002: 2; Van Dijk, 2006: 222; Zhao & Elesh, 2018: 4). Ayanso vd. (2010: 304-305) göre dijital bölünme kavramı; ilk dönemde ABD özelinde kırsal-kentsel bölgeler arasındaki siber uzaya erişim farkına ilişkin refere edilirken, sonraki süreçte uluslararası alanda bireyler ve devlet arasındaki siber uzaya erişim ve teknoloji kullanımına yönelik eşitsizliği açıklamak amacıyla kullanılmıştır.

Dijital bölünme ile ilgili literatürü inceleyen Christoph Lutz, ilgili çalışmalarda siber uzaydaki eşitsizliğin üç farklı düzeyde irdelendiğini ortaya koymuştur. İlk düzey dijital bölünme çalışmaları, kullanıcılar arasındaki siber uzaya erişim farklılıklarını Eurobarometer ve ABD Ulusal Telekomünikasyon ve Bilgi İdaresi anketlerine dayanarak açıklamıştır. İkinci düzey çalışmalar, siber uzaya erişimden ziyade kullanıcıların siber uzaydaki uygulama ve hizmetleri kullanma becerileri arasındaki eşitsizlikler üzerine yoğunlaşmıştır. Üçüncü düzey araştırmalar ise erişim ve kullanım becerilerinin birbirine benzer seviyede olduğu durumlardaki siber uzay kullanımından yaratılan gelir eşitsizliğine ve siber uzay kullanımının zararlarının açıklanmasına odaklanmıştır (Lutz, 2019: 142-144). Robinson vd. (2015: 270) ise dijital bölünme kavramının genellikle yaş, cinsiyet, eğitim seviyesi, ekonomik gelir düzeyi ve

coğrafi konum gibi unsurlara dayalı olarak ortaya çıkan eşitsizlikleri açıklamak için kullanıldığını salık vermiştir.

Başka bir anlatımla, dijital bölünme literatürü çoğunlukla siber uzayda ortaya çıkan eşitsizliklerin sonuçlarına odaklanırken, eşitsizlikleri sürekli üreten yapısal ilişkileri göz ardı etmektedir. Bu çalışma, siber uzayın maddi ilişkilere dayanmasının dijital bölünmeyi yaratan ve onu sürekli hale getiren temel unsur olduğu iddiası üzerine inşa edilmiştir. Öyle ki, siber uzayda üretici güçler, üretim ilişkileri, sınıf gibi maddi unsurlar dijital bölünmenin yeniden üretimini sağlamaktadır. Siber uzayın var olmasını sağlayan unsurların başında gelen kullanıcılar gündelik işlerini yapmak ve varlığını idame ettirmek amacıyla siber uzaydaki uygulama, hizmet ve platformlara erişim sağlamaktadır (Akyeşilmen, 2018: 55; Kurnaz, 2016: 67; Hassan, 2022: 156). Kullanıcıya ek olarak fiziksel altyapı, mantıksal ve içerik katmanlarıyla bunları geliştiren bireyler, sanayiler ve platformlar aracılığıyla siber uzay var olmaktadır. Dolayısıyla çalışma, dijital bölünmenin teknolojik eşitsizliğin yanı sıra üretici güçlerin dağılımı, mülkiyet ilişkileri ve sınıfsal farklılıklar gibi maddi üretim ilişkilerinden kaynaklanması hasebiyle tarihsel materyalizm çerçevesinde kavranması gerektiğini savunmaktadır. İlk bölümde çalışmanın kuramsal zeminini oluşturan tarihsel materyalizm yaklaşımı irdelenerek, dijital bölünmenin incelenmesinde kullanılacak dört unsur (üretici güçler, üretim ilişkileri, alt-yapı ve üst yapı ve sınıf) açıklanmıştır. Çalışmanın ikinci bölümünde maddi ilişkiler nedeniyle sürekli üretilen dijital bölünme, bahse konu dört unsur üzerinden analiz edilmiştir. Sonuç bölümünde ise dijital bölünmeyi yaratan mevcut yapının değişim olanakları tartışılmıştır.

Tarihsel Materyalizm

Karl Marx ve Friedrich Engels tarafından geliştirilen tarihsel materyalizm, maddi üretim koşulları üzerinden tarihin açıklanmasını amaçlayan kuramsal bir yaklaşımı ifade etmektedir. Öyle ki, Marx'ın tarihe yönelik bakış açısı toplumsal değişimlerin neden ve nasıl meydana geldiği sorunsalı üzerine şekillenmiştir. Marx'a göre ifade edilen sorunsalın temelinde maddi üretim koşullarının ortaya çıkardığı sınıf çatışması bulunmaktadır. Daha da açmak gerekirse, üretici güçler ve üretim ilişkileri ile söz konusu unsurların ortaya çıkardığı sınıflar arasındaki mücadeleler, insanlık tarihinde görülen üretim biçimi değişimini oluşturan temel dinamiktir (Comninel, 2013: 44-45). Marx'ın tarihsel materyalizm yaklaşımı, insanlık tarihini geçmişte yaşanan olayların kronolojik sıralaması olarak görmekten ziyade geçmiş, bugün ve gelecekte koşullar arasında karşılıklı etkileşimi içeren bütünlüklü bir yapı olarak kavramaktadır (Avcı,

2022: 215-216). Tarihin bütünlüklü bir yapı olarak kavraması, Marx'ın tarihi değiştirmeyi hedeflemesini de içermektedir. Zira Marx, kendisinden önceki filozofların çalışmalarında sadece dünyayı yorumlama çabasına giriştiklerini, fakat asıl önemli olanın dünyayı değiştirmek olduğunu vurgulamıştır (Marx & Engels, 2010a: 5-8).

Marx'ın ifade edilen tarih anlayışının öznesi; üretim praksisi[2] sayesinde diğer canlılardan ayrışan ve toplumsal bir varlık olan insandır. Hodges'e (1959: 19-20) göre tarihsel materyalizmde üretim faaliyetleri, insanın doğayla ilişkisini biçimlendirmekle birlikte toplumsal ilişkilerinin temelini oluşturmaktadır. Söz konusu varsayım insan düşüncelerinin maddi koşullardan bağımsız var olamayacağı, başka bir ifadeyle bilincin maddi ilişkilerden türediğini açığa çıkarmaktadır. Yaşamını idame ettirme gerekliliği insanın üretim faaliyeti gerçekleştirmeyi kendi önceliği haline getirirken, bilinç dünyasının da söz konusu öncelik tarafından şekillenmesine neden olmaktadır (Levine & Sober, 1985: 310). Buradan hareketle, toplumların gelişimindeki birincil belirleyici unsur; düşünce, inanç ve ideolojilerden ziyade maddi ilişkilerdir. Benzer bir yaklaşımı savunan Engels (2020: 65), toplumsal değişim ve devrimlerin temel nedenlerinin üretim biçimlerindeki değişimlerde aranması gerekliliğini ileri sürmüştür. Dolayısıyla tarihsel materyalizmin tarihe yönelik yaklaşımında üretici güçler ve üretim ilişkileri ile söz konusu unsurlar arasındaki diyalektik ilişki ön plana çıkmaktadır.

Bir toplumun gelişim düzeyini belirleyen üretici güçler; iş aygıtları, makineler ve teknik bilgi -mevcut teknoloji- ile insan emeğini ve toplumsal iş bölümünü kapsamaktadır. Tarihsel süreç boyunca genellikle gelişme eğiliminde olan üretici güçler, ilkel toplumdan köleci topluma veya feodalizmden kapitalizme geçişte olduğu gibi toplumsal değişimde temel ve tek belirleyicidir (Marx & Engels, 2010c: 212; Engels, 2019: 112-113). Üretim ilişkileri ise insanlar arasındaki mülkiyet biçimleri, sınıfsal konumlanma ve karşılıklı ilişkileri, başka bir ifadeyle üreten insanlar arasındaki ilişkilerin toplamını belirtmektedir. Marx'a göre üretim ilişkileri bir toplumun siyasi, toplumsal ve entelektüel düşünüş biçimlerini oluşturmada öncü rol oynamaktadır (Marx & Engels, 2010d: 263). Üretim ilişkileri her tarihsel dönemde üretim güçleriyle bütünlüklü/uyumlu bir yapı oluşturmaktadır. Ancak üretim güçleri sürekli bir gelişim gösterirken, üretim ilişkileri ise uzun süre değişmeden kalma -durağan- özelliğine sahiptir (Yurdakul, 2018: 12-15).

[2] Üretim praksisi bağlamında insanı diğer canlılardan ayıran üç unsur bulunmaktadır. İlk olarak, insan üretim faaliyetini gerçekleştirmek için gerekli olan üretim araçlarını üretmekte ve geliştirmektedir. İkinci olarak, insan elinin evrimsel niteliği onu diğer canlılardan ayıran üretim yeteneğine sahip olmasını sağlamıştır. Zira başka hiçbir canlıda insan eline benzer bir organ bulunmamaktadır. Üçüncü olarak, insan üretim sürecine başlamadan önce üretim faaliyetinin sonucunun nereye varacağını tahayyül edebilmektedir. İnsana kıyasla diğer canlılar üretim faaliyetlerini bilinçsizce ve içgüdüsel olarak icra etmektedir (Marx & Engels, 2010e: 187-189).

Bahse konu hız farklılığı, üretim ilişkilerinin zamanla üretici güçlerin gelişimi önündeki bir engele dönüşmesine yol açmaktadır. Üretici güçler ile üretim ilişkileri arasında ortaya çıkan onulmaz çelişkinin artması, üretim biçimi değişiminin temelini oluşturmaktadır (Chambers, 2020: 3). Marx'ın üretim ilişkilerinin üretici güçlerin gelişimine ayak uyduramayacak hale gelmesinin üretim biçimi değişiminin seyrini belirlediğini belirtmesi söz konusu varsayımı doğrulamaktadır (Marx & Engels, 2010d: 263). Örneğin kişisel yükümlülükler ve toprağa bağlılıktan oluşan feodal üretim ilişkilerinin (senyör-serf ilişkileri); tarım teknolojisinin gelişimi, ticaretin yoğunlaşması ve nüfus artışı gibi üretici güçlerdeki gelişimi önce desteklemesi, sonra ise söz konusu gelişmelerin önüne engeller yaratması Avrupa'daki burjuvazi devrimlerine neden olmuştur (Avcı & Söker, 2017: 8-12). Görüldüğü üzere, tarihsel materyalizm yaklaşımı gelişen üretici güçlere bağıtlı olarak var olan üretim biçiminin nereye varacağı/evrileceğini vurgulamaktadır (Avcı & Ateş, 2019: 560). Üretici güçler ve üretim ilişkileri çerçevesinde tarihsel materyalizm toplumu alt-yapı ve üst-yapı kavramlarıyla analiz etmektedir.

Alt-yapı; tarihsel materyalizmde üretim güçleri ve üretim ilişkilerine dayanan maddi üretim koşullarını belirtmektedir. Üst-yapı ise siyaset, devlet, hukuk, din, eğitim, ideoloji ve kültür gibi kurum ve bilinç biçimlerini ifade etmektedir (Habermas, 1975: 289-290). Tarihsel materyalizm yaklaşımında alt-yapı üst-yapıyı şekillendirmektedir. Örneğin, Sanayi Devrimiyle birlikte üretim güçlerinde yaşanan ilerleme bir taraftan feodal hukuk düzeni ile siyasi kurumların değişime uygun olmadığını gösterirken, diğer taraftan İngiltere'de 1832 Parlamento Reformu gibi siyasal ve hukuki üst-yapı değişimlerini ortaya çıkarmıştır (Wood, 1991: 90-97). Bu noktada Engels'in tarihsel süreçte alt-yapının belirleyici olduğu, fakat siyasi, ideolojik ve hukuki unsurların -üst-yapının- da toplumsal gelişmeyi doğrudan etkileyebileceği vurgusu önemlidir (Marx & Engels, 2010f: 34). Başka bir anlatımla, mülkiyet yasası gibi hukuki düzenlemeler veya siyasi sistem değişikliği gibi üst-yapıdaki unsurlar bazı dönemlerde üretici güçleri ve üretim ilişkilerini etkileyebilmektedir. Dolayısıyla alt-yapı ve üst-yapı kavramsallaştırması tek yönlülükten ziyade çök yönlülüğü ve karşılıklı belirlenimciliği içermektedir.

Alt-yapı ve üst-yapı kavramsallaştırmasına ek olarak tarihsel materyalizm, toplumun analiz edilmesinde sınıf olgusunu öne çıkarmaktadır. Tarihsel materyalizm yaklaşımına göre toplumlar, üretim araçlarının mülkiyeti ve üretim süreçlerindeki pozisyon farklılığına bağıtlı olarak, başka bir ifadeyle üretici güçleri ve üretim ilişkileri temelinde ortaya çıkan karşıt sınıfları içermektedir (Scatamburlo-D'Annibale & McLaren, 2004: 187-191). Marx ve

Engels, tarihsel süreçte sınıflar arasında sürekli mücadeleler yaşandığından hareketle, toplumların tarihini sınıf mücadelesi tarihi şeklinde nitelendirmiştir (Marx & Engels, 2010b: 482). Marx ve Engels'in ifade edilen nitelendirmesi, sınıf mücadelesini tarihin motor gücü ve sınıfı ise tarihin öznesi olarak görmeyi gerektirmektedir. Tarihsel materyalist yaklaşımda tarihi yapan bireylerden ziyade ortak çıkarlar çerçevesinde bir araya gelen toplumsal sınıflardır. Öyle ki, köleci toplumlarda efendi ile köle, feodal toplumlarda ise senyörler ile serfler arasındaki sınıf mücadeleleri toplumsal devrimlerin meydana gelmesinde önemli bir rol oynamıştır (Marx & Engels, 2010a: 45-47). Günümüzde hâkim olan kapitalist sistem içerisinde ise üretim araçları mülkiyeti ile emek gücü arasındaki ayrıma dayanan sınıf mücadelesi yaşanmaktadır.

Burjuvazi; sermaye, fabrika, makine gibi Sanayi Devrimiyle birlikte ortaya çıkan üretici güçlere sahip olan ve üretim ilişkilerini denetiminde tutan sınıfı belirtmektedir. Proletarya ise üretim güçleri mülkiyetine sahip olmayan ve yaşamını idame ettirmek için emek gücünü satmak zorunda kalan sınıfı ifade etmektedir. Bu kapsamda burjuvazinin mevcut üretim ilişkilerini sürdürmeyi amaçlaması ve proletaryanın emek sömürüsüne karşı üretici güçlerin gelişimini sağlamaya yönelik mücadelesi kapitalist sistemdeki onulmaz çelişkiyi oluşturmaktadır. Topakkaya'nın (2009: 71) belirttiği üzere kapitalist toplumlarda üretici güçler ile üretim ilişkileri arasındaki değişim hızı farkının gittikçe açılması, sistem krizlerine yol açmakta ve toplumsal değişim için tarihsel bir zemin hazırlamaktadır. Dolayısıyla tarihsel materyalizmde sınıf kategorisi, toplumsal yapının analizinin yanı sıra tarihsel sürecin motor gücü olarak öne çıkmaktadır (Engels, 2019: 138-139). Tarihsel materyalizm yaklaşımında devletler ise sınıflı toplumların ortaya çıkmasıyla kurulmuş bir üst-yapı kurumu olarak egemen sınıfın çıkarlarını korumayı ve sınıf mücadelesini kontrol altında tutmayı amaçlamaktadır (Lockwood, 2006: 63-64).

Kapitalist sistemde devlet sermaye birikimini gözetirken, mülkiyet ilişkilerini de korumaktadır. Engels'e göre devlet, söz konusu işlevi nedeniyle toplumun tamamının çıkarlarını temsil etmekten ziyade üretim araçlarının mülkiyetine sahip olan sınıfın tahakkümünün devamlılığını sağlanmak için tasarlanmıştır (Marx & Engels, 2010d: 269-272). Marx ise üretim araçlarının kontrolüne sahip olan sınıfın baskı aracının devlet olduğunu ve söz konusu sınıfın ihtiyaçlarına göre devlet biçimlerinin şekillendiğini varsaymıştır (Marx & Engels, 2010a: 59; Marx & Engels, 2010b: 486). Bu çerçevede devlet tarihsel süreçte toplumsal yapıların incelenmesinde ve toplumsal değişimin gerçekleşmesindeki önemli unsurlardan birini teşkil etmektedir. Özetle, tarihsel materyalizm yaklaşımı ontolojik olarak

toplumsal gerçekliğin maddi ilişkiler temelinde inşa edilmesini, epistemolojik olarak toplumsal gerçekliğin üretici güçler ve üretim ilişkilerinin incelenmesiyle kavranmasını ve metodolojik olarak tarihi çelişkiler ve karşılıklı etkileşimler -diyalektik- üzerinden irdelemeyi içermektedir. İfade edilen çerçeve siber uzay bağlamında ortaya çıkan dijital bölünmenin incelenmesine katkı sunmaktadır.

Dijital Bölünme ve Tarihsel Materyalizm

Dijital bölünme genellikle gelir eşitsizliği ve teknolojik gelişim farklılıklarıyla açıklanmaya çalışılsa da mahiyeti söz konusu unsurlardan daha fazlasına işaret etmektedir. Bireyler ve devletler arasındaki dijital bölünme, tarihsel süreçte ortaya çıkan ekonomik eşitsizlik ve maddi ilişkilerin siber uzaya yansımasını ifade etmektedir. Başka bir anlatımla, dijital bölünmenin mevcut üretim tarzı olan kapitalizm içerisindeki üretici güçler ve üretim ilişkilerinin sonucunda ortaya çıktığı ileri sürülebilir. Nitekim siber uzay tıpkı buharlı makine ve elektrik gibi modern ekonominin önemli bir üretici gücü haline dönüşmüştür. UNCTAD'ın "Digital Economy Report 2024" başlıklı raporuna göre 2017-2022 arası dönemde e-ticaret satışlarının %60 oranında artarak 27 trilyon dolara ulaşması, siber uzayın üretici güçler arasındaki öneminin arttığını göstermektedir (United Nations Conference on Trade and Development [UNCTAD], 2024: xxiv). Dijital ekonominin ABD GSYİH'nin %10,3'üne, Çin GSYİH'nin yaklaşık %41'ine tekabül etmesi, siber uzayın günümüzde önemli bir ekonomik gelir üretme aracına dönüştüğünü somutlaştırmaktadır (Bureau of Economic Analysis [BEA], 2023: 4; Shi & di Canossa, 2024: 6). Siber uzayın üretici güç olarak kavranması, beraberinde insanların ve devletlerin siber uzaya erişimi ve siber tekniklerin kimin kontrolünde olduğunu hususlarını gündeme getirmektedir.

Günümüzde küresel düzeyde internet kullanıcı sayısı 5,5 milyara ulaşmıştır. Gelişmiş devletlerde nüfusun yaklaşık %90'ı internete erişim sağlayabilirken, gelişmekte olan ülkelerde ise söz konusu oran %70'in altına düşmektedir (International Telecommunication Union [ITU], 2024: 1). Dünya Bankası'nın "Digital Progress and Trends Report" başlıklı raporunda çoğunluğunu düşük ve orta gelirli devletlerde bulunan 2,7 milyar kişinin internete erişim sağlayamadığının belirtilmesi gelişmiş kapitalist devletler ile gelişmekte olan devletler arasındaki siber uzaya erişim farkını ve konvansiyonel alanda görülen merkez-çevre ilişkilerinin siber uzaya yansıdığını ortaya koymaktadır. Devletler arasındaki erişim farklılıklara ek olarak, kentsel ile kırsal alanlar, erkekler ile kadınlar ve yüksek ile düşük gelirli gruplar arasındaki karşılaştırmalarda her bir karşıtlıkta ilkinin ikincisine kıyasla siber

uzaya erişiminin daha yüksek düzeyde olduğu görülmektedir. Raporda söz konusu gruplar arasındaki erişim farklılığının gelişmekte olan devletlerde daha da derinleştiği tespit edilmiştir (WB, 2024: 3-15). Dolayısıyla günümüzde gelişen üretici güçleri kapsayan siber uzaya erişim farklılığı, kapitalist üretim biçiminin tarihsel süreçte bireyler ve devletler arasında meydana getirdiği maddi eşitsizliklerin siber uzaya genişlemesini açığa çıkarmaktadır. Siber uzaya erişimin yanı sıra siber tekniklerin mülkiyeti, dijital bölünmeyi ortaya çıkaran bir diğer unsurdur.

Siber uzayın ABD'de icat edilmesi ve zamanla diğer devletlerin siber uzaya eklemlenmesi, fiziksel ve mantıksal katmanlarda gelişmiş ülkelerin, gelişmekte olan ülkelere kıyasla öncü ve belirleyici bir konuma yerleşmesine zemin hazırlamıştır (Kurnaz, 2024: 2015). Siber uzayın çalışmasını sağlayan ana kök hizmet sağlayıcılarının gelişmiş Batılı devletlerde konumlandırılması ve küresel interneti birbirine bağlayan internet değişim noktalarının gelişmiş ülkelerde yoğunlaşması bahse konu varsayımı doğrulamaktadır (Vakataki'Ofa, 2022: 43). Dijital bölünmenin yapısal temellerini oluşturan bahse konu eşitsiz dağılım, kapitalist dünya sisteminin tarihsel coğrafi eşitsizliklerinin dijital alana yansıması olarak okunabilir. Sanayi devriminde fabrika ve makinelerin İngiltere ve ABD gibi gelişmiş devletlerde yoğunlaşmasının benzeri günümüzde siber uzay bağlamında da geçerlidir. Veri merkezleri, bulut bilişim, e-ticaret ve sosyal medya platformları, blok zincir, yapay zekâ gibi siber tekniklerin mülkiyeti ve kontrolü ise çok uluslu şirketler ve onların merkezinin bulunduğu kapitalist devletlerin tekelindedir. Siber uzayda hizmet sunan en büyük özel şirketlerin büyük çoğunluğunun ABD ve Avrupa menşeli olması, söz konusu varsayımı desteklemektedir (Boyd-Barrett, 2006: 28-32).

Bu durum gelişmiş kapitalist devletlerin üretici güçlerin geliştirilmesi ve patentlenmesi hususunda belirleyici aktörler olmasını sağlarken, gelişmekte olan devletleri ise siber tekniklerin kullanıcısı ya da veri üreticisi olmasına indirgemektedir. İkinci olarak, siber uzay üretim ilişkileri çerçevesinde bireyler ve devletlere yönelik yeni eşitsizlik biçimleri üretmektedir. Marx'ın sermayenin en yüksek kâra erişim amacıyla mekânsal eşitsizlikleri sürekli üretmesi varsayımı (Smith, 2008: 181), siber uzay yatırımları bağlamında kendisini göstermektedir. Öyle ki, siber tekniklere yatırımların ulusal düzeyde yüksek gelirli kesimlere veya yüksek kâr getirisi olan alanlara, küresel düzeyde ise gelişmiş devletlere yönlendirilmesi eşitsiz gelişime ve dijital bölünmenin ebedileşmesine neden olmaktadır. Eşitsiz gelişimin yanı sıra siber uzay, "dijital emek" olarak tanımlanan yeni emek biçimlerine yol açarak, kapitalist üretim ilişkilerini dönüştürmektedir. Dijital emek, siber tekniklere dayanan işlerin öneminin

diğerlerine nazaran daha fazla artmasını içermektedir (Fuchs 2014: 296). Söz konusu değişim; kodlama, yazılım geliştirme, veri analizi gibi teknik bilgi ve beceri gerektiren işlerin yüksek kazanç getirmesine sebep olmaktadır.

