CYBERPOLITIK JOURNAL
Siber Politikalar Dergisi

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

www.cyberpolitikjournal.org

ABOUT THE JOURNAL

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

Issue Editor
Dr. Kamil Tarhan

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

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.

CONTENTS / İÇİNDEKİLER

EDITORIAL PREFACE: AI ENABLED WEOPANS AND INTERNATIONAL LAW

Dear Readers

We are proud to present to you the 21st issue of the *Cyberpolitik Journal*. It is a great honour 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 artificial intelligence cannot be overstated. The articles featured in the 21st issue of the *Cyberpolitik Journal* bring forth a compelling narrative, shedding light on diverse facets of cyber landscapes, from ethical considerations and human rights to human rights, from cybersecurity and data protection in a digitally enriched environment.

In contemporary international law, few questions carry as much moral weight as the one addressed in this debate: Can the decision to end a human life be delegated to a machine? In less than a decade, lethal autonomous weapon systems, capable of selecting and striking targets without human intervention once activated, have moved from speculative fiction to operational reality. We see munitions and increasingly autonomous unmanned aerial vehicles (UAVs) roaming battlefields. These are becoming increasingly attractive tools for major powers and developing countries. The most influential factor in the development of these tools is artificial intelligence. Major powers have begun to delegate critical functions to systems that are no longer dependent on human hands. Many states globally, primarily the US and China, are making significant investments in these weapons. International law, as is often the case, is lagging behind in managing this dangerous technology.

The legal starting point of the issue is deceptively simple. International humanitarian law is applicable to any weapon, no matter how new. However, its fundamental principles are based on human judgment, generally on distinction, proportionality, and precaution. Distinguishing a combatant from a rifle-wielding farmer, or recognizing a wounded or surrendered combatant as a non-combatant, is rarely a matter of pattern recognition. It is a matter of context, and context is one of the things machine perception handles worst. Proportionality requires something even more delicate: comparing civilian life to military advantage under conditions

no programmer can fully predict. Whether such judgments can be codified into software, or at least pre-executed by humans, divides the field by tightly limiting the targets, geography, and duration of a system. It provides a basis for international procedures that compel states to review the legality of new weapons. But this basis is designed for predictable technologies rather than learning systems whose behavior can be uncertain even to their designers.

Underlying the doctrinal questions lies a structural question: who is accountable, or what is accountability? International criminal law presupposes a human perpetrator who has intent, makes a decision, and can be held responsible for what happens afterward. However, a machine has no intent and cannot be judged. Any military operation may have acted reasonably based on the available information. However, the programmer is far from harm in terms of time and space. Robert Sparrow's warning about the **"liability gap"** raises the concern that when an algorithm makes a mistake, no one can be held responsible for deaths. Others argue that the law of command responsibility and state responsibility could be adapted to close this gap, meaning that a commander who unleashes an unpredictable weapon into a crowded area is guilty in the oldest sense of the word. The reader will decide which view is more convincing. What neither side disputes is that the application architecture built since Nuremberg is strained under the weight of distributed algorithmic action.

The ethical debate is equally polarized. For opponents, the objection is deontological and absolute. To be killed by an algorithm means to be reduced to a data point, to be deprived of human dignity, a life weighed on doubt, hesitation, and mercy. For supporters, especially those associated with Ronald Arkin, the question is empirical rather than categorical. Machines don't panic, seek revenge, or fire out of fear, and if they can save more civilians than soldiers under stress, refusing to deploy them would be a moral failure in itself. Between these poles, the concept of "**meaningful human control**" has emerged as the common language of diplomacy. It is attractive in principle, vague in specification, and clouded by automation bias that is, the tendency for humans to submit to the machine they are tasked with controlling.

The diplomatic landscape reflects this unresolved tension. Decades of negotiations under the Conventional Arms Treaty have produced guiding principles, not binding rules. This has been hampered by the need for compromise and resistance from major military powers. Consequently, momentum has shifted to the UN General Assembly. The General Assembly's recent resolutions have been adopted by an overwhelming majority, requesting the Secretary-

General to enact a binding regulation. This regulation would ban autonomous weapons operating without human control and tightly regulate the rest. Whether these efforts will translate into treaty law, or whether state practices will quietly normalise autonomy, much like the once-normalised armed drones, will be the defining question of the coming years.

Contents of the New Issue

As artificial intelligence moves from the margins of technological debate to the very centre of security, diplomacy, and governance, the questions it raises grow more urgent and more complex. Algorithms now shape not only how states defend their networks but also how societies perceive truth, how power is distributed across the international system, and how individuals experience security in their daily lives. The contributions to this issue of Cyberpolitik Journal take up these questions from a variety of disciplinary and regional perspectives, examining the intersection of artificial intelligence, cybersecurity, and international politics through articles, opinion pieces, and reviews.

The first article of the new issue, The *Gendered Dimensions of AI-Driven Security*, Muskan Moazzam and Haris Bilal Malik bring a critical and often overlooked perspective to debates on artificial intelligence and security. The study explores how AI-driven security technologies from surveillance systems to automated decision-making tools are neither designed nor deployed in a gender-neutral manner. Drawing attention to algorithmic bias, unequal patterns of vulnerability, and the underrepresentation of women in the design of security technologies, the article argues that a genuinely comprehensive approach to AI security must incorporate gender analysis. In doing so, it enriches the literature by connecting feminist security studies with contemporary debates on emerging technologies

In the second article, *Siber Güvenlik Tehdidi Olarak Dezenformasyon: Dijital Güvenlik ve Diplomasi Açısından Etkileri* by Hüma Gül Çakır, addresses disinformation as a genuine cybersecurity threat rather than a mere communication problem. The article examines how deliberately manufactured and rapidly disseminated false information undermines digital security, erodes public trust, and complicates the conduct of diplomacy between states. By situating disinformation within the broader architecture of digital security, the author demonstrates that countering it requires not only technical defenses but also coordinated diplomatic responses, and offers a framework for understanding how states can protect both their information environments and their foreign policy credibility in an era of weaponized narratives.

The third article, *Lebanon's Strategic Position in the Age of AI-Driven Defense and Cybersecurity* by Sarkis Karaguezian**,** turns the reader's attention to the regional level. The study assesses how a small state situated in one of the world's most volatile regions navigates the accelerating competition over AI-enabled defense capabilities and cybersecurity infrastructure. Analysing Lebanon's geopolitical constraints, institutional capacities, and external dependencies, the article discusses both the risks that AI-driven military technologies pose for the country and the opportunities that strategic adaptation may offer. It thereby contributes a valuable case study to the growing literature on small states and emerging technologies.

The last article, *Gıda Rejimi ve Dijitalleşme: Teknolojik Örgütlenmeye Yapısal Bir Yaklaşım* by Salim Bülent Yüksel, addresses a significant gap in the existing literature by re-examining the relationship between digital technologies and food regimes. The study positions digitalization not as an external factor, but as a structural dynamic shaping food production and circulation through data, platforms, and algorithms.

The first opinion piece of the issue, *Cyber Security in the Age of Artificial Intelligence* by Mehmet Emin Erendor, offers a panoramic reflection on how artificial intelligence is transforming the fundamental logic of cybersecurity. The author considers the dual-use character of AI as both a powerful defensive instrument and an unprecedented tool in the hands of malicious actors and reflects on what this duality means for states, institutions, and individuals alike.

In the second commentary, *Digital World-System Hierarchies and AI-Driven Security Competition*, Fahad Nabel presents a powerful and original piece that blends world-systems theory with the realities of contemporary technological rivalry. The author maps the emerging hierarchy of core, semi-peripheral, and peripheral actors in the digital domain and argues that competition over artificial intelligence is reproducing – and in some respects deepening – the structural inequalities of the international system. The commentary offers the reader a crucial perspective on how AI-driven security competition is reshaping global power relations.

The third opinion piece, *Geleneksel İstihbaratın Sınırında Siber Operasyonlar: Mossad'ın Hizbullah'a Yönelik Çağrı Cihazı Saldırısı* by Necati Yıldız examines one of the most striking intelligence operations of recent years. Taking the pager attack attributed to Mossad against

Hezbollah as its case, the commentary discusses how cyber capabilities, supply-chain infiltration, and traditional intelligence tradecraft have converged, blurring the boundaries between espionage, sabotage, and armed conflict. The piece raises important legal and ethical questions about the future of covert operations at the intersection of the physical and digital worlds.

Finally, two reviews provide valuable insights into the current literature. Müfide Onur reviews *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*, a volume that explores how autonomous systems and machine intelligence are redefining the threat landscape and the requirements of national defense. In the second review, Saliha Nur Köşger evaluates *The Ethics of Information*, guiding the reader through its philosophical treatment of information as a moral concern and highlighting its relevance for anyone seeking a normative foundation for debates on the digital age.

In summary, the articles, commentaries, and reviews in this issue contribute to a better understanding of the opportunities and risks that artificial intelligence brings to the domains of security, diplomacy, and international order. These contents, prepared with academic depth, 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 Editör

RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ

THE GENDERED DIMENSIONS OF AI-DRIVEN SECURITY[*]

Muskan Moazzam and Haris Bilal Malik [*]
ORCID ID: 0009-0000-4182-7491 and 0000-0001-9410-6575

Declaration[*]

Abstract

This chapter is a critical analysis of the implications of AI-based security systems on gender and power. It states that so-called neutral technologies in fact carry and enhance the previous prejudices. In all parts of the world, AI is employed in national defense, and domestic surveillance, but it remains a reflection of the values and the blind spots of the developers. Algorithms and policies tend to be quite militarized and state-focused in the security sphere, disregarding the daily requirements of women and the marginalized populations. We integrate feminist international relations theory and new work on AI and cybersecurity to demonstrate that the existing systems do not often pose the question of "whose security is at stake"? or "if the security of the most vulnerable groups is ensured?" Facial-recognition technology, as an example, is much less effective with women and dark-skinned individuals. Females are the disproportionate victims of online harassment and doxxing. Even protective measures, such as CCTV in women's shelters, frequently become new avenues on which abuse of surveillance is exercised. The Global South particularly is affected by this issue, as the gendered digital inequalities and imported, uniform ("one-size fits all") cyber policies exacerbate underlying actual disparities in the offline world. Using an intersectional feminist lens, we argue that "security" must be redefined as empowerment rather than control. Co-created policies should embed inclusion, dignity, transparency, and accountability into AI and cyber-governance. Practical principles include gender-aware threat models, diverse decision-making teams, South-South collaboration, and proactive digital inclusion. We conclude that feminist approaches do not weaken security; they strengthen it by making systems more just, humane, and resilient to the needs of those historically at risk.

Keywords: AI security, Gender bias, Feminist International Relations's Theory, Cybersecurity, Surveillance

[*] This is the full text of the paper presented at the 9th Cybersecurity Conference.
[*] Both author Research Associte, Institute of Strategic Studies Islamabad (ISSI), muskanmoazzam7@gmail.com, harismalik000@gmail.com
[*] This article has been prepared without the use of any Artificial Intelligence (AI) tools or assistance.

Introduction

Artificial intelligence (AI) is being integrated in national security, law enforcement, and the global cyber-governance at an accelerated pace. (OECD, 2019; UNESCO, 2021). This integration also broadens their applications in the military (Scharre, 2018) (Identifying and targeting), in which machine learning is used to determine potential targets. This has also incentivized domestic usage by governments for surveillance by deploying these technologies in public spaces. They are commonly presented as impartial and objective tools, however, in practice, they are known to shape and influence online behaviour, regulate access to power, and contribute to vulnerability (APC, 2020; UNESCO, 2021). Stated differently, AI mirrors social values and hierarchies of the social groups that create it. Gender relations on the internet, such as online gender dynamics have been demonstrated to strengthen or even enhance offline disparities (APC, 2020; Buolamwini & Gebru, 2018). In such a way, a critical gender analysis of AI-powered security could demonstrate some latent power structures and subtle violence that traditional methods fail to detect (Tickner, 1992; Enloe, 2014). The analysis is grounded within feminist international relations lens and human security theory to support the arguments laid out.

The study will be based on a qualitative and interdisciplinary research methodology to perform a critical review of scholarly sources, policy reports, and news sources on AI, cybersecurity, and gender (Creswell & Creswell, 2018). This literature will be analyzed through the prism of feminist international relations and critical security studies, especially the concepts of intersectionality (Crenshaw, 1989); how identity factors such as gendering, racially and in classes influence experience and human-centered security (United Nations Development Programme [UNDP], 1994). By drawing on both theoretical works and tangible evidence, we endeavor to cast the human aspects of AI regulation in the limelight that are usually marginalized within dimensions of AI governance models.

The theoretical framework for this study will be based on feminism school of thought. As per the feminist theorists, the security is neither a goal nor a gender-neutral term. Rather, it is a political and socially constructed term (Tickner, 1992; Enloe, 2014; Ferl & Perras, 2024). The mainstream security paradigm has long been focused on the state, borders, and military force which is a male paradigm that places states as protectors and people (particularly women) as the vulnerable (Tickner, 1992). As a matter of fact, the discussion of digital security has been influenced by a rather homogenous- white and male - group, i.e., the voices of the women and other voices are pushed to the background as an example, decision-makers have been

discovered to set cybersecurity objectives without including women or minorities, meaning that the solutions to the policies are targeted at the ancient power structures instead of real human security. (Brown & Pytlak, 2020; Ferl & Perras, 2024). Feminist IR thus offers a critique of the conventional protector-protected scheme of security, calling out that it must be transferred to more democratic ideas of human security (Enloe, 2014; Tickner, 1992).

We use these concepts throughout this chapter by posing the following questions: 1) What bodies are covered by security? 2) Who are surveilled or attacked, and how identity factors (gender, race, and class, etc.) interfere in digital space? We develop out of such a framework as the Women, Peace and Security agenda of the UN, (United Nations Security Council [UNSC], 2000) as well as feminist foreign policy, (Thompson & Clement, 2019) which remind us that threats may be structural, daily, and gendered, and not necessarily military. The normative objective that we pursue is a feminist digital security paradigm: one that understands security as empowerment, (Hudson, 2005; Tickner, 1992) is made in collaboration with the communities affected, and one that incorporates dignity and inclusion into AI systems at its core.

Literature Review

Feminist Security Studies: Feminist IR literature has maintained that traditional security studies do not pay attention to the experiences of half the population. Theorists (Tickner, 1992; Enloe, 2014; Sjoberg, 2010) who are considered pioneers of the field demonstrated that the concept of traditional security is highly gendered (Tickner, 1992; Enloe, 2014; Ferl & Perras, 2024); it is shaped by masculine militarism and conceals the mechanisms of violence and power at home or on a psychological scale. As an example, feminist theorists suggest that violence is a continuum (Cockburn, 2004); in addition to physical violence, structural, cultural, and everyday violence (e.g., domestic violence, disinformation, etc.) are also a part of the same systemic control of the body and voice of women and marginalized individuals (Ferl & Perras, 2024; Lipede, 2025). When this is applied to the cyberspace, it would be possible to argue that online harms (sexual harassment, doxxing, disinformation, etc.) are part of the same systemic control of the body and voice of women and the marginalized (UN Women, 2023).

Studies also indicate that there is a close connection between the rate of women representation and larger peace/security results (UN Women, 2022). Peace process (UN Women, 2015) studies discover that gender-sensitive policies are likely to be attained when women are

involved in the process. Through analogy, by adding women into cyber and AI policies-making, the latter would be more sensitive to various needs. However, in reality, female representation in cyber diplomacy, cybersecurity occupations, and disarmament talks is simply enormous (Ferl & Perras, 2024; APC, 2020). Indicatively, women have made up of 20-24 percent (UNIDIR, 2023) of the delegates in major UN cyber and AI forums over the last few years (Ferl & Perras 2024). This bias implies that the gender perspectives are not easily listened to. According to one PRIF analysis, the culture of security and technology (PRIF, 2024) has been discussed within paradigms of supposed gender-neutrality which are highly male-centric and militarized. We thus anticipate that the feminist theory will reveal how current AI-security policies promote existing power structures and not general safety.

Gender and Cybersecurity: The current body of literature on gender and cybersecurity demonstrates that the experiences of men and women (APC, 2020) on the Internet may vary significantly, although the technical aspect appears to be unbiased. As an example, gender is at work in the online environment (what is sought and shared), and social networks tend to reproduce the structure of power in the real world. Most recent studies are focused on two topics gender-based online violence (UN Women, 2023) (e.g. hate speech, cyberstalking against women) and gender inequality in the ICT workforce. Both apply to security. It is also evident that a significant percentage of women across the world have encountered any form of digital harassmentuneca.org, but these do not feature in the conventional cyber policy agendas. In the meantime, the proportion of women as cybersecurity professionals is low, (ISC², 2023) just 24 percent of the professionals worldwide, with smaller percentages among technology-based jobs and managerial positions and leadership. It implies that it is common that cybersecurity policies are made and enforced by male-dominant teams, which are unaware of such issues like online domestic abuse or algorithmic discrimination.