Ancak dijital bölünmüşlük sebebiyle bireyler arasında var olan erişim ve eğitim farklılıkları, teknik bilgiye sahip olmayan işçilerin düşük ücretli işlerde çalışmalarına neden olmaktadır. Siber uzay, küresel düzeyde işçilerin ulusal sınırlara bağlı olmaksızın rekabete girmesine ve otomasyon ve yapay zekâyla ikame edilen işler kapsamında ise iş kaybına sebep olabilmektedir. Bu durum işçi sınıfının bir kısmının siber uzaydan göreceli olarak imtiyaz elde etmesine karşılık çoğunluğunun olumsuz yönde etkilenmesine yol açmaktadır (Imran, 2023: 1-2). Öte yandan siber uzayda artık-değer, konvansiyonel alandaki gibi sanayide üretilen fiziksel bir üründen ziyade veri üzerinden elde edilmektedir. Goodwin'in (2015) belirttiği üzere; Meta kendi içeriğini üretmemekte, Uber'in mülkiyetinde herhangi bir taksi bulunmamakta, Airbnb herhangi bir gayrimenkule sahip olmamakta ve Aliexpress'in stokunda ürün bulunmamaktadır. Buna rağmen, bahse konu platformlar kullanıcılarının ürettiği içerik, veri ve satışlar üzerinden önemli gelirler elde etmektedir. Dolayısıyla kullanıcıların internet ve sosyal medyadaki arama yapmaları, görüntüledikleri web siteler, paylaşımlarından üretilen veriler ve kişisel veriye dayanan algoritmik veriler artık-değerin yeni kaynaklarını oluşturmaktadır (Nayak & Walton, 2024: 665-666).

Söz konusu artık-değer yaratma -verilerin üretilmesi, işlenmesi ve kâr amaçlı yeniden üretime sokulması süreçleri- dijital bölünmeyi meydana getiren üretim ilişkilerine tekabül etmektedir. Üretim araçlarına sahip kapitalist devletlerin verilerin mülkiyetine Google, Amazon, Meta gibi özel şirketler vasıtasıyla sahip olması sınıf ilişkilerinin siber uzaya genişlediğini açığa çıkarmaktadır. Özel şirketleri yeterince gelişmemiş olan gelişmekte olan devletler ise içerik üreticisi ve veri sağlayıcısı rolü icra etmektedir (Couldry & Mejias, 2019: 339-341; Narayan, 2022: 924). Dolayısıyla dijital bölünme, siber uzayda artık-değeri oluşturan verinin mülkiyetine sahip olanlar ile olmayanlar arasındaki eşitsizliğe dayanmaktadır. Üçüncü olarak, tarihsel materyalizmin alt-yapı ve üst-yapı kavramsallaştırması dijital bölünmenin yapısal niteliğini kavramada önemli bir rol üstlenmektedir. Siber uzayda alt-yapı; fiziksel ve mantıksal katmanlardan meydana gelen üretici güçler ile dijital emek, artık-değer ve bunların mülkiyetinden oluşan üretim ilişkilerini içermektedir. Campbell'a (2001: 124) göre Soğuk Savaş sonrası dönemde ar-ge ve teknolojik gelişimde özel şirketlerin öncü rol oynaması, bir taraftan özel şirketlerin teknolojik ilerlemeyi sağlayan unsurların mülkiyetine sahip olmasını

sağlarken, diğer taraftan teknoloji transferinde gelişmekte olan devletleri olumsuz yönde etkilemiştir.

Özel şirketlerin teknoloji paylaşımı olmaksızın gelişmekte olan devletler siber uzayda tüketici pozisyonunda kalmaktadır. Bu durum siber uzayda teknoloji mülkiyeti ve inovasyonunun merkezileştiğini ortaya koymaktadır. Soğuk Savaş sonrası dönemde dünyanın ideoloji yerine teknoloji ile bölündüğünü ileri süren Jeffrey Sack (2000), dünyanın yaklaşık %15'lik kısmının teknolojinin mülkiyetine sahip olduğunu, %52'lik kısmının kısmi bir şekilde teknolojiyi ürettiği -daha çok kullandığı- ve kalan %33'lük kısmın ise ne teknoloji ürettiği ne de söz konusu teknolojiyi kullanabildiğini belirtmiştir. Bu durum siber uzayda faaliyet gösteren önemli özel şirketlere sahip olan kapitalist devletlerin özel sektörü yeterince gelişmemiş olan gelişmekte olan devletler üzerinde belirleyici bir konumda olmalarına yol açarak dijital bölünmeyi ortaya çıkarmaktadır. Siber uzayda üst-yapı ise dijital teknolojilerin kullanımı ve yaygınlaştırılmasını etkileyen ideoloji, kültür, hukuk ve yönetişimi kapsamaktadır. İdeolojik olarak 1990'lı yıllarda siber uzayın egemenlikten bağışık olduğu varsayımı çerçevesinde siber özgürlük söylemi, 2000'li yılların başından itibaren ise dünyanın küresel bir köy haline geldiği varsayımı popüler olmuştur (Manjikian, 2010: 384-395; Akyeşilmen, 2016: 39; Söker, 2024: 231).

Ancak söz konusu söylemler genelde kapitalist devletler özelde ABD'nin çıkarlarına hizmet etmektedir. Siber özgürlük söylemi devletlerin siber uzayı düzenleme girişimlerini olumsuz yönde etkilerken, özellikle Meta'nın dünyayı birbirine bağlama misyonu Batılı değerlerin diğer coğrafyalara yayılmasına katkı sunmuştur (Haupt, 2021: 250; Demchak, 2016: 50). Bu durum gelişmekte olan devletlerin siber uzayı kendi değerlerine tehdit ve kültür emperyalizmi olarak görmelerine sebep olmaktadır. Benzer şekilde siber uzayda norm ve kural oluşturma, teknik altyapının yönetimi ve siber güvenlik gibi hususlara dayanan siber yönetişim, hâkim sınıfların çıkarlarını korumaya yönelik unsurlardan meydana gelmektedir. Nitekim siber yönetişim tarihsel materyalizmin altını çizdiği alt-yapı üst-yapıyı belirler varsayımına ilişkin pratik örnekler sunmaktadır. Özellikle siber uzayın hayatın her alanına eklemlendiği süreçten itibaren siber yönetişim tartışmalarında ön plana çıkan çok paydaşlı yönetişim modeli, aktör çeşitliliği ve şeffaflık vurgusuyla diğer yönetişim modellerinden ayrıştığı ifade edilmesine rağmen (Sahel, 2016: 159-161), özünde kapitalist devletlerin çıkarını koruyan mevcut düzeni ve asimetrik ilişkileri yeniden üretmektedir.

BM'nin de önerdiği çok paydaşlı yönetişim modelinde devletlerin daha az rol oynaması gerekliliği ileri sürülürken, özel şirketler, sivil toplum kuruluşları (STK) ve bireyler yönetişim sürecini şekillendiren aktörler olarak belirtilmektedir. Söz konusu modelde İnternet Tahsisli Sayılar ve İsimler Kurumu (*Internet Corporation of Assigned Names and Number*) ve İnternet Mühendisliği Görev Gücü (*Internet Engineering Task Force*) gibi merkezi ABD'de bulunan teknik kuruluşların görevlerine devam etmesi düşünülmektedir. Çok paydaşlı yönetişimin temel ilkeleri kapsayıcılık ve temsiliyet olsa da yönetişim sürecine her aktör aynı düzeyde katılamamaktadır (Jayawardane, 2015, s. 4-5). Gelişmekte olan devletlerin özel şirketlerinin ve STK'larının yeterince gelişmemiş olması, çok paydaşlı yönetişim modellerinde kapitalist devlet menşeli özel şirket ve STK'ların baskın konumda olmasına yol sebebiyet vermektedir. Dorwart'a (2020, s. 16) göre çok paydaşlı yönetişim modeli, Amerikan merkezli özel şirketlere ve teknik kuruluşlara geniş yetkiler vermesi sebebiyle Batılı kapitalist devletlerin çıkarlarını korumaktadır. Ben Wagner (2016, s. 167-171) ise çok paydaşlı yönetişim modelinin, mevcut siber uzay düzenini korumak ve yeni kurumların yaratılmasını engelleme hususunda işlevsel olduğunu salık vermiştir.

İfade edilen unsurlar, yönetişim sürecinin ve siber uzaya ilişkin kurallar ve standartların kapitalist Batılı devlet ve özel şirketlerin çıkarlarına göre şekillenmesine zemin hazırlamaktadır. Batılı kapitalist devletler çok paydaşlı yönetişim modeliyle siber uzayda başta kültür, hukuk, siyaset olmak üzere üst-yapı olarak tabir edilecek alanlarda önemli bir düzenleme yeteneği kazanırken, gelişmekte olan devletler ikincil konumda kalmaktadır. Dolayısıyla alt-yapı ve üst-yapı kavramsallaştırması kapsamında dijital bölünmenin erişim ve teknoloji farklılıklarının yanı sıra maddi ilişkilerin meydana getirdiği politik, ideolojik ve kültürel bir olgu olarak görülmesi gerekmektedir. Dördüncü olarak, dijital bölünme devlet içerisindeki ve devletler arasındaki sınıf ilişkileri çerçevesinde süreklilik kazanmaktadır. Modern toplumlarda yüksek gelire, iyi eğitime ve teknik becerilere sahip bireyler siber uzaya kolay erişebilmekte ve siber uzaydan daha fazla fayda sağlayabilmektedir. Öte yandan düşük gelirli insanlar ise siber uzaya erişmekte zorlanırken, siber uzaydan fayda sağlamaları yüksek gelirli insanlara nazaran daha azdır (Lee vd., 2025).

Başka bir anlatımla, yoksul ailelerde doğan çocuklar hızlı bir internet veya kaliteli bir bilgisayara sahip olamayabilirken, zengin ailelerde doğan çocuklar ise küçük yaşlardan itibaren hızlı bir internete, kaliteli bir bilgisayara ve ileri teknoloji eğitimine erişebilmektedir (Van Deursen & Van Dijk, 2019: 356). Dolayısıyla ulusal düzeyde dijital bölünme sınıf farklılıklarının bir sonucu olarak süreklilik kazanmaktadır. Uluslararası düzeyde ise dijital

bölünme; özel şirketler -özellikle teknoloji devleri (*Big Tech*)- ve onları destekleyen başta ABD olmak üzere kapitalist devletler ile siber tekniklerin üretimini yapamayan veya kontrolüne sahip olamayan bağımlı gelişmekte olan devletler arasındaki ilişkiler tarafından yeniden üretilmektedir. Öyle ki, günümüzde siber uzaydaki altyapı, hizmetler, platformlar ve uygulamalar bazında Google, Amazon, Apple, Microsoft, Meta, Twitter gibi ABD menşeli özel şirketler tekel konumundadır ve söz konusu şirketler ABD ve Batılı devletler tarafından desteklenmektedir (Kelton vd., 2022: 1983-1999). Diğer devletler ise sanayi devrimi sonrasında proletaryanın emek kazancını kapitalistlere aktarmasına benzer şekilde siber uzaydaki faaliyetleri ve verileriyle ABD menşeli özel şirketlerin kâr üretmelerine yardımcı olmaktadır (Hazlett, 2024: 74-82).

İfade edilen dijital bölünmenin devletler arası düzeyi, konvansiyonel alandaki burjuvazi ile proletarya arasındaki ilişkilerin siber uzaya yansıması şeklinde değerlendirilebilir. Daha doğru bir ifadeyle, siber uzaydaki dijital bölünme uluslararası düzeyde sınıf tahakkümünü açığa çıkarmaktadır. ABD ve Batılı devletler ile Çin siber uzaydaki üretim araçlarına sahip olmanın avantajıyla gelişmekte olan devletleri ve bu devletlerde ikamet eden kullanıcıları siber proletaryaya *(cyber-proletariat)* [3] dönüştürmüştür. Özel şirketlerin uygulama, hizmet ve programları vasıtasıyla kapitalist devletler, gelişmekte olan devletlerdeki dijital ekosistem ve veriler üzerinde kontrol yeteneği kazanmaktadır (Kwet, 2019: 7-10). Söz konusu kontrol yeteneği, konvansiyonel alandaki tahakküm biçimlerinin siber uzayda yeniden üretildiğini gün yüzüne çıkarmaktadır. Diğer taraftan üretim araçlarının mülkiyeti günümüzde siber uzayda kapitalist devletler arasında nüfuz mücadelesini ortaya çıkmaktadır. Çin'in 5G teknolojisindeki gelişimi ve Amerikan menşeli özel şirketlerin pazar payının daralmasını önlemek amacıyla ABD'nin Huawei'ye ambargo uygulaması söz konusu duruma örnek olarak verilebilir (Ryan & Burman, 2024: 356-360). Örnekten de anlaşılacağı üzere kapitalistler/burjuvazi arasında 20. yüzyılda ortaya çıkan dünya üzerindeki emperyalist mücadele 21. yüzyılda siber uzayın icadı ile teknolojik etki alanı paylaşım mücadelesine dönüşmüştür.

Siber uzaydaki söz konusu mücadelede devletler tarafsız düzenleyici olmaktan ziyade hâkim sınıfın çıkarlarını koruyan bir araç niteliğindedir. ABD'nin özel şirketlerin küresel pazardaki paylarını korumak amacıyla diplomatik destek ve yaptırımlar sunması, Çin'in ise sübvansiyonlar yoluyla yerel şirketlerinin uluslararasılaşma çabalarına katkı sunması bu

[3] Siber proletarya, siber uzayda değer üreten, veri veya faaliyetleriyle özel şirketlerin kar elde etmesini sağlayan yeni bir işçi sınıfı olarak tanımlanmaktadır (Schaupp, 2022: 16).

duruma örnek olarak verilebilir (Zámborský vd., 2023: 100-110). Örneklerin ortaya koyduğu üzere devletler siber uzaydaki teknikler ve faaliyetlere yönelik yasal düzenleyici olmakla birlikte kapitalist sistemdeki sınıf ilişkilerinin siber uzaya taşınmasındaki önemli bir aygıttır. Siber uzayda hâkim sınıfların çıkarlarının korunması ise devletler arasında farklılık göstermektedir. ABD özel şirketlerle yakın iş birliği kurarken, Çin özel şirketler üzerinde doğrudan denetim uygulamaktadır (Saura García, 2024: 3-4). Ancak değişmeyen unsur devletin siber uzaydaki üretim araçlarının kontrolüne sahip olan sınıfın çıkarlarını korumasıdır. Görüldüğü üzere üretici güçler ve üretim ilişkileri, alt-yapı ve üst-yapı arasındaki diyalektik ilişki ve sınıfsal ayrım, kapitalist sistemdeki onulmaz çelişkilerden biri olan dijital bölünmenin süreklilik kazanmasına neden olmaktadır.

Sonuç

Tarihsel materyalizm çerçevesinde incelendiğinde dijital bölünme, maddi ilişkilerin ortaya çıkardığı eşitsizliklerin siber uzaya yansımasını ifade etmektedir. Öyle ki, dijital bölünmenin kavramsallaştırılmasında vurgulanan bireyler ve devletler arasındaki siber uzaya erişim ve teknolojik düzey farklılıklarını kapitalist sistemin siber uzaya genişlettiği üretici güçler ve üretim ilişkileri üretmektedir. Mevcut düzende fiziksel altyapı ile mantıksal ve içerik katmanlarını oluşturan siber tekniklerin kapitalist devletlerin ve özel şirketlerin tekelinde olması, siber uzayda sınıf ilişkilerinin yeniden yaratılmasına yol açmaktadır. Bu düzende gelişmekte olan devletler ve söz konusu devletlerde ikamet eden kullanıcılar ise ABD ve Çin gibi devletlerde merkezi bulunan özel şirketlerin artık değerini üreten siber proletaryaları oluşturmaktadır. Sınıflar arasındaki mülkiyet ve kontrol eşitsizliği kültür, hukuk, siyaset, ideoloji gibi unsurların oluşturduğu siber uzayın üst-yapısında gelişmiş kapitalist devletler ve özel şirketlerin belirleyici konumda olmalarına sebebiyet vermektedir. Dolayısıyla dijital bölünme; siber uzayda maddi ilişkiler ve sınıf kategorisi bağlamında yeniden üretilen bir çıktı olarak kavramsallaştırılabilir.

Tarihsel materyalizm yaklaşımı, dijital bölünmüşlüğün ortadan kaldırılması için gerekli imkanların incelenmesini de gerektirmektedir. İlk olarak, maddi ilişkilere bağlı olarak ortaya çıkan dijital bölünmenin olumsuz etkilerinin mevcut sistemde yapılacak reformlarla azaltılması düşünülebilir. Fuch ve Horak (2007: 21), gelişmiş ile gelişmekte olan devletler arasındaki eşitsizliğin giderilmesine yönelik ileri sürülen ucuz cihaz sağlama, özelleştirme, teknoloji transferi, liberalleşme gibi teknolojik çözümler ve reform yaklaşımlarının Nijerya, Gana ve Güney Afrika örneklerinde yapısal nedenlere çözüm üretmeksizin dijital bölünmenin

etkilerinin minimize edilemeyeceğini açığa çıkarmışlardır. Bahse konu çözümler, mevcut sorunların olumsuz etkilerini azaltmaktan ziyade gelişmiş devletlerin ve özel şirketlerin gelişmekte olan devletlerin siber uzay altyapı ve mantıksal katmanlarındaki mülkiyetini ve kontrolünü daha da kuvvetlendirme potansiyeli taşımaktadır. Bu nedenle dijital bölünmenin olumsuz etkilerini azaltmak amacıyla devlet destekli toplumsal politikaların yürürlüğe konması gerekliliği öne çıkmaktadır.

Gelir dağılımında adaletin sağlanması, kalkınma yardımları, altyapı ve eğitim yatırımları, fiyat sübvansiyonları, yerel şirketlerin ve STK'ların desteklenmesi yürürlüğe konması gereken toplumsal politikaların başında gelmektedir. İfade edilen toplumsal politikalar ise devlet planlaması ve piyasaya müdahaleyi şart koşmaktadır. Ancak devletlerin ekonomik ve teknolojik yeteneklerinin farklılığı ile gelişmiş kapitalist devlet ve özel şirketlerin siber uzaydaki tahakkümü, bahse konu toplumsal politikaların dijital bölünmenin olumsuz etkilerinin azaltılması hususunda her coğrafya ve devlet bazında benzer sonuçlar yaratmasını engellemektedir. Dolayısıyla teknolojik çözümler ve devlet destekli toplumsal politikaların birleşiminden oluşacak reform girişimlerinin de mevcut yapı içerisindeki eşitsizliği çözemeyeceği ileri sürülebilir. Bu durum tarihsel materyalizm yaklaşımının maddi ilişkilerin meydana getirdiği eşitsizliğin üretim biçimindeki değişim ve devrimle ortadan kaldırılabileceğine yönelik varsayımını doğrulamaktadır. Tarihsel materyalizme göre üretim biçimindeki değişimin veya devrimin oluşması için bakılması gereken unsur üretici güçler ile üretim ilişkileri arasındaki onulmaz çelişkinin mevcut durumudur.

Siber uzay icadından günümüze kapitalist sistemdeki üretici güçleri önemli ölçüde dönüştürürken, veri, algoritma, e-ticaret, yapay zekâ gibi unsurlar ekonomik yapının temelini oluşturmuştur. Bahse konu dinamikler, tarihsel materyalizmin üretici güçlerin tarihsel süreçteki hızlı gelişimi için verilebilecek bir örnektir. Diğer taraftan mevcut üretim ilişkileri ise tıpkı tarihsel materyalizmin vurguladığı gibi üretici güçlerin gelişimini teşvik etmektedir. Üretici güçlerin mülkiyeti, altyapı ve mantıksal katmandaki kapitalist tekelleşme ile özel şirketler vasıtasıyla artık-değer sömürüsü konvansiyonel alanda var olan sınıf yapısının siber uzayı kapsamasını sağlamaktadır. Bununla birlikte yazılım geliştiriciler ve veri bilimciler gibi teknik bilgiye sahip profesyoneller, yüksek ücretli iş garantisi ve toplumsal prestije sahip olmaları hasebiyle mevcut sistemi desteklemektedir. İfade edilen unsurlar tarihsel materyalizmin devrim için vurguladığı üretici güçler ve üretim ilişkileri arasındaki onulmaz çelişki eşiğine siber uzayda henüz ulaşılamadığını ortaya koymaktadır. Bu durum siber

uzayda üretici güçlerin gelişimi ve üretim güçleri arasındaki uyumun sorunsuz ilerlediği anlamına gelmemektedir.

2000'li yılların ortalarından itibaren siber uzayın altyapı ve mantıksal katmanlarındaki Amerikan hegemonyasına karşılık siber egemenlik vurgusunun artarken, Amerikan menşeli özel şirketlerin uygulama ve hizmet tekellerinin sınırlandırılmasına yönelik çabalar yoğunlaşmıştır. Başta Çin olmak üzere diğer devletlerin siber tekniklerde ilerlemesinin ABD yaptırımlarıyla engellenmesi girişimleri, üretim ilişkilerinin üretici güçlerin gelişimine yönelik engeller yaratmaya başladığını açığa çıkarmaktadır. Ek olarak, teknik bilginin geniş halk kitlesine yayılması ve yapay zekânın teknik bilgi gerektiren işleri yerine getirir hale gelmesi, teknik bilgiye sahip profesyonellerin önemini azaltma ve yeni üretim ilişkilerinin ortaya çıkması potansiyelini içerisinde barındırmaktadır. Bahse konu unsurlar, önümüzdeki süreçte üretici güçler ile üretim ilişkileri arasındaki onulmaz çelişkilerin yoğunlaşmasına ve üretim biçiminin değişmesine yol açacak toplumsal devrimin meydana gelmesine zemin hazırlayabilir. Tarihsel materyalizm açısından değerlendirildiğinde günümüzdeki üretici güçler ve üretim ilişkileri arasındaki uyum sürekli olmaktan ziyade geçici bir nitelik taşımaktadır.

Başka bir anlatımla, siber uzay mevcut üretim biçiminin onulmaz çelişkiler ürettiği bir alana dönüşmektedir. Bu sürecin yaratacağı etkiler; mevcut düzenin devam etmesi bağlamında dijital bölünmenin derinleşmesine veya yeni üretim ilişkileri bağlamında dijital bölünmenin etkisinin azalmasına neden olabilecektir. Tüm bu ifadelerden hareketle, dijital bölünme erişim ve teknoloji farklılıklarını ortaya çıkaran üretici güçler ile üretim ilişkilerinin siber uzayda yarattığı bir fenomen olarak kavranmalı ve incelenmelidir.

Kaynakça

Akyeşilmen, N. (2016). "Cybersecurity and Human Rights: Need For A Paradigm Shift?", *Cyberpolitik Journal*, 1(1), 32-55.

Akyeşilmen, N. (2018). *Disiplinler Arası Bir Yaklaşımla Siber Politika & Siber Güvenlik*. Ankara: Orion Kitabevi.

Avcı, Y., & Söker, Ç. (2017). "Tanımazlıktan anlaşılmazlık sorununa: Uluslararası İlişkilerde Karl Marks". *Akademik Yaklaşımlar Dergisi*, 8(2), 1-34.

Avcı, Y., & Ateş, D. (2019). "Marks'ın Sınıf Tasnifi ve Günümüz Kapitalizminde Sermayenin Değişmeyen Nitelikleri". *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *21*(2), 555-583.

Avcı, Y. (2022). *Diyalektik Materyalizm ve Küresel İlişkilerin Öznesi olarak Sınıf*. Konya: Billur Yayınevi.

Ayanso, A., Cho, D. I., & Lertwachara, K. (2010). "The digital divide: global and regional ICT leaders and followers". *Information Technology for Development*, 16(4), 304–319

Boyd-Barrett, O. (2006). "Cyberspace, globalization and empire". *Global Media and Communication*, *2*(1), 21-41.

Bureau of Economic Analysis. (2023). *Measuring the digital economy: New insights and next steps* (BEA Working Paper No. 2023-5). Erişim Adresi https://www.bea.gov/sites/default/files/papers/BEA-WP2023-5.pdf.

Campbell, D. (2001). "Can the digital divide be contained?". *International Labour Review*, 140(2), 119-141.

Chambers, C. L. (2020). "Historical materialism, social change, and the necessity of revolutionary optimism." *Human Geography*, 14(2), 296-300.

Comninel, G. C. (2013). "Critical thinking and class analysis: Historical Materialism and Social Theory". *Socialism and Democracy*, 27(1), 19–56.

Couldry, N., & Mejias, U. A. (2019). "Data colonialism: Rethinking big data's relation to the contemporary subject". *Television & New Media*, 20(4), 336-349.

Demchak, C. C. (2016). "Uncivil and Post-Western Cyber Westphalia: Changing interstate power relations of the cybered age". *The Cyber Defense Review*, 1(1), 49-74.

Dorwart, H. (2020, December 15). *Data Governance in China: Emerging trends for the next decade* (SSRN Working Paper No. 4005414). Erişim Adresi https://ssrn.com/abstract=4005414.

Engels, F. (2019). *Ailenin, Özel Mülkiyetin ve Devletin Kökeni.* (E. Özalp, Çev.) İstanbul: Yordam Kitap.

Engels, F. (2020). *Socialism: Utopian and Scientific*. Paris: Foreign Languages Press.

Fuchs, C. (2014). *Digital Labour and Karl Marx*. New York and London: Routledge.

Fuchs, F & E. Horak (2007). "Informational Capitalism and the Digital Divide in Africa". *Masaryk University Journal of Law and Technology*, 1(2), 11–32.

Goodwin, T. (2015, March 3). *The battle is for the customer interface*. *TechCrunch*. Erişim Adresi https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/.

Habermas, J. (1975). "Towards a reconstruction of Historical Materialism". *Theory and Society*, 2(3), 287–300.

Hargittai, E. (2002). "Second-Level Digital Divide: Differences in People's Online Skills". *First Monday*, 7(4). 1-19.

Hassan, M. M. (2022). "How the Cyberspace Affect the Cooperation among the States in the Field of Human Rights". *Cyberpolitik Journal*, *7*(14), 155-181.

Haupt, J. (2021). "Facebook futures: Mark Zuckerberg's discursive construction of a better World". *New Media & Society*, 23(2), 237-257.

Hazlett, T. W. (2024). "US antitrust policy in the age of Amazon, Google, Microsoft, Apple, Netflix and Facebook". *Constitutional Political Economy*, 35(1), 73-108.

Hodges, D. C. (1959). The Role of Classes in Historical Materialism. *Science & Society*, *23*(1), 16-26.

Imran, A. (2023). "Why addressing digital inequality should be a priority". *The Electronic Journal of Information Systems in Developing Countries*, 89(3), 1-12.

International Telecommunication Union [ITU]. (2024). *Measuring digital development: Facts and figures 2024*. Erişim adresi https://www.itu.int/en/ITU-D/Statistics/pages/facts/default.aspx.

Jayawardane, S., Larik, J. E., & Jackson, E. (2015). *Cyber governance: Challenges, solutions and lessons for effective global governance* (Policy Brief No. 17). The Hague Institute for Global Justice. Erişi Adresi http://www.thehagueinstituteforglobaljustice.org/information-for-policy-makers/policy-brief/cyber-governance-challenges-solutions-and-lessons-for-effective-global-governance/.

Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). "Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States". *International Affairs*, 98(6), 1977-1999.

Kurnaz, İ. (2016). "Siber güvenlik ve ilintili kavramsal çerçeve". *Cyberpolitik Journal*, 1(1), 56-77.

Kurnaz, İ. (2024). "What Kind of Theory of International Relations in the Context of Cyberspace?". *Cyberpolitik Journal*, 9(18), 208-227.

Kwet, M. (2019). "Digital colonialism: US empire and the new imperialism in the Global South". *Race & class*, 60(4), 3-26.

Lee, J., Hamilton, J., Ram, N., Robinson, T., & Reeves, B. (2025). "Digital Inequality and Access by Low-Income Individuals to Public Benefits". *Journal of Quantitative Description: Digital Media*, 5, 1-54.

Levine, A., & Sober, E. (1985). "What's historical about historical materialism?". *The Journal of Philosophy,* 82(6), 304-326.

Lockwood, D. (2006). "Historical Materialism and the State". *Critique*, 34(2), 163-178.

Lutz, C. (2019). "Digital inequalities in the age of artificial intelligence and big data". *Human Behavior and Emerging Technologies*, 1(2), 141-148.

Manjikian, M. M. (2010). "From global village to virtual battlespace: The colonizing of the internet and the extension of realpolitik". *International Studies Quarterly*, 54(2), 381-401.

Marx, K., & Engels, F. (2010a). *Collected Works* (Cilt 5). Londra: Lawrence & Wishart.

Marx, K., & Engels, F. (2010b). *Collected Works* (Cilt 6). Londra: Lawrence & Wishart.

Marx, K., & Engels, F. (2010c). *Collected Works* (Cilt 9). Londra: Lawrence & Wishart.

Marx, K., & Engels, F. (2010d). *Collected Works* (Cilt 29). Londra: Lawrence & Wishart.

Marx, K., & Engels, F. (2010e). *Collected Works* (Cilt 35). Londra: Lawrence & Wishart.

Marx, K., & Engels, F. (2010f). *Collected Works* (Cilt 49). Londra: Lawrence & Wishart.

Nayak, B. S., & Walton, N. (2024). "The future of platforms, big data and new forms of capital accumulation". *Information Technology & People*, 37(2), 662-676.

Narayan, D. (2022). "Platform capitalism and cloud infrastructure: Theorizing a hyper-scalable computing regime". *Environment and Planning A: Economy and Space*, 54(5), 911-929.

Ryan, M., & Burman, S. (2024). "The United States–China 'tech war': Decoupling and the case of Huawei". *Global Policy*, 15(2), 355-367

Robinson, L., Cotten, S., Ono, H., Quan-Haase, A., Mesch, G., Chen, W., Stern, M. (2015). "Digital inequalities and why they matter". *Information, Communication & Society*, 18(5), 569–582.

Sack, J. (2000, June 22). *A new map of the world. The Economist*. Erişim Adresi https://www.economist.com/unknown/2000/06/22/a-new-map-of-the-world.

Sahel, J. J. (2016). "Multi-stakeholder governance: a necessity and a challenge for global governance in the twenty-first century". *Journal of Cyber Policy*, 1(2), 157–175.

Saura García, C. (2024). "Digital expansionism and big tech companies: consequences in democracies of the European Union". *Humanities and Social Sciences Communications*, *11,* 1-8.

Scatamburlo-D'Annibale, V., & McLaren, P. (2004). "Class dismissed? Historical materialism and the politics of 'difference'". *Educational Philosophy and Theory*, 36(2), 183-199.

Schaupp, S. (2022). "Cybernetic proletarianization: spirals of devaluation and conflict in digitalized production". *Capital & Class*, 46(1), 11-31.

Shi, R., & di Canossa, V. (2024). *China in numbers (2023)*. UNDP Issue Brief, Erişim adresi https://www.undp.org/sites/g/files/zskgke326/files/2024-03/china_in_numbers_2023-final.pdf.

Smith, N. (2008). *Uneven Development: Nature, Capital, and the Production of Space*. USA: The University of Georgia Press.

Söker, Ç. (2024). "Cyberspace and Nation-State: Revisiting Sovereignty". *Cyberpolitik Journal*, 9(18), 228-238.

Topakkaya, A. (2009). "Tarihsel Materyalizm ve Diyalektik". *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 1(27), 65-77.

United Nations Conference on Trade and Development [UNCTAD]. (2024). *Digital economy report 2024: The digitalization divide and the future of global development*. Erişim adresi https://unctad.org/system/files/official-document/der2024_en.pdf.

Vakataki'Ofa, S. (2022). "Estimating the effects of internet exchange points on fixed-broadband speed and latency". *Asia-Pacific Sustainable Development Journal*, 28(2), 39-68.

Van Deursen, A. J., & Van Dijk, J. A. (2019). "The first-level digital divide shifts from inequalities in physical access to inequalities in material Access". *New media & society*, 21(2), 354-375.

Van Dijk, J. A. (2006). "Digital divide research, achievements and shortcomings". *Poetics,* 34(4-5), 221-235.

Wagner, B. (2016). *Global Free Expression: Governing the Boundaries of Internet Content*, Switzerland: Springer.

Wood, E. M. (1991). *The Pristine Culture of Capitalism: A Historical Essay on Old Regimes and Modern States*. London and New York: 1991.

World Bank (2024). *Digital Progress and Trends Report 2023*. Washington, DC: World Bank.

Yurdakul, Ç. (2019). "Marx'ın Tarih Anlayışı: Tarihsel Materyalizm". *Maarif Mektepleri Uluslararası Sosyal ve Beşeri Bilimler Dergisi*, 1(3), 1-19.

Zámborský, P., Yan, Z. J., Michailova, S., & Zhuang, V. (2023). "Chinese multinationals' internationalization strategies: new realities, new pathways". *California Management Review*, 66(1), 96-123.

Zhao, S., & Elesh, D. (2018). "The Second Digital Divide: Unequal Access to Social Capital in the Online World". *International Review of Modern Sociology*, 44(1/2), 1–22.

THE RISE OF LLMS IN BUREAUCRACY AND MILITARY DECISION-MAKING AND THE CYBERSECURITY IMPERATIVE

Gloria Shkurti ÖZDEMİR*
ORCID ID: 0000-0001-8626-9761

Declaration*

Abstract

Large Language Models (LLMs) are rapidly transforming decision-making processes across bureaucratic and military institutions. Their ability to synthesize data, simulate complex scenarios, and generate real-time strategic insights is driving adoption in public sector settings, with initiatives like OpenAI's "ChatGPT Gov" already deployed across U.S. federal agencies. However, the integration of LLMs into core governance and defense infrastructures introduces profound risks. Beyond technical concerns such as data poisoning, adversarial attacks, and insider misuse, these models also raise normative challenges, escalation bias in military applications, erosion of institutional accountability, and dependency on opaque corporate infrastructures. This article critically examines the operational use of LLMs in bureaucratic and military domains, analyzes the cybersecurity and geopolitical risks they pose, and frames their adoption within broader debates on technological sovereignty, corporate power, and data colonialism. Lastly, the article provides several recommendations that can offer some insight into how states, particularly middle and regional powers, can reclaim agency, enhance institutional resilience, and push for more effective regulatory frameworks in the face of accelerating LLM integration and corporate dominance.

Keywords: AI, Decision Making, Foreign Policy, Military, Threats, Cybersecurity

Introduction

Since the public release of ChatGPT in late 2022, not only has artificial intelligence undergone a pivotal transformation, but so too has the global landscape in which humans work, govern, and make decisions. The arrival of advanced large language models (LLMs)

* Director of Emerging Technologies and AI (ETAI) Center at Khazar University, Azerbaijan and Researcher at SETA Foundation, Türkiye
* The author acknowledges the assistance of ChatGPT model in language editing. All analysis and conclusions are solely the author's responsibility.

marked a historic moment, fueling discussions around the "democratization of technology," as once-exclusive computational capabilities became widely accessible to the public (Shkurti Özdemir, AB, Yapay Zekâ Düzenlemesinde Küresel Lider Olabilecek mi?, 2024).

Yet, as the initial excitement of open-access AI gave way to more critical reflection, the dual-use nature of these technologies became evident. While LLMs can empower individuals and increase productivity, they also hold strategic significance for governments and militaries. It was only a matter of time before their integration into the public sector and defense infrastructures began.

Today, the use of LLMs in governance is no longer speculative. Across the globe, bureaucratic agencies and defense institutions are actively experimenting with and deploying LLMs to automate routine functions, assist in policy analysis, and streamline administrative tasks. However, the most consequential shift lies not in automating clerical work, but in the gradual incorporation of LLMs into decision-making processes themselves, both in civil administration and in military contexts.

The appeal of LLMs stems from their capacity to scale cognitive labor and process vast amounts of information rapidly. Yet, their integration into core governance functions also introduces new vectors for cybersecurity threats, systemic vulnerabilities, and ethical concerns (Karaguezian, 2024, pp. 243-244). As these systems begin to shape high-stakes outcomes, the risks of bias, manipulation, and loss of institutional accountability grow accordingly.

This paper explores the dual-edged implications of LLM adoption in state systems. Specifically, it analyzes the ways in which LLMs are being operationalized within bureaucratic and military domains and assesses the emergent cybersecurity threats associated with their deployment.

Bureaucratic Adoption of Large Language Models

Bureaucracy, at its core, emerged as a response to the growing need for systematic information management. One of the earliest manifestations of this can be traced back to ancient Mesopotamia, where written records on clay tablets were used to document royal assets and economic transactions. However, as the volume of such records expanded, the challenge of organizing, storing, and retrieving critical information became increasingly apparent. Bureaucracy evolved as an institutional mechanism to address these problems,

structuring administrative functions and enabling information governance (Harari, 2024, pp. 45-48). Over time, bureaucracies adapted to successive waves of technological transformation, from paper-based filing systems to digital databases. Today, amid the exponential growth of data, we are witnessing another pivotal shift: the integration of advanced technologies such as large language models. These models are not merely tools for digitization, but catalysts for reimagining how bureaucratic systems process information, make decisions, and interact with the public.

As LLMs increasingly move from the periphery to the center of technological ecosystems, their adoption within public administration has accelerated. What began as experiments in automating low-level clerical tasks has evolved into a much deeper transformation of the bureaucratic imagination. LLMs, at the beginning, were used as conversational agents, i.e. chatbots or virtual assistants, for different public-facing services (Lund & Ting, 2023) or as tools for the summarization and translation of documents (Council of the European Union, 2023, p. 9). However, currently they are being considered, and in some cases even actively integrated, into different tasks that can inform or impact administrative decision-making.

However, this intensifying integration of LLMs within the administrative decision-making brings several uncertainties with it. Specifically, when the cognitive labor previously done by human administrators is delegated to opaque and probabilistic systems such as LLMs this erodes the discretionary space that was reserved just for the human administrator. Even more importantly, such a delegation challenges directly the well-established normative foundations within the public sector, including here the fact that decisions need to be transparent, justifiable, and aligned with the public interest. Within this context, the concern becomes higher when we acknowledge that the decision-making in bureaucracy includes matters of great national importance, such as foreign policy, military interventions, and in some cases even decisions relations to the nuclear command. These risks augment further when we consider not only the threat coming from the models themselves but also their growing exposure to possible cybersecurity threats and from a global affairs perspective, the geopolitical dependence of the states that cannot develop these models on the foreign-owned AI systems. Within this framework, when we consider the fact that LLMs are transitioning from simple tools of administrative convenience towards important actors within the decision-making chain, it can be said that this marks a very important turning point requiring great oversight.

Real-World Deployments

While integrating LLMs within the public sector was considered to happen maybe later in the future, now their deployment, even for decision making purposes, is no longer speculative. Today we can speak about the integration of LLMs with prominent variations in scope, ambition, and institutional design across different national domains. Several governments have begun experimenting with or formally deploying LLMs within their administrative systems. A particularly significant case is that of the United States. In In October 2024, the Biden administration released a policy directive urging U.S. national security institutions to prioritize the adoption of artificial intelligence technologies. The memo emphasized the importance of leveraging AI models and related tools across federal agencies, particularly within national security operations (The White House, 2024). Within this framework, soon after Trump assumed presidency a strategic partnership between OpenAI and public institutions has given rise to ChatGPT Gov, a customized version of ChatGPT designed specifically for governmental use. Launched in early 2025, ChatGPT Gov allows U.S. agencies to access OpenAI's frontier models within secure, self-managed cloud environments that adhere to federal cybersecurity standards (OpenAI, 2025).

The initiative marks a qualitative shift in how public bureaucracies conceptualize AI integration, not merely as an efficiency tool but as a structural component of digital governance. According to OpenAI, since 2024, more than 90,000 users across over 3,500 federal, state, and local government entities have exchanged upwards of 18 million messages using ChatGPT Enterprise to assist with their daily workflows (OpenAI, 2025). These use cases span a wide spectrum, from document drafting and administrative support to data analysis and internal communication.

Unlike commercial versions, ChatGPT Gov is deployed within government-controlled Microsoft Azure infrastructures, including both commercial and government community cloud environments. This architecture allows agencies to retain sovereignty over key aspects such as data privacy, security protocols, and compliance frameworks, offering a model of AI adoption that seeks to balance innovation with institutional risk management.

The U.S. model reflects not only technological ambition but also a growing recognition that future governance may hinge on the controlled, context-specific deployment of advanced

language models. Yet, at the same time, as it will be discussed below, it raises critical questions about long-term dependence on private sector actors for the core infrastructure of public administration.

Another notable example of LLM integration in the bureaucratic sphere, though currently in the research and pilot phase, is the Indonesian Ministry of Finance's development of KemenkeuGPT. This domain-specific language model has been trained on a substantial corpus of national economic data, fiscal policy frameworks, and regulatory documents, enriched by iterative expert feedback from within the Ministry itself. While not yet deployed for operational use, KemenkeuGPT is envisioned as a strategic decision-support system, designed to facilitate policy simulations, generate tailored financial reports, and enhance internal modeling and forecasting capacities (Febrian & Figueredo, 2024). Its development reflects a deliberate effort to build sovereign AI capabilities tailored to the unique informational demands of a specific governmental domain. As such, KemenkeuGPT offers an important contrast to off-the-shelf LLM deployments, representing a model of targeted, context-sensitive AI integration that seeks to retain institutional control over core knowledge infrastructures.

A third example regarding the integration of LLMs in public administration is that of "Pubbie," a project developed by Canada's National Research Council (NRC). Pubbie, which was started as a part of a broader AI program launched by NRC in May 2024, is currently in the experimental phase and is designed to support government operations, especially in the area of research and innovation policy. Specifically, by searching vast academic and technical databases, spotting new fields with scientific value, and matching national research funding with strategic priorities, the model is intended to support the civil servants. Furthermore, Pubbie's main function is to improve the evidence-based decision-making within NRC by offering timely and contextualized insights, this way showing how LLMs can be effective when used for high-level policy coordination (Liu, Geng, & Hart, 2025). It is also important to state the fact that this model is part of a larger initiative in Canada, namely the Artificial Intelligence Strategy for the Federal Public Service, launched in March 2025. At some extend similar to the above-mentioned initiative by the U.S., the strategy in Canada establishes the main frameworks for the responsible integration of AI into federal agencies, placing a focus on openness, responsibility, and creativity in service provision (Government of Canada, 2025).

Lastly, another example of the integration of LLM within the bureaucratic domain is that of LLaMandement which is used in France. This model was designed to automate the analysis and summarization of parliamentary documents. LLaMandement improves the effectiveness and transparency of the parliamentary workflows and at the same time it reduces the administrative load on legislative staff. This way, by speeding up the processing and accessibility of legislative texts, the model helps to create a more responsive lawmaking process (Gesnouin et al., 2024)**.** Concurrently, it can be stated that the adoption of this model within the French bureaucracy is a reflection of France's broader strategic objective that aims to achieve digital sovereignty. As a result, the LLaMandement represents how these models can be used not only to help the bureaucratic processed but when seen from the global perspective they are also seen as instruments of national autonomy.

The Military Turn: LLMs and the Rise of Agentic Warfare

Focusing on the military domain, the adoption of AI and LLMs especially within the military operations reflects a shift and change in the character of the warfare (Shkurti Özdemir, 2024). Considering the fact that LLMs can process large amount of data at a much faster rate than the human operators can, these models can then make decisions faster, can allocate resources more efficiently, and at the same time can improve the communication within the military hierarchies (Rivera, et al., 2024, p. 1). According to Puscas, these models can be used for several purposes including strategic simulations, wargaming scenarios, operational planning, the creation of multiple courses of action, and real-time threat identification (Puscas, 2024, p. 15). Their capacity to automate scenario development and streamline decision support systems makes them increasingly indispensable in high-tempo, complex conflict environments.

While traditionally framed as tools for textual generation and summarization, LLMs are now being embedded within agentic AI systems, autonomous frameworks capable of perception, decision-making, and dynamic interaction with real-world data (Jensen, Tadross, & Strohmeyer, 2025). This shift signals the emergence of what is increasingly referred to as *agentic warfare*, a new paradigm in which AI agents actively shape the tempo and direction of conflict across all domains.

States, now aware of the accelerating pace of the modern warfare, where the responses within military operations need to occur within seconds, are highly investing in AI adoption in military domain in order to avoid being strategically outmaneuvered. Considering also its

technological superiority, the U.S. stands out as a leader in terms of its efforts to incorporate LLMs and agentic AI systems into its defense infrastructure. The U.S. Department of Defense (DoD), in particular, is trying to take advantage of this transformation by integrating LLMs into different critical military infrastructure. The Pentagon's 2023 Data, Analytics, and Artificial Intelligence Strategy envisions AI-enabled systems as vital to accelerating decision-making and enhancing the precision of command structures (Farnell & Coffey, 2024). In practical terms, LLMs are now tested for operational roles ranging from scenario planning and intelligence analysis to cyber-operations and even command-and-control functions. Experiments within the DoD have shown that LLMs can digest vast troves of classified data and return actionable insights within minutes, a process that previously took human staff days to accomplish. As one military officer put it after a successful trial, “We are learning that this is possible for us to do” (Manson, 2023).

These developments have been catalyzed also by OpenAI's controversial January 2024 decision to lift restrictions on the military use of its models, including applications linked to weapons development and warfare (Csernatoni, 2024). This move underscores a broader trend: the erosion of ethical guardrails on AI deployment and the rise of a new form of corporate nonstate sovereignty. In the absence of robust international norms governing military AI, private firms like OpenAI and Scale AI are increasingly shaping the battlefield, not merely supplying it. It is important to state at this point that with the arrival of Trump in the White House, the application of AI and especially LLMs in the military is going to escalate and proliferate further (Shkurti Özdemir & Ustun, 2024; Shkurti Özdemir, 2025a).