Important reports focus on the fact that cybersecurity is inherently connected (Office of the High Commissioner for Human Rights, 2022) with human rights, as well as that gender is a major factor of vulnerability. An instance is a 2020 report by feminist researchers claiming that there is a gender issue to international cyber security since it is based on the broader structural inequalities and that it needs a comprehensive response. Online gender-based violence (GBV) - including image-based abuse to doxxing - has been found to be instilled by structural inequalities. Nevertheless, global cyberspace discourses tend to divide cyberspace security and human rights, that is, the harmful effects on gender are under-investigated. Concisely, literature provides evidence that the harms of online are gendered, and the

protection of human rights (including women rights) is particularly important in the context of cybersecurity policyapc.orguneca.org.

AI and Gender: There is an increasing amount of literature analyzing the ways AI recreates gender (and racial) stereotypes (UNESCO, 2021). What machine-learning models learn is information that is guided by historical stereotypes (Buolamwini & Gebru, 2018). As an example, computer-vision research has shown that facial-recognition systems (Buolamwini & Gebru, 2018) are highly effective with white men but they miss by a large margin with women of color (Young Women's Movement, nd). This intersectional bias implies that the AI-based police and surveillance systems falsely identify or overlook non-white, female victims disproportionately. (UN Women, 2023; APC, 2020). In the same manner, the language-processing algorithms (UNESCO, 2021) tend to fall back to the usage of male pronouns when addressing things such as doctor or CEO, which perpetuates sexist associations. Gender bias in AI can be disastrous in terms of security. A recent study reports that close to 45 percent of the machine-learning systems reviewed are gender-biased (and more than 25 percent are gender and racial-biased) (Ferl & Perras, 2024). Any bias, no matter how minor, is perilous in military AI: an autonomous targeting system, which is skewed to recognize only military-aged men, can miss female combatants or civilian women in war-torn areas. Besides, emerging AI-powered threats such as deepfake pornography (UN Women, 2023) pose new gendered threats: fake images and videos can be used as an instrument of the so-called image-based sexual violence, which will predominantly harm women and their reputations and safety.

This is how a feminist view cautions that unless it is diverse, AI will merely replicate and amplify the existing inequality (Ferl & Perras, 2024). Moral AI ethics initiatives remind that to avoid gender bias in AI; we first need to address gender bias in our society. Practically, it involves the need to have varied development teams (OECD, 2019) and training information incorporating women, minorities, and Global Souths views. The literature, therefore calls on gender-conscious AI design and governance: developing algorithms and policies that are conscious of various social groups and do not reinstate old hierarchies.

Online Harassment and Surveillance: Related literature shows that digital threats affect women (UN Women, 2023) in a unique way. UN Women states that 16-58 percent of women all over the world have been victims of digital violence- the number spans both online harassment and stalking as well as non-consensual sharing of intimate images (Lipede, 2025).

Crucially, this is not the online violence, but it has severe consequences in real life (trauma, loss of career, threats to physical safety). The critical discussions by the scholars note that digital violence (Association for Progressive Communications, 2020) is inherently gendered: activists, journalists, and young women are more likely to be the victims of it, which can be explained by the occurrence of the patriarchal norms. As an example, an APC report states that online doxxing of women can lead to the threat of death or rape in real life (APC, 2020).

Ironically, most of the so-called protective technologies increase the state and individual surveillance on women. Feminist critics have been able to highlight such instances as the use of hidden cameras in women shelters or salons- supposedly to ensure safety but only to blackmail or harass the residents (Ali, 2024). Accordingly, the literature postulates that in the absence of a gender lens, the digital security provisions may work against them, making women spaces a location of control instead of safety.

In general, the historical studies are united around the point that technology, security and gender are self-affirming concepts. Feminist reading further demands that cybersecurity should extend (Hudson, 2005) past the militaristic defense and human security, taking into account such concerns as privacy, community coherence, and the absence of harassment. That insight is further developed in this chapter to examine AI-driven security in particular.

Analysis and Discussion

Human Security vs. State-Centric security

The main issue with this is that the majority of cyber and AI security frameworks are still state-centric (UNDP, 1994) and militarized concepts of security. Instead of concentrating on individual or community wellbeing, they concentrate in border control, deterrence, (Tickner, 1992) and national infrastructure- which are the traditional areas of military strategy. Since one commentator notes, international security remains heavily defined by state- and military-based security and structural violence, gendered aspects of which have been left out (Ferras & Perras, 2024). Security in this kind of paradigm means surveillance, to find the presence of foreign threat or repression of dissent at the cost of citizen rights. The key focus of cyber strategies is secrecy, offense/defense capability, and global competitiveness, which do not give much space to issues such as online gender-based violence or data privacy of vulnerable groups.

That leads to the question; whose security is it? (Enloe, 2014). Feminist response: almost always the safety of the already powerful (of states, armies, elites) and not of ordinary people. Vernacular structures seldom pose the question of whether the women, LGBTQ+, ethnic minorities or the poor are safer in these structures. As an illustration, predictive policing (Richardson, Schultz, & Crawford, 2019) tools are meant to forecast the crime location, although they tend to utilize data filled with bias, that shows historical over-policing of marginalized group. Equally, border-control algorithms can be used to monitor immigrants or refugees (UNHCR, 2022) and disregard digital risks to displaced women like fake online up to the scam or harassment of refugees. The consequence is that the gains of the security (such as order in the country or national stability) are distributed unevenly whereas the costs (data mining invasion, false allegations) are incurred by the weakest.

AI as a Mirror of Society

Artificial intelligence is often portrayed as a neutral (UNESCO, 2021) decision-maker, but in fact it acts as a mirror of the society that built it. Any algorithm trained on historical data (Barocas & Selbst, 2016) will absorb patterns of inequality in that data. In the security realm this is especially treacherous. For instance, widely used facial recognition (Buolamwini & Gebru, 2018) systems have been demonstrated to identify white male faces with very high accuracy, yet they often *fail to recognize Black women's faces*. This is not a technical quirk but a systemic bias: the training sets and design priorities were skewed toward one demographic. When law enforcement deploys these cameras, women and people of color may find themselves wrongly flagged or ignored, undermining both fairness and safety. (Young Women's Movement, 2025)

The bias is not limited to vision. Natural language processing can encode stereotypes (Bolukbasi et al., 2016) (e.g. associating careers with men), and allocation algorithms (for credit, jobs, or policing resources) can disfavor marginalized groups. Crucially, security is about threats – but what counts as a threat is itself gendered. A male-centric policy might see only traditional men-in-uniform as combatants, ignoring how women could both be combatants or victims. As one study points out, if autonomous targeting systems carry gender biases, *"'military-aged men' will most likely be disproportionately miscategorized as combatants and thus as potential targets"*. Meanwhile, crimes that mainly affect women (like domestic violence or online harassment) might not even register as "cybersecurity" issues, so they go unmodeled by threat-detection algorithms.

Crucially, technology also creates new gendered threats. The advent of deepfake technology (UN Women, 2023) – AI-generated images and videos – has led to a surge in "image-based sexual violence." Women are disproportionately victims of deepfake pornography, which is harder to police and can ruin reputations and careers. In addition to this, artificial intelligence is deployable to produce tailored disinformation. Misogynistic propaganda or anti-LGBTQ propaganda is propagated by automated bots (UNESCO, 2023) and tends to silence women in the general conversation. These emergent harms elucidate that cybersecurity cannot continue to exist in the technical sense; it must also confront gendered social forces.

Gendered Impacts of AI-Driven Security

The practical consequences of ignoring gender in AI security are manifold. We highlight a few illustrative domains:

Predictive Policing and Surveillance: AI-driven surveillance tools (from predictive policing (Richardson et al., 2019) algorithms to license-plate readers) tend to target poor and minority neighborhoods, which also often have higher numbers of women and children in precarious situations. Attack and targeting in socio-political context might subject whole communities to greater scrutiny. Predictive policing systems, including PredPol, have been studied empirically to show that a feedback loop of biased input, e.g. a history of over policing, can create a vicious cycle, where the algorithm will seemingly anticipate more law-enforcement presence in already heavily-surveilled districts (Young Women's Movement, 2025). Such a vested relationship is more than problematic in environments marked by cannibalistic gendered inequities where so many women are already facing domestic violence or have inadequate access to vital support.

Facial Recognition Bias: Computer vision studies consistently find that facial-recognition software has higher error rates for women and especially for women of color (Buolamwini & Gebru, 2018). This has two implications: women may be wrongly flagged by security systems (leading to humiliating stops or arrests) or worse, not identified when needed (e.g. if a missing child has a photo on file). If those systems are trained on biased data, they could exacerbate gender and racial profiling within the country's growing surveillance apparatus.

Online Harassment and Cyberstalking: Women in all societies face higher rates of certain digital harms. UN Women reports that *16–58% of women* (UN Women, 2023) and girls have experienced some form of digital violence (online harassment, stalking, non-consensual

image sharing) (Lipede, 2025). This violence is strongly linked to offline gender norms: a woman speaking out publicly online may invite sexist threats that aim to silence her. These threats are security issues too – they create fear and inhibit half the population from participating fully in the digital sphere. Moreover, online abuse often spills into offline life. For example, the APC report notes that being doxxed (having personal data published) has escalated into women receiving in-person rape and death threats (APC, 2020). Yet conventional cybersecurity frameworks often treat these as "private" or legal issues rather than security matters. The slide rightly notes that issues like doxxing, harassment, and cyberstalking, which overwhelmingly affect women, remain under-prioritized in cyber policy agendas, making cyberspace a hostile environment for women.

Protective Measures Becoming Surveillance**:** Paradoxically, some measures introduced to "protect" women have backfired by subjecting them to new surveillance. The Dawn report on Pakistan describes CCTV cameras being installed in women's shelters, hostels, and even beauty salons – ostensibly for security – but then misused by staff or intruders to record and blackmail residents. In these cases, technology meant to provide safety actually invaded private spaces, creating "a hostile environment of mistrust and insecurity" among women (Ali, 2024 & Privacy International, 2021). These instances illustrate a pattern: without careful oversight, AI-driven tools tend to expand policing into everyday life, frequently without consent or accountability.

Taken together, these impacts show that an AI-driven security regime can worsen the situation for many women and marginalized people, even as it purports to protect the population as a whole. Biased algorithms reinforce existing structural inequalities, turning the digital sphere into an extension of offline power imbalances.

The Global South Perspective

These issues are compounded by other factors in the Global South. One is that technical policies and systems are often brought in from the North without adequate localization. Numerous countries have adopted cyber security frameworks (UNESCO, 2021) and AI tools from other countries, believing they will be effective in their own country. However, threats and social contexts are different. South Asia and Africa are where gendered disinformation campaigns on the Internet and mobile economies of harassment are considered serious issues, but not ones engaged by imported policies. Making digital security local-to-life is difficult for

women's movements in these areas. Another observer's words capture the offline inequities in the Global South that "replicate themselves online" (APC, 2020).

Second, there are significant gender disparities in Internet use and digital literacy in most countries in the Global South. Only around 48% of women in the world use the internet (as opposed to 58% of men) and the gap is much higher in some areas such as South Asia and Africa (ITU, 2023; GSMA, 2024).

Third, there is an underrepresentation (UNIDIR, 2023) of women in regional processes of AI and cyber policy. Few (if any) women are part of advisory boards on technology or cybersecurity in many governments in the Global South. This disparity ignores matters such as gendered harassment, data privacy for survivors of violence, gender-responsive algorithms, and more.

Finally, there are specific risks for the Global South that don't always get noticed. One such example that has been found is the use of AI to spread misinformation about women's rights or reproductive health matters, which is more prevalent in certain regions, such as India and Pakistan, and is not a topic that typically comes to mind with cybersecurity concerns. In certain countries, such as Brazil and India, deepfakes have been employed in harassment campaigns. These risks are not mitigated because they do not have inclusive data or threat models. This leads to a "digital power divide" (World Bank, 2023) in which the offline status quo of women as subjects of subjugation in education, economy and law becomes the same status quo in cyberspace (Ali, 2024). To sum up, current inequalities of a patriarchal and postcolonial nature are being inscribed into cyber space if we do not do something about it.

Given that today's cyber policies fail to pass the gender test, what can be done?

These gendered aspects are not being addressed by the existing national and international cyber strategies. The majority of frameworks focus on deterrence, secrecy and state sovereignty – which excludes individual wellbeing. It is common to hear little or no mention of human security, if it is mentioned at all. For example, while the discussion of cybersecurity has been about critical infrastructure protection, data confidentiality for businesses or strategic cyber defense, it does not necessarily pay much attention to the harms when they occur at the community level. In cybersecurity, as with so many other areas, a "largely male-centric… view" that "often overlooks the unique experiences, expertise, and vulnerabilities of women and other marginalized groups" (Ferl & Perras, 2024) reigns supreme.

A case in point is international cyber diplomacy. As UN groups or summits on emerging tech gather, there is little representation from women, gender advocates say. The problems they talk about are never social justice issues, but technical puzzles or national security puzzles. At present, policies to date have little on the agenda to protect gendered data (such as reproductive health data), to regulate harassment enabled by AI, and to support the victims of online harassment. The mention of gender occurs mostly when looking at more ways to include women (a narrow "add women" approach) and not when considering (re)thinking threat models.

The slide "security becomes synonymous with surveillance, while safety remains neglected" is well-suited. In fact, in many states, investing in AI surveillance or digital protection will automatically ensure the protection of all citizens, but evidence indicates that only the powerful will be protected. Different measures are needed to gauge women's real security – their freedom from violence, abuse, and exclusion. The current policies leave out the emotional and social issues such as everyday concerns for girls and women to be followed on social media and their private lives to be exposed due to data breaches. To put it simply, the mainstream focus on security is technical, not social, and it's neglecting half the people.

Toward a Feminist Digital Security Paradigm

So what would a feminist security framework be if it failed in these ways? First and foremost, it restates the concept of security as empowerment, rather than control (Hudson, 2005). Rather than "How can we watch people better?", it asks "How can we keep people safe in ways that respect their dignity?" The focus on security policy would no longer just be on crisis management but on developing resilience – such as through digital literacy, community networks, and support for online vulnerable groups.

Creating policies and technologies together with the communities they are meant for, rather than being imposed from above is inclusive co-creation (OECD, 2019). This includes the engagement of women, gender minorities and other marginalized groups in every stage: from threat assessment to system design and governance. An example of a smart city surveillance system would be the creation of a system only after taking the concerns of women's rights into account as well as the placement of surveillance cameras away from sensitive areas. The APC report warns that the inclusion of women in negotiation processes increases the likelihood of gender provisions being included; and involving a variety of actors in cyber policy increases the chances of identifying blind spots (such as a feminist approach to misinformation).

Transparency and Accountability: AI and security systems need to be transparent and auditable (NIST, 2023). A specific issue is secret algorithms: when a predictive policing tool identifies a neighborhood as being "high risk" the residents should be able to find out why and appeal. Rules and policies must be made explainable (European Commission, 2024) and have ways to counteract biases when using AI to make decisions. This gives the public the power to challenge government and other entities if they are not delivering fair and equitable results.

Gender-aware threat modeling: Threats to security architectures should be gendered (UN Women, 2023). The classic view is threats to infrastructure such as cyberattacks or national espionage. A feminist approach would include online GBV, digital privacy violations (particularly of victims of violence), gendered disinformation and privacy for reproductive data. The PRIF analysis recommends that data breaches of health records should be considered a separate issue, as these breaches can specifically pose risks to women's reproductive rights. Likewise, the potential for the use of AI surveillance apparatus to trap LGBT+ people and minority women should be assessed (e.g. profiles on malicious dating apps used to blackmail vulnerable people). When policies are expanded to include anything that can be construed as a cyber-threat, the policies become more human-centered (Feral & Perras, 2024).

Embedding Diversity: A practical principle is to ensure diversity (UNESCO, 2021) in technical and policy teams. Research on tech organizations shows that homogenous teams are more likely to overlook biases (Ferl & Perras, 2024). Therefore, ministries and companies working on AI security should recruit and retain women, people of colour, and Global South experts. We saw in Turkey's context that only 22% of AI professionals are women (Ahmed, 2024); raising this number would help bring feminist insights into the design of new systems.

Global South Collaboration: Feminist tech governance should foster South–South exchanges (UNCTAD, 2023). Countries facing similar challenges (like gendered misinformation in South Asia) can share best practices and co-develop standards. This counters the top-down nature of policy transfers. For example, Pakistan and Turkey might jointly research how to regulate AI-driven deepfakes that target women, and propose regional guidelines that reflect local social norms.