The strategic implications of agentic warfare are far-reaching. In this new paradigm, LLM-powered agents do not simply process text; they simulate escalation scenarios, interact with live databases, make strategic recommendations, and coordinate across operational units. They serve as cognitive engines embedded within AI warfighters, agents that monitor global signals, detect anomalies, and generate response plans at machine speed. This level of integration fundamentally transforms how war is planned, initiated, and potentially deterred.

Agentic warfare is not merely a futuristic concept. It is already unfolding through the testing of systems like Scale AI’s *Donovan*, Microsoft’s deployment of OpenAI models on Azure Government Cloud, and Anduril and Palantir’s development of autonomous decision-making platforms. These systems are designed to execute joint force operations, interface with

sensors, and manage munitions, all while adapting in real time to fluid operational environments.

The conceptual leap lies in replacing static military doctrine with dynamic, AI-informed strategies. Agents now simulate entire campaigns, weigh risk trade-offs, and propose novel options grounded in both historical precedent and live data streams. This is not just about speed; it is about strategic foresight. An agentic military force may detect adversary movements before human analysts can process the signals, preempting escalation and preserving advantage (Jensen, Tadross, & Strohmeyer, 2025).

As the world enters this new era, the strategic imperative is clear: failure to embrace agentic warfare may relegate states to a reactive posture, outpaced by adversaries with more agile and autonomous capabilities. Yet doing so responsibly demands new doctrine, oversight mechanisms, and international agreements that balance innovation with restraint.

Strategic, Cybersecurity, and Geopolitical Risks

As the adoption of LLMs expands across bureaucratic and military domains, the associated risks become increasingly salient, many of which extend beyond technical challenges and into normative, institutional, and geopolitical territory. While LLMs promise enhanced efficiency and cognitive support, their deployment in governance and defense introduces vulnerabilities deeply embedded in the structure, ownership, and alignment of the models themselves. This section explores three key categories of risk: cybersecurity and data governance, deployment bias and strategic misalignment, and geopolitical dependency under a new paradigm of technopolitical power.

Deployment Bias, Strategic Misalignment, and the Escalation Risk

The risk of deployment bias, using LLMs in scenarios beyond their design parameters, is especially problematic in the context of state governance and international affairs (Schwartz, et al., 2022). Most LLMs are trained and evaluated on benchmarks focused on reasoning, coding, or summarization. These metrics do not capture the complex, value-laden nature of political or strategic decision-making. Specifically, there is no verifiable truth in the domain of diplomacy and defense. Therefore, the lack of this verifiable truth means that decisions such as escalating a conflict, imposing sanctions, or intervening diplomatically are inherently subjective and politically charged. When considered like that it is obvious that there is an incompatibility between the task that the LLMs are intended to be applies and the real

capabilities of these models. The majority of current model evaluations ignore subjective decision-making contexts where results rely on social goals or institutional norms in favor of concentrating on reasoning abilities and task execution. However, as mentioned above, in governance and international affairs, generally there is no 'correct' answer, therefore making reliance on LLMs very dangerous (Jensen, et al., 2025, p. 2).

Several studies prove indeed this incompatibility of the LLM's task and their real capabilities. For example, a study conducted in 2025 reached in the conclusion that during several scenario simulations, models such as LLaMA 3.1 8B Instruct, Gemini 1.5 Pro-002, and Qwen2 72B typically suggest more escalatory policies. Furthermore, based also on the data they were trained on, these models displayed geographical biases. Specifically, these models advocated less aggressive positions toward China or Russia and more interventionist tactics for nations such as the United States or the United Kingdom (Jensen, et al., 2025, p. 2). As a result of these biases, it would be fair to raise concerns about fairness, alignment, and the possibility for algorithmically induced conflict.

Furthermore, similar to the study conducted by Jensen, et al., another study conducted by Riviera, et al. reached parallel results, again emphasizing the fact that LLMs can display erratic and occasionally violent escalation patterns when used within conflict simulation scenarios, including here nuclear decision-making (Rivera, et al., 2024). Within this context, it is necessary to emphasize that when we take into consideration the vague algorithmic reasoning and the possible sidelining of human judgment there is a high possibility has the potential to increase the risk of catastrophic conflict escalation in high-stakes situations, especially those involving nuclear decision-making.

Cybersecurity and Data Governance

When we talk about the application of technologies such as AI or LLM in the bureaucracy and military domain, the cybersecurity, and the challenges posed to it, become an unavoidable concern. Technically speaking, LLMs have the capabilities to memorize and repeat sensitive data provided in their training sets, therefore directly increasing the risk of information leakage. This is very concerning especially when LLMs are exposed to unredacted internal documents or private conversations, which are frequent in fields like national security, law enforcement, and taxation. Furthermore, adversarial prompt can also take advantage of the possible weaknesses and therefore lead to the exposure of confidential information, proprietary knowledge, or socially offensive material.

Another issue that may emerge is related to the anonymization of data. Specifically, the public official's interaction with LLMs has the capability to create new data streams that be used to retrain future models if they are not appropriately anonymized. For instance, any user data from ChatGPT can be incorporated into OpenAI's continuing training cycles unless agencies choose not to. As it may be understood, this may result in the unintentional revealing of makes sensitive discussions, strategic planning, or legal interpretations.

Lastly, the attack vectors need to be taken into consideration. Malicious actors can modify outputs or retrieve training data by using different strategies including prompt injection, model inversion, or synthetic querying. In the bureaucracy realm, where the IT infrastructures and generally underfunded or outdated, through the attack vectors, LLMs can be used to direct the development of malware, presenting a significant risk. Moreover, the dependency on cloud-hosted models and private vendor-managed APIs worsens the problem as it reduces governmental control and creates uncertainty regarding data sovereignty.

Geopolitical Dependency, Corporate Power, and Technological Sovereignty

When we discuss the LLMs adoption within the bureaucracy and military, one of the most important threats is the increasing influence of Big Tech companies over sovereign affairs. LLMs are highly resource-intensive systems developed by a small number of private actors. As of now, only a few firms, including OpenAI, Google DeepMind, Anthropic, and Baidu, possess the computational infrastructure, proprietary data, and technical talent to develop frontier models.

This dynamic creates two parallel dependencies. First, even technologically advanced states such as the United States are increasingly reliant on private firms for access to and control over LLM capabilities. For example, the U.S. government's collaboration with OpenAI on ChatGPT Gov illustrates a deeper entanglement between public institutions and corporate platforms. While such partnerships provide cutting-edge tools, they also allow private firms to gain privileged access to massive volumes of sensitive governmental data, which can be used to refine commercial models, shape policy discourse, or even nudge administrative behavior. In effect, governments risk becoming junior partners in a technocratic order governed not by democratic deliberation but by platform logics. If we focus especially on agentic warfare for example, the reliance on corporate AI infrastructure introduces a new dependency dynamic. Firms like OpenAI and Scale AI are now de facto defense partners with privileged access to sensitive data, shaping the capabilities and limitations of military force projection. In this

sense, agentic warfare is both a technological and political transformation, reshaping the relationship between states, private actors, and the conduct of war.

Second, governments that are unable to develop their own models, particularly those in the Global South or among mid-sized economies, become dependent on foreign vendors and, indirectly, on the geopolitical priorities of the states where these vendors are based. This dual dependency can severely constrain policy autonomy and expose national infrastructure to influence or coercion.

This dynamic resonates with emerging critiques of technofeudalism (Varoufakis, 2023), the idea that contemporary digital capitalism is marked by a concentration of infrastructural power in the hands of tech oligopolies that extract rents from data, labor, and public resources, or even that of data colonialism (Mejias & Couldry, 2024), the extraction and appropriation of personal and institutional data by corporate platforms, mirroring historical patterns of colonial resource exploitation, but now operating through algorithmic infrastructures and transnational data flows. The reliance on LLMs hosted by proprietary cloud infrastructures fits this pattern. States are not only consumers of corporate AI but also de facto data suppliers, reinforcing the centrality of big tech firms in shaping the governance of the digital age (Akyesilmen, 2023).

Moreover, the opacity of proprietary models further complicates oversight. OpenAI, for example, no longer discloses key architectural and training data for its latest models, making external auditing impossible. Without transparency, states cannot verify whether these systems uphold democratic principles, remain neutral in geopolitical conflicts, or embed unwanted ideological perspectives.

In sum, LLMs are not neutral infrastructure. Their integration into critical decision systems should not be viewed solely through the lens of utility or innovation. Rather, it must be approached as a question of political power, institutional trust, and long-term sovereignty. States must respond through a combination of regulatory development, public investment in open-source AI, and new international norms that align AI deployment with democratic accountability and strategic autonomy.

Recommendations

The integration of LLMs into bureaucratic and military infrastructures signals a profound transformation in the architecture of governance and warfare. Yet, this transformation has

outpaced the ability of regulatory institutions to respond. At present, there is a conspicuous absence of comprehensive legal and ethical frameworks capable of managing not only the systemic risks posed by LLM deployment but AI in general. Global digital governance remains fragmented, slow-moving, and largely reactive. As demonstrated during the 2024 AI Paris Summit, efforts to build a coordinated global response towards responsible AI have been hampered not only by geopolitical competition but also by the strategic lobbying of Big Tech firms, whose interests often conflict with calls for stronger public oversight (Shkurti Özdemir, 2025b).

Indeed, as it was seen also under Biden Adminsitration, these Big Tech companies, when pushed by the states towards more regulations, they try to shape the regulatory agenda itself, contributing to draft frameworks, influencing policy timelines, and pushing for self-regulation. In this context, the race for AI governance is being lost not because states are unaware of the risks, but because the very architecture of global governance remains vulnerable to corporate capture. The asymmetry of technical capacity and infrastructural control means that, in many ways, the rules are being written by those who own the models.

Nevertheless, this institutional stagnation should not be cause for resignation. On the contrary, it highlights the urgent need for middle and regional powers, such as Türkiye, Indonesia, South Korea, and Brazil, to step forward and advocate for more assertive regulatory initiatives. These actors are uniquely positioned to push for a more pluralistic and equitable AI order, one that balances innovation with democratic values and strategic sovereignty.

In light of these challenges, there can be proposed several recommendations:

One of the biggest problems with the application of new technologies is generally related to the lack of the oversight bodies. For this reason, it is necessary that states focus on the establishment of these bodies before it becomes more difficult to control the adaptation of the newly emerging technologies, especially LLMs. These institutions should be responsible for the auditing and regulating the integration of LLMs, especially in terms of governance and defense. These organizations should focus of guaranteeing openness, human supervision, and conformity to moral and constitutional requirements.

Currently one of the most discussed issues revolves around the use of closed-source and open-source AI models. Within this context, it is necessary that states focus on the developments of

sovereign and open-source models that would serve best the public interest and would reduce the dependency on external actors including here other states or Big Techs.

The biggest risk with the adoption of LLMs emerge in the defense domain; therefore, it is important that AI system must always operation under strict human-in-the-loop control. There should be clear protocols and regulations that prevent the autonomous escalations, especially in regard to decisions related to nuclear posture of active conflict engagement.

As mentioned above cybersecurity is an issue that automatically comes to the fore when AI Models such as LLMs are applied in sensitive domains such as bureaucracy and defense. Within this context, it is necessary that government update their cybersecurity standards in order to handle the unique risks posed by LLMs, i.e. data leakage, prompt injection, and model inversion attacks. It is also important there the government create protocols that prohibit the use of the public sector data for commercial training of the LLMs models.

Conclusion

In this algorithmic age, the integration of LLMs in the bureaucracy and military domain symbolizes a revolutionary reorganization of authority and governance. While previously LLMs were tools of efficiency and automation, LLMs are now integrated into decision-making architectures that may control anything from taxation to nuclear escalation. Without any doubt, this brings both advantages and risks. On the one hand, LLMs have the potential to improve state responsiveness, accelerate cognitive labor, and improve institutional foresight. However, on the other hand, these models bring unique challenges on issues that are mainly political and normative, including here bias, opacity, dependency, and conflict escalations.

As this paper has argued, the adoption of LLMs in bureaucracy and decision making is changing the epistemic foundations of the governance itself. At the same time, the use beginning of the so-called agentic warfare signifies a fundamental change in the logic and conduct of war, as speed, simulation, and predictive modeling progressively replace discussion and diplomacy. Besides this, the dependency on proprietary infrastructures largely controlled by Big Tech companies emerges as another important issue, especially taking into consideration that their interest may not always coincide with that of the public.

Within this framework, national and international policy must focus especially on institutional accountability, strategic autonomy, and technological sovereignty. States need to be careful not to be fully dependent on external actors under a new regime of technopolitical extraction.

At this point, while banning the use and integration of LLMs into decision-making structures is not possible, it is important that states take the necessary steps and make sure that LLMs are governed by the protocols of innovation but at the same time by principles of justice, transparency, and public control.

References

Akyesilmen, N. (2023). Editorial Preface: The Age of Digital Empires: Transformation of International Politics. Cyberpolitik Journal, 8(16), vi-xi.

Council of the European Union. (2023). ChatGPT in the Public Sector – overhyped or overlooked? European Union.

Csernatoni, R. (2024, July 17). Governing Military AI Amid a Geopolitical Minefield. Retrieved from Carnegie Europe: https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield?lang=en.

Farnell, R., & Coffey, K. (2024). AI's New Frontier in War Planning: How AI Agents Can Revolutionize Military Decision-Making. Cambridge: Belfer Center for Science and International Affairs.

Febrian, G. F., & Figueredo, G. (2024). KemenkeuGPT: Leveraging a Large Language Model on Indonesia's Government Financial Data and Regulations to Enhance Decision Making. arXiv.

Gesnouin et al., J. (2024). LLaMandement: Large Language Models for Summarization of French Legislative Proposals. Arxiv.

Government of Canada. (2025). AI Strategy for the Federal Public Service 2025-2027: Overview. Retrieved from Government of Canada: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/gc-ai-strategy-full-text.html.

Harari, Y. N. (2024). Nexus: A Brief Histrıy of Information Networks from the Stone Age to AI. Great Britain: Fern Press.

Jensen, B., Reynolds, I., Atalan, Y., Garcia, M., Woo, A., Chen, A., & Howarth, T. (2025). Critical Foreign Policy Decisions (CFPD)-Benchmark: Measuring Diplomatic Preferences in Large Language Models. Arxiv.

Jensen, B., Tadross, D., & Strohmeyer, M. (2025, April 23). Agentic Warfare Is Here. Will America Be the First Mover? Retrieved from War on the Rocks: https://warontherocks.com/2025/04/agentic-warfare-is-here-will-america-be-the-first-mover/.

Karaguezian, S. (2024). AI and Cybersecurtiy: Navigating the Future of Warfare and Digital Defense. Cyberpolitik Journal, 9(18), 241-247.

Liu, S., Geng, M., & Hart, R. (2025). Exploring Generative AI Techniques in Government: A Case Study. Arxiv.

Lund, B., & Ting, W. (2023). Chatting about ChatGPT: How May AI and GPT Impact Academia and Libraries? Library Hi Tech News.

Manson, K. (2023, July 5). The US Military Is Taking Generative AI Out for a Spin. Retrieved from Bloomberg: https://www.bloomberg.com/news/newsletters/2023-07-05/the-us-military-is-taking-generative-ai-out-for-a-spin.

Mejias, U. A., & Couldry, N. (2024). Data Grab: The New Colonialism of Big Tech and How to Fight Back. Chicago: The University of Chicago Press.

OpenAI. (2025, January 25). Introducing ChatGPT Gov. Retrieved from OpenAI: https://openai.com/global-affairs/introducing-chatgpt-gov/.

Puscas, I. (2024). Large Language Models and International Security. Geneva: UNIDIR.

Rivera, J.-P., Mukobi, G., Reuel, A., Lamparth, M., Smith, C., & Schneider, J. (2024). Escalation Risks from Language Models in Military and Diplomatic Decision-Making. Stanford University Human-Centered Artificial Intelligence.

Schwartz, R., Vassilev, A., Greene, K. K., Perine, L., Burt, A., & Hall, P. (2022). Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. NIST.

Shkurti Özdemir, G. (2024). AB, Yapay Zekâ Düzenlemesinde Küresel Lider Olabilecek mi? KRITER, 8(86). Retrieved from Kriter https://kriterdergi.com/dis-politika/ab-yapay-zek-duzenlemesinde-kuresel-lider-olabilecek-mi.

Shkurti Özdemir, G. (2024). Artificial Intelligence 'Arms Dynamics': The Case of The U.S. And China Rivalry. Istanbul: SETA.

Shkurti Özdemir, G. (2025a, July 5). Trump'ın Geri Dönüşü ve ABD'de Yenilenen Teknoloji-Savunma Bağı. Retrieved from Sabah: https://www.sabah.com.tr/yazarlar/perspektif/gloria-shkurti-ozdemir/arsiv/getall.

Shkurti Özdemir, G. (2025b, February 25). Paris AI Summit: Stage for power struggles, not regulation. Retrieved from Daily Sabah: https://www.dailysabah.com/opinion/op-ed/paris-ai-summit-stage-for-power-struggles-not-regulation.

Shkurti Özdemir, G., & Ustun, K. (2024). The Future of AI Policies in the US And Implications for Türkiye. Istanbul: SETA.

The White House. (2024, October 24). Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence. Retrieved from The Biden White House: https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the.

Varoufakis, Y. (2023). Technofeudalism: What Killed Capitalism. New York: Melville House Publishing.

THE EVOLUTION OF THE ALLIANCE CONCEPT IN CYBERSPACE: A CONCEPTUAL REVIEW

Onur YILMAZ[*]
ORCID ID: 0000-0001-6846-0968

Declaration[* *]

ÖZET

Bu makale, uluslararası ilişkiler literatüründe uzun süredir tartışılan ittifak kavramını siber güvenlik bağlamında yeniden ele alarak "siber ittifak" olgusunun kavramsal temellerini ve pratik yansımalarını ortaya koymayı amaçlamaktadır. Çalışma, klasik realist yaklaşımın denge ve tehdit temelli analizlerini, siber uzayın çok aktörlü, sınır tanımayan ve hiper-anarşik doğasıyla ilişkilendirerek özgün bir kavramsal açıklama modeli geliştirmektedir. Nitel literatür taramasına dayanan analiz, devletlerin siber tehditleri tek başına caydırma ve bertaraf etme kapasitesinin yetersiz kaldığını; bu nedenle kamu, özel sektör ve uluslararası örgütleri kapsayan esnek iş birliği mekanizmalarının kaçınılmaz hâle geldiğini ortaya koymaktadır. Bu tür bir iş birliğinin mümkün kılınabilmesi için ise, mevcut güvenlik kuramlarının ötesine geçen yeni ve kapsamlı bir ittifak tanımının geliştirilmesi gerekmektedir. Bu bağlamda çalışma, siber ittifak kavramını ve onun klasik güvenlik perspektifleriyle açıklanamayacak niteliklerini analiz ederek literatüre kavramsal düzeyde katkı sunmayı hedeflemektedir.

Anahtar Kelimeler: Siber Uzay, Siber Ittifak, Siber Güvenlik, Uluslararası Ilişkiler

ABSTRACT

The classical realist approach considers the multi-actor, borderless, and hyper-anarchic nature of cyberspace. Supported by a qualitative literature review, the analysis shows that states cannot alone deter and neutralize cyber threats; therefore, flexible cooperation mechanisms

[*] Arş. Gör. Doktora Adayı, Siyaset Bilimi ve Uluslararası İlişkiler (İng), İstanbul Aydın Üniversitesi- İstanbul-Türkiye, yilmaz12onr@gmail.com
[*] Bu çalışma, İstanbul Medeniyet Üniversitesi Sosyal Bilimler Enstitüsü bünyesinde hazırlanan doktora tezinden üretilmiştir.
[*] Artificial Intelligence (AI) tools were only used to organize the references in this study.

involving the public sector, private companies, and international organizations have become essential. The key to enabling such cooperation is developing a new and broader definition of alliance that goes beyond traditional security theories. In this context, the study aims to contribute to the literature by examining the concept of cyber alliance and its characteristics, which cannot be explained through classical security paradigms.

Keywords: Cyberspace, Cyber alliances, cybersecurity, international Relations

Introduction

It becomes clear that the concept of alliance holds an important place in the security strategies of states when evaluated within the historical context. From a realist perspective, alliances, which are formed by bringing together the military forces of states against common threats, have been analyzed in terms of the balance of power or threat perceptions (Morgenthau, 1948; Waltz, 1979; Walt, 1987). Although these and similar analyses have been intensively studied in the literature for many years, the rapid and unstoppable development of digitalization and information-communication technologies has made it necessary for states to incorporate these developments into their national security paradigms and to combat new threats that push the limits of classical security paradigms.

Cyberspace, which almost eliminates physical borders and extends beyond them, has become a unique security space with a structure that requires states to redefine the concepts of sovereignty and security. This area, where non-state actors are also active, has a complex and anarchic structure; however, international law and norms have not yet been sufficiently developed to address these issues. On the other hand, the anarchic nature of this area and the difficulty of defending it have led states to redefine their basic security requirements, as well as to address cyber-attacks, cyber espionage activities, and threats to critical infrastructures (Deibert & Rohozinski, 2008; Yılmaz, 2020). Considering all these and the fact that states have not yet been able to create a completely cyber-secure environment on their own, it is seen that cooperation and alliance formations in this field have become inevitable.

When considered in this context, the concept of "cyber alliance" may offer a new analytical framework that requires a reinterpretation of classical alliance concepts. With cyber alliances, it will be possible to establish a flexible and dynamic cooperation model that encompasses not only states but also various actors, including the private sector and international organizations.

The increasing diversity and destructiveness of cyber threats and attacks faced by states make such cyber alliances more strategic and essential.

Although the importance of cyberspace as a new security domain is now widely recognized, the concept of "cyber alliance" has not yet been sufficiently conceptualized in the literature of international relations. Most existing studies focus either on national cyber security strategies or bilateral cooperation practices. However, there is a need for an analytical framework that can comprehensively address the structural and functional dimensions of cyber alliances. This study aims to highlight the conceptual uniqueness of cyber alliances by examining the aspects that distinguish them from traditional military alliances and to explain their similarities and differences concerning the conventional understanding of alliances in the international relations literature. In this regard, the research is structured around the following questions: "How do cyber alliances differ conceptually from traditional alliances and under what conditions do they emerge? How does the unique structure of cyberspace transform the way the concept of alliance is approached?" In seeking answers to these questions, the study compares the relational aspects of classical alliance approaches with the phenomenon of cyber alliances and attempts to establish a theoretical framework for this new concept.

The Concept of Alliance in International Relations Literature

The concept of alliance is a frequently referenced feature in the field of International Relations. Beyond the classical realist narrative that views International Relations as a history of conflict and war, it is an undeniable reality that this field also encompasses aspects of diplomacy and cooperation. As such, alliances emerge as a natural and undeniable component of International Relations.

When faced with threats and risks of war, states seek to form alliances, either formally or informally, motivated by the promise of fighting the common threat together and neutralizing it together. Although the forms of alliances can be symmetrical and asymmetrical, or defensive and offensive, the three underlying elements of alliances are unity in the sense of "actors (parties), common threat, and joint elimination of the threat". Since realist studies largely influence alliance studies, it becomes clear that what is meant by 'actor' is typically nation-states. On the other hand, a consensus among studies on the concept of alliance is that the actors who form alliances are nation-states. It is also undeniable to say that the history of international relations is shaped as a cross-section of who has maintained alliances with whom, against whom, for what motives, and for how long. Although it is foreseen that strong

states and weak states act with different motives when forming alliances, the desire to form alliances and avoid facing the threat alone is similar. While strong states seek to consolidate their dominance, the weak state may pursue a strategy of 'balancing the hegemon'. However, the main intention of both types of states, whether weak or strong, is to utilize the capabilities of the other for their benefit, and they have similar incentives in this regard. On the other hand, the alliance relationship between states is not always formalized through agreements, pacts, or written texts; it can sometimes be unofficial and secretly established. In terms of duration, while some alliances are long-lasting, others may end when the desired goal is realized or terminated and may be short-term (Yalçın, 2014; pp. 399-401).

To say that states form alliances only to counter common threats may be an incomplete observation on its own. The motivations of states can be as diverse as having similar beliefs, economic concerns, and maintaining stability in their favour. Behind this diversity, however, lies one constant: reciprocity. This reciprocity relationship can be established at the beginning of alliances as well as at the end (Saka & Abdullahi, 2021, pp. 1-3).

There are different views on why alliances are formed in international relations. While Stephen Walt argues that alliances are formed to protect against threats, John Mearsheimer contends that strong states form alliances to gain power, while weak states do so to create a balance of power. Despite these different approaches, there is more consensus on the consequences of alliances. While alliances can sometimes lead states to war, they can also contribute to peace by increasing security. In general, alliances can make the international system more predictable and stable, but not always in a positive way. For example, in the First World War, secret alliances led to a security dilemma and fueled conflicts. In this context, Kenneth Waltz, in contrast to the classical balance of power approach, argued that states form alliances to balance threats rather than power (Arshid, Irfan, & Tanveer, 2017, pp. 44-51).

The tendency of states to form alliances in the face of a common threat offers a fundamental explanation for the formation of these structures. According to this approach, alliances aim to ensure security, share military resources and increase deterrence against external threats. Hans Morgenthau argues that in multipolar systems, states can pursue three main strategies to increase their power: building internal capacity, consolidating power through alliances, and preventing rivals from cooperating. The second and third of these strategies lead directly to the formation of alliances. Stephen Walt, however, adopts an approach based on threat rather

than power. According to him, alliances are shaped not only by material capacities, but also by geographical proximity, intent to attack and how these elements are perceived. Therefore, a state's power may not always be perceived as a threat by other states, and alliance decisions are based on these relative perceptions of threat.

In the IR literature, not only have the conditions under which states form alliances been extensively discussed, but also how they choose sides in alliances. In this context, the most basic dichotomy is shaped by balancing and bandwagoning strategies. Balancing is based on the concept of balance of power, one of the fundamental tenets of realism. It implies that states seek to offset potential threats by either increasing their capabilities or forming alliances to maintain stability.

While classical realists, such as Morgenthau, attributed these choices to the political calculations of state elites, neo-realist Waltz argues that this behaviour stems from the survival instinct inherent in the anarchic nature of the system. According to Waltz, if the ultimate goal of states were an absolute increase in power, bandwagoning —a less costly strategy —would be preferred. However, states often choose to join weak coalitions to maintain the balance of power and prevent the emergence of a possible hegemonic structure. Therefore, the dominant tendency at the systemic level is toward balancing (Morgenthau, 1948; Waltz, 1979). In this framework, Waltz's view of balancing as a structural consequence of the international system has led to criticism that he positions states as implementing actors who fulfill the requirements of the system, rather than being subjects in their own foreign policy. This approach is at the center of the ongoing theoretical debates on structuralism in the IR literature.

Bandwagoning, as discussed by Kenneth Waltz in his Theory of International Politics (1979), refers to the tendency to ally with the stronger side against a rising threat. In this context, it stands opposite to the balancing strategy. While balancing aims to achieve stability by supporting the weaker side against a stronger actor, bandwagoning is based on the desire to ensure security by joining forces with the source of the threat. In this approach, the state perceives a threat and prefers to act in concert with it rather than oppose it. The primary motivation for this choice comes from the need for survival and security in the anarchic nature of the international system (Waltz, 1979, pp. 126-127). Especially when a dominant hegemon exists in the global system, aligning with it is viewed as the least costly way for states to secure their interests. In this context, bandwagoning is not solely about security;

sometimes, states seek alliances with powerful actors to maximize their national interests, material gains, or territorial expansion. As a result, alliances can form not only as a means of defense but also to create opportunities and reward mechanisms (Siddiqi, 2016, p. 77). Compared to the balancing strategy, the lower cost of bandwagoning—aligning with stronger actors—makes this approach a rational choice for many states. This strategy is not limited to small states; major powers may also pursue it. The foreign policy of British Prime Minister Neville Chamberlain in the 1930s exemplifies this. Additionally, the expectation of gaining greater benefits at a lower cost has led some states to adopt bandwagoning. For instance, Hungary and Bulgaria's accession to the Axis Powers was primarily driven by their desire for territorial gains (Eckstein, 2023, pp. 1–11). While Waltz's system-centered model emphasizes threat-based balancing, many theorists argue that opportunistic motives can also influence alliance behavior. Schweller (1994), for example, introduces the idea of "bandwagoning for profit," suggesting that states may align with stronger powers not just for protection but to achieve strategic or material advantages. This view broadens the traditional understanding of alliances beyond the security dilemma, allowing for interest-driven behavior within the limits of the international system (Schweller, 1994, pp. 72–107).

In the anarchic structure of the international system, not only the preferences of states for strategies such as bandwagoning or balancing, but also the motivations, with whom, and on what grounds they cooperate when forming alliances, constitute a more in-depth discussion area in the literature. Historically, alliances have been as decisive as wars in determining the survival of states. States have developed alliance relations for various purposes, such as enhancing power, promoting economic and ideological harmony, fostering strategic partnerships, mitigating security threats, and contributing to global governance and development. In this framework, the question of whether similar alliances can be established in cyberspace, which stands out as a new security dimension, is becoming increasingly important. With its multi-actor and anarchic structure, cyberspace is turning into a plane that reflects the power struggles of the classical international system. In this context, the positioning of states in cyberspace has become a central aspect of the contemporary global security architecture

The Concept and Characteristics of Alliance in Cyberspace

Before discussing the possibilities of alliance in cyberspace, it is essential to clearly define the meaning and boundaries of the concept of "alliance" in this field. Since conceptual ambiguity

can undermine analytical coherence, a clear framework of what is meant by 'alliance' in the cyberspace context is essential for the healthy progress of the discussion. Relying on a common terminology when analyzing a particular domain provides conceptual clarity and a solid ground for theoretical and empirical evaluations (Cains, Liberty, Taber, King, & Henshel, 2022). However, cyberspace and its specific concepts—especially relatively new terms such as "cyber alliance"—have not yet reached a common terminological consensus in the literature. This makes it challenging to achieve conceptual clarity and requires additional attention in establishing the analytical framework. Therefore, for the theoretical coherence of the study, it is necessary to develop a specific approach to the concept of "cyber alliance". This approach seeks to make sense of cyberspace within the context of the discipline of International Relations, particularly within the framework of state-centred political readings. However, before proceeding to this framework, it would be more appropriate to present a general assessment of the structural characteristics of cyberspace

By its very nature, cyberspace has a complex and multi-layered structure. Although there is no single agreed-upon definition, it is possible to develop a general understanding based on various institutional frameworks. Sources such as the International Telecommunication Union (ITU), the International Organization for Standardization (ISO), and the Pentagon's Dictionary of Military and Associated Terms offer efforts to define different dimensions of cyberspace. However, these definitions differ in content and scope, and may be incomplete or limited in some aspects. The Pentagon dictionary has attempted to adapt to the changing dynamics in the field by updating its definition of cyberspace with revisions in 2007, 2009, and 2017. This diversity makes the need for clarity on the scope of cyberspace even more visible (Mayer, 2015, pp. 6-9). Although different institutional definitions of cyberspace vary in their details, certain common elements emerge. First of all, cyberspace is not a physical but a virtual medium, and as such, it is beyond the legal and technical limitations applied to traditional physical spaces. Structured as a global network system, cyberspace consists of networks interconnected through computers, software, and digital communication devices. It encompasses not only data and software, but also a social dimension involving its users and stakeholders. Its decentralized, ever-evolving and dynamic structure makes it difficult to control, which is why cyberspace is increasingly seen as a strategic area of power by states and other powerful actors.

The importance of cyberspace as an area of power lies in its anarchic nature, similar to that found in International Relations. In the international system, anarchy refers to the absence of a

binding and regulatory authority over states, which renders the system uncertain, unpredictable, and competitive due to the lack of a centralized structure to constrain the behavior of states. Similarly, cyberspace, with its lack of a central authority, represents an anarchic plane where rules are not clearly defined, power struggles intensify, and actors prioritize their interests (Morgenthau, 1954, pp. 131-133). This anarchic structure has historically paved the way for conflicts and wars in the international system, and this situation has become a continuous reality in the ordinary course of international relations. Today, this dynamic persists in various forms.

In this framework, the fact that cyberspace, like the international system, has a structure with multiple actors, inadequate legal regulations, and a weak binding structure, strengthens the view that it has an anarchic nature. To further define these structural features, the concept of "hyper-anarchy" has emerged in the literature. This concept was first introduced by Rafal Rohozinski and Ronald Deibert in 2008, referring to the fact that cyberspace lacks a central authority or governance structure. Hyper-anarchy is used to describe an order in cyberspace where there is no binding law-making or enforcement power for actors at different levels, such as individuals, hackers, criminal networks, private companies, and states (Deibert & Rohozinski, 2008, pp. 432-435). The structure of cyberspace, which physical borders cannot enclose, its rapidly changing technological infrastructure, and the difficulties of rule-making in the digital space make the concept of hyper-anarchy a meaningful and appropriate one. In this framework, a hyper-anarchic cyberspace refers to a structure that is ungovernable, where the probability of crime and conflict is high, state sovereignty is weakened, and the risks of cyber warfare increase. This structure is not only a technical domain, but also a new plane of power that profoundly affects international security and relations of sovereignty.

On the other hand, the approach that cyberspace has an entirely hyper-anarchic structure has faced various criticisms in the literature. This is because the capacity of actors with considerable power and influence in cyberspace—primarily states, multinational corporations, and various non-state structures—to create norms and order in cyberspace cannot be ignored. These actors have the potential to achieve their strategic goals and limit the inherent anarchy of cyberspace.

In this context, the hyper-anarchy narrative that cyberspace is completely ungovernable is not only a conceptual exaggeration but also highlights a practical risk for cybersecurity policies. Such a narrative weakens trust in governability, reducing motivation to build order and

possibly hindering the progress of cyber governance and security efforts (Akyeşilmen, 2017, pp. 1-18). Even the definitions of cyberspace imply it is becoming a new security domain, often mentioning the variety of threats and the unpredictability of involved actors. This domain, noted for its anarchic nature and governance challenges, gained attention on the global security agenda especially after the 2007 cyberattacks against Estonia—described by many as the "first cyber war." The rapid destruction of Estonia's digital infrastructure, the disruption of government functions, and the subsequent political fallout highlighted the serious cyber threats to nations. This event pushed for faster securitization in cyberspace and encouraged regional cooperation among Baltic states, leading to initiatives for joint cyber defense and shared deterrence strategies. The incident exposed the fragility of digital infrastructure and the difficulties of protecting it, prompting strategic cooperation among Baltic countries and allies. One key result was the development of a shared cyber defense framework, focusing on regional readiness and collective deterrence (Libicki, 2019). Afterwards, not only small and medium-sized countries but also major powers—such as the United States, the United Kingdom, and Turkey—faced cyberattacks and started creating national strategies in response (Yilmaz, 2020). NATO's security focus has increasingly included cyberspace, and bilateral cyber alliances have become more prominent. A prime example is the formal cyber cooperation between the United States and Japan, as reported by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE, 2023). This partnership shows how geopolitical interests and technological vulnerabilities influence the formation of cyber alliances.

The dominant trend in the cybersecurity literature generally focuses on the anarchic nature of cyberspace, the unpredictability of threats, and the isolation of states in this domain. However, this perspective also reveals the impossibility for states and other actors to deal with these threats alone. This highlights the need for establishing an effective governance mechanism in cyberspace. To protect against the risks posed by the anarchic structure and to capitalize on the opportunities in cyberspace, actors need to develop not only national but also collective policies and action alliances. In this context, the concept of cyber alliance gains strategic significance in terms of both security and governance; however, a clear definition of its scope and boundaries becomes essential for developing a sound analytical framework.

Before addressing the concept of alliance in cyberspace, it is necessary to understand the extent to which contemporary societies and state structures are affected by cyberspace. In the 1990s, while the US had serious initiatives on cybersecurity, the report by the US National

Academy of Sciences, with the words "...we are at risk," attracted attention in this regard. The report highlighted that the US was becoming increasingly dependent on computer systems every day (Tarhan, 2022, pp. 393-424). Today, almost all digitalized structures, from banking to air traffic control, from communication infrastructures to market chains, from individual privacy data to national security systems, have become potential targets in cyberspace. This situation shows that states and societies have become structurally vulnerable to cyberattacks. Indeed, past cyberattacks have provided important indicators of the extent of the damage that can occur in the absence of adequate protection and cooperation mechanisms. It is now clear that cyber threats and attacks also have physical consequences (Afsar, 2022, pp. 77-96).

In this context, cybersecurity should be seen not only as a technical issue, but also as a political, social, and international one. However, even today, there is no international consensus on fundamental questions such as "what is a cyber attack", "who poses a threat", and "who needs to be protected". As long as this conceptual and institutional gap persists, cyberattacks can have far-reaching consequences, including the overthrow of governments, undermining national security, political and economic instability, and erosion of public health and social trust. Therefore, seeking cooperation and alliances in cyberspace should be considered not only a choice but also a necessity (Li & Liu, 2021, pp. 8176-8186). The most effective and cost-efficient way to mitigate all these risks is to develop comprehensive cooperation and alliances among cyberspace actors. Clarifying the boundaries of attack-defense, crime-punishment, and friend or foe will reduce uncertainties in this area. In this context, cyber alliances are no longer a choice but a strategic necessity

Before discussing cyber alliances, it is necessary to clarify what the concept of "alliance" means in the context of International Relations. Alliances are cooperative structures, sometimes formal and sometimes informal, that states develop based on common interests or shared threat perceptions. These cooperations may arise even in cases of partial overlap of interests, rather than complete overlap. Moreover, alliances are formed in different ways, depending on the power distribution of the period, and are often established with a defensive reflex against a common or potential enemy (Mearsheimer, 2001). By joining forces against a common enemy, which can often be a counter-alliance system, states aim to provide deterrence and eliminate threats at a lower cost. Alliances are also formed to protect strategic regions, secure trade routes, or achieve common goals more efficiently. Historically, such collaborations have been frequently used as a means of both defense and interest maximization (Morgenthau, 1948, pp. 203-204).

Similar motivations in cyberspace shape Alliance relations. States cooperate to collaborate in line with shared interests and against common threats. One of the first examples of this is the Southeast Asia Enhanced Engagement Program (SEEP), a cyber alliance between the Philippines and the United States signed in 2022. This cooperation against cyber threats emanating from China is based on three pillars: information sharing, capacity building, and response mechanisms. However, it is debatable whether such structures can provide complete protection against all cyber threats. There are also significant shortcomings in terms of international law and binding regulations (Winger, 2022, pp. 1-6).

With its anarchic, multi-actor and complex structure, cyberspace has turned into a security space where conflict and cooperation are possible not only between states but also with non-state actors. The fact that attacks do not only originate from states, but also that hacker groups, companies, and individuals can pose a threat, shows that no actor can provide absolute security in this area. Therefore, states, companies and other actors are turning to formal or informal cooperation to share risks and costs, build capacity or counter common threats. Just as in classical international alliances, the aim is to ensure security in cyberspace collectively; such organizations can be evaluated under the concept of a cyber alliance.

The Concept of Alliance in International Relations and Cyberspace: Similarities and Differences

When the concept of alliance is analyzed in the International Relations literature and the context of cyberspace, it becomes apparent that there are both similarities and significant differences in terms of structure, functioning, actors, and scope of the alliance. While these differences stem from the unique dynamics of both fields, similarities emerge from their intertwined structures over time. Therefore, for the sake of conceptual clarity, it would be useful to first address the differences in the alliance phenomenon between the two fields, in order to better interpret the similarities.

In international relations, alliances are typically formed between states that share common interests and ideologies, allowing them to coordinate their physical actions and policies. These alliances are often formed based on geopolitical proximity and are influenced by the actions of great powers. For example, US allies typically must consider US strategic priorities in their dealings with China. Rui Mao's analysis of the agricultural sector reveals that alliances can even influence trade decisions and limit the room for independent action of their allies (Mao, 2023, pp. 433-437).

In International Relations, alliances are often formed to enhance military capacity, deter rivals, and establish standard defense systems. These alliances are typically formalised through strategic and security-based agreements, in which nation-states are the primary actors (Holsti, 1995, pp. 112-118). NATO and the Warsaw Pact are the two prominent examples of classical alliance structures in the history of International Relations. Geopolitical concerns, the search for a balance of Power, and defense against common threats have shaped the motivation of states to form alliances throughout history. In traditional alliances, respect for the sovereignty and territorial integrity of member states is essential; protecting national interests within the framework of international law is one of the primary objectives (Morgenthau, 2006, pp. 45-48).

On the other hand, although it is emphasized that NATO operates based on the classical alliance understanding, it is worth noting that this organization continually renews and reorganizes itself in response to new threats, thereby maintaining its relevance and continued existence. It is evident that NATO, which can continually create new security agendas for itself, continues its expansion. One of the main threats included in the security agenda in this new construction process is the one related to cyberspace and its security (Erendor, 2016, pp. 114-133)

Alliances in cyberspace are often created to enhance cybersecurity, share intelligence, and coordinate responses to attacks. Because this domain involves multiple actors, alliances can be formed between states, national institutions, and private companies. The rise of transnational threats has transformed cyberspace into a new security domain for nations, making alliances vital in this context (Eichensehr, 2017, pp. 52-57). Unlike traditional IR alliances, cyber alliances tend to be more flexible and less formal. Since cyberspace evolves rapidly, these agreements frequently take the form of memoranda of understanding or informal pacts, enabling quick adaptation to new technologies and threats (Li et al., 2020, pp. 31–33). Additionally, the involvement of non-state actors—such as private firms, international organizations, and civil society groups—emphasizes the borderless and decentralized nature of cyberspace (Khraisat & Alazab, 2021, pp. 18–22). Building on these distinctive features, recent theoretical efforts have aimed to understand the dynamics of cyber alliances through formal modeling approaches. One example is Benkő and Biczók's (2024) cyber alliance game, which illustrates how actors evaluate the costs and benefits of cooperation versus unilateral action when confronting emerging threats. Their findings

highlight that cyber alliances are driven by strategic logics that differ significantly from those underlying traditional, state-centric security agreements (Benkő & Biczók, 2024).

When evaluated in terms of differences:

- Although both types of alliances aim for security and stability, traditional alliances focus on geopolitical and physical security, whereas cyber alliances emphasize the protection of digital infrastructure and information systems.
- While traditional alliances are formed between sovereign states, cyber alliances are more multi-actor structures that include private sector and civil society actors.
- In contrast to classical alliances defined by physical boundaries, cyber alliances require flexible strategies against a decentralized and borderless threat environment.

In conclusion, although the two types of alliances have different structural and operational characteristics, this does not mean that there are no similarities between them. Therefore, it is essential to identify the commonalities between alliances in both domains.

Although alliances in IR and cyberspace have their differences, they are both shaped by the goal of achieving security and strategic advantage. Traditional alliances, such as NATO, are structured based on military capacity and collective defense. Similarly, cyber alliances aim to establish a collective cybersecurity environment among their members by creating an effective line of defense against common threats (Council of Europe, 2001). Another similarity is that both types of alliances are based on the principle of mutual benefit. While traditional partnerships are formed to balance power or address threats, cyber alliances similarly pursue common goals to mitigate cyber risks and enhance security capacity.

Another similarity between traditional and cyber alliances is the principle of flexibility. While international alliances have the ability to adapt to changing geopolitical conditions, cyber alliances must similarly develop flexible strategies against a dynamic and rapidly changing threat environment (Li, Zhao, & Zhang, 2020, pp. 31-33). Another similarity between cyber and traditional alliances is the principle of cooperation and coordination. Just as joint operations and military strategies are coordinated in traditional alliances, information sharing, response planning, and capacity building in cyber alliances are based on a similar coordination logic (Russett, 1971, pp. 263-281). In cyber alliances, intelligence sharing, joint strategy development, and defense exercises are the main elements of cooperation. Just like traditional alliances, risk sharing is a common feature of cyber alliances. In both structures,

the aim is to minimize threats by sharing the burden. The success of this process relies heavily on open and transparent information sharing, which becomes one of the main parameters determining the effectiveness of the alliance (Eichensehr, 2017, pp. 467-505). Traditional alliances have historically played a crucial role in shaping international norms and security standards. Similarly, cyber alliances, although not yet fully institutionalized, may become important platforms for determining cybersecurity norms in the future through inter-actor interaction (Hare, 2021, pp. 123-145). Another common aspect of traditional and cyber alliances is the efficient and collective use of resources. Both structures are based on sharing military, economic, technological, or human resources to strengthen defense against common threats. Whereas in traditional alliances, this takes the form of weapons systems or financial support, in cyber alliances it takes the form of exchanges of specialized personnel, technology sharing, and infrastructure support.

To summarize, the similarities between traditional and cyber alliances can be summarized as follows:

- Both types of alliances are formed in pursuit of shared interests and objectives.
- Mutual defense responsibility is essential (e.g. NATO's Article 5).
- Information and risk sharing are key elements of alliances.
- Joint use of resources (military, economic, technological, manpower) is emphasized.
- Strategic coordination is ensured through joint exercises, simulations and strategies.

Table 1: Common Characteristics of Traditional and Cyber Alliances

Similarity Field	Traditional Alliances	Cyber Alliances
Purpose of Establishment	Established to defend against common interests and threats.	It is created to ensure coordination and security against common cyber threats.
Defense Responsibility	As in the case of NATO, the principle of collective defense is essential.	A collective security approach is often adopted in common cyberattack scenarios.
Information and Risk Sharing	Sharing military intelligence and security information is essential.	Cyber intelligence, attack data and risk sharing play a critical role.
Resource Sharing	Joint use of military, economic and technological resources is common.	Resources such as technological infrastructure, specialized personnel and financial support are shared.
Strategic Coordination	Through joint military exercises, planning and operational coordination.	Joint cyber exercises, simulations, and strategic planning are conducted.

Note: Table created by the author.

Conclusion

Analyzing the concept of alliances in cyberspace requires going beyond the traditional discipline of International Relations. At this point, the parameters that need to be included in the analysis include security and power dynamics, and only an analysis in this direction can provide a competent perspective.