Proactive Digital Inclusion: Lastly, the ultimate need must be to incorporate inclusivity at an early stage. Instead of responding to crises, policymakers and civil society organizations

should invest in empowering women with digital skills and safety connectivity and legal guarantees. Programs that teach digital literacy (ITU, 2023), such as privacy protocols, anti-harassment reporting systems, and critical thinking about fake news, can make people resistant to AI-related dangers. The promotion of women participation in the fields of STEM and security and the creation of grassroots security options, as emphasized by the PRIF blog, is invaluable (Ferl & Perras, 2024). In practice, it may mean funding community technology locations that serve women, finish feminist hackerspaces, or integrate gender-aware cybersecurity education in the K-12 curriculum.

With the support of the general principles, namely, co-creation, transparency, diversity, intersectionality and inclusion, the new paradigm of feminist digital security can be imagined. Justice and empowerment are the key security outcomes that are raised in this paradigm. An example is instead of extending CCTV cameras to try to prevent crime, a feminist approach would focus on sound privacy laws that protect the data of women and invest more in social projects that focus on the causal factors associated with violence. Its end goal is to build a technology ecosystem that empowers the voices of the marginalised groups instead of silencing them.

Principles for Equal Digital Governance

To summarize, key operational principles for an equal (feminist) digital governance model include:

Diverse Representation: Women and minorities deserve to be incorporated in AI policy boards, cybersecurity agencies, and data science teams as this is absolutely necessary (OECD, 2019). Diversity is important to conceive not as a tokenistic inclusion but as a conscious architectural response; the available data represents that diverse teams with a mix of genders developed a more equitable outcome (Ferl and Perras, 2024). The greater representativeness will naturally integrate gender issues into the processes of planning.

Gender-Aware Threat Models: Expenses elaborate threat evaluations that are express in integrating gendered harms (NIST, 2023). As an example, cybercrime units should track the online GBV patterns and work in liaison with the gender-based violence support organizations. The standards of AI should include assessments of bias, including the evaluation of facial-recognition effectiveness in relation to gender and race, before it is used.

Collaboration and Knowledge Sharing**:** It is necessary to promote the creation of interdisciplinary networks that allow feminist technologists and policymakers to collaborate (UNESCO, 2021) and exchange knowledge both in the Global South and the Global North. The actors of civil society have taken the lead in places (Pakistan, Turkey, and elsewhere) in overcoming digital violence already; official spaces can be very helpful in sharing the best practices, organizing campaigns, and collectively creating gender-sensitive regulatory policies.

From Reactive to Proactive: Switch between crisis response and preventive resilience (European Commission, 2024). Instead of catching the harassers after they occur, we must invest in community education, secure social media design, and empowerment of the at-risk groups. Active approach also involves regular auditing of AI systems to identify emerging vulnerabilities and revision of policies before the damage spreads.

Conclusion

AI-assisted security is an instrument with no neutrality (UNESCO, 2021); conversely, AI becomes very much intertwined with the political sphere and supports pre-existing hierarchies between genders and races. The chapter has followed the way in which the current AI security paradigm, which centers around the power of the state, has continued to obstruct women and other communities historically repressed. Digital security practices reinforce, not reduce, structural inequalities since they are based on biased algorithms (Barocas & Selbst, 2016), a one-size-fits-all policy framework, and a narrow definition of a threat. With the leaders starting to admit (though not necessarily in reality) that artificial intelligence systems can, in fact, enhance the already existing biases, and particularly those that discriminate against women (Ahmed, 2024, & Buolamwini & Gebru, 2018), the importance of a remedy model becomes apparent. However, a feminist approach (Tickner, 1992; Hudson, 2005) provides a path of transformation. A gender-focused and justice-based policy can enhance the resilience system by improving the effectiveness of the system in serving all the stakeholders, instead of compromising security. Once the current thinking of security as empowerment (UNDP, 1994), then technology can be used to fight the causes of violence and insecurity. To act as an example, inclusive AI would be better able to protect the survivors of violence with automated harassment filtering, break privacy traps through diversity in policy-makers, and rally digitally enabled vulnerable communities to develop common defenses. The real security should start with the most vulnerable people at the end. Existing AI systems safeguard the

agendas of major nation-states, senior leadership, corporate entities, and other powerful lobbying organizations, thereby putting other groups at the risk of new types of violence and surveillance. Feminist digital security paradigm, in its turn, does not consider justice, accountability, and inclusion as peripheral matters but makes it its mission. In turn, only by defying the tendency to marginalize any group, AI and cybersecurity may operate in the best way. The construction of the future of AI-premedicated security will thus require the incorporation of human safety and dignity into our algorithms and policies -not through efficiency or power. By doing such, the feminist approaches offer a more humane, fair and efficient security environment to all.

References

Association for Progressive Communications. (2020). *Technology-facilitated gender-based violence: Making rights and realities visible*. Association for Progressive Communications.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732.

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Polity Press.

Bolukbasi, T., Chang, K.-W., Zou, J. Y., Saligrama, V., & Kalai, A. T. (2016). Man is to computer programmer as woman is to homemaker? Debiasing word embeddings. In D. D. Lee, M. Sugiyama, U. Luxburg, I. Guyon, & R. Garnett (Eds.), *Advances in Neural Information Processing Systems* (Vol. 29). Curran Associates.

Brown, D., & Pytlak, A. (2020). *Why gender matters in international cyber security*. Women's International League for Peace and Freedom & Association for Progressive Communications.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of Machine Learning Research* (Vol. 81, pp. 77–91).

Cockburn, C. (2004). The continuum of violence: A gender perspective on war and peace. *Women's Studies International Forum, 27*(1), 24–29.

Crenshaw, K. (1989). Demarginalizing the intersection of race and sex: A Black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum, 1989*(1), 139–167.

Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.

Enloe, C. (2014). *Bananas, beaches and bases: Making feminist sense of international politics* (2nd ed.). University of California Press.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

European Commission. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Publications Office of the European Union.

Ferl, A.-K., & Perras, C. (2024). *Beyond the code: Unveiling gender dynamics in AI and cybersecurity for international security* (PRIF Spotlight No. 2/2024). Peace Research Institute Frankfurt.

GSMA. (2024). *The mobile gender gap report 2024*. GSMA.

Hudson, H. (2005). 'Doing' security as though humans matter: A feminist perspective on gender and the politics of human security. *Security Dialogue, 36*(2), 155–174.

International Telecommunication Union. (2023). *Facts and figures 2023*. International Telecommunication Union.

ISC². (2023). *2023 cybersecurity workforce study*. ISC².

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.

Office of the United Nations High Commissioner for Human Rights. (2022). *The right to privacy in the digital age*. United Nations.

Organisation for Economic Co-operation and Development. (2019). *OECD principles on artificial intelligence*. OECD Publishing.

Privacy International. (2021). *Safe cities or surveillance cities? The impact of surveillance technologies on women and marginalized communities*. Privacy International.

Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review Online, 94*, 192–233.

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton.

Sjoberg, L. (Ed.). (2010). *Gender and international security: Feminist perspectives*. Routledge.

Thompson, L., & Clement, R. (2019). *Defining feminist foreign policy*. International Center for Research on Women.

United Nations Conference on Trade and Development. (2023). *Digital economy report 2023*. United Nations.

United Nations Development Programme. (1994). *Human development report 1994: New dimensions of human security*. Oxford University Press.

United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO.

United Nations Educational, Scientific and Cultural Organization. (2024). *Challenging systematic prejudices: An investigation into bias against women and girls in large language models*. UNESCO.

United Nations High Commissioner for Refugees. (2022). *Global trends: Forced displacement in 2022*. UNHCR.

United Nations Institute for Disarmament Research. (2023). *Gender perspectives in international cyber policy*. UNIDIR.

United Nations Security Council. (2000). *Resolution 1325 (2000): Women, peace and security*. United Nations.

UN Women. (2023). *Technology-facilitated violence against women: Global perspectives and policy responses*. UN Women.

World Bank. (2023). *World development report 2023: Migrants, refugees, and societies*. World Bank.

SİBER GÜVENLİK TEHDİDİ OLARAK DEZENFORMASYON: DİJİTAL GÜVENLİK VE DİPLOMASİ AÇISINDAN ETKİLERİ

Hüma Gül ÇAKIR*
ORCID ID: 0000-0003-2796-1058

Declaration*

Abstract

The circulation of information has experienced significant transformations on a global scale with the development and acceleration of digitalization. While this transformation has made access to information easier, it has also created the conditions for maniplative content and disinformation to spread rapidly and on a large scale. The main question of this article is why disinformation is increasingly viewd as a cyber security threat and how it affects diplomatic processes in the contemporary digital environment. The article applied a qualitative research method based on document analysis and case study methodology. Academic literature and institutional reports were examined to investigate the transformation of disinformation and conceptualization as a cyber threat. Case study such as 2026 U.S. presidential election, the Brexit referendum and the Russian-Ukraine War were analyzed tos how the effects and political consenquences of cyber-enabled disinformation. The findings indicate that disinformation has become an integral part of the cyber space today. States and other actors in the cyber space are engage in disinformation activities by using social media platforms, algorithmic dissemination, data analysis and Al-generated content and thereby achieve various objectives. In this regard, it appears that disinformation disseminated in the cyber space can be understood as a multidimensional phenomenon at the intersection of cyber security, strategic communication and diplomacy.

Keywords: Disinformaiton, Cyber Security, Information Operations, Digital Diplomacy

Özet

Dijitalleşmenin gelişimi ve hızlanmasıyla bilgi dolaşımı küresel ölçekte önemli dönüşümler yaşamıştır. Bu dönüşüm bilgiye erişimi kolaylaştırırken aynı zamanda manipülatif içeriklerin

* Selçuk Üniversitesi, Uluslararası İlişkiler Bölümü, Doktora öğrencisi, humagulcakir@gmail.com
* Bu çalışmanın yazım sürecinde makale organizasyonunun oluşturulması, yabancı dil çevirisi ve dilsel düzenleme amacıyla yapay zeka araçları kullanılmıştır.

ve yanlış bilgilerin de hızlı ve geniş ölçekte yayılmasına zemin hazırlamıştır. Bu makalenin temel sorusu, dezenformasyonun neden giderek artan bir siber güvenlik tehdidi olarak görüldüğü ve çağdaş dijital ortamda dezenformasyonun diplomatik süreçleri nasıl etkilediğini inceleme üzerinedir. Makalede belge analizi ve vaka incelemesi metodolojisine dayalı nitel araştırma yöntemi kullanılmıştır. Dezenformasyonun dönüşümünü ve siber tehdit olarak kavramsallaştırılmasını incelemek için akademik literatür ve kurumsal raporlar incelenmiştir. 2016 ABD Başkanlık seçimleri, Brexit referandumu, Rusya-Ukrayna Savaşı gibi seçilen örnekler ise siber destekli dezenformasyonun yansımalarını ve siyasi sonuçlarını göstermek için analiz edilmiştir. Bulgular, dezenformasyonun günümüzde siber alanın ayrılmaz bir parçası haline geldiğini göstermektedir. Devletler ve diğer siber alan aktörleri, sosyal medya platformlarının, algoritmik yayılımların, veri analizinin ve yapay zekâ üretimi içeriklerin kullanılması yoluyla dezenformasyon faaliyetleri oluşturulmakta ve bunun sonucunda çeşitli hedeflere ulaşabilmektedir. Bu bağlamda siber ortamda yayılan dezenformasyonun, siber güvenlik, stratejik iletişim ve diplomasi kesişiminde çok boyutlu bir olgu olarak anlaşılması mümkün görünmektedir.

Anahtar Kelimeler: Dezenformasyon, Siber Güvenlik, Bilgi Operasyonu, Dijital Diplomasi

Giriş

Bilgiye erişim ve bilgi kullanımı, tarihin her safhasında hem bireyler hem de devletler için büyük önem taşımıştır. Bu noktada başarılı olan aktörler hem siyasi hem de ekonomik olarak bilgi gücünün avantajlarından yararlanmışlardır. Küreselleşme ile bilgi ve iletişim teknolojilerinin artması, dünya çapındaki en önemli gelişmelerden biri olan dijitalleşmenin önünü açarak hem bireylerin hem de ulusların iletişimlerini dijital ağlar aracılığıyla gerçekleştirmelerine neden olmuştur. Bu dönüşümle birlikte bilginin ve iletişimin uluslararası sistemdeki rolü değişmiş ve yeni bir güvenlik alanı doğmuştur. Teknoloji ilerledikçe, geleneksel uluslararası güvenlik ortamının sınırları ortadan kalkmaya başlamış ve teknolojik alanın güvenliği ön plana çıkmaya başlamıştır. Bu bağlamda bilginin ve onun güvenliğinin sağlanması hem ulusal hem de uluslararası alanda uluslararası güvenliğin önemli bir bileşeni haline gelerek siber güvenlik, bilgi güvenliği ve dijital güvenlik gibi modern kavramların ortaya çıkmasına sebep olmuştur.

Nye, uluslararası politikada bilgi ve güç arasındaki ilişkiyi analiz ederken bilginin çeşitli boyutlarının analiz edilmesi gerektiğini belirtmektedir. Bu noktada birinci olarak bilgi,

haberler, istatistikler ve kamuya açık bilgi biçimleri de dahil olarak sınırlar arası veri akışını ifade edebilir. Son yıllarda bu sınır ötesi bilgi akışları genişlerken, bilgiye erişim ve iletim maliyetleri düşmüş ve dijital teknolojiler sayesinde erişim noktaları sayısı artmıştır. Bu dönüşüm sayesinde daha küçük devletler ve devlet dışı aktörler küresel bilgi ağına daha aktif katılım sağlamışlardır. İkinci olarak bilgi, stratejik veya ekonomik rekabette avantaj elde etmek için kullanılan bir kaynak olarak kullanılabilir. Bu noktada bilginin zamanlaması önemlidir çünkü rakiplerden daha önce bilgi edinen ve kullanan aktörler avantaj elde ederler. Rekabetçi bilgiler genelde ekonomik faaliyetler ile ilişkilendirilse de askeri alanlarda da bilgi üstünlüğünün sonuçları önemlidir. Üçüncü olarak bilgi, potansiyel rakiplerin niyetleri, kapasiteleri ve planları hakkında stratejik bilgi olarak belirlenmektedir. Stratejik bilgiler, uluslararası arenanın merkezinde olan istihbarat ve casusluk gibi uygulamalarla ilişkilendirilebilir. Teknolojik gelişmeler belirli istihbarat araçlarını genişleterek daha fazla aktörün bilgi toplamasına olanak sağlasa da avantajlı konum hala büyük ve daha geniş kaynaklara sahip olan devletlerin elindedir (Nye, 2002, s. 68).

Bilgi mücadeleleri, devletlerin hem barış hem de kriz dönemlerinde siyasi hedeflerine ulaşmak için kullandıkları önemli bir araç haline gelmiştir. Uluslararası ilişkiler rekabet ve iş birliğinin eş zamanlı var olduğu bir yapıya sahip olduğu için bilgi üzerindeki mücadeleler uluslararası sistemin kalıcı bir özelliği olarak görülmektedir. Bilgi üretimi, yayılımı ve kamuoyu algısını şekillendirme faaliyetleri bilgi etkisindedir. Bu çerçevede dezenformasyonun yayılması, bilgi akışlarının manipülasyonu gibi uygulamalar önemli etki araçlarını oluşturmaktadır (Talinshinsky, 2026, s. 7). Günümüzde sosyal medya, algoritmik manipülasyon, bot ağları, deepfake teknolojileri gibi yeni faaliyetler dezenformasyonu çok daha etkili ve ölçeklenebilir hale getirmiştir. Bu nedenle dezenformasyon artık sadece bir propaganda aracı değil, siber güvenlik tehdidi (Caramancion, 2020), hibrit savaş aracı (Bērziņš, 2014) veya diplomatik ilişkileri etkileyen bir stratejik araç (Nye, 2019) olarak görülebilir.

Çalışmanın temel sorusu siber güvenlik, uluslararası ilişkilerde ve diplomatik süreçlerde dezenformasyonla mücadeleye nasıl bir katkı sağlar şeklinde oluşturulmuştur. Alt sorular olarak dezenformasyonun neden siber güvenlik tehdidi olarak görüldüğü, dezenformasyonla mücadele için hangi siber güvenlik stratejilerinin kullanılması gerektiği ve bu stratejilerin uluslararası diplomasi ve normları nasıl etkilediği şeklinde belirlenmiştir. Bu bağlamda

makalede uluslararası ilişkilerde bilginin stratejik kullanımına odaklanarak dezenformasyon, siber güvenlik ve diplomasi arasındaki ilişkiye değinilmiştir.

Dezenformasyon ve Siber Güvenlik

Dezenformasyon Kavramı

Dijital iletişim teknolojilerinin artan önemi, çağdaş toplumlarda bilgi üretimi, dolaşımı ve tüketimini temelden dönüştürdüğü görülmektedir. Bilgi kavramı giderek artan şekilde dijital platformlar ve ağ tabanlı iletişim sistemleri üzerinden akmaya devam ederken içeriklerin hızlı yayılması hem ulusal hem de uluslararası siyasi ortamlarda yeni fırsatlar yaratırken yeni güvenlik açıkları da yaratmaktadır. İletişim teknolojileri, sosyal medya platformları ve siber alandaki gelişmeler hem devletlerin hem de devlet dışı aktörlerin bilgiyi daha önce görülmemiş bir ölçekte yayma kapasitelerini genişletmiştir. Bu noktada küreselleşme ile dijital teknolojilerin artan öneminin, uluslararası arenada aktörlerin bilgiyi siyasi süreçleri ve kamuoyunu etkilemek için kullanabilecekleri bir kaynağa dönüştürdüklerini söylenebiliriz. Bilgi uluslararası ilişkilerde önemli bir etki aracı haline gelirken dezenformasyon faaliyetleri yoluyla bilginin manipülasyonu hem siber güvenlik hem de diplomasi için giderek daha önemli bir zorluk olarak ortaya çıkmıştır.

Bu bağlamda bilgi manipülasyonları siyasi istikrarı, kamu güvenliğini ve diplomatik ilişkileri etkileyen önemli bir zorluk olarak ortaya çıkmaktadır. Bunlara ek olarak yanlış ve yanıltıcı bilgilerin tüm biçimleri aynı özelliklere, niyetlere veya sonuçlara sahip değildir. Bu sebeple dezenformasyon ve dijital güvenlik arasındaki ilişkiyi doğru şekilde analiz etmek için çeşitli kavramlar arasındaki ayrımların yapılması gerekir. Bu noktada dezenformasyon (disinformation), yanlış bilgilendirme (misinformation) ve kötü amaçlı bilgilendirme (malinformation) şeklinde üç bilgi bozukluğu kavramı karşımıza çıkmaktadır. Bu kavramlar bilgi bozukluklarının farklı biçimlerini gösterir ve çağdaş dijital tehditleri ve stratejilerini anlamak için önemli bir kavramsal çerçeve oluşturur.

İlk olarak dezenformasyon (disinformation) kavramı, bireyleri, grupları, kurumları ve kuruluşları manipüle etmek veya onlara zarar vermek amacıyla kasıtlı olarak yanlış veya yanıltıcı bilgilerin yayılması olarak tanımlanabilir (Wardle & Derakhshan, 2017, s. 20). Ancak siber güvenlik açısından bakıldığında, belirli bir bilginin tamamen yanlış mı yoksa sadece yanıltıcı mı olduğu sorusu genelde ilk aşamada önemli değildir. Daha önemli olan

nokta, kurumların faaliyetlerine, itibarlarına veya istikrarlarına zarar vermek amacıyla tasarlanmış bilgi faaliyetlerine karşı geliştirdikleri önleme ve bunlara yanıt verme kapasiteleridir (Boevink, Mok, & M.Int, 2023, s. 6). Bu noktada önemli örneklerden biri 2016 Amerika Birleşik Devletleri başkanlık seçimleri sürecidir. Rus devlet bağlantılı aktörlerin seçim süreçlerini etkilemek ve demokratik kurumlara olan kamu güvenini zayıflatmak amacıyla sosyal medya platformları üzerinden dezenformasyon kampanyaları yürüttükleri belirlenmiştir. Bu dezenformasyon sürecinde kutuplaştırıcı ve yanıltıcı bilgiler yayılarak bu tür operasyonların dijital platformlar aracılığıyla nasıl siyasi müdahale ve stratejik etki araçları olarak kullanılabileceği görülmüştür (U.S Senate Intel Committee, 2019).

İkinci olarak yanlış bilgilendirme (misinformation), kasıtlı olarak zarar verme veya kitleleri manipüle etme amacı olmaksızın paylaşılan yanlış veya hatalı bilgileri ifade eder. Bu durumlarda aktörler doğru veya güvenilir olduğuna inanarak yanıltıcı içerik yayabilirler (Wardle & Derakhshan, 2017, s. 20). Yakın bir örnek olan COVID-19 pandemisi, yanlış bilgilendirme kavramı temelinde yanlış ve yanıltıcı bilgilerin yayılarak halk sağlığı ve toplumsal güvenlik açısından önemli zorlukların ortaya çıktığı önemli bir örnektir. Virüsün kökeni, tedavi yöntemleri, aşılar ve önleyici tedbirler hakkındaki iddialar halk arasında büyük bilgi düzensizliğine yol açtı ve resmi sağlık kurumlarının bilgileri ile uyumsuzluklar ortaya çıktığı görüldü. Sağlık konusundaki yanlış bilgilerin hızla yayılması ve teyit edilmesinin güçlüğü, insanla arasında sadece belirsizlik ve kaygıları arttırmakla kalmayarak bazı durumlarda hastalığın yayılmasına doğrudan sebep olduğu görülmüştür. Bu nedenle pandemi, dijital ortamdaki dezenformasyonun bir iletişim sorununun ötesine geçerek kamu güvenliği ve kurumsal güveni etkileyen geniş bir güvenlik tehdidine nasıl dönüşebileceğini göstermiştir. Ek olarak bu süreç sosyal medya platformlarındaki içerik denetleme mekanizmalarının zayıflıklarını da göz önüne çıkarmıştır (Hsu, 2022).

Buna karşılık olarak üçüncü kavram kötü niyetli bilgilendirme (malinformation), gerçeğe dayanan ancak bireylere, kuruluşlara veya devletlere zarar vermek amacıyla kasıtlı olarak üretilen ve kullanılan bilgileri ifade eder. Bu bilgi bozukluğu biçimi genellikle siyasi, sosyal veya itibar zedelenmesi amaçlı olarak gerçek bilgilerin stratejik anlamda ifşa edilmesini, manipüle edilmesini veya çarpıtılmasını içermektedir (Wardle & Derakhshan, 2017, s. 20). 2012 yılında LinkedIn şirketinin yaşamış olduğu büyük veri ihlali olayı, milyonlarca kullanıcının şifre ve hesap bilgilerinin ifşa edilmesine yol açarak önemli bir örnek olmuştur. Bu olayın ardından birçok kullanıcı, kişisel bilgilerini ele geçiren kötü niyetli kişilere fidye

ödemesi yapılmadığı takdirde hesap bilgilerinin kötüye kullanılması tehdidi ile karşı karşıya kalmışlardır. Birkaç yıl sonra çalınan bilgilerin deepweb pazarında satıldığını gösteren raporlar ortaya çıkmış ve bu durum büyük ölçekli veri ihlallerinin uzun vadeli güvenlik sorununun etkilerini ortaya koymuştur. (Krebs, 2016).

2023 yılında yayınlanan Birleşmiş Milletler (BM) Dijital Platformlarda Bilgi Bütünlüğü raporunda bilgi bütünlüğünün korunması ve dezenformasyonla mücadele edilmesi uluslararası toplum için acil bir öncelik olarak belirtilmiştir. Raporda dezenformasyon ve türlerinin dijital alanın ötesine uzandığı ve kamu güveni, demokratik yönetişim ve barış gibi alanları etkileyen çok boyutlu riskleri barındırdığı vurgulanmıştır (UN, 2023, s. 25). Görüldüğü üzere dijital ortamlarda giderek yaygınlaşan dezenformasyon, yanlış bilgilendirme ve kötü niyetli bilgilendirme faaliyetleri, bilginin siyasi, sosyal ve güvenlik dinamiklerini etkileyen stratejik bir araç haline geldiğini göstermektedir. Dijital iletişim teknolojileri bilginin sınırlar ötesinde hızlı bir şekilde yayılıp manipüle edilmesini mümkün kılarken aynı zamanda bilgi de devlet ve devlet dışı aktörler arasındaki çekişmenin merkezi bir alanı haline gelmiştir. Bu bağlamda bilginin siyasi etkileme ve toplumsal manipülasyon için stratejik kullanımı çağdaş uluslararası ilişkilerde geniş bir anlama sahip olan bilgi savaşı ile de yakından ilgili olduğu söylenebilir.

Bilgi savaşı, bilişsel savaş (cognitive warfare) ve hibrit savaş (hybrid warfare) ile açıklanabilecek çok yönlü bir stratejik alan olarak görülebilir. İnsan zihnine yönelen bilişsel kısım ile devlet stratejileri içerisindeki yeri hibrit bir savaş alanı ile ilişkilendirilebilir. Bu bağlamda bilginin yalnızca iletişim aracı olarak değil stratejik bir çatışma alanı olarak kabul edilmesi mümkündür. Bilginin bir savaşın parçasına dönüşmesi sürecinde dijital iletişim sistemlerine olan bağımlılığın artması, bilgiyi siyasi bilişsel algıları, kamuoyu ve devlet davranışlarını etkileyebilecek stratejik bir araca dönüştürdüğü görülmektedir (Marangione, 2021, s. 151).

Dezenformasyonun tek başına hareket etmediği, daha geniş hibrit stratejiler ağının bir parçası olduğunu söylemek mümkündür. Bu bağlamda bilişsel savaş alanı önemli bir kavram olarak karşımıza çıkmaktadır. Bilişsel savaş, genel olarak bir düşmanın algısını hedefini zayıflatmak, etkilemek veya etkisiz hale getirmek amacıyla manipüle etmek amacıyla tanımlanabilir. NATO (North Atlantic Treaty Organization) bilişsel savaşı, bilişsel üstünlük için verilen bir mücadele olarak kavramsallaştırmıştır. Bu mücadele, bilişsel bir avantaj elde etmek ve korumak için tasarlanmış koordineli bir askeri ve sivil faaliyetleri içerir. Bu savaş biçiminin en önemli amacı ise karar alma süreçlerini şekillendirmek ve manipüle etmek için mevcut tüm

bilgi, strateji ve araçları kullanarak bilişsel yollarla insan davranışlarını etkilemektir (Blatny & Søndergaard, 2025, s. 6-7). Bilişsel savaş, bilginin silahlandırılmasına ve kamu güveninin kasıtlı olarak manipüle edilmesine dayandırılmıştır. Düşman aktörler propaganda, dezenformasyon ve deepfake gibi teknolojiler aracılığıyla siyasi süreçleri etkilemeyi ve kamuoyu algısını şekillendirmeyi amaçlamaktadır. Bu bağlamda koordineli bilgi operasyonları yoluyla bilişsel zaaflar kullanılarak bireylerin algıları hedef alınmaktadır (Blatny & Søndergaard, 2025, s. 13-14). Görüldüğü üzere modern çatışmalar artık insanların düşünme süreçlerini hedef almaktadır. Bu bağlamda insan zihninin çatışma alanı haline geldiğini ve dezenformasyonun bilişsel savaşta kullanılan temel silahlardan biri olduğunu söylemek mümkündür. Özellikle dijital platformlar üzerinden toplumun düşünme biçimleri, karar alma süreçleri ve algıları hedef alınmaktadır. Bilişsel savaşın bu önemli ve geleneksel olmayan çatışma süreçleri toplumsal güveni, seçim süreçlerini ve kurumlara güveni azaltarak güvenlik boyutunda yeni boyutların kapılarını açmaktadır.

Öte yandan hibrit savaş ile dezenformasyonun arasında doğrudan ve tamamlayıcı bir ilişki bulunmaktadır. Dezenformasyon, modern hibrit tehditlerin en temel araçlarından biri olarak kullanılmaktadır. Hibrit savaş, devlet veya devlet dışı aktörler tarafından belirli siyasi hedeflere ulaşmak için askeri veya askeri olmayan, geleneksel veya geleneksel olmayan çeşitli yöntemlerin koordineli kullanımı olarak açıklanabilir. Bu bağlamda aynı stratejik amaçlar çerçevesinde yürütülen siber saldırılar, kimyasal saldırılar ve dezenformasyon faaliyetleri bu kapsamın içine girmektedir (EEAS, 2018). Bu bağlamda dezenformasyonun toplumları istikrarsızlaştırmak, zayıflatmak veya siyasi bağlamda karar alma süreçlerini etkileyen karşılıklıkları yaratmayı amaçlayan hibrit savaş bileşenlerinden önemli bir tanesi olduğunu söylemek mümkündür.

Görüldüğü üzere dezenformasyon ve güvenlik arasındaki ilişki, günümüz uluslararası güvenlik ortamında daha önemli ve karmaşık bir hale gelmiştir. Dijital iletişim teknolojilerinin gelişimi sadece bilgi üretimi ve dolaşımını dönüştürmekle kalmamış aynı zamanda bilgi manipülasyonları ve siber alanda gerçekleştirilen yeni güvenlik açıkları da yaratmıştır. Bu bağlamda dezenformasyon iletişim ile ilgili bir kavramdan öteye evrilerek çok boyutlu bir dijital güvenlik sorunu haline gelmiştir. Bilgi savaşı, bilişsel savaş ve hibrit savaş tehditlerinin artan kullanımı da siber alanda işlenen bilgilerin stratejik önemini arttırmıştır. Bu nedenle dezenformasyon ve dijital güvenlik arasındaki etkileşimin, çağdaş güvenlik tehditleri

temelinde hem teknolojik hem de bilişsel boyutlarını kapsayan daha geniş bir çerçeveye sahip olduğu görülmektedir.

Dezenformasyonun Siber Güvenlik Tehdidi Olarak Kavramsallaştırılması

Dezenformasyonun, sadece dar kapsamlı bir iletişim ve bilgi temelli bir sorun olarak değil, aynı zamanda siyasi istikrarı, kurumsal güveni ve demokratik sistemi etkileyen çok boyutlu bir dijital güvenlik tehdidi olarak anlaşılması önemli bir noktadır. Bu bağlamda dezenformasyonun klasik anlamda donanım ve yazılım çökertmeyi hedefleyen siber operasyonların ötesinde, dijital ağlar ve ileri seviye teknolojilerle entegre edilmiş geniş çaplı bir bilişsel güvenlik tehdidi olduğunu söylemek mümkündür.

Dezenformasyon, hedef kitleleri aldatmak ve algıları, davranışları veya siyasi sonuçları etkilemek amacıyla bilginin kasıtlı şekilde manipüle edilmesi anlamına gelirken, benzer şekilde siber tehditler de genellikle hedef alınan sistemlere, kurumlara veya toplumlara zarar vermek amacıyla belirli saldırı çeşitleri aracılığıyla gerçekleştirilen kasıtlı eylemler olarak tanımlanabilir. Bu açıdan bakıldığında dezenformasyon kampanyaları, organize olmuş aktörler, stratejik hedefler, hedef seçimleri ve amaçlanan etki de dahil olmak üzere siber tehditlerle ilişkili benzer yapısal özelliklere sahiptir (Caramancion, Li, Dubois, & Jung, 2022, s. 3-4). Bu bağlamda epistemolojik olarak bakıldığında dezenformasyon ve siber tehditlerin birbirleri ile uyumlu bir kavramsal çerçeve içerisinde oldukları görülmektedir. Bu durum aynı zamanda dezenformasyonun yalnızca iletişimle ilgili bir olgu olmaktan ziyade çok boyutlu bir dijital güvenlik tehdidi olarak anlaşılmasını güçlendirmektedir.

Dezenformasyon, manipüle edilmiş bilgiler ve deepfake gibi teknolojiler kullanarak insan zihnindeki bilişsel zaafları, önyargıları ve mantıksal hataları olumsuz manada kullanmayı hedeflemektedir (Jaiman, 2021). Başka bir değişle geleneksel siber saldırılar teknolojik sistemleri alt etmek için kullanılırken dezenformasyon insan düşüncelerini ve algılarını doğrudan etkilemek için teknolojiyi kullanmaktadır (Boevink, Mok, & M.Int, 2023, s. 7). Bu durum literatürde bilişsel hackleme (cognitive hacking) olarak adlandırılmıştır ve siber güvenliğin doğrudan insan zihnine yöneltilmiş bir boyutu olarak ele alınmıştır (Bone, 2018). Bilişsel hackleme genellikle meşru bilgi kaynaklarına benzeyen, tasarlanmış aldatıcı içerikler aracılığıyla mevcut inançları güçlendirmeyi veya bireylerin gerçeklik algılarını çarpıtmayı amaçlamaktadır. Bilişsel süreçlere yapılan bu müdahale, kamuoyu, davranış ve karar alma süreçlerini etkileyerek bazı durumlarda kritik altyapılara yönelik doğrudan yapılan siber

saldırıların etkisinden daha büyük sonuçlar doğurabilir. Ortaya çıkan bilgi karmaşası ve gerçekler arasındaki belirsizlik kurumsal güvenilirliği zayıflatabilir ve toplum işleyişini aksatabilir (Caramancion, Li, Dubois, & Jung, 2022, s. 1-2).