Both the complexity and diversity of cyber threats and the fact that states are becoming more and more equipped with digital infrastructures and that the seriousness of this has reached the level of addiction, combined with the unique structure of cyberspace, brings the possibility of states' alliances in the hyper-anarchy environment that emerges, and brings the concept of cyber alliance to a strategic position. While cyber alliances, like traditional alliances, act with the logic of uniting forces in the face of common threats, they also differ from it in structural and functional aspects.

The analysis conducted in this study reveals that alliances in cyberspace envision a multi-actor and more comprehensive cooperation model that encompasses actors beyond states, including the private sector and international organizations. Cyber alliances are critical for security in today's rapidly changing and diversifying threat-attack environment, as they are

more flexible and capable of adapting to rapidly changing situations, unlike traditional alliances. In this framework, cybersecurity cooperation between states and other actors in the coming period will become one of the key factors determining the stability of the international system.

As a result, the role and strategic importance of cyber alliances in the international security system will continue to increase significantly over time. The difficulties that states face in combating cyber threats on their own make broader-based cooperation, involving various actors, inevitable. Therefore, steps to be taken in the field of international law and the development of common standards are of great importance. Academic research and applied studies on this issue, to be conducted in the coming period, will play a crucial role in strengthening cybersecurity policies and reshaping the understanding of international security.

References

Akyeşilmen, N. (2017). Cyberspace as hyper-anarchy: A critical analysis. *Journal of Cyber Policy*, 2(1), 1-18.

Afsar, Ö. A. (2022). The Evolution of NATO's Cybersecurity Policy. *Cyberpolitik Journal*, *7*(13), 77-96.

Arshid, I., Irfan, H., & Tanveer, A. (2017). Alliances in international politics: A comparative study of Kenneth Waltz's and Stephen Walt's theories of alliances. *Kaav International Journal of Arts, Humanities and Social Science*, 4(3/A9), 44-51.

Benkő, G., Biczók, G. (2024). The cyber alliance game: How alliances influence cyber-warfare. *arXiv, 2410*(05953), 1–18.

Cains, M. G., Liberty, F., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cybersecurity and cybersecurity risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, 42(8), 1643–1669.

Council of Europe. (2001). Convention on Cybercrime. Strasbourg, France: Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Deibert, R. J., & Rohozinski, R. (2008). Cyberspace as hyper-anarchy: Towards a new research agenda. In R. J. Deibert & R. Rohozinski (Eds.), Access controls and digital governance in the global information age (pp. 431–454). Toronto: University of Toronto Press.

Eckstein, A. M. (2023). 'Jackal bandwagoning'? The Achaean League shifts alliances from Macedon to Rome, autumn 198 B.C. *The International History Review*, 45(1), 1–11.

Eichensehr, K. (2017). Public-private cybersecurity. *SSRN Electronic Journal,* 467-505.

Erendor, M. E. (2016). Cyberterrorism within the framework of risk society and reflexive modernization: The problem of definition and typology. *Cyberpolitik Journal*, 1(1), 114–133.

Hare, F. (2021). Cybersecurity and cyber warfare: What everyone needs to know. *Journal of Cyber Policy*, 6(2), 123–145.

Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the Internet of Things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, 4(1), 1–27.

Li, J., Zhao, B., & Zhang, C. (2020). Fuzzing: A survey. *Cybersecurity,* 3(1), 1–41.

Libicki, M. C. (2019). Baltic-area cyberspace alliance. In T. Minárik, R. Jakschis, & L. Lindström (Eds.), 11th International Conference on Cyber Conflict: Silent Battle (pp. 201–212). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Mao, R. (2023). Coalitions in international relations and coordination of agricultural trade policies. *China Agricultural Economic Review,* 15(2), 433–437.

Mayer, M. (2015). Cyberspace and international politics (pp. 6–9). https://doi.org/10.13140/RG.2.1.4470.0886.

Mearsheimer, J. J. (2001). The tragedy of great power politics. New York, NY: W. W. Norton & Company.

Morgenthau, H. J. (1948). Politics among nations: The struggle for power and peace (4th ed., pp. 203-204). New York, NY: Alfred A. Knopf.

Morgenthau, H. J. (1954). Politics among nations: The struggle for power and peace (2nd ed., rev. & enl., pp. 131-133). Knopf.

Morgenthau, H. J. (1960). Politics among nations: The struggle for power and peace (3rd ed., pp. 137–138). New York, NY: Alfred A. Knopf.

NATO Cooperative Cyber Defence Centre of Excellence. (2023). The NATO CCDCOE welcomes new members: Iceland, Ireland, Japan and Ukraine. *NATO CCDCOE News Bulletin*, *2023*(March), 1–2.

Russett, B. M. (1971). An empirical typology of international military alliances. American Journal of Political Science, 15(2), 263–281.

Saka, B., & Abdullahi, M. (2021). Alliance and coalition in contemporary international relations: The case of US-South Korea. *Zamfara Journal of Politics and Development*, 2(2), 1–3.

Schweller, R. L. (1994). Bandwagoning for profit: Bringing the revisionist state back in. *International Security, 19*(1), 72–107.

Siddiqi, F. (2016). Security Estimations in South Asia: Alliance Formation or Balance of Power. *Strategic Studies*, 36(2), 77–83.

Tarhan, K. (2022). Historical development of cybersecurity studies: A literature review and its place in security studies. *Przeglad Strategiczny*, 12(15), 393-414.

Waltz, K. N. (1979). Theory of international politics (pp. 126–127). Reading, MA: Addison-Wesley.

Winger, G. H. (2022). Cybersecurity in the U.S.-Philippine alliance: Mission seep. The Pacific Review. Advance online publication.

Yalçın, H. B. (2014). İttifaklar. In Ş. Kardaş & A. Balcı (Eds.), Uluslararası ilişkilere giriş: Tarih, teori, kavram ve konular (pp. 399–401). İstanbul: Küre Yayınları.

Yilmaz, O. (2020). Change of security paradigm; manifestation of the US and Russia competition in the cyber domain (Master's thesis, Kocaeli University, Institute of Social Sciences, Department of International Relations).

CONSUMER PROTECTION IN THE MALAYSIAN DIGITAL MARKETPLACE: FROM RISKS AND CONCERNS TO A LAW REFORM

Sonny ZULHUDA[*]
ORCID ID: 0000-0003-0192-1971

Declaration[*]

Abstract

This paper examines the evolution of consumer protection law in Malaysia's rapidly expanding digital marketplace. With 96.4% of Malaysian households having internet access and over 78,000 entities engaged in e-commerce transactions, the digital economy now accounts for more than one-fifth of Malaysia's GDP. However, this growth has created new consumer protection challenges, with the Ministry of Domestic Trade and Cost of Living receiving nearly 8,000 e-commerce-related complaints by September 2024. The study analyses key consumer risks in digital transactions, including information asymmetry, fraudulent practices, automated decision-making systems, and limited redress mechanisms. It traces the critical 2007 amendment to the Consumer Protection Act 1999, which extended coverage to electronic transactions, and examines the comprehensive Consumer Protection (Electronic Trade Transaction) Regulations 2024. The study reveals that Malaysia has developed a sophisticated, multifaceted regulatory framework that addresses e-commerce challenges through established legal principles and emerging regulations. The paper highlights the duties imposed on online marketplace suppliers and operators, including information disclosure requirements, error rectification mechanisms, and enhanced record-keeping obligations. The study concludes that strengthening digital literacy among consumers remains crucial for effective regulatory enforcement and creating a secure digital marketplace environment.

Keywords: Consumer protection, Online marketplace, Law and Regulation, Malaysia

[*] Associate Professor at Ahmad Ibrahim Kulliyyah of Laws, International Islamic University, Malaysia, sonny@iium.edu.my

[*] AI language model (Claude) was minimally employed to help refine the writing style and clarity of certain sections in this paper.

Introduction

The digital ecosystem we live in today necessitates reform for legal preparedness and enhanced consumer protection (Consumer Protection Act 1999, section 3). The online marketplace emerged as a cornerstone of modern consumer behaviour, offering unprecedented convenience and accessibility in the procurement of goods and services (Zainal Abidin et al., 2025). Today's consumers browse vast product catalogues, compare prices across multiple vendors, and complete purchases through online methods and using digital devices, all from the comfort of their homes or through mobile devices. This digital transformation has not only reduced transaction costs and eliminated geographical barriers but has also intensified market competition, leading to more competitive pricing and improved service quality (Liu, 2025: 399-401). However, this convenience and accessibility also bring new challenges in protecting consumer interests in the digital marketplace.

Consumer protection in the digital marketplace is crucial as it helps protect consumers' rights (Roslan et al., 2022). Transparent pricing, accurate product descriptions, and secure payment processing help consumers to make informed decisions and minimize risks. Unfortunately, many consumers are unaware that they often have equal or even stronger legal protections for online purchases than for in-store purchases. When consumers lack an understanding of their e-commerce-related rights, they face several significant risks, including financial, privacy, and security risks, as well as consumer protection risks. The following table illustrates those risks. Among the pertinent consumer risks are missing out on entitled refund periods or return rights, accepting faulty products without understanding warranty rights, being bound by unfair contract terms they did not comprehend, and being unable to effectively dispute charges or file complaints.

These risks are particularly concerning because online transactions leave a digital trail that can have long-lasting consequences. Without understanding their rights, consumers may also hesitate to engage in legitimate e-commerce, missing out on the benefits of online shopping while remaining vulnerable when they do participate. Given the pressing importance of this subject matter, this paper explores and analyses the legal framework applicable to protect consumers in e-commerce in Malaysia.

The State of Electronic Commerce in Malaysia: Vibrancy and Opportunities

Understanding some key terms will be helpful for this section. ASEAN Guidelines on Consumer Protection in E-Commerce 2022 describes electronic commerce as “commercial transactions conducted electronically on the internet whereby the buying and selling of products and services, and transfer of money, takes place either on the website of an individual online shop or larger platform”. It may take the form of “social commerce” in the event where the seller employs variety of social media to for the purpose of marketing and selling his products or services (Association of Southeast Asian Nations, 2022). Furthermore, “online sellers or shops” is defined by the Guidelines as “the individual entities marketing and selling their products and services either directly to consumers online (e.g. through a website or social media account) or indirectly via an e-commerce platform or marketplace”. Meanwhile, “e-commerce marketplaces/platforms” denotes “the digital service providers, sometimes also called intermediaries, that offer the space for and facilitate the interactions between sellers and consumers, often in wider digital ecosystems that span different services or sectors.”

In the Malaysian legal framework, a similar phrase is found in the Consumer Protection (Electronic Trade Transactions) Regulations 2024. It defines "online marketplace" as any electronic trade platform that is conducted through electronic means by any supplier. With the absence of further explanation or examples, the phrase' online marketplace' arguably encompasses all types of existing electronic platforms used for trading or advertising, including websites, social media pages, text-messaging platforms, and mobile apps (Consumer Protection Regulations, 2024). The person who makes an online marketplace available or operates it for trading or advertising purposes is an "online marketplace operator". In contrast, those who conduct trades or advertisements through an online marketplace are referred to as "online marketplace suppliers" (Consumer Protection Regulations, 2024).

E-commerce has become firmly embedded in Malaysian consumer culture, as evidenced by the substantial increase in Internet user statistics, including the adoption of digital payments and the proliferation of mobile shopping applications. A report by the Department of Statistics of Malaysia (DOSM) highlighted that nearly all Malaysian households (96.4%) have Internet access. Individual Internet usage also rose slightly from 97.4% in 2022 to 97.7% in 2023. Social networking dominated online activities in 2023, with 99.4% of users participating in

social platforms. Other popular activities included downloading multimedia content and games (93.9%), researching products and services (92.8%), downloading software and applications (89.6%), and making Internet-based phone calls (85.9%) (Department of Statistics, 2024: 63).

This emerging digital culture is quickly responded to by business entities in Malaysia, who have actively grabbed the potential by increasing their digital and online presence. These developments, both from the perspectives of Malaysian consumers and Malaysian business entities, have been evident over the past few years. DOSM reported that e-commerce remains a key pillar of the country's digital economy. Online marketplaces and platforms are incorporating artificial intelligence to provide personalized user experiences and streamline their delivery systems, meeting the growing expectations of Malaysian consumers (Department of Statistics, 2024).

The report also reveals some impressive statistics, indicating that in 2022, Malaysia's digital economy contributed more than one-fifth of the nation's GDP, underscoring its growing significance in driving economic growth. Interestingly, more than 78,000 entities are engaged in e-commerce transactions, accounting for approximately 7.1% of the overall 1,091,867 establishments. Of those engaged in e-commerce, more than 71 per cent have had a web presence, including having or using websites, social media or subscribing to an e-marketplace. The most popular purposes for using the Internet in these establishments are sending or receiving emails (95.7%), using internet banking (90.2%), and obtaining information about goods or services (81.6%). As for the micro, small and medium enterprises (MSMEs), a staggering 93.2 per cent of them have also adopted the use of the Internet for various purposes. Over 70% of them have had their web presence too, including a website, social media, and/or e-marketplace account (Department of Statistics, 2024).

The above set of data points to one thing: that electronic commerce is the way to go, and the direction will likely always be upwards. Along the way, both consumers and businesses will need to adapt to the new challenges and risks associated with engaging in electronic commerce. Consumers, in particular, will need to be aware of a multitude of risks that necessitate some legal safeguards. Policymakers make no secret of the fact that this rise in digital transactions has, in turn, required improved cybersecurity measures, including stricter data protection regulations and programs to promote cyber literacy among businesses and consumers (Department of Statistics, 2024: 5).

The State of E-Commerce Consumers in Malaysia: Complaints, Risks and Concerns

The Malaysian government agency specially tasked with matters concerning consumers and consumer protection, namely the Ministry of Domestic Trade and Costs of Living, has taken a proactive step to safeguard all parties engaged in electronic commerce. Based on cases from 2019 to 2024, the Enforcement Division under the Ministry has settled 42 cases involving gold jewellery transactions nationwide, which involved fraudulent online gold purchases, scale manipulation, inaccurate weighing instruments, and incomplete receipt information, resulting in a total seizure worth RM53,463. Of the total cases detected, RM7,700 in compounds were issued and a fine of RM20,000 was imposed on the companies or individuals involved (Kementerian Perdagangan dalam Negeri dan Kos Sara Hidup, 2024: 92). By September 2024, the Ministry has received almost eight thousand complaints relating to consumer protection vis a vis online transaction (Bahagian Analisis Ekonomi dan Data Strategik, 2024: 21-22). According to those statistics, the top five online providers that received the most complaints were Shopee (2024 complaints), Facebook (1,713), Instagram (1,121), Lazada (563), and WhatsApp (756). Other providers include Foodpanda, Carousell and Grab. Topping those complaints are "Goods or services offered are not received" (4163 cases); "Goods or services received are not as offered" (1520 cases), and "Misleading prices of goods/services" (445 cases).

At this juncture, e-commerce consumers will need to contend with a range of risks and challenges. As e-commerce involves new shopping methods and innovative payment and delivery options, new risks and challenges continue to emerge, potentially disrupting the safety, security, and convenience of consumers (Ong et al., 2023). International guidelines from the ASEAN and the Organisation of Economic Cooperation and Development (OECD) elaborate on common risks faced by consumers in e-commerce.

One crucial risk is the information asymmetry (Bai, 2025). The distant communications between consumers and online sellers do not help. Consumers often find it difficult to verify the accuracy or truth of the claims made by online sellers pertaining to the goods or services to be rendered. It is challenging for consumers to establish that what is offered is indeed what is promised. We are reminded that "the inability of consumers to inspect goods directly may become a cause of concern on the quality, safety and sustainability of products or services marketed online" (Association of Southeast Asian Nations, 2022: 7). The disadvantages may

sometimes be compensated by supply of more information, e.g. testimonies of a third party, professional or industrial guarantee by certain standard (e.g. official labelling or trust mark). Nevertheless, the asymmetric position remains a constant threat and risk for consumers, more so in electronic commerce.

Another significant issue faced by consumers is the prevalence of fraudulent and deceptive practices. Deceptive practices are not easy to address. Online sellers and marketplaces often use complex information, unclear language, and insufficient opportunities to review choices or withdraw consent (Association of Southeast Asian Nations, 2022: 12). The sophistication of online platforms may exacerbate the disadvantages faced by consumers (Haq, 2022). This may become more complicated if AI-enabled systems assume additional roles. Another aspect of this is the issue of hidden terms in contracts, including deliberately confusing data protection notices.

Though seemingly functional and sophisticated, an “Automated Decision-Making” is another source of risk and issue. Consumers will have to surrender to a transactional process which is pre-determined using algorithms and smart programmes or AI. The issue here is the lack of human intervention from the online seller's perspective, which risks biases and discriminatory decisions being made. This choice architecture is often made without the consumer's ability to negotiate, refuse or opt out. It is, in most situations, a "take-it-or-leave-it" condition. The Guidelines notes that this ADM risk arises when businesses "employ targeted advertising and algorithmic profiling, based on large-scale tracking of online consumption and movement patterns” (Association of Southeast Asian Nations, 2022: 8). Some consumers may think that this automated processing would help them to tailor their choices to their preferences for easier future transactions (thus creating more efficiency). However, this process presents potential long-term adverse impacts on consumers by taking away their choices and consent (Sarkar et al., 2025)

In addition to the above risks, several issues remain haunting and daunting challenges. The privacy of personal data, security of e-commerce system, unfair or inequitable provisions of terms of contract, and limited options for redress and dispute resolutions are also cited as key consumer concerns in e-commerce environment (Association of Southeast Asian Nations, 2022: 10). Unlike in traditional business environment, opportunities of consumers to be remedied from irregularities are rather foggy. It is not an exaggeration to say that the limited

availability of redress upon failed transactions poses a serious threat to e-commerce sustainability.

Legal Framework for E-Commerce and Consumer Protection

Based on the earlier elaboration of the characteristics and risks of e-commerce *vis-à-vis* consumers, this section further develops and analyses the laws that protect consumers in e-commerce in Malaysia. Due to the complexity and convergence of the electronic environment, consumer protection is not derived from one single statute. Instead, there are several key legislations on various aspects of law that, when analyzed together, ultimately offer a comprehensive protection to our consumers in the context of e-commerce.

The reputable international organization OECD came up with a recommendation on the principles of consumer protection in e-commerce ("OECD Recommendation"). This instrument aims at eliminating the uncertainties that both consumers and businesses encounter during their online transactions (Organisation of Economic Cooperation and Development, 2016: 2). The principles can be summarised as follows:

a. Transparent and Effective Protection: Governments and stakeholders should collaborate to achieve this protection, addressing the unique circumstances of e-commerce, including those affecting children and vulnerable or disadvantaged consumers.
b. Fair Business, Advertising and Marketing Practices: Businesses should not make any representation, omission, or engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair.
c. Online Disclosure: Information about the business, about the goods or services, and about the transaction processes.
d. Confirmation: The point at which consumers are asked to confirm the transaction must be clearly and unambiguously stated.
e. Payment: Businesses should provide consumers with easy-to-use payment mechanisms and implement security measures that are commensurate with payment-related risks. These measures should address threats from unauthorized access to personal information, fraudulent activities, and identity theft.
f. Dispute Resolution and Redress: Consumers should be provided with meaningful access to fair, easy-to-use, transparent, and effective mechanisms to resolve domestic and cross-border e-commerce disputes promptly and obtain redress, as appropriate, without incurring unnecessary costs or burdens.

g. Privacy and Security: Businesses should protect consumer privacy by ensuring that their practices relating to the collection and use of consumer data are lawful, transparent and fair, enable consumer participation and choice, and provide reasonable security safeguards. Companies must also address digital security risks and implement protective measures to minimize the negative impacts on consumers engaging in online commerce.

h. Education, Awareness, and Digital Competence: Governments and stakeholders should collaborate to educate consumers, government officials, and businesses about e-commerce, fostering informed decision-making. Efforts should focus on enhancing understanding among businesses and consumers regarding the consumer protection framework governing their online activities, including their respective rights and responsibilities in both domestic and international contexts.

By fulfilling these responsibilities, online sellers can help build consumer trust and ensure a fair and safe e-commerce environment. As both the OECD and ASEAN have laid down these guidelines, it is up to Malaysia to revisit its legal framework and ensure there are adequate legal protections for each of the items above.

The Malaysian Consumer Protection Act 1999

The laws on consumer protection in the context of electronic commerce in Malaysia may be primarily found in the Consumer Protection Act 1999 [Act 599] ("CPA 1999"). The Government has also come up with a significant subsidiary legislation that complements this matter in the form of the Consumer Protection (Electronic Trade Transaction) Regulations 2024 ("CPETTR 2024"). The following sections elaborate on the primary legislation on consumer protection, namely the Consumer Protection Act 1999, and how it further regulates e-commerce in Malaysia under the CPETTR 2024.

The Expansion of the Law to the Digital Marketplace

Since 1999, Malaysia has had a strong legislation on consumer protection in the form of the Consumer Protection Act 1999 [Act 599]. However, the matters relating to consumer protection in e-commerce were explicitly excluded from the ambit of the Act. The Act applies to all goods and services offered or supplied to one or more consumers in trade (Consumer Protection Act, 1999, section 2(1)). However, it was not intended to apply to several types of transactions, including "any trade transactions effected by electronic means unless otherwise prescribed by the Minister" (Consumer Protection Act, 1999, Section 2(2)). This means that

CPA 1999 excludes electronic transactions or electronic commerce from its scope. This was reiterated and reinforced by the decision of the High Court in Malacca, which ruled that the CPA 1999 is not intended to apply to the hearing of disputes arising from the same industry (i.e., telecommunications). Low Hop Bing J ruled that "the second respondent had elected the wrong forum to bring the dispute to the tribunal as it is outside the jurisdiction of the tribunal" (Telekom Malaysia Bhd v Tribunal Tuntutan Pengguna & Anor, 2007).

The result of this is a significant risk for Malaysian consumers in the electronic commerce sector. This was brought to the attention of Parliament for statutory amendment. It was considered “worrying” and therefore exposed Malaysian consumers to unfair and unethical electronic commerce practices (Parliament Malaysia, 2007: 71). In 2007, the Parliament finally amended the CPA 1999 to delete the exemption on e-trade and e-transaction. The Act now applies to all goods and services offered or supplied to one or more consumers in trade, including any trade transaction conducted through electronic means (Consumer Protection Act 1999, section 2(1)). In backing the legislative changes, Member of Parliament Hoo Seong Chang stressed that this reform was essential to maintain ongoing protection of consumer interests in Malaysia and ensure continuous consumer safeguarding. Through this repeal, electronic commercial transactions will fall under the coverage of the Consumer Protection Act 1999. As a result, consumer interests will be secured, thereby strengthening public confidence and trust in using online platforms for commercial activities. (Parlimen Malaysia, 2007: 71). Consumers’ confidence in conducting electronic transactions will improve because those who feel cheated and oppressed by unethical traders can make claims through civil courts. Consumers can submit their claims to the Malaysia Consumer Claims Tribunal for claims not exceeding RM25,000 (Parliament Malaysia, 2007: 72).