Görüldüğü üzere dezenformasyon ile siber saldırı arasındaki farklardan en önemlisi hedeftir. Fakat eylemler, stratejiler ve zararlar büyük oranda benzerlik göstermektedir. Örneğin kötü niyetli aktörlerin sahte haberlerle dijital platformlarda gerçekleri perdelemeleri veya yanlış iletmeleri, siber güvenlikteki sunucuları kitleme hedefinde olan DDoS saldırıları ile aynı mantığa dayanmaktadır. Benzer şekilde insanların bilişsel düzeyde duygularını manipüle etmek, bir siber saldırı yöntemi olan oltalama saldırılarının temel motivasyonları büyük bir benzerlik göstermektedir (Jaiman, 2021). Her iki saldırı biçimi de hedeflerine ulaşmak için bireylerin teknolojiye, dijital platformlara ve tanıdık arayüzlere olan güvenlerini istismar etmektedir. Buna ek olarak siber alandaki kimlik ağı operasyonları genellikle finansal kazanç veya veri hırsızlığı gibi amaçlarla gerçekleştirilirken bilişsel saldırılar yoluyla yayılan dezenformasyon faaliyetleri ise kamuoyu manipülasyonu, sosyal kutuplaşmanın yaratılması, seçim süreçlerine müdahale ve siber savaş stratejilerinin geliştirilmesi gibi daha geniş stratejik hedeflere sahiptir. (Caramancion, Li, Dubois, & Jung, 2022, s. 14).

Dezenformasyonun dolaşım sağladığı sosyal medya platformlarının yapısal özellikleri, dezenformasyonun temel dijital altyapısını oluşturmaktadır. Bu platformlar, kullanıcı davranışlarını analiz eden makine öğrenmesi algoritmaları ile içerik dağıtımını gerçekleştirir. Faaliyetler genellikle bot ağları, sahte hesaplar, koordineli manipülasyon stratejileri ve deepfake teknolojileri gibi birbirine bağlı mekanizmalara dayanmaktadır. İnsan davranışlarını taklit edebilen sistemler aracılığıyla bot ağları yapay olarak etkileşim yaratır ve seçilen anlatıları güçlendirerek kamu etkileşimi görünümü oluşturur (Aras, 2026, s. 165-166).

Özellikle seçim dönemlerinde bot hesaplar ve sahte sosyal medya profilleri, propaganda içeriklerini yaymak ve dezenformasyon kampanyalarını yürütmek için kullanılmaktadır. Belirli siyasi aktörleri destekleyen veya hedef alan içerikler sistematik olarak yayılır ve siyasi söylemler yapay olarak şekillendirilmektedir. Bu uygulamalar, dijital ortamlarda kamuoyunun gerçekliğini bozar ve siyasi kutuplaşma yaratarak demokratik süreçlerin manipülasyonunu kolaylaştırmaktadır. Bu bağlamda algoritmik olarak yönlendirilen dezenformasyon kampanyaları dijital platformların nasıl siyasi etki ve algı yönetimi araçlarına dönüştürülebileceğini göstermektedir.

Siber Destekli Dezenformasyon

Siber destekli dezenformasyon, belirlenen hedefe ulaşmak için bilgi ortamını değiştirmeyi veya bulanıklaştırmayı amaçlamaktadır. Amacı, karar vericilerin algılarını etkilemek ve karar aşma süreçlerinde mevcut bilgiler konusunda belirsizlik yaratmaktadır. Güvenilir veya güvenilmez bilgiler arasındaki ayrım bulanıklaşır ve dezenformasyon olayların değerlendirilmesini zorlaştırır. Bu bağlamda bilgi karmaşasının yaratılması karar vericilerin sorunları etkili şekilde değerlendirme süreçlerini etkilemektedir. Gerçek bilgiler konusunda fikir birliği sağlansa bile medya organları veya diğer kaynaklar aracılığıyla dolaşıma sokulan bilgilerin manipüle edilmiş olabileceği algısı, bilgi ekosistemine olan güveni zedeleyebilmektedir (Baştan & Oran, 2024, s. 1214-1215).

Çağdaş çalışmalar devletlerin stratejik hedeflerine yalnızca geleneksel askeri yeteneklerle değil aynı zamanda bilgi ortamının kontrolü ve manipülasyonu yoluyla da ulaşmaya çalıştığını göstermektedir. Bu bağlamda çevrimiçi alanda dijital platformlar aracılığıyla yürütülen bilgi operasyonları, dezenformasyon kampanyaları ve siber destekli iletişim stratejileri devlet yönetiminin önemli araçları haline gelmiştir (Jabrailov, 2025, s. 716).

Demokratik süreçlere yönelik en bilinen dijital müdahalelerden biri olan Cambridge Analytica skandalı, dijital manipülasyon ve siyasi dezenformasyon arasındaki ilişkiyi seçim süreçlerinde gösteren önemli örneklerden biri olarak karşımıza çıkmaktadır. 2016 Amerika Birleşik Devletleri (ABD) başkanlık seçimleri ve Brexit kampanyası sırasında, Cambridge Analytica'nın milyonlarca Facebook kullanıcısının kişisel verilerini izinsiz olarak topladığı ve bu bilgileri seçmen profili oluşturmak ve siyasi mesajlar iletmek için kullandığı tespit edildi. Bu skandal, eski şirket çalışanının firmanın bireylerin psikolojik kırılganlıklarını ve davranışsal eğilimlerini kullanmak üzere tasarlanmış algoritmalar geliştirdiğini ve bunun sonucunda kullanıcıları etkileyen büyük ölçekli veri gizliliği ihlallerine yol açtığını açıklamasıyla uluslararası gündemde dikkat çekmiştir. Bu olay ayrıca dijital veri analitiğinin ve algoritmik hedeflemenin modern siyasi kampanya stratejilerini nasıl şekillendirdiğini göstermiştir (Persily, 2017, s. 65-66).

Organize sosyal medya manipülasyonu faaliyetlerinde en öne çıkan örneklerden biri ise Rusya'nın ''troll fabrikası'' olarak bilinen İnternet Araştırma Ajansıdır (IRA) (McCombie, Uhlmann, & Morrison, 2020, s. 97-98). Rus siyasileri ve istihbarat yapıları ile bağlantılı olduğu iddia edilen bu yapının faaliyetleri, dijital ortamlarda gerçek kamuoyu katılımını

simüle etmek için tasarlanmış koordineli ve kurumsallaşmış yöntemlere dayanmaktadır. Çalışanların gerçek bir siyasi tartışma görünümü yaratmak için büyük miktarda çevrimiçi içerik ürettikleri, farklı aktörlerin kasıtlı olarak karşıt görüşleri benimseyerek bölücü anlatıları güçlendirdikleri ve kamuoyu algısını manipüle ettikleri tartışmalar arasında yer almaktadır. Ayrıca güvenilirlik ve meşruiyet oluşturmak için sahte hesapların uzun vadede geliştirildiği bilinmektedir (Aras, 2026, s. 168). Bu troll fabrikasının gelişmişliği özellikle 2016 ABD başkanlık seçimlerine Rus müdahalesine ilişkin soruşturmalar sırasında belirgin hale gelmiştir. Miller'in (2019) çalışmasına göre, IRA ile bağlantılı olduğu belirlenen 3.814 Twitter hesabından paylaşılan 200.000 tweet üzerinde araştırma yapılmıştır. Bu araştırma, Rus dezenformasyon kampanyalarına yerleştirilmiş manipülasyon stratejilerinin analiz edilmesini sağlamış ve çağdaş bilgi savaşında dijital propaganda ve algı yönetiminin stratejik kullanımını göstermiştir.

Görüldüğü üzere dezenformasyonun dijital altyapısı seçim güvenliğini yalnızca fiziksel sandık güvenliği olmaktan çıkarıp bilişsel ve algısal bir güvenlik meselesine dönüştürmüştür. Dijital dezenformasyon, seçmen davranışlarını manipüle etmek, siyasi rakipleri itibarsızlaştırmak ve demokratik süreçlere olan güveni sarsmak için sistematik bir silah olarak kullanılmaktadır. Bu tür operasyonların amacı, tek bir doğru oluşturmak veya bunu dayatmak değil, siyasi ve sosyal gerçeklikler konusunda belirsizlik, güvensizlik ve kutuplaşma yaratarak bilgi ortamının kendisinin istikrarsızlaştırılması olarak ifade edilebilir.

Dezenformasyonun Stratejik ve Diplomatik İşlevi

Diplomasinin Dönüşümü

Dijital çağda dezenformasyon, uluslararası ilişkilerde ve diplomaside stratejik bir silah ve hibrit savaşın temel unsurlarından biri haline gelmiştir. Geleneksel savaşların aksine günümüzde devletlere veya kurumlara zarar vermek için fiziksel sunucular veya sınır ötesi operasyonlardan ziyade toplumun yapısına, kurumların itibarına ve algılara zarar vermek yeterli olabilmektedir. Dezenformasyon ve diplomatik ilişkiler arasındaki bağlantının, bilginin stratejik bir silah olarak görülmesi ve devletlerin dış politika hedeflerine ulaşmak için siber alanı bir savaş alanı olarak kullanması zemininde şekillendiği söylenebilir. Bu noktada kamu diplomasisi, dijital diplomasi, siber diplomasi ve stratejik iletişim kavramları önemlidir.

Kamu diplomasisi, 1960'larda kitle iletişim teknolojilerinin gelişimi ve siyaset üzerindeki etkisiyle birlikte ayrı bir diplomasi yöntemi olarak ortaya çıkmıştır. Devletlerarası ilişkilerden farklı olarak kamu diplomasisi devletler ve toplumsal arasındaki iletişim süreçlerine ve toplumların kendi aralarındaki etkileşimlerine dayanmaktadır. Bu noktada kamu diplomasisi, devletlerin kitle iletişim araçlarıyla yabancı kamuoyunu etkilemelerini ve onlarla iletişim kurmalarını amaçladıkları stratejilerini ifade etmektedir (Ekşi, 2022a, s. 6). Bilgi ve iletişim teknolojilerinin hızlı gelişimi, kamu diplomasisinin yapısını, yöntemlerini ve kapsamını önemli ölçüde dönüştürmüştür. Dijitalleşme hızlanırken diplomatik uygulamalar da geleneksel iletişim kanallarının ötesine geçerek teknolojik gelişmeler ve değişen küresel siyasi dinamikler temelinde yeniden şekillenmeye devam etmiştir. Bu süreçte dijital diplomasi, siber diplomasi, sosyal medya diplomasisi gibi kavramlar ortaya çıkmıştır. Kavramsal farklılıklara rağmen bu yaklaşımlar temelde giderek birbirine daha fazla bağlanan dijital ortamlarda faaliyet gösteren kamu diplomasisinin çeşitli boyutlarını temsil ettiği söylenebilir (Ekşi, 2022b, s. 36-37).

Dijital diplomasi ve siber diplomasi kavramları birbirleri ile karıştırılsa da temelde ayrılırlar. Dijital diplomasi kavramı genel olarak diplomatik faaliyetlerin yürütülmesinde dijital teknolojilerin kullanımını ifade ederken siber diplomasi ise siber alanda ortaya çıkan sorunları ve çatışmaları ele almak için diplomatik mekanizmaların ve süreçlerin kullanımı ile ilgilidir (Riodan, 2016). Bu bağlamda dijital diplomasinin diplomatik uygulamaların dijitalleşmesine odaklandığı, siber diplomasinin ise öncelikle siber güvenlik ile ilgili siber alanda devletlerarası iş birliğine odaklandığı söylenebilir.

Modern dijital teknolojiler ve sosyal medya araçları uluslararası diplomaside yaygınlaşsa bile dijital diplomasi geleneksel diplomasinin bir alternatifi olarak görülemez (Alethawy, 2022, s. 82). Dijital diplomasi geleneksel diplomasinin yerini almaktan ziyada onun hedeflerini daha hızlı ve az maliyetli şekilde gerçekleştiren kullanışlı bir uzantısı ile tamamlayıcı olarak işlev görmektedir (Alethawy, 2022, s. 87).

Uluslararası ilişkilerde dijital diplomasinin gelişmesi, devletlerin dijital platformlar üzerinden eş zamanlı olarak diyalog halinde olmalarını sağlamaktadır. Bu sanal ortamda üretilen bilgilerin diplomasi üzerindeki etkisi sadece teknolojik bir gelişme olarak görülmemelidir. Bu durum aynı zamanda küresel olarak gücün nasıl kullanıldığının da bir dönüşümü olarak yorumlanmalıdır (Jabrailov, 2025, s. 718) Siber alanda gerçekleştirilen bu diplomasi süreci, siber alanın doğası gereği çeşitli riskleri de barındırmaktadır. Dijital diplomasinin

yaygınlaşması, hükümetlerin siber güvenlik politikalarını da doğrudan etkilemektedir. Hükümetlerin çevrimiçi ağlardaki resmi kurum verilerinin, diplomatların iletişim trafiğinin ve dijital varlıklarının güvenliği büyük bir zorunluluk olarak karşımıza çıkmaktadır. Bu doğrultuda devletlerin dijital diplomasinin yaratmış olduğu bu yeni etkileşim alanını korumak ve sağlıklı işleyebilmek için ulusal düzeyde savunma güçlerini arttırmaları gerekmektedir. Çünkü dijital diplomasi yoluyla geleneksel anlamda ulaşılamayan olumlu ve olumsuz gelişmeler uluslararası arenayı kolaylıkla etkileyebilmektedir.

Bu kolay etkileşim ve erişilebilirlik alanı, iletişim ve bilgi paylaşımı için sınırsız bir bilgi kirliliğine sebep olmaktadır. Böyle bir ortamda güvenilir kaynakların belirlenmesi ve gerçek bilgilerin yanlış bilgilerden ayırt edilmesi zorlaşmaktadır. Bu bağlamda sosyal medya yerleşik medya kurumlarının bilgi denetleme rolünü zayıflatmaktadır. Bireyler geniş kitlelere ulaşabilir ve yüksek etkileşimli içerikler sayesinde kamuoyunu şekillendirebilir. Bu bağlamda dezenformasyon, kullanılabilecek önemli bir güçtür. Geleneksel diplomasinin tıkandığı veya doğrudan askeri çatışmanın yapılmadığı durumlarda devletler bu geniş bilgi ağı içerisinde dezenformasyonu hibrit savaşın ve psikolojik operasyonların merkezine yerleştirebilir (Aras, 2026, s. 165-166). Dijital diplomasi, devletlerin dış politika hedefleri çerçevesinde uluslararası prestij kazanmak ve yumuşak güç oluşturmak için dijital kanalları kullanması olduğu için bu noktada dezenformasyon ise bu durumu tersine çevirerek aynı dijital kanalları yalan ve manipülatif bilgi yaymak için kullanmaktır. Bu bağlamda dezenformasyon yanlışlıkla yapılan bir hatadan ziyade rakipleri zayıflatmak ve uluslararası müzakereleri manipüle etmek için kasten tasarlanmış diplomatik bir silah olarak karşımıza çıkmaktadır (NextGen Diplomat, 2026). Bu bağlamda dijital diplomasi, sadece bir dış politika temelinde iletişim veya tanıtım aracı olarak değil, devletlerin bilgi operasyonları yapabildiği ve dezenformasyonu kolaylıkla yayabildiği bir alan olarak yorumlanabilir.

Dezenformasyon ve Diplomatik Meşruiyet Mücadeleleri

Dijital iletişim teknolojilerinin gelişimiyle uluslararası arenanın aktörleri kamuoyu algısını şekillendirmek ve siyasi sonuçları etkilemek için giderek daha fazla rekabet içerisine girerken bilgi ortamları jeopolitik çatışmaların da önemli bir alanı olarak ortaya çıkmıştır. Bu bağlamda dezenformasyon sadece yanlış bilginin yayılmasıyla sınırlı görülmemelidir. Aksine dezenformasyon siyasi meşruiyeti inşa etmek, güçlendirmek veya zayıflatmak için kullanılabilecek stratejik bir araçtır. Anlatıları çeşitli hedefler doğrultusunda şekillendirerek kamuoyunu etkilemek ve gerçeklik algılarını değiştirmek dezenformasyon faaliyetleri

kapsamında değerlendirilebilir. Bu bağlamda bilgi manipülasyonu, diplomatik meşruiyet sağlama, uluslararası güvenilirlik oluşturma ve siyasi etki üzerindeki mücadelelerle ilişkili görülebilir. Bu dinamik yapı, özellikle rekabet eden aktörlerin bilgi operasyonları yoluyla çıkarlarını sağlamaya çalıştıkları küresel çatışmalarda sıklıkla görülmektedir.

Bu noktada yakın dönemde gerçekleşmiş olan Rusya-Ukrayna savaşı, dezenformasyonun diplomatik ve siyasi meşruiyet aracı olarak nasıl kullanılabileceğini göstermektedir. Krizin ilk aşamalarında ABD Dışişleri Bakan Yardımcısı ile ABD Ukrayna Büyükelçisi arasındaki telefon görüşmesinin sosyal medya platformlarına sızdırılması olayı ile siber operasyonlar ve stratejik iletişim arasındaki ilişkinin önemi görülmüştür. Olay, savaş başlamadan önce Rusya'nın Batı'ya güvenilirliği zayıflatmayın amaçladığı ve iletişim ağlarına sızma yeteneklerinin göstermek istemesi olarak yorumlanmıştır (Lange-Ionatamishvili & Svetoka, 2015, s. 107).

Rusya-Ukrayna savaşı boyunca sosyal medya, Rus yanlısı stratejik anlatıların yayılması için önemli bir platform görevi görmüştür. Bu faaliyetler genelde Ukrayna yetkililerinin ve silahlı kuvvetlerinin davranışlarına yönelik olmuştur. Hedef kitleler arasında korku, kızgınlık ve güvensizliği artırmayı ve Ukrayna'nın uluslararası meşruiyetini de zayıflatmayı amaçladıkları iddia edilmektedir (Lange-Ionatamishvili & Svetoka, 2015, s. 108). Bu durum dezenformasyonun günümüz bilgi savaşlarında anlatı oluşturma ve diplomatik etki aracı olarak nasıl kullanılabildiğini göstermektedir.

Rusya-Ukrayna savaşı sırasında bilgi operasyonlarının en belirgin örneklerinden biri Ukrayna'nın Nazilerden kurtarılması anlatısının yayılması olmuştur. Bu anlatının tarihsel yorumlamaların ve siyasi gerçeklerin çarpıtılmasıyla oluşturulduğu ve Rusya'nın Ukrayna'ya yönelik saldırılarını meşrulaştırma amaçlı bir propaganda aracı olduğu iddia edilmiştir. Sosyal medya platformları aracılığıyla yayılan bu anlatılar hem yerel hem de uluslararası kitlelerin algılarını şekillendirmek için kullanılmıştır (Aras, 2026, s. 168).

Sosyal medyada dolaşıma sokulan ve Ukrayna Başkanı Zelensky'nin Ukraynalılara seslendiği video siber alanda gerçekleştirilen dezenformasyonun bir başka örneğidir. Bu videoda Zelensky'nin savaşta başarısız olduklarını ve askerlere silahlarını bırakıp teslim olmaları gerektiğini ilan ettiği görülmektedir. Bu video sonrasında Ukrayna hükümeti yetkilileri kısa süre içerisinde bu videonun deepfake teknolojisi kullanılarak yapılan sahte bir video olduğu,

sosyal medya üzerinden dezenformasyon amaçlı bilinçli bir şekilde dolaşıma sokulduğu ve bu konuda vatandaşları uyardıkları bir uyarı yayınladılar (Burgess, 2022).

Bir diğer önemli dezenformasyon faaliyeti ise biyolojik laboratuvar komplo teorisidir. Pyrra Technologies aslı siber güvenlik şirketi, sosyal medyada işgalden 10 gün önce bir kullanıcının Ukrayna'da ABD'ye ait biyolojik laboratuvar bulunduğunu belirten bir içerik paylaştığını ve bu içeriğin işgal gününden sonra aşırı sağcı sitelerde yüzlerce kez paylaşıldığını belirtmiştir. İşgal günü Twitter'da yine bu teorinin savunulduğu paylaşımlar yapılmıştır. Bunun üzerine Rus yanlısı web sitelerde bu anlatının baskın hale getirildiği belirtilmiştir (Collins & Collier, 2022). Rusya ise bu iddialar çerçevesinde, Ukrayna'nın ABD desteğiyle biyolojik silah laboratuvarına sahip olduğunu iddia ederek Birleşmiş Milletler Güvenlik Konseyi (BMGK)'nin toplanmasını talep etti. BM ve üye ülkeler bu iddiaların tamamen yalan olduğunu belirterek reddettiler. ABD BM Büyükelçisi Greenfield, Rusya'nın bu iddialarına hiçbir kanıt sunamadığını ve bu yalan iddiaların Rusya'nın Ukrayna işgali sırasında kimyasal ve biyolojik silahlar kullanmak için zemin hazırlamasına bir bahane olabileceğinden endişe duyduklarını vurguladı (Landay, Pamuk, & Lewis, 2022).

Yukarıda bahsedilen olaylar, Rusya'nın eylemlerini haklı çıkarma temelinde gerçekleştirdiği dezenformasyon faaliyetlerinden birkaçını göstermektedir. Savaş başlamadan önce Rusya'nın gizli dezenformasyon planları ve Ukrayna işgali için bir ''sahte bayrak operasyonu'' düzenleneceği ABD yetkilileri tarafından kamuoyuna açıklanmış ve Rusya'nın diplomatik alanda işgale gerekçe üretme sebebi engellenmeye çalışılmıştır (BBC, 2022). Fakat Rusya'nın işgalini meşru göstermek ve ABD ve Batı ülkelerinin Ukrayna'ya verdikleri desteği azaltmak için dezenformasyon faaliyetlerine devam ettiği görülmektedir.

BM'nin Mali'de yürüttüğü MINUSMA (Birleşmiş Milletler Mali Çok Boyutlu Entegre İstikrar Misyonu) barış misyonuna yönelik faaliyetler, BM tarafından önemli bir dezenformasyon kampanyası örneği olarak belirtilmiş ve bilgi savaşlarının uluslararası örgütlerin meşruiyetini ve operasyonel kapasitesini hedef alan dezenformasyon faaliyetlerinden biri olduğu vurgulanmıştır. BM'nin 2023 tarihli raporuna göre 2023 yılında Sevare'de gerçekleşen saldırıların ardından sosyal medyada MINUSMA karşıtı manipülatif içeriklerde artış olmuştur. Bu süreçte sosyal medya üzerinden yayılan sahte haberler BM barış misyonuna yönelik güvensizliği arttırmış ve BM personeline yönelik şiddet çağrıları içeren söylemler üretilmiştir. Raporda MINUSMA'nın bu içeriklere karşı sosyal medyada açıklamalar yayınladığı, yayılan yanlış bilgileri düzeltmeye çalıştığı ve şiddet çağrısı içeren

bir videonun kaldırılması için ilgili dijital platform şirketiyle iletişime geçildiği belirtilmiştir. Bu bağlamda BM, barış misyonunun yeniden yapılandırılması kapsamında bilgi operasyonları ve stratejik iletişim kapasitesinin güçlendirilmesini gündeme getirmiştir (UNSC, 2023, s. 7-11). MINUSMA örneği, dezenformasyonun yalnızca kamuoyu algısını etkileyen bir araç olmadığını, aynı zamanda uluslararası örgütlerin sahadaki operasyonel etkinliğini, meşruiyetini ve güvenliğini hedef alabilen bir tehdit aracı olarak kullanılabildiğini göstermektedir. Özellikle sosyal medya platformlarının çatışma alanlarında etki alanına dönüşmesi bilgi güvenliği ile fiziksel güvenlik arasındaki sınırların bulanıklaştığını ortaya koymaktadır.

Sonuç

Dijital iletişim teknolojilerinin hızlı gelişimi ve yayılımı bilginin üretimi, yayılımı ve tüketimini temelden dönüştürmüştür. Bu dönüşüm sürecinde bilgiye erişim kolaylaşmış ve küresel bağlantı güçlenmiş olsa da aynı zamanda bilgi ortamlarının manipülasyonu için de yeni alanlar yaratmıştır. Bu bağlamda bilginin dezenformasyonu iletişimle ilgili bir sorun olmaktan çıkıp siber güvenlik ve uluslararası ilişkiler alanlarında daha önemli bir sorun haline gelmiştir.

Bu çalışmada dezenformasyonun neden bir siber güvenlik tehdidi haline geldiği ve dijital çağda diplomatik süreçleri nasıl etkilediği incelenmiştir. Bulgular, sosyal medya platformlarının, algoritmik güçlendirme mekanizmalarının, veri analizinin ve yapay zekânın entegrasyonunun artmasıyla birlikte dezenformasyon faaliyetlerinin büyük bir ölçekte uygulanmasına olanak sağladığını göstermektedir. Bu noktada dezenformasyonun yalnızca bilgi bütünlüğünü değil aynı zamanda siyasi süreçleri, kamu güvenini ve kurumsal güvenilirlikleri etkileyen bir siber olgu haline geldiğini söylemek mümkündür.

Örneklerde görüldüğü üzere dezenformasyon hem bir güvenlik sorunu hem de stratejik bir araç olarak işlev görmektedir. 2016 ABD Başkanlık seçimleri ve Brexit referandumu örnekleri, dijital ortamda gerçekleştirilen bilgi manipülasyonlarının siyasi süreçleri ve kamuoyunu nasıl etkilediğini ortaya koymaktadır. Rusya-Ukrayna Savaşı ve MINUSMA örneği ise dezenformasyonun stratejik anlatıları şekillendirmek, siyasi meşruiyeti sorgulamak ve uluslararası algıları etkilemek için dijital ortamda kullanılabileceğini göstermektedir. Bu örnekler, jeopolitik rekabetlerin giderek geleneksel askeri ve ekonomik alanların ötesine genişlediğini ve bilgi ortamının alana dahil olduğunu göstermektedir.

Sonuç olarak dezenformasyon, siber güvenlik, stratejik iletişim ve diplomasi kesişiminde yer alan çok boyutlu bir olgu olarak karşımıza çıkmaktadır. Dijital bilgi ortamları siyasi rekabetin merkezi alanları haline geldikçe, bilgi bütünlüğünü koruma ve dezenformasyon faaliyetlerine verilen tepkiler hem ulusal güvenlik hem de uluslararası diplomatik uygulamalar açısından önemi artan bir güvenlik bileşeni oluşturmaya devam edecektir.

Kaynakça

Alethawy, M. (2022). Digital Diplomacy and Cybersecurity. *Ahi Evran Akademi*, 3(1), 82-90.

Aras, H. (2026). Dijital Diplomasiden Siber Saldırıya: Sosyal Medyanın Hibrit Savaş Stratejilerindeki Rolü. *Karadeniz Araştırmaları*, XXIII(89), 161-180.

Bērziņš, J. (2014). Russia's New Generation Warfare in Ukraine: Implications for Defense Policy. *The Journal of Military Operations*, 2(4), 4-7.

Baştan, Y., & Oran, F. Ç. (2024). Rus Dış Politikasında Siber Müdahale Yöntemi Olarak Dezenformasyon Operasyonları. *Yönetim Bilimleri Dergisi*, 22(53), 1205-1230.

BBC. (2022). Russia-Ukraine: US warns of 'false-flag' operation. 15 January, Retrieved from https://www.bbc.com/news/world-europe-59998988 (Accessed Time: 10 May 2026).

Blatny, J. M., & Søndergaard, S. (2025). Cognitive Warfare. NATO Science & Technology Organization. Retrieved from https://www.sto.nato.int/document/cognitive-warfare/ (Accessed Time: 03 May 2026.

Boevink, J., Mok, E., & M.Int, M. P. (2023, Mayıs). How Disinformation Might Hurt Your Business. Compact "Digital Trust: Cyber Security, Privacy & Ethics", Retrieved from https://www.compact.nl/articles/how-disinformation-might-hurt-your-business/ (Accessed Time: 07 April 2026).

Bone, J. (2018, Mart 5). Cognitive Hack: Trust, Deception and Blind Spots. Nisan 2026 tarihinde Corporate Compliance Insights. Retrieved from https://www.corporatecomplianceinsights.com/cognitive-hack-trust-deception-blind-spots/ (Accessed Time: 11 April 2026).

Burgess, S. (2022, Mart 17). Ukraine war: Deepfake video of Zelenskyy telling Ukrainians to 'lay down arms' debunked. Retrieved from https://news.sky.com/story/ukraine-war-deepfake-video-of-zelenskyy-telling-ukrainians-to-lay-down-arms-debunked-12567789 (Accessed Time: 05 May 2026).

Caramancion, K. M. (2020). An Exploration of Disinformation as a Cybersecurity Threat. 2020 3rd International Conference on Information and Computer Technologies (ICICT), (s. 440-444). San Jose, CA, USA. https://doi.org/10.1109/ICICT50521.2020.00076.

Caramancion, K. M., Li, Y., Dubois, E., & Jung, E. S. (2022). The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats. *Data,* 7(49), 1-18.

Chee, F. Y. (2022, Mart 2). EU bans RT, Sputnik over Ukraine disinformation. Retrieved From https://www.reuters.com/world/europe/eu-bans-rt-sputnik-banned-over-ukraine-disinformation-2022-03-02/ (Accessed Time: 05 May 2026).

Collins, B., & Collier, K. (2022, Mart 14). Russian propaganda on Ukraine's non-existent 'biolabs' boosted by U.S. far right. Retrieved from https://www.nbcnews.com/tech/internet/qanon-ukraine-biolabs-russian-propaganda-efforts-boosted-us-far-right-rcna19392 (Accessed Time: 05 May 2026).

EEAS. (2018, Haziran 13). A Europe that Protects: Countering Hybrid Threats. Retrieved from https://www.eeas.europa.eu/node/46393_en (Accessed Time: 10 May 2026)

Ekşi, M. (2022a). Kamu Diplomasisinde Post-Truth: Bir Meydan Okuma Olarak Dezenformasyon. *İletişim ve Diplomasi,* (9), 3-24.

Ekşi, M. (2022b). Dezenformasyon Çağında Kamu Diplomasisi. *Cihannüma* (11), 36-42.

Hsu, T. (2022, Aralık 28). As Covid-19 Continues to Spread, So Does Misinformation About It. Retrieved from https://www.nytimes.com/2022/12/28/technology/covid-misinformation-online.html (Accessed Time: 12 May 2026).

Jabrailov, M. (2025). Infoimperialism and Security: Cyberattacks, Disinformation, and State Defense Strategies. *Akademik Tarih ve Düşünce Dergisi*, 12(4), 713-724.

Jaiman, A. (2021, Ocak 30). Disinformation Is a Cybersecurity Threat. Retrieved from https://medium.com/swlh/disinformation-is-a-cybersecurity-threat-335681b15b48 (Accessed Time: 25 April 2026).

Krebs, B. (2016, Mayıs 18). As Scope of 2012 Breach Expands, LinkedIn to Again Reset Passwords for Some Users. Retrieved from https://krebsonsecurity.com/2016/05/as-scope-of-2012-breach-expands-linkedin-to-again-reset-passwords-for-some-users/ (Accessed Time: 24 April 2026).

Landay, J., Pamuk, H., & Lewis, S. (2022, Mart 11). U.N. says no evidence to back Russian claim of Ukraine biological weapons program. Retrieved from https://www.reuters.com/world/un-says-not-aware-any-biological-weapons-program-ukraine-2022-03-11/ (Accessed Time: 16 May 2026).

Lange-Ionatamishvili, E., & Svetoka, S. (2015). Strategic Communications and Social Media in the Russia-Ukraine Conflict. K. Geers içinde, Cyber War in Perspective: Russian Aggression against Ukraine (s. 103-111). Tallinn: NATO CCDCOE Publications.

Marangione, M. S. (2021). Words as Weapons: The 21st Century Information War. *Global Security and Intelligence Studies*, 6(1), 149-187.

McCombie, S., Uhlmann, A. J., & Morrison, S. (2020). The US 2016 presidential election & Russia's troll farms. *Intelligence and National Security*, 35(1), 95-114.

Miller, D. T. (2019). Topics and Emotions in Russian Twitter Propaganda. *First Monday*, 24(5). https://doi.org/10.5210/fm.v24i5.9638.

Milli İstihbarat Akademisi. (2026). Yapay Zekâ Çağında Siber Güvenlik ve Türkiye'nin Stratejik Öncelikleri. Ankara: *Millî İstihbarat Akademisi.* Retrieved from https://mia.edu.tr/uploads/f/24042026_1.pdf.

NextGen Diplomat. (2026, Mart 7). Disinformation Campaigns Countermeasures: Practical Guidance For Diplomats. Retrieved From https://blog.modeldiplomat.com/disinformation-campaigns-countermeasures (Accessed Time: 10 May 2026).

Nye, J. S. (2002). The Information Revolution and American Soft Power. *Asia-Pacific Review*, 9(1), 60-76.

Nye, J. S. (2019). Protecting Democracy in an Era of Cyber Information War. Cambridge: Belfer Center for Science and International Affairs. Retrieved from https://www.belfercenter.org/publication/protecting-democracy-era-cyber-information-war (Accessed Time: 10 April 2026).