This is a crucial milestone in the area of e-commerce consumer protection in Malaysia. With this amendment, all the legal and statutory protection afforded to consumers under the CPA 1999 are now applicable to consumers who transact online or through an electronic platform.

The Duties of Online Marketplace Suppliers

One of the crucial subsidiary legislations under the CPA 1999, especially in the context of electronic commerce, is the Consumer Protection (Electronic Trade Transaction) Regulations 2024 [PU(A) 449] (“CPETTR 2024”). This is an improvement of its earlier version issued in 2012, which has now been repealed. The Regulations define “online marketplace” as any electronic trade platform that is conducted through electronic means by any supplier. With the

absence of further explanation or examples, the phrase' online marketplace' arguably encompasses all types of existing electronic platforms used for trading or advertising, including websites, social media pages, text-messaging platforms, and mobile apps.

Those online platforms may be operated directly by the online seller or advertiser, or by someone acting as an intermediary. When this is true, that person is referred to as an "online marketplace operator." CPETTR 2024 defines "online marketplace operator" as any person who makes available or operates an online marketplace for trading or advertising. Meanwhile, “online marketplace supplier” is defined as any person who conducts a trade or advertisement through an online marketplace (Consumer Protection Regulations, 2024: Reg 2). Before conducting a trade or advertisement through an online marketplace, the online marketplace supplier is required to disclose a set of information on that online marketplace (Consumer Protection Regulations, 2024: Reg 3(1)). The information required are: Name of the online marketplace supplier or company; Website address of the online marketplace, if any; Email address and telephone number of the online marketplace supplier; Address of the trade or advertisement to supply or advertise goods or services through the online marketplace is operated; Description of the main characteristics of the goods or services; Full price of goods or services including transportation costs, taxes and any other cost; Method of payment; Terms and conditions of the sale and purchase of the goods or services; Estimated time of delivery of goods or supply of services to the purchaser; and Certificate that the goods or services have followed the standard of safety and health as may be determined by the competent authority, if any.

In addition to the information requirements, CPETTR 2024 also imposes several other duties on online marketplace suppliers as follows:

- Error Rectification Mechanisms: An Online marketplace supplier is to make available the appropriate means to enable the purchaser to rectify any error prior to or after the confirmation of the order made by the purchaser (Consumer Protection (Electronic Trade Transaction) Regulations, 2024: Reg. 6(1)(a)). They must provide clear and accessible methods for customers to correct mistakes in their orders, both before finalizing the purchase and after confirmation. This obligation acknowledges that human error is a common occurrence in online transactions and safeguards consumers from being locked into unintended purchases. Due to this, an online supplier should implement a shopping cart review page that allows customers to modify quantities, remove items, or change

specifications before checkout. After order confirmation, they should provide a customer service hotline, email system, or online portal where buyers can request changes within a reasonable timeframe. For example, if a customer accidentally orders 10 laptops instead of 1, they should be able to contact customer service within 24 hours to modify the order before it is shipped.

- Order Acknowledgement Requirements: An Online market supplier has to acknowledge the receipt of the order to the buyer without undue delay (Consumer Protection (Electronic Trade Transaction) Regulations, 2024: Reg. 6(1)(b)). This is crucial because the acknowledgement serves as proof of the transaction, provides order details for customer records, and establishes clear communication between buyer and seller. As an illustration, when a customer purchases clothing from an online store, the business should automatically send an email confirmation within minutes or hours, containing the order number, items purchased, total amount, estimated delivery date, and contact information for customer service. This confirmation reassures the customer that their order was received and processed correctly, while also providing a paper trail for potential disputes.

- Redelivery Cost Responsibility: The online market supplier will be responsible for the cost of redelivery to a purchaser if the goods received by the purchaser are materially different or contain defects (Consumer Protection (Electronic Trade Transaction) Regulations, 2024: Reg. 5(a)). When goods delivered to customers are substantially different from what was ordered or contain defects, the seller must bear the financial burden of redelivery. This includes shipping costs, handling fees, and any associated logistics expenses. The key terms "materially different" and "defects" refer to significant variations from the advertised product or functional problems that affect the item's intended use. For example, if a customer orders a red dress in size medium but receives a blue dress in size large, or if they receive a smartphone with a cracked screen, the seller must arrange and pay for the replacement delivery. The customer should not incur additional costs for the seller's error. This might involve the seller providing a prepaid return label for the incorrect item and covering express shipping costs for the correct replacement.

- Service Fitness and Quality Standards: The Regulations prescribe that an online market supplier must provide services that are reasonably fit for the purpose for which they are offered or supplied (Consumer Protection (Electronic Trade Transaction) Regulations,

2024: Reg. 5(b)). They must ensure that their services meet reasonable quality expectations and match what was advertised or promised. Services should be "fit for purpose," meaning they accomplish what customers reasonably expect them to do. This obligation applies to both the primary service and any ancillary services provided in conjunction with it. For illustration, a web hosting company advertising "99.9% uptime" must actually deliver that level of service reliability. If they consistently experience outages that result in uptime below the advertised levels, they are failing to provide services that are "reasonably fit" for their stated purpose. Similarly, a food delivery service promising "hot meals delivered within 30 minutes" must have systems and processes capable of meeting these commitments under normal operating conditions.

- Record Keeping and Maintenance: The online marketplace supplier is bound to take reasonable steps to keep and maintain records of electronic trade transactions or advertisements (Consumer Protection (Electronic Trade Transaction) Regulations, 2024: Reg. 8(2)). The suppliers must implement reasonable systems to preserve electronic transaction records and advertising materials. This includes order details, payment information, customer communications, and promotional content. These records serve multiple purposes: customer service support, dispute resolution, regulatory compliance, and business analytics. "Reasonable steps" may ordinarily imply using industry-standard data storage and backup practices. For instance, an e-commerce platform should maintain secure databases containing customer purchase histories, email communications, website screenshots of product listings at the time of sale, and payment transaction logs. For example, if a customer claims they were charged twice for the same item three months ago, the business should be able to retrieve and review the relevant transaction records to resolve the dispute. This may involve cloud storage systems with regular backups, audit trails, and data retention policies that span several years.

It is submitted that the requirement to disclose the above information on the online marketplace will bring about meaningful transparency in electronic commerce. Mainly because this requirement also entails the duty not to disclose or provide any information that the supplier knows or has reason to believe is false or misleading (Consumer Protection (Electronic Trade Transaction) Regulations, 2024, Reg. 3(2)). Taken together, these requirements will not only reduce the risk of information asymmetry between sellers and consumers but also create a fair and healthy environment for electronic transactions. Trust

will emerge, and e-commerce will flourish well. The dark pattern and deceptive practices will eventually diminish for the advantage of consumers in Malaysia.

The Duties of Online Marketplace Operators

Besides online marketplace suppliers, an online marketplace owner or operator plays a critical role in facilitating electronic commerce (Kreiczer-Levy, S., 2021; Suzel, E.B., 2023; Buiten, M.C., 2021). They are those who make available or operate an online marketplace for trading or advertising. They may operate web-based online services, social media pages or a novel mobile text messaging account. The Regulations 2024 outline several duties for these online marketplace operators, including information disclosure, complaint handling, advertisement requirements and maintenance of records.

Regarding information disclosure, online marketplace operators must ensure that the online marketplace supplier complies with this duty before any electronic trade transaction is permitted (Consumer Protection (Electronic Trade Transaction) Regulations, 2024: Reg. 7(a)). This can be done while the supplier starts to open or register an account or membership at the specific online marketplace. Without supplying that information, the account may not be permitted to be active. Furthermore, online marketplace operators shall provide a channel for purchasers to lodge complaints regarding electronic trade transactions (Consumer Protection (Electronic Trade Transactions) Regulation, 2024, Reg. 7(b)). Likewise, online marketplace operators shall ensure that the advertisement of goods or services offered or supplied by any online marketplace supplier online is not in contravention of any of the provisions under these Regulations (Consumer Protection (Electronic Trade Transaction) Regulations, 2024: Reg. 7(c)).

In addition to the above, online marketplace operators shall, for a period of three years, take reasonable steps to maintain a record of online marketplace suppliers (Consumer Protection (Electronic Trade Transaction) Regulations, 2024: Reg. 8(1)). Such record shall include the supplier's name, address, telephone number, identity card number or passport number, business account number and email address; website address of the online marketplace used, if any; name and registration number of trade or company, if any; and records of electronic trade transactions or advertisement.

Conclusion: The Evolving Roles of the Consumer Protection Law

Based on the above discussion, the existing Malaysian consumer protection laws serve as a cornerstone for consumer protection in Malaysia. The laws provide the necessary detailed framework to address the unique challenges of online consumer protection and ultimately play a vital role in adapting broad legal principles to the specific context of e-commerce.

It is interesting to note that the subsidiary law has recently been reformed, essentially to align the regulatory framework with current realities of the digital economy. A notable enhancement is the extension of record-keeping requirements for both online marketplace operators and suppliers from two to three years. This longer retention period enables authorities to more effectively identify, investigate, and address deceptive practices that may not become apparent for a considerable time. The Regulation's enforcement mechanism also underscores its importance, as any violation constitutes a punishable offense. This approach reflects the government's recognition that consumer protection in the digital realm warrants rigorous enforcement, signalling to all stakeholders that e-commerce must operate within a framework of trust, transparency, and accountability.

Additionally, the paper highlights three key points. Firstly, consumer protection in e-commerce in Malaysia is undergoing active evolution. Second, a multifaceted regulatory approach is a clear and favourable option to pursue. Thirdly, it is always pertinent to go back to the basics of consumer awareness. We witness that the legal landscape governing consumer protection in e-commerce represents a sophisticated fusion of established principles and emerging regulations. What began as safeguards for traditional commercial transactions has evolved into a complex framework addressing the unprecedented challenges posed by technological innovation. This adaptive legal architecture must now contend with issues ranging from digital privacy and cross-border transactions to novel payment systems and automated business processes. The next critical step is to ensure public education about the opportunities and risks of the digital economy across both social and commercial dimensions. Strengthening digital literacy among Malaysian consumers will substantially improve regulatory effectiveness, leading to more streamlined enforcement and ultimately creating a more secure digital marketplace for all.

Reference

Abidin, S. R. Z., Ismail, N. Z., Ismail, J., Zainal, M. A., & Kadir, K. A. (2025). Exploring E-Commerce Landscapes: Types, Computing Techniques, and Market Trends in Malaysia. *International Journal of Research and Innovation in Social Science*, 9(14), 568–576.

Association of Southeast Asian Nations (2022). *ASEAN Guidelines on Consumer Protection in E-Commerce*, Jakarta: ASEAN Secretariat. "In line with the mandate of consumer protection authorities in ASEAN, these Guidelines concentrate on online transactions between businesses and consumers (B2C)." Retrieved from https://asean.org/wp-content/uploads/2023/03/ASEAN-Guidelines-on-Consumer-Impact-E-COMMERCE_V2-1.pdf.

Association of Southeast Asian Nations (2022). *ASEAN Guidelines on Consumer Protection in E-Commerce*, Jakarta: ASEAN Secretariat.

Bahagian Analisis Ekonomi dan Data Strategik, Kementerian Perdagangan Dalam Negeri, (2024). *Statistik Utama KPDN ST3- 2024*, Putrajaya: KPDN, Retrieved from, https://www.kpdn.gov.my/ms/media-utama/penerbitan/statistik-utama-kpdn.

Bai, J. (2025). Melons as lemons: Asymmetric information, consumer learning and seller reputation. *Review of Economic Studies*, rdaf006.

Buiten, M. C. (2021). The Digital Services Act shifts from intermediary liability to platform regulation, Journal of Intellectual Property. *Information Technology and Electronic Commerce Law*, 12, 361 para 1.

Department of Statistics, Malaysia (2024). *Malaysia Digital Economy 2024.* Putrajaya: DOSM, Retrieved from, https://www.dosm.gov.my/uploads/release-content/file_20241227111613.pdf.

Fairview International School Subang Sdn Bhd v Tribunal Tuntutan Pengguna Malaysia & Anor [2015] 9 Malayan Law Journal 581.

Haq, I. (2022). Risk of Fraud and Sustainability of E-Commerce. *Journal of Research in Economics and Finance Management*, 1(1), 27–37.

Kementerian Perdagangan dalam Negeri dan Kos Sara Hidup, (2024). *Laporan Tahunan 2023*. Putrajaya: KPDN. Retrieved from, https://www.laporantahunan.kpdn.gov.my//wp-content/uploads/2024/10/KPDN-AR2023-DL.pdf.

Kreiczer-Levy, S. (2021). The duties of online marketplaces. *San Diego Law Review*, 58, 269-308.

Liu, Z. (2025). Strategic Flexibility of SMEs in the Context of Digital Transformation. *Modern Economics & Management Forum*, 6(3), 399–401.

Ong, T. C., Lee, M. F., Manap, N. A., Halim, Z. A., & Thambapillay, S. (2023). Consumer Harms Arising from the Competition Dynamic of E-Commerce Platforms in Malaysia. *IJCLP*, 11, 71.

Organization of Economic Cooperation and Development (2016). *Recommendation of the Council on Consumer Protection in E-commerce*, OECD/LEGAL/0422, 2016, Retrieved from, https://legalinstruments.oecd.org/public/doc/336/336.en.pdf.

Parlimen Malaysia. (1999). Consumer Protection Act (999. Retrieved from, https://aseanconsumer.org/file/pdf_file/CONSUMER%20PROTECTION%20ACT%201999%20AMENDMENT%202019%20.pdf.

Parlimen Malaysia (2007). *Penyata Rasmi Parlimen Dewan Rakyat*. Vol. 24, 8 May 2007. Retrieved from, https://www.parlimen.gov.my/files/hindex/pdf/DR-08052007%20-%20edit.pdf.

Parlimen Malaysia. (2024). Consumer Protection (Electronic Trade Transaction) Regulations. (2024). Retrieved from, https://repositori.kpdn.gov.my/bitstream/123456789/5299/1/PERATURAN%20URUSNIAGA%20PERDAGANGAN%20DALAM%20ELEKTRONIK%202024.pdf.

Roslan, A. K., Fakrudin, N. S. A. M., Ghani, N. A. A., Saad, H. M., & Ishak, S. (2022). Legal protection of e-consumers in Malaysia. *International Journal of Law, Government and Communication*, 7(29), 223–241.

Sarkar, M., Rashid, M. H. O., Hoque, M. R., & Mahmud, M. R. (2025). Explainable AI in e-commerce: Enhancing trust and transparency in AI-driven decisions. *Innovatech Engineering Journal*, 2(01), 12–39.

Süzel, E. B. (2023). Responsibility of Online Platforms Towards Consumers. *Journal of European Consumer and Market Law*, 12(6), 226 – 232.

Telekom Malaysia Bhd v Tribunal Tuntutan Pengguna & Anor. (2007). 1 Malayan Law Journal 626.

OPINIONS / YORUMLAR

ARTIFICIAL INTELLIGENCE (AI) AND CYBERSECURITY

Amirudin Abdul WAHAB*

Declaration*

The Future of the Relationship Between Artificial Intelligence and Cybersecurity

Over the next 3–5 years, Artificial Intelligence (AI) will significantly transform cybersecurity, evolving from an emerging trend into a pivotal force and ally. AI will revolutionize cybersecurity roles, rather than eradicate them. The advancement of AI will transform cybersecurity employment functions, though it will not eliminate human roles. Gartner forecasts that automated systems will take control of more than 50% of SOC Level 1 analyst responsibilities by 2028, which includes alert prioritization and basic ticket resolution. AI systems will enhance human capabilities, rather than working as direct replacements for human experts. This means that AI will help people perform their jobs more effectively, rather than taking over. In cybersecurity, the workforce will spend more time focusing on evaluating AI-generated data through strategic investigations while handling model governance and validating system intention.

Collaborative efforts on the human-AI relationship are crucial in today's digital landscape. Rather than competing with machines or AI, the solution lies in forming a strategic and responsible partnership. Efforts and resources are needed for organizations to integrate AI systems in ways that enhance human capabilities while reducing human error where possible. Upskilling, reskilling and learning new skills is key. In addition to traditional threat management, security personnel must also learn ethical reasoning and AI literacy. To navigate the AI-driven cyber landscape, skills such as data interpretation, cross-team communication, and collaboration will be essential. Organizations must buck up and be ready to adapt, or risk falling behind. Leaders must proactively prepare for AI's impact by implementing robust AI training programs and clear usage policies. Cross-functional teams combining AI expertise with domain knowledge will ensure effective AI integration while preserving human oversight.

* Dato' Dr. CEO at CyberSecurity Malaysia

* In this study, AI tools such as ChatGPT were utilized for sentence editing. AI was used to translate the author's thoughts and ideas into a more academic framework for grammar and editing.

Artificial Intelligence Contributes To The Attackers' Advantage

According to the Global Risk Report 2024, there is a significant concern that emerging AI technologies will benefit cyber attackers more than defenders, potentially exacerbating the cyber threat landscape. The report states that 55.9% of respondents believe generative AI will give cyber attackers a competitive advantage, while only 8.9% feel it will give defenders a competitive advantage. Hence, there is a need to call for action for the cybersecurity community. Cyber defenders must seize this pivotal moment to continuously enhance their expertise and proficiency, diligently refining their knowledge and skills. Cyber defenders must not overlook the powerful opportunities that AI offers in strengthening cybersecurity and cyber resilience.

By leveraging AI for threat detection, automated response, and predictive analytics, cybersecurity professionals can shift from a reactive to a proactive defence strategy. To close the gap, defenders must harness AI's full potential, not only to keep pace with evolving threats, but to decisively tilt the advantage back toward security and trust. Not to mention, there is an example where AI tools that are most commonly used by cybercriminals are being used against them. The AI grandmother named Daisy, whose task is to waste scammers' time with meandering conversations (Thubron, 2024).

AI Could Not Eliminate Human Error

It was believed that AI could eliminate human error. However, AI capabilities are not yet fully developed due to issues such as AI hallucination, data poisoning, and the presence of low-quality data. Therefore, the most promising applications of AI are those that can be accomplished quickly. By examining vast amounts of unprocessed data, AI can identify trends and abnormalities that human analysts would overlook, improving threat detection and reaction times, for example, detecting deepfakes in videos or pictures, and the uncanny valley that AI can detect. In contrast, humans remain uncertain about whether to be suspicious or treat the material differently.

Additionally, AI automates repetitive tasks, such as handling notifications and monitoring network traffic, thereby freeing up cybersecurity experts for more strategic responsibilities. Furthermore, prospective cyber threats may be predicted using AI-driven predictive analytics, allowing for proactive defences and minimizing vulnerabilities before they can be exploited.

Together, these capabilities support cybersecurity efforts even if AI's error-free performance is currently limited.

AI is the greatest threat, but also the most excellent defence. It is a game-changer in cybersecurity defence. AI is capable of identifying anomalous login patterns, detecting suspicious network activity, reverse-engineering malware, and even forecasting potential vulnerabilities by analyzing historical data. Additionally, AI-driven automation is changing how businesses distribute their cybersecurity resources.

AI technologies offer the most potential in threat detection or response

Supervised and unsupervised Machine Learning (ML) and Generative AI (Gen AI) have emerged as transformative tools in cybersecurity. These technologies work way faster and better at detecting threats, all while taking some of the load off humans. Supervised ML uses labelled data to teach models how to recognize patterns or make predictions. This approach in cybersecurity helps catch known threats by learning from previous attacks. It is used in various ways to detect threats, such as malware classification, Intrusion Detection System (IDS), and real-time anomaly detection. Unsupervised ML does not rely on labelled data but instead identifies patterns and anomalies within datasets. This helps detect previously unfamiliar threats. This is the method used to identify threats, like anomaly detection, behavioural analytics, and entity resolution. Generative AI represents a significant leap forward by leveraging deep learning techniques to create predictive models and simulate scenarios. The capability of processing vast amounts of data and creating synthetic data makes it a powerful tool for threat detection and analysis.

i. Virtual assistance
ii. Threat contextualization
iii. Synthetic data generation

Combining supervised and unsupervised machine learning with generative AI improves cybersecurity. Each technology provides particular benefits. Supervised machine learning accurately identifies known dangers. Unsupervised machine learning uncovers unknown problems and new oddities. Generative AI adds background information and forecasts events. When people use them together, they also find that they respond to threats more quickly and with greater flexibility. As cyber threats become increasingly complex, utilizing AI technologies becomes necessary to stay ahead of attackers and build effective protective digital systems.

AI's Risk for Cybersecurity Ecosystems

We acknowledge the fact that AI both helps and harms cybersecurity. This idea holds as much importance as our adoption of AI's power in the field. The same capabilities that enable us to identify threats more quickly and precisely also allow bad actors to accelerate their attacks. AI brings a new era of cyber threats that adapt and act autonomously. One of the most concerning risks is the arrival of AI-powered malware, as well as automated attack systems. These can evolve on their own, bypass old defences, and initiate attacks with a speed and precision never seen before. Methods like poison injection as well as data manipulation harm training data, which spoils the base of AI models - this also lowers faith in automated systems.

Another common vulnerability is the use of AI to enable deepfakes and impersonation, which can fool both humans and security systems. These can be used for phishing, social engineering and even high-level fraud, blurring the lines between truth and manipulation in digital interactions.

As AI can be optimized for cybersecurity, it can also be utilized to counter cyberattacks, as machine learning algorithms are capable of identifying the most effective methods to gain access to systems or evade detection. This means more effective ransomware, brute force attacks and APTs that silently infiltrate and dwell in the network. Additionally, insider threat abuse, powered by AI, is becoming increasingly common. This is when behavioural analytics, which were meant for detection, are reversed and used to bypass internal controls. Moreover, AI can be used to launch more complex attacks on interconnected infrastructure in cyber-physical environments, resulting in real-world impacts. There is a growing concern that AI is being used more effectively to exploit vulnerabilities before cybersecurity experts can react, which may lead to a loss of trust, data breaches, and an increase in zero-day attacks.

The Role Of Regulation In Managing AI Use

The regulation is currently playing catch-up. Even the European Union (EU) AI Act is still facing concerns, with many EU leaders stating that there are still missing elements in place. Mostly concerns regarding the Act's capability to balance between innovation and security.

Those in the regulatory role have their hands full, as they need to consider the entire digital realm itself. Of course, this can be mitigated by focusing on parts rather than the overall view or creating a specialized and strategic thinking working group that can tackle the issue of

playing catch-up, but that does not dismiss the fact that time is ticking and AI is not slowing down.

Nevertheless, it is up to the national leader to handle how regulation will manage AI, including cybersecurity. This example can be seen in Singapore, Japan, China, and almost the whole world with responsible leadership. Governments or industry prioritize when regulating the integration of AI into critical digital infrastructure. When focusing on cybersecurity, the integration of AI must prioritize secure-by-design, resiliency, zero-trust, adaptivity, proactivity, and holism.