Persily, N. (2017). Can Democraracy Survive The Internet?. *Journal of Democracy*, 28(2), 63-76.

Riodan, S. (2016, Mayıs 12). Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction. Retrieved from https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction (Accessed Time: 18 April 2026)

Talinshinsky, E. (2026). Bilgi Savaşının Teorik Temelleri ve Modern Uluslararası İlişkiler Sistemindeki Stratejik Rolü. *Akademik Tarih ve Düşünce Dergisi*, 13(3), 1-11.

U.S Senate Intel Committee. (2019, Ekim 8). Senate Intel Committee Releases Bipartisan Report on Russia's Use of Social Media. Retrieved from https://www.intelligence.senate.gov/2019/10/08/press-senate-intel-committee-releases-bipartisan-report-russia-e2-80-99s-use-social-media/ (Accessed Time: 13 April 2026).

UN. (2023, Temmuz). Our Common Agenda- Policy Brief 8: Information Integrity on Digital Platforms. Retrieved from https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrity-en.pdf (Accessed Time: 05 May 2026).

UNSC. (2023). S/2023/402 Situation in Mali Report of the Secretary-General. Retrieved from https://docs.un.org/en/s/2023/402 (Accessed Time: 10 May 2026).

Wardle, C., & Derakhshan, H. (2017). Informatıon Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Retrieved from https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (Accessed Time: 10 May 2026).

LEBANON'S STRATEGIC POSITION IN THE AGE OF AI-DRIVEN DEFENSE AND CYBERSECURITY

Sarkis KARAGUEZİAN[*]

ORCID ID: 0009 - 0008 - 7575 - 329X

Declaration[*]

Abstract

The application and integration of artificial intelligence (AI) and cybersecurity technologies are rapidly advancing within Lebanon's defense and national security sectors. This research investigates how AI can enhance Lebanese military capabilities, with particular emphasis on cyber defense functions and related operational applications. It assesses current and prospective uses of AI in the Lebanese military context, analyzing their strategic, operational, and institutional impacts. The study further examines how AI-powered systems affect military effectiveness, resilience, and threat reduction, identifying capability gaps and operational challenges in deploying these technologies within resource-limited and politically complex settings. Special focus is given to Lebanon's evolving cyber threat environment, marked by rising exposure to cyberattacks, hybrid threats, and asymmetric security risks. Additionally, the research evaluates the strategic importance of implementing AI-driven solutions in the Lebanese defense sector, while carefully considering ethical issues, governance needs, and institutional preparedness.

Keywords: Lebanon, Non-State Actors, Artificial Intelligence (AI), Cybersecurity, Military Strategy, National Security, Cyberattacks, Intelligence Gathering, Geopolitics of the Middle East, Counterterrorism

Introduction

In this analysis, the strategic impact of artificial intelligence (AI) on the defense system of the state of Lebanon is assessed. As one of the nations positioned at the center of the Middle East, Lebanon faces a variety of defense-related challenges triggered by its complex geopolitical position. Situated at the crossroads of regional power struggles, the country contends with a fragile internal security architecture while simultaneously navigating external pressures from

[*] PhD is affiliated with Haigazian University, Beirut, Lebanon. He is a university lecturer and Senior Policy Advisor at the International Center for Geopolitical and Economic Research (ICGER).

[*] The author acknowledges the use of artificial intelligence (AI)-assisted tools during the preparation of this manuscript for purposes including idea organisation, improving manuscript structure, language refinement, and proofreading. All intellectual contributions, theoretical analysis, arguments, and conclusions are the sole responsibility of the author.

state and non-state actors (Norton, 2014; Traboulsi, 2007). Its weak political system is compounded by possible dangers posed by hostile entities from outside its borders, rendering traditional defense paradigms increasingly insufficient. Under such conditions, turning towards more advanced defense system innovations is warranted with the intention of securing the state's sovereignty and territorial integrity (Harris, 2014).

The contemporary global security landscape has witnessed a profound transformation driven by the rapid advancement of artificial intelligence technologies. AI has gained increasing significance within state defense systems, cybersecurity frameworks, and intelligence processes, offering unprecedented capabilities in threat detection, predictive analytics, and autonomous decision-making (Horowitz, 2018; Geist, 2016). For nations like Lebanon, which operate within resource-constrained environments yet face asymmetric and multidimensional threats, AI represents both a critical opportunity and a strategic imperative. The integration of intelligent systems into national defense architectures promises to enhance situational awareness, streamline command and control structures, and fortify cyber resilience against an expanding threat landscape. However, realizing these benefits requires navigating complex technical, institutional, and geopolitical hurdles that are particularly acute in the Lebanese context.

This analysis aims to investigate the potential beneficial effect artificial intelligence is bound to have on military capabilities, cybersecurity, and intelligence processes within Lebanon's defense system (World Economic Forum, 2019). To achieve this objective, the research employs a qualitative methodological approach designed to capture the multifaceted nature of AI integration in a complex operational environment. The study synthesizes existing scholarship through a comprehensive literature review to establish a robust background on Lebanon's technological infrastructure and defense posture. This foundational understanding is complemented by primary data collection through interviews with military officials, cybersecurity professionals, and AI specialists, whose firsthand perspectives reveal both the practical opportunities and the systemic challenges of deploying AI in Lebanon's defense sector.

Historical Context of Lebanon's Defense Strategy

The defense system of Lebanon has been shaped by a history dotted with civil rifts, foreign incursions, and inter-regional conflicts. The impact of such influences still prevails and continues to shape the current defense and cybersecurity environment for the Lebanese. It is

important to explain the influence of artificial intelligence on the defense and security environment for the Lebanese by exploring the history underpinning the defense system of this particular state.

The Lebanese Civil War (1975–1990): Sectarian Fragmentation and the Erosion of State Monopoly on Violence

The Lebanese Civil War (1975–1990) represents a critical turning point in contemporary Lebanese history, marked by deep-seated internal conflict fueled by sectarian differences and sustained international interference. Groups including Lebanese Christians and Muslims, as well as Palestinians, vied for state power, while Syria, Israel, and Iran were among the international actors who made a significant impact on the trajectory of the conflict (Khalaf, 2002; Traboulsi, 2007; U.S. Department of Defense, 2025). The war fundamentally fractured Lebanon's institutional framework, dispersing armed authority across militias and non-state actors and establishing a pattern of fragmented sovereignty that persists in the country's defense architecture today. This historical legacy of divided loyalties and weakened state institutions continues to complicate efforts to build a unified, technologically advanced national defense system capable of integrating AI-driven capabilities.

The Israel-Lebanon Conflict: Persistent Asymmetric Warfare and the Struggle for Sovereign Defense

The close geographical proximity between Israel and Lebanon has contributed to several clashes between the two nations; however, the most consequential modern conflict was the 2006 Lebanon War between Israel and Hezbollah. During this conflict, significant harm was inflicted on Lebanese military infrastructure and civilian assets alike, with over 1,100 Lebanese civilians and combatants killed and approximately one million people displaced (Britannica, 2024; Matthews, 2011). Despite the passage of nearly two decades, the threat posed by both Hezbollah's military posture and Israel's periodic military operations continues to undermine Lebanese sovereignty, while the chronic lack of development and modernization within the Lebanese Armed Forces leaves the state perpetually vulnerable (Harris, 2014; Norton, 2014).

This ongoing asymmetry wherein non-state actors possess more advanced military capabilities than the national army creates a uniquely challenging environment for AI integration, as defense modernization must navigate internal political sensitivities while

addressing external security gaps. The 2024 conflict between Israel and Hezbollah introduced a new dimension to this asymmetric relationship: the deployment of advanced AI-driven targeting systems by Israel. Israeli forces utilized an AI tool named "Habsora" (The Gospel) to maintain a comprehensive "target bank" cataloguing Hezbollah operatives, their locations, and routines, enabling rapid and precise strikes that decapitated much of Hezbollah's leadership (Jerusalem Post, 2026; Arab Center Washington DC, 2025).

Regional Instability and the Syrian Civil War: Spillover Effects on Lebanese Security and Cyber Vulnerability

For Lebanon, the Syrian Civil War has intensified the complex threat environment within which its defense institutions must operate. The Syrian conflict has posed multidimensional threats to the Lebanese state, including a massive refugee crisis, cross-border militant activity, and the risk of direct military escalation. In this context, the Lebanese Army operates under conditions whereby non-state groups and jihadist militias represent as significant a threat as state-based adversaries (Salem, 2017; European Parliament, 2017). The conflict has further eroded the state's capacity to maintain territorial control and has strained an already burdened security apparatus.

The Syrian civil war has equally impacted the cyber capacity and vulnerability of the Lebanese state. As the Syrian government is known to be engaged in cyber activities and information operations within the broader Middle East context, Lebanon is exposed to heightened risks of state-sponsored cyberattacks relative to other states in the region (CSS ETH Zurich, 2017). In this regard, the adoption of artificial intelligence by the Lebanese state can be viewed as a necessary preemptive measure to secure the Lebanese cyber environment and detect sophisticated intrusion attempts before they compromise critical national infrastructure.

Lebanon's Security Landscape: Non-State Actors, Asymmetric Warfare, and Cyber Vulnerabilities

The Lebanese state is threatened by multiple non-state actors, including Palestinian factions, jihadist groups such as ISIS and Al-Qaeda, which operates as both a political party and an armed militia with capabilities exceeding those of the national army (Norton, 2014; U.S. Department of State, 2021). This fragmentation of armed authority has compelled the Lebanese Armed Forces (LAF) to adopt unconventional combat tactics, including guerrilla

and cyber warfare, while navigating a political environment where external patrons principally Iran for Hezbollah, and the United States and France for the LAF compete for influence (Harris, 2014; Salem, 2017).

Adding to these conventional security challenges is Lebanon's increased vulnerability to cyber threats. The state is susceptible to various cyber threats such as state-sponsored espionage activities and cyber terrorism, correlating with the growing reliance on cyberspace for state and military activities (CSS ETH Zurich, 2017; Singer & Brooking, 2018). Israeli and Syrian cyber activities have targeted Lebanese communication networks and military infrastructure during periods of high tension, while cyber-criminal gangs have increasingly targeted Lebanese banks and governmental entities (CSS ETH Zurich, 2017; CSS ETH Zurich, 2020). These vulnerabilities highlight the need for a proactive and comprehensive approach to cybersecurity that leverages artificial intelligence to bolster preparedness and response capabilities.

The Lebanese Armed Forces and Cybersecurity Infrastructure

The Lebanese Armed Forces (LAF) have faced persistent difficulties regarding resources and weaponry, yet have made significant advancements in force structure and operational capabilities, particularly in response to the Syrian Civil War and the 2006 Israel-Hezbollah War (Harris, 2014; Salem, 2017). France and the United States have been at the forefront of assisting Lebanese military strength, with the U.S. continuing to provide advanced military platforms, equipment, and training (U.S. Department of State, 2021; Lebanese Armed Forces, 2025). However, the LAF's ability to secure the state independently remains contested due to the significant role that non-state actors play, which maintains de facto military autonomy (Norton, 2014; The Public Source, 2026).

In the cyber domain, Lebanon has taken incremental steps toward institutionalizing cybersecurity governance. The establishment of the National Cyber Security Center in 2017 was followed by the adoption of a comprehensive National Cyber Security Strategy in November 2024, which proposes eight strategic pillars: defending against cyber threats; developing international cooperation; enhancing state ICT capacities; promoting cybersecurity education; strengthening industrial and technical capabilities; supporting Lebanese cybersecurity companies; fostering public-private collaboration; and reinforcing law enforcement and intelligence agency roles (National Cybersecurity Committee, 2024). The strategy mandates the creation of the National Cyber Security and Information System

Agency (NCSIA) as a centralized coordinating body. However, the Lebanese cyber defense system still faces significant challenges, including a lack of expert personnel, outdated infrastructure, and inadequate funding, creating a gap between strategic ambition and operational reality (UNESCWA, 2020; Factosecure, 2025).

AI Applications in Lebanon's Defense and Security Sector

Military Operations

The application of artificial intelligence within a military context offers several potential benefits for the Lebanese government. AI can be implemented in intelligence collection, autonomous surveillance, predictive analysis, and military decision support. AI-powered drones and robotic platforms may be employed by the Lebanese Armed Forces for surveillance and precision targeting, limiting collateral damage and enhancing operational efficiency (Horowitz, 2018; Boulanin & Verbruggen, 2017). Machine learning and image recognition can process vast quantities of satellite imagery and signals intelligence for real-time anomaly detection, providing vital information on activities and potential threats from non-state actors such as Palestinian groups and jihadists (Geist, 2016; Horowitz, 2018).

The 2024 Israel-Hezbollah conflict demonstrated the transformative potential of AI-augmented surveillance. Israel deployed high-altitude drones that orbited the border continuously, monitoring cell signals, tracking vehicles, and transmitting data to intelligence systems in real time, creating what analysts described as a "testing ground for remote territorial control" (Peoples World, 2025). For Lebanon, developing comparable capabilities scaled to its resources could provide early warning of cross-border threats without requiring massive troop deployments.

Cyber Defense

In the field of cybersecurity, artificial intelligence is poised to be a game-changer for the Lebanese state. AI-powered intrusion detection solutions can identify unusual behavior on government and military networks, while machine-learning algorithms can examine network traffic to detect malicious attacks such as Denial-of-Service (DoS) and phishing before they cause pervasive network disruptions (Palo Alto Networks, n.d.; Syracuse University, 2025). Natural language processing (NLP) technologies can monitor social media platforms and online forums to detect threat indicators, allowing anticipatory measures against cyber threats that may also cause physical harm (Singer & Brooking, 2018).

The application of AI-based cybersecurity solutions can help defend Lebanon's government, financial infrastructure, and military networks from advanced cyberattacks. In light of the region's tendency to fall victim to proxy cyberwars, especially those involving state-sponsored cyberattacks, the ability to identify and eliminate cyber threats in real time is critical for Lebanese national security (CSS ETH Zurich, 2020).

Intelligence Processes

AI-driven predictive analytics can transform Lebanon's approach to threat assessment by analyzing patterns from multiple data sources including satellite imagery, communications intercepts, social media monitoring, and historical conflict data to anticipate potential security incidents before they materialize (Singer & Brooking, 2018). Social network analysis using machine learning algorithms can identify the structure and key nodes of terrorist and criminal organizations operating within Lebanon, supporting targeted counterterrorism operations while minimizing collateral impact on civilian populations.

Ethical and Legal Considerations

Despite the apparent benefits of artificial intelligence in military and cyber defense scenarios, there is a vital need for the Lebanese state to examine the ethical and legal repercussions of deploying such technologies. The reliance on autonomous machines for strategic defense decision-making raises concerns regarding accountability and human control (Heyns, 2016; Sharkey, 2018). AI systems can perpetuate and amplify existing biases present in training data, potentially leading to discriminatory outcomes in security operations (Etzioni & Etzioni, 2017). Ensuring accountability for decisions made or informed by AI systems presents significant challenges, particularly when algorithmic reasoning is opaque even to system operators.

A clear ethical framework for the use of AI in military and cyber operations should be created and implemented by the Lebanese state, including transparency within decision-making processes and ensuring that human review is maintained as a core element within AI deployment (Floridi et al., 2018). Lebanon should bring its AI policy into alignment with international norms and principles on humanitarian law, ensuring that AI-based technologies are used responsibly, do not impact the rights of civilians, and do not increase the potential for conflict (ICRC, 2020). Active participation in international forums on AI regulation for military use, such as the UN Convention on Certain Conventional Weapons (CCW) Group of

Experts on Lethal Autonomous Weapons Systems, would further strengthen Lebanon's ethical posture (Heyns, 2016).

Recommendations for Lebanon's Future Defense Strategy

For greater benefit and risk reduction with the application of artificial intelligence, this research proposes the following recommendations tailored specifically to the Lebanese context:

1. Develop a Dedicated National AI Defense Strategy

While the National Cyber Security Strategy (2024) provides a foundation, Lebanon needs a dedicated strategy for AI integration in defense that coordinates efforts across military, intelligence, and civilian cybersecurity domains. This strategy should explicitly address how to enhance state capabilities without triggering destabilizing responses from non-state actors and should prioritize non-lethal applications (surveillance, cyber defense, predictive analytics) in the initial phase to build institutional confidence and capability.

2. Leverage Educational Assets for Human Capital Development

Rather than relying on expensive foreign consultants, Lebanon should mobilize its existing academic infrastructure AUB, LAU, CNRS-L, and the BDD ecosystem to train LAF personnel in AI fundamentals, data science, and cybersecurity. The Google AI grant to AUB demonstrates that such partnerships are feasible. A "train-the-trainer" model, where Lebanese academics train military officers who then train their subordinates, would maximize impact while minimizing cost and external dependency.

3. Direct International Assistance Toward AI-Enabled Priorities

The $117 million in expanded U.S. security assistance announced in January 2025, and the approximately $496 million in total FY2024 aid, should be strategically directed to include AI-enabled capabilities. Specifically, donor funds should support: (a) AI-driven border surveillance pilots along the Syrian frontier; (b) machine-learning-based cyber threat detection systems for critical infrastructure; and (c) predictive analytics tools for counterterrorism operations. Donors should condition assistance on transparent governance frameworks to prevent misuse for domestic repression.

4. Establish Ethical and Legal Safeguards Before Deployment

Lebanon must enact comprehensive data protection legislation and establish ethical guidelines for AI use in security applications before deploying systems operationally. These frameworks should mandate meaningful human control over lethal decisions, require algorithmic auditing for bias, and create independent oversight mechanisms. Lebanon should actively participate in the UN CCW Group of Experts on Lethal Autonomous Weapons Systems to align its policies with emerging international norms.

5. Build Domestic Cybersecurity Industry Through Public-Private Partnerships

The National Cyber Security Strategy's call for supporting domestic cybersecurity companies should be operationalized through government contracts, tax incentives, and research grants. Lebanese firms such as CME Cybersecurity, LIRIS, and others already possess baseline capabilities that could be scaled with modest investment. A domestic industry reduces dependency on foreign suppliers mitigating supply chain risks demonstrated by the 2024 pager attacks while retaining technical talent that would otherwise emigrate.

6. Address Infrastructure Barriers as a Security Priority

Electricity and internet connectivity are not merely economic development issues but fundamental enablers of AI defense capabilities. Lebanon should treat infrastructure rehabilitation as a national security priority, exploring innovative solutions such as solar-powered computing centers for military installations and satellite internet connectivity for rural border posts. International assistance programs should explicitly include infrastructure components, recognizing that advanced AI systems are useless without reliable power and data transmission.

Conclusion

The defense system of Lebanon is beset by a peculiar set of circumstances, ranging from the dynamic interplay between state and non-state entities to the escalating threat of cyberattacks and AI-enabled asymmetric warfare (Harris, 2014; Norton, 2014). The 2024 Israel-Hezbollah conflict demonstrated that AI is no longer a future prospect but an operational reality reshaping the regional security landscape. For Lebanon, artificial intelligence represents both an urgent necessity and a formidable challenge.

The question is not whether Lebanon can afford to integrate AI into its defense architecture, but whether it can afford not to, particularly when its adversaries are already weaponizing AI capabilities that may soon render conventional defenses obsolete. Lebanon possesses underappreciated assets for this transformation: a robust higher education sector with dedicated AI programs, a nascent private cybersecurity industry, and a newly adopted National Cyber Security Strategy that provides institutional foundation. However, realizing these benefits requires navigating severe economic constraints, infrastructural deficiencies, political fragmentation, and the unique complications posed by Hezbollah's parallel military capacity.

The path forward requires neither technological determinism nor institutional fatalism, but a pragmatic, phased approach that leverages Lebanon's existing assets, addresses its structural constraints, and maintains the ethical and legal standards befitting a state committed to international humanitarian law and human rights. With the proper policies and investments, the Lebanese state has the potential to increase national security and defense power within the context of a complex threat environment.

References

Arab Center Washington DC. (2025). The impact of Israeli cyber operations on Hezbollah. Retrieved from https://arabcenterdc.org/resource/the-impact-of-israeli-cyber-operations-on-hezbollah (Accessed Time: 18 February 2026)

Atlas of Urban Tech. (2022, April 7). Beirut Digital District. Retrieved from https://atlasofurbantech.org/cases/lbn-beirut-bdd (Accessed Time: 20 January 2026)

Boulanin, V., & Verbruggen, M. (2017). Mapping the development of autonomy in weapon systems. Stockholm International Peace Research Institute (SIPRI). Retrieved from https://www.sipri.org/publications/2017/sipri-background-papers/mapping-development-autonomy-weapon-systems (Accessed Time: 25 January 2026).

Britannica. (2024). 2006 Lebanon War. Encyclopaedia Britannica. Retrieved from https://www.britannica.com/event/2006-Lebanon-War (Accessed Time: 12 February 2026)

CSS ETH Zurich. (2017). Cyber activities in the Syrian conflict. Center for Security Studies. Retrieved from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities studies/pdfs/Cyber-Reports-2017-05.pdf (Accessed Time: 08 March 2026)

CSS ETH Zurich. (2020). Israel's national cybersecurity and cyberdefense posture. Center for Security Studies. Retrieved from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf (Accessed Time: 08 March 2026)

Elgar Online. (2026). Artificial intelligence in contemporary conflicts and the future of military law. In Research Handbook on Artificial Intelligence and International Law. Edward Elgar Publishing. Retrieved from https://www.elgaronline.com/edcollchapoa/book/9781035353507/chapter9.xml (Accessed Time: 15 June 2026)

Etzioni, A., & Etzioni, O. (2017). Incorporating ethics into artificial intelligence. *The Journal of Ethics*, 21(4), 403–418.

European Parliament. (2017). Syrian crisis: Impact on Lebanon. European Parliamentary Research Service. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599379/EPRS_BRI(2017)599379_EN.pdf (Accessed Time: 30 January 2026)

Factosecure. (2025, June 11). Top 10 cybersecurity companies in Lebanon. Retrieved from https://factosecure.com/top-10-cybersecurity-companies-in-lebanon/ (Accessed Time: 20 June 2026)

Floridi, L., Cowls, J., Taddeo, M., & van Wynsberghe, A. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines,* 28, 689–707.

Geist, E. (2016). It's already too late to stop the AI arms race. *Bulletin of the Atomic Scientists*, 72(5), 318–321.

Harris, W. (2014). *The Levant: A Land of Conflict*. Routledge.

Heyns, C. (2016). Autonomous weapons in armed conflict and human rights law. UN Human Rights Council, A/HRC/32/L.36.

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, 1(3), 36–57.

ICRC. (2020). *Artificial intelligence and autonomous weapons: Ethical and legal challenges*. International Committee of the Red Cross.

Jerusalem Post. (2026, May 10). Inside Israel's AI targeting system: How data from a phone becomes a death sentence. Retrieved from https://www.jpost.com/defense-and-tech/article-895697 (Accessed: 18 May 2026)

Khalaf, S. (2002). *Civil and uncivil violence in Lebanon: A history of the internationalization of communal conflict*. Columbia University Press: New York.

Lebanese Armed Forces. (2025). Army capabilities development plan (CDP) 2023–2027. Retrieved from https://www.lebarmy.gov.lb/en/content/army-capabilities-development (Accessed: 20 April 2026)

Matthews, M. M. (2011). *We were caught unprepared: The 2006 Hezbollah-Israeli war*. Long War Series, Occasion Paper 26. U.S. Army Combined Arms Center.

MDPI. (2026, March 6). Governing artificial intelligence for sustainable territorial development in fragile contexts: Insights from North Lebanon. *Administrative Sciences*, 16(3), 130.

National Cybersecurity Committee. (2024). Lebanon national cyber security strategy. Retrieved from https://dig.watch/resource/lebanon-national-cyber-security-strategy (Accessed Time: 22 January 2026)

Norton, A. R. (2014). *Hezbollah: A short history* (3rd ed.). Princeton University Press.

Palo Alto Networks. (n.d.). What is the role of AI in threat detection? Cyberpedia. Retrieved from https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection (Accessed Time: 05 April 2026)

Peoples World. (2025, November 12). Israel turns Lebanon into testing ground for high-tech 'remote occupation' tools. Retrieved from https://peoplesworld.org/article/israel-turns-lebanon-into-testing-ground-for-high-tech-remote-occupation-tools/ (Accessed Time: 02 July 2026)

Salem, P. (2017). The Syrian conflict and its impact on Lebanon. Carnegie Middle East Center. Retrieved from https://carnegie-mec.org/2017/04/06/syrian-conflict-and-its-impact-on-lebanon-pub-68617 (Accessed Time: 08 February 2026)

Sharkey, N. (2018). *Meaningful human control and autonomous weapons*. Working paper prepared for the CCW Group of Experts Meeting, Geneva.

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt.

Syracuse University. (2025). AI in cybersecurity: How AI is changing threat defense. School of Information Studies. Retrieved from https://ischool.syracuse.edu/ai-in-cybersecurity/ (Accessed Time: 22 June 2026)

The Public Source. (2026). Sovereignty without defense: The army, the state, and Hezbollah's weapons. Retrieved from https://thepublicsource.org/lebanese-army-hezbollah-sovereignty (Accessed Time: 08 July 2026)

Traboulsi, F. (2007). *A history of modern Lebanon*. Pluto Press.

U.S. Department of Defense. (2025, April 7). Lebanese Civil War 1975–90. Defense Technical Information Center. Retrieved from https://media.defense.gov/2025/Apr/07/2003683785/-1/1/0/20250407_LEBANESECIVILWAR_1975-90_FINAL.PDF (Accessed Time: 18 April 2026)

U.S. Department of State. (2021). Country Reports on Terrorism 2020: Lebanon. Retrieved from https://2021-2025.state.gov/reports/country-reports-on-terrorism-2020/lebanon/ (Accessed Time: 28 January 2026)

UNESCWA. (2020). Advisory report on the development of an artificial intelligence strategy for Lebanon. United Nations Economic and Social Commission for Western Asia. Retrieved from https://www.unescwa.org/sites/default/files/event/materials/advisory-report-development-artificial-intelligence-strategy-lebanon-en.pdf (Accessed Time: 14 February 2026)

World Economic Forum. (2019). Artificial intelligence in the Middle East. Retrieved from https://www.weforum.org/reports/artificial-intelligence-in-the-middle-east/ (Accessed Time: 12 January 2026)

GIDA REJİMİ VE DİJİTALLEŞME: TEKNOLOJİK ÖRGÜTLENMEYE YAPISAL BİR YAKLAŞIM

Salim Bülent YÜKSEL[*]
ORCID ID: 0009-0006-5492-1501

Declaration[*]

Özet

Bu makale, dijitalleşme ile gıda rejimleri arasındaki ilişkiyi tarihsel ve ilişkisel bir çerçevede yeniden değerlendirmektedir. Gıda rejimi yaklaşımı, tarımsal üretim ve gıda dolaşımını belirli sermaye birikimi biçimleri, devletler sistemi, uluslararası iş bölümü ve sınıfsal güç ilişkileri ile bağlantılı olarak inceler. Öte yandan dijital teknolojilerin tarım-gıda sisteminde yaygınlaşması, üretimden dolaşıma, finansmandan perakendeye kadar gıda zincirinin farklı aşamalarını yeniden düzenlemektedir. Bununla birlikte, dijital tarım literatürü çoğunlukla teknik yeniliklerin kullanım alanlarını sıralayan betimleyici bir yaklaşımla teknolojilerin toplumsal etkilerine odaklanırken, gıda rejimi yaklaşımında teknolojik örgütlenmenin yapısal konumu yeterince açıklığa kavuşturulmamıştır. Bu çalışma, söz konusu iki literatür arasında Althusserci yapısal nedensellik anlayışından hareketle sistematik bir kuramsal bağlantı kurmayı amaçlamaktadır. Gıda rejimi, çeşitli ve özerk düzeylerin tarihsel olarak özgül eklemlenmesinde var olan çelişkili bir temel birlik olarak ele alınmaktadır. Teknolojik örgütlenme ekonomik düzey içinde üretim, dolaşım, vb. gibi görece özgül eklemlenen bölgelerden biri olarak tanımlanmıştır. Bu çerçevede dijitalleşme, şirketleşmiş gıda rejimine dışarıdan eklenen özerk bir teknoloji olarak değil, teknolojik örgütlenme bölgesinin veri, platform ve algoritmik sistemler temelinde farklılaşan tarihsel bir alt bölgesi olarak kavramsallaştırılacaktır. Dijitalleşme verileştirme, platformlaşma ve algoritmik yönetişim olmak üzere birbiriyle bağlantılı üç süreç/unsur üzerinden yapılandırılmıştır. Çalışmanın temel savı, dijitalleşme, şirketleşmiş gıda rejimine dışarıdan eklenen özerk bir teknoloji değil; ekonomik düzey içerisindeki teknolojik örgütlenme bölgesinin veri, platform ve algoritmik sistemler temelinde farklılaşan, rejim tarafından belirlenirken ekonomik ilişkilerin maddi işleyişini koşullandıran tarihsel alt bölgesidir. Burada simetrik bir karşılıklı belirlenim değil;

[*] PhD. Candidate, Ankara University Institute of Social Sciences, sbulentyuksel@gmail.com
[*] In this study, artificial intelligence (AI) was used solely for the purpose of improving language and expression. The author is solely responsible for all scientific content and ultimate aspects of this study.

yapı, düzey ve bölge bağlantısı üzerinden her yapılaşmanın terimlerinde içkin olarak var olduğu metonimik bir ilişki söz konusudur.

Anahtar kelimeler: Gıda sosyolojisi, Teknoloji sosyolojisi, Gıda rejimi, Dijital tarım, Şirketleşmiş gıda rejimi, Teknolojik örgütlenme, Verileştirme, Platformlaşma, Algoritmik yönetişim, Yapısal nedensellik

Abstract

This article re-evaluates the relationship between digitalization and food regimes within a historical and relational framework. The food regime approach examines agricultural production and food circulation in relation to particular forms of capital accumulation, the interstate system, the international division of labour, and class power relations. Meanwhile, the proliferation of digital technologies throughout the agri-food system is reorganizing different stages of the food chain, from production and circulation to finance and retail. Nevertheless, while the literature on digital agriculture generally adopts a descriptive approach that catalogues the fields of application of technological innovations and focuses on their social consequences, the structural position of technological organization within the food regime approach has not been sufficiently clarified.

Drawing on the Althusserian conception of structural causality, this study aims to establish a systematic theoretical connection between these two bodies of literature. The food regime is conceptualized as a contradictory fundamental unity that exists through the historically specific articulation of multiple, relatively autonomous levels. Technological organization is defined as one of the relatively specific and articulated regions within the economic level, alongside production, circulation, and other such regions. Within this framework, digitalization is conceptualized not as an autonomous technology externally added to the corporate food regime, but as a historically differentiated subregion of the region of technological organization, structured around data, platforms, and algorithmic systems.

Digitalization is analysed through three interconnected processes or elements: datafication, platformization, and algorithmic governance. The central argument of the study is that digitalization is not an autonomous technology externally added to the corporate food regime; rather, it constitutes a historical subregion of technological organization within the economic level, differentiated on the basis of data, platforms, and algorithmic systems. While it is determined by the regime, it simultaneously conditions the material operation of economic

relations. What is at stake here is not a symmetrical form of mutual determination, but a metonymic relation established through the connection between structure, level, and region, in which the structure exists immanently within its constituent terms.

Keywords: Sociology of food, Sociology of technology, Food regime, Digital agriculture, Corporate food regime, Technological organization, Datafication, Platformization, Algorithmic governance, Structural causality

Giriş

1980'li yılların sonlarından itibaren Harriet Friedmann ve Philip McMichael tarafından geliştirilen gıda rejimi kavramsallaştırması, sermayenin tarımsal ilişkileri şekillendirmesine ve aynı zamanda emeğin tarımsal üretim süreçlerine getirdiği açıklamalarla tarımı ve tarım bağlamında gıda sorunlarını ele almak için verimli bir analitik çerçeve sunar. Kurucu makalelerinde Friedmann ve McMichael (1989, ss. 93–117), tarımı yalnızca kırsal üretimin konusu olarak değil, kapitalizmin tarihsel gelişiminin kurucu bileşenlerinden biri olarak ele alır. Tarım ve gıda sistemlerini yalnızca üretim teknikleri veya tarım politikaları üzerinden değil, kapitalist dünya ekonomisinin tarihsel örgütlenmesi içinde analiz eden bu kuramsal çerçevenin temel varsayımı, belirli tarihsel dönemlerde tarımsal üretim, ticaret, tüketim, devlet politikaları ve uluslararası güç ilişkileri arasında görece istikrarlı bir bütünlük oluştuğudur; bu bütünlüğün ise kapitalist sermaye birikiminin özgül biçimlerini mümkün kıldığıdır. Makalede detaylandırılan gıda rejimleri yaklaşımına göre benimsenen kapitalist birikim biçimine bağlı olarak farklı dönemlerde farklı gıda rejimlerinin tesisi suretiyle tarım ve gıda üretiminin küresel ölçekte şekillendiğini savunulmaktadır. (Friedmann & McMichael, 1989).

Son yıllarda tarım-gıda sisteminde yaşanan dönüşüm ise bu yaklaşım açısından yeni kuramsal sorular ortaya