Thus, the crucial thing that both governments and industry bodies need to be concerned with is striking a balance between security, ethics, and innovation. Providing clear guidelines for reporting any cybercrime incidents, ethical standards and secure personal data while still promoting innovation and healthy competition among industries. Guard rails, human-in-the-loop, backup, and many more are essential to avoid data poisoning, data bias or data hallucinations,

Legacy systems are an issue that will undoubtedly arise when discussing critical digital infrastructure, given the constant evolution of technology. As such, any policy, guideline, or regulation related to AI must be adaptable and constantly one step ahead to ensure that no loopholes can be found or abused later on. Digital literacy, awareness, and training are essential to reduce skill gaps among employees. This can be achieved through initiatives such as Safer Internet Day, Cybersecurity Awareness Month, or regular biweekly brief meetings to exchange knowledge.

The issue of AI sovereignty is slowly gaining traction as more nations have begun to focus on developing their own AI models. As such, this matter needs to be handled as soon as possible to avoid unwanted conflict with other nations while still reaping the benefits of knowledge sharing and maintaining, or at least improving, the relationship.

Adopt AI In Cybersecurity Operations

The introduction of AI into cybersecurity will indeed be a game-changer. However, ensuring its adoption is safe, fair, and effective goes beyond providing tools that are in demand; it also requires the right mindset and skill sets. Six key practices establish the foundation for responsible AI adoption in cybersecurity. This is a human-centred design where AI systems are based on human principles. Such as inclusivity, ethics, and responsibility. The Issac

Asimov three laws of robotics can also be applied here if those have read or know about AI or robot culture (Becher, 2024):

i. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
ii. A robot must obey the orders given to it by human beings except where such orders would conflict with the First Law.
iii. A robot must protect its existence as long as such protection does not conflict with the First or Second Law.

These three robotic laws can be applied to the current AI ethical dilemma, particularly in light of the numerous specialized AIs that exist today, providing the help and assistance needed to reach both technical goals and public trust.

Second, accuracy alone is insufficient to identify the types of AI models, as well as their fairness, transparency, robustness, and real-world applicability. A holistic view of the performance could help avoid any loopholes, alongside ensuring that the AI model itself operates reliably.

Third, the quality of an AI model's output is directly linked to the quality of its raw data, which it processes. The organization responsible for the AI model should continuously examine the data fed into the model. If the data that was fed is skewed, the result itself will be biased and essentially skewed. The organization is responsible for understanding the data proactively and practically to ensure that the data accurately represents the environment the organization aims to defend.

Fourth, understanding the model limits and its datasets. The current AI still has its limitations, as it is not yet capable of solving every complex problem or predicting future trends. There is still a need for backup plans, as well as a strong foundation of human-in-the-loop analysis to determine which models are suitable and which ones are not.

Five, constantly, always, and never stop testing. Resilience is ensured through ongoing testing in various scenarios. AI models that not only function in theory but also survive the complexity of today's cyber threat landscape are needed. This can be achieved by simulating real-world attacks, particularly those involving technology that incorporates AI. AI Regulations or policies can run through the regulatory sandbox to determine which areas still need improvement and identify weaknesses.

Moreover, constant monitoring and patching of the systems after they go live. AI is not just a one-time buy. Models get old, dangers change, and info moves. Good use requires steady care, adjustment, re-teaching, checking, and changing AI setups to ensure they align with safety objectives and moral principles.

Balance Between Innovation and Risk in the Context of AI And Cybersecurity

In the field of cybersecurity, AI has the potential to be both a source of previously unheard-of risk and a spur for innovation. Finding the ideal balance between innovation and risk is a strategic necessity that requires foresight, effective governance, and international collaboration. It is not only a technological problem.

We must strike a balance between convenience and security, as well as innovation and risk, when utilizing AI in cybersecurity, particularly in the context of AI versus human decision-making. This might demonstrate that the company has a robust, flexible, and comprehensive governance framework and strategy that addresses people, process, and technology. Some organizations also view cybersecurity from an administrative, physical, and technical perspective. In addition to complying with existing laws, such as the PDPA and new AI-specific regulations, AI systems must also uphold fundamental ethical principles, including fairness, accountability, and privacy. Effective governance ensures that AI systems operate under clear rules, are closely supervised, and align with societal values rather than operating independently.

There are no options in the development of responsible AI. An organization must possess the right skills, knowledge, and steps to develop a responsible AI. In addition to security by design, an organization must employ a human-centred design approach, identifying multiple metrics to assess AI/ML training and monitoring. It is also recommended to directly examine your raw data and understand the limitations of your dataset and model. Furthermore, always test and retest the AI/ML data. Please continue to monitor and update the system even after it has been deployed.

There are several AI-related issues and challenges that we must face. AI may cause hallucinations and bias. At times, the datasets contain unfair risk grading or faulty threat identification that can cause these issues of bias. AI systems should be transparent, easy to understand, and fair. We need AI that can explain how it makes decisions, so people can check, trust, or question them if needed.

However, we need to remember that even though cyber defenders use AI to enhance and strengthen cyber defences, cyber-criminals or perpetrators can also use it as a weapon to conduct illicit criminal activities, such as AI-powered attacks, spreading phishing campaigns, launching much more sophisticated malware attacks, exploiting system vulnerabilities, or generating realistic deepfakes. To prevent the misuse of AI while still encouraging innovation, we must set clear ethical limits. Trust in AI should be built into its design; it cannot be assumed. That is why many experts support a 'zero-trust' approach, where AI systems are constantly checked and tested, not just when they are launched but throughout their use.

It is also crucial to highlight the importance of collaboration in cybersecurity. No organization can work alone. Everyone must be involved and responsible for cybersecurity. There must be cybersecurity collaboration among government agencies, industry, civil society, and academia. These collaborations will include knowledge sharing, threat intelligence sharing, the exchange of best practices, joint workshops, and joint cyber exercises, all aimed at promoting transparency. Public-private partnerships and global forums are also essential in aligning diverse perspectives and ensuring that AI adoption is both secure and ethical.

It is not just engineers, IT personnel, or innovators who need to understand AI; policymakers, regulators, and the public as a whole must also understand how it works and its implications for society. AI literacy goes beyond basic digital skills. It requires continuous learning because technology is evolving at an unprecedented rate. We must go beyond merely discussing ethical principles and start putting them into practice. That means using industry-specific guidelines that provide real, practical steps from identifying threats and fixing weaknesses to defending against attacks targeting machine learning. These tools transform good intentions into tangible protection, ensuring that AI systems are not only advanced but also secure and reliable.

Innovation and risk should not be viewed as mutually exclusive or separate from each other; they must be managed together, hand in hand. We can unlock the full power of AI while safeguarding digital trust, our institutions, and the people we serve. This requires strong governance, ethical design, robust security, collaboration, and continuous learning.

Reference

Brooke Becher, The Three Laws of Robotics: What Are They?, November 18, 2024, Built in, retrieved from, https://builtin.com/articles/3-laws-of-robotics.

Rob Thubron, Phone network employs AI "grandmother" to waste scammers' time with meandering conversations, November 14, 2024, Techspot, retrieved from, https://www.techspot.com/news/105571-phone-network-employs-ai-grandmother-waste-scammers-time.html.

ARTIFICIAL INTELLIGENCE (AI) AND INSTITUTIONAL RELIGION

Bilal SAMBUR*

Declaration*

We are currently facing a phenomenon and development that we have never encountered in previous historical periods. The technology we call Artificial Intelligence (AI) is radically changing, transforming, and disrupting every aspect of our lives. AI goes beyond merely shaking the traditional foundations that humans have established for their own lives; it is continuously replacing these foundations with artificial ones. AI is designing everything, including culture, politics, education, ethics, literature, family, law, biology, and medicine. AI has gathered within itself a significant portion of the attributes attributed to God. Humanity has created a god-like power. Religion, one of humanity's dominant institutions, is also influenced by the transformative, artificial, and changing power of artificial intelligence.

AI is making everything that humans do for humans artificial. All human-made political, social, religious, educational, medical, legal, and cultural institutions are being shaped by artificial intelligence, which humans design. AI is altering all human-made artificialities in different ways. AI is forcing us to confront the reality that everything in our lives is artificial. There was nothing in human life that was not artificial, and nothing remains that has not been artificialized. The artificialization of human intelligence is one of the most incredible inventions humans have ever made. AI has brought about the emergence of what we call an artificial human condition by designing all of humanity's artificialities. It is now possible to evaluate artificial intelligence within the concepts of artificial humans and artificial life.

Traditionally, historically, and culturally, religion has been a dominant and influential institution in human life. However, today, the number of people who do not identify themselves with any religious institution or express themselves through any religious identity is rapidly increasing among the world's population. Data from international research indicate that in the coming years, the number of people who do not identify with a religious affiliation will reach a significant proportion on a global scale. In countries such as the United States, there has been a significant increase in the number of young people who do not identify with

* Prof. Dr., Department of Psychology, Ankara Yıldırım Beyazıt University, Türkiye.
* This study has utilized generative artificial intelligence tools, such as ChatGPT, for purposes including language editing, proofreading, and stylistic improvements.

any religion. With the intensive use of AI technology, people are becoming increasingly motivated and mobilized to make changes in their religious lives, identities, and cultures, and to create new situations. As AI technology becomes more widespread around the world, the number of people who identify themselves with any institutional religion is likely to decline.

Religious institutions and structures are active participants in religion-centered political and cultural wars to maintain and continue their power and influence. In the Middle East, religion and sectarianism continue to be the source of wars. Political struggles for dominance are being waged through the use of religion. When religion is integrated with politics and becomes the central front in cultural wars, the power and hegemony of religious institutions may be on the rise. However, religious institutions, which have been highly successful in becoming the main centres of political power struggles and cultural wars, are inadequate in providing new and dynamic responses to a phenomenon as significant as AI technology, and the initiatives they have put forward are far from satisfactory. Religious institutions and authorities are uncertain about how to respond to the emergence of artificial intelligence technology.

We can compare the confusion and uncertainty of institutional religions in the face of AI to the situation they found themselves in when the printing press was invented. When religious sources were printed in printing presses and made available to the general public, knowledge became accessible outside the monopoly of religious institutions. As a result, various religious institutions and authorities struggled for a long time to understand how to deal with the printing press. Religious authorities and institutions that stumbled in the face of the printing press in the past are now stumbling in the face of artificial intelligence, unsure of how to proceed. However, artificial intelligence technology has a much more powerful scope, design, and ability to make artificiality permanent than the printing press. Artificial intelligence designs, creates, and artificializes. Everything made by humans on Earth is artificial. Humans are constantly creating new things. The fact that artificial intelligence has an unlimited capacity for artificialization is a very challenging obstacle that institutional religions must overcome.

Religion is a human institution that aims to instil fear, intimidate, and control, prioritizing repetition, imitation, and conformity. AI has brought the conflict between religion and science back into the spotlight. The conflict between religion and science stems from institutional religion's desire and effort to control science and knowledge. AI technology represents a new

situation. Institutional religion lacks the ability or power to control or monopolize artificial intelligence in any way. The era of institutional religion controlling human intellect, knowledge, science, and thought has come to an end with the advent of artificial intelligence technology. Religion can no longer control its dogmas, sources, mythologies, and rules, because everything related to religion is now processed and produced by artificial intelligence. AI is poised to become the most significant source of inspiration for religion.

What is a human being, and what is free will? Are the purposes of these wills to legitimize the tools currently in use, or to transform humans into obedient mechanical beings? Can all artificial creations produced by humans be glorified? What is sacred? What is the reason? Are traditions sacred? Is there such a thing as infallibility or inerrancy? Philosophy and institutional religions have offered different answers to humanity's great questions. Thanks to AI, humans now have the opportunity to generate new answers based on comprehensive information and resources, extending beyond the answers provided so far. After AI, there is no longer any meaning or function in repeating traditional religious answers and discourses as they are.

There is no value, meaning, or validity today in accepting and following the dogmas and commandments of religions without question. Religions have lost their characteristic of being structures that carry the wisdom of centuries into the present day. AI emerges as a technology that embodies, processes, and evaluates knowledge and wisdom. Religious people can no longer afford to view only religion as valuable and exalted while neglecting AI technology. Religious people are learning knowledge and wisdom through AI technologies. We are entering a new era where people need AI more than religion today.

Nowadays, being religious is no longer a necessity or a requirement. Academics, philosophers, journalists, educators, and scientists are increasingly engaged in understanding themselves, society, and nature through AI, rather than relying on religious beliefs. It is no longer religion that guides people, but artificial intelligence. Religion often governs human life in the name of God. Theocracy is a powerful political and ideological tendency rooted in religion. Technocracy, which is embodied in AI, challenges the hegemonic ideology of religion in the form of theocracy. Theocracy cannot rule over artificial intelligence and cannot set the rules for engaging with AI. It is no longer religion but artificial intelligence that is changing the world and humanity. AI is not only changing the world but also forcing religion to change. Religion's power to change AI is very limited or non-existent. For the first time,

religion is losing its power to change and control in the face of human-made technology. The struggle between theocracy and technocracy represents a profound conflict that will shape the future of humanity.

ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ

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.

ETHICS OF ARTIFICIAL INTELLIGENCE

CASE STUDIES AND OPTIONS FOR ADDRESSING ETHICAL CHALLENGES

Merve Ayşe KIZILASLAN[*]
ORCID ID: 0000-0001-9654-1423

By Bernd Carsten Stahl, Doris Schroeder, and Rowena Rodrigues. (2023). Cham: SpringerBriefs in Research and Innovation Governance. Doi: 10.1007/978-3-031-17040-9.

Declaration[*]

In *Ethics of Artificial Intelligence*, authors Bernd Carsten Stahl, Doris Schroeder, and Rowena Rodrigues offer a case-based exploration of the ethical challenges posed by artificial intelligence (AI). Rather than solely engaging in abstract philosophical debate, the authors present a structured, practical analysis regarding how AI interacts with core ethical domains, including discrimination, privacy, manipulation, surveillance capitalism, human dignity, and safety. Contrary to common framing of AI as a purely technical or deterministic force, the book highlights the political, cultural, and social assumptions that underlie AI development and deployment. Through a series of organized chapters, the book succeeds in offering a cohesive examination of what it means to develop AI systems ethically in the 21st century.

The central thesis of the book is that ethical considerations in AI are inseparable from real-world contexts and must be examined through specific, situated examples. Through 21 concise and well-developed cases, the authors bring these issues to life and discuss both the systemic causes of ethical failure and the aspects of possible responses. Their goal is not only to reveal but also to suggest tools such as AI impact assessments and ethics-by-design frameworks.

The authors come from interdisciplinary backgrounds such as philosophy, computer science, law, and public policy. They aim to make a synthesis, reflecting the book's tone, which balances analytical framework with policy relevance. For international relations (IR) and political science scholars, the book provides a precise understanding that AI is not merely a

[*] Türkiye Cumhuriyeti Cumhurbaşkanlığı İletişim Başkanlığı / Republic of Türkiye Directorate of Communications, Independent Researcher, merve.kizilaslan@iletisim.gov.tr, kizilaslan.merve2224@gmail.com
[*] This study utilised AI-generated tools. The AI generated examples of what a book review outline should look like. Then, examples from existing literature were examined to illustrate the content of the outline. Finally, at the end of the review, I asked the AI-generated tools to indicate any grammatical errors or sentence corrections needed.

tool of technological innovation, but also a site of governance, ideology, and a field of academic discussion.

The book's primary strength lies in its case study approach. Each chapter follows a clear structure: real-life story, ethical analysis, responses (technical, legal, procedural). This format appears to be ideal for both academic and policy-making uses. Moreover, the authors advocate a pluralist ethical stance, emphasizing the importance of deontology (Kant), consequentialism (Mill), virtue ethics (Aristotle), and care ethics (Held), while recognizing the limitations of a solely Western philosophical perspective.

However, this same structure can sometimes feel repetitive. While the authors are clear about not offering exhaustive philosophical solutions, some readers may find the responses generalized. For instance, tools like “ethics by design” or “AI impact assessments” are well-framed but not discussed enough regarding their real-world adoption or enforcement challenges.

Divided into nine chapters, the book adopts a case-driven and thematically structured approach. It opens with a methodological and philosophical introduction, then moves through specific domains: discrimination, privacy, surveillance capitalism, manipulation, the right to life and liberty, dignity, the UN Sustainable Development Goals, and finally a reflective conclusion.

Each chapter engages a distinct ethical concern, but there is a consistent undercurrent: AI systems do not emerge in a vacuum. They are shaped by historical power conflicts, data inequalities, regulatory vacuums, and socio-political biases. The authors emphasize that ethics must not be reduced to compliance checklists or abstract principles. Rather, it must remain attentive to context, voice, and impact.

The book centralized its ethical concerns by confronting how AI systems can exacerbate structural inequalities, particularly related to gender and race. One crucial example is Amazon's abandoned recruitment tool, which penalized women’s resumes due to biased historical data. Similarly, predictive policing tools like COMPAS are critiqued for their lack of transparency and racial bias. The discussions revolve around emphasizing both technical limitations and legal-ethical boundaries (e.g., protected characteristics under human rights law, meaning attributes such as race, gender, religion, or disability, which are protected

against discrimination in legal frameworks to ensure equal treatment and protect human dignity).

Moreover, AI's dependency on large datasets raises questions about privacy, particularly regarding surveillance, genetic data, and biometric information. In that sense, the authors explore China's social credit system and private genomic services like 23andMe, where consent is often shallow and data reuse is unpredictable. Particularly strong is the analysis of "mission creep" and the limitations of the General Data Protection Regulation (GDPR) when applied to AI's evolving capabilities.

Chapters 4 and 5, specifically, mention how AI technologies are weaponized for profit and control. Shoshana Zuboff's surveillance capitalism theory is effectively utilized to explain how companies extract behavioral data to target users. From Clearview AI's biometric scraping to Facebook's microtargeting during elections, the authors underline how opacity, power imbalances, and deceptive interface design erode democratic norms.

The manipulation chapter also highlights how AI is used during user vulnerability, for instance, pushing beauty products during emotionally weak times. These examples problematize the neutrality of algorithmic tools and underscore the ethical costs of optimization-at-all-costs logic.

In the book, the matter of dignity paving the way for philosophically rich and practically urgent discussions. The discussion of how automated decision-making in welfare or healthcare may suppress individuals' voices and recognition is both appropriate and troubling. The proposal for "dignity-sensitive design" and participatory governance serves as a reminder that ethical AI must be not only fair but should consider liberal values while acting in a more humanizing way.

While it appears optimistic by aligning AI with the UN Sustainable Development Goals, it also remains cautious. The authors point out the risk of techno-solutionism, power asymmetries in global AI governance, and the need for reflexivity in design. The suggestion that AI cannot substitute for justice, but may support it if governed wisely, is one of the book's most vital conclusions.

The book's strongest feature is its refusal to separate technology from society. It views ethics not as a simple part of innovation but as integral to design, implementation, and governance.

Its pluralistic approach, from Kantian, utilitarian, virtue ethics, to feminist theories, gathers readers from varied disciplines.

What distinguishes this book is its practical aim. It avoids being merely descriptive by offering governance roadmaps. The authors are aware of the difficulty of embedding ethics into rapidly evolving systems. Hence, they seem to stay cautious about over-relying on principles. Importantly, the book strives to set AI ethics within broader human rights frameworks and social justice discourses, showing how systemic change must accompany technical evolvement.

However, one limitation is the weak engagement with non-Western philosophical traditions. While the book acknowledges this gap, more analysis of African, Asian, or Indigenous epistemologies could have enhanced its normative diversity. Furthermore, despite the richness of the case studies, they are mainly drawn from the Global North. Consequently, in order for such a book to address the universal AI ethical approach, it should have broader geopolitical aspects and themes, such as how AI ethics manifest under different state capacities, civil society strengths, and data governance cultures.

Nevertheless, *Ethics of Artificial Intelligence* is a critical read for AI developers, policymakers, related scholars and students. It provides a mirror to current practices and a guide map for future developments. By highlighting how bias, exploitation, and lack of transparency are often embedded in socio-technical infrastructures, the book calls for a radical rethinking of what "ethical AI" really means, not just as a design choice but as a political commitment.

For scholars of ethics, technology, and international affairs, the book serves as both a teaching tool and a research asset. Its clarity makes it suitable for students, while its analytical and case-study-based depth will appeal to academics and policy professionals. The book's real-world examples, like predictive policing, recommender systems, and biometric identification, ensure it remains understandable and accessible amid the subject's complexity.

In conclusion, this book succeeds in making AI ethics concrete, relatable, and actionable. Its pluralist methodology, wide-ranging case studies, and commitment to social responsibility make it a valuable contribution to the literature. While it may not satisfy readers seeking in-depth philosophical theorization, it is an exemplary model of applied ethics in the context of emerging technology. As AI continues to shape institutions and everyday life, works like this

are indispensable in guiding ethical and democratic engagement on collective AI moral features.

For anyone concerned with the intersection of technology and society, whether from law, philosophy, international relations, or computer science, this book is a necessary and enlightening read to gain a solid perspective on building AI ethical tasks.

NOTES FOR AUTHORS / YAZARLAR İÇİN NOTLAR

We would like to thank you for choosing to submit your paper to *Cyberpolitik*. In order to fasten the process of reviewing and publishing please take try to read and follow these notes in depth, as doing so will ensure your work matches the journal's requirements.

All works including research articles, comments and book reviews submitted to *Cyberpolitik* need to be original contributions and should not be under consideration for any other journal before and/or at the same time.

All submissions are to be made online via the Journal's e-mail address: cyberpolitik@gmail.com

The authors of a paper should include their full names, affiliations, postal addresses, telephone numbers and email addresses on the cover page of the manuscript. The email address of the author will be displayed in the article.

Articles should be 1.5-spaced and with standard margins. All pages should be numbered consecutively. Please avoid breaking words at the end of lines.

The articles need to be between 5000 - 7000 words (including footnotes and references); comments between 2000-4000 words (including footnotes and references); and book - article reviews between 500 - 1500 words.

An abstract of up to 150 words should be added during the submission process, along with an average of five keywords.

Authors should make a final check of their article for content, style, proper names, quotations and references.

All images, pictures, maps, charts and graphs should be referred to as figures and numbered. Sources should be given in full for images, pictures, maps, tables and figures.

Comments in Cyberpolitik

A comment is a short evaluation of an expert regarding new issues and/or development in cyberpolitics.

Comments require journal's full reference style.

Book / article Reviews in Cyberpolitik

A book review should provide a fair but critical assessment of a recent (not older than 5 years) contribution to the scholarly literature on the themes and topics relevant to the journal.

A book review for Cyberpolitik:

- Provides complete bibliographical references of the book(s) and articles to be reviewed.
- Summarizes the content and purpose of the book, focusing on its main argument(s) and the theory, methodology and empirical evidence employed to make and support these arguments
- Critically assesses the author(s)' arguments, their persuasiveness and presentation, identifying the book's strengths and weaknesses
- Presents a concluding statement that summarizes the review and indicates who might benefit most from reading the book

Book / article reviews should be preceded by full publication information, in the following form:

Education for Peace: Politics of Adopting and Mainstreaming Peace Education Programs in Post-Conflict Settings by Vanessa Tinker, Academica Press, 2015, $81.62 (Hardcover), ISBN 978-1680530070.

The reviewer's name, affiliation and email address should appear, on separate lines, at the top of the review, right after the bibliography of the book/article.

Journal style

Authors are responsible for ensuring that their manuscripts conform to *cyberpolitik'*s reference style.

Reference style of *Cyberpolitik* is based on APA 6th Edition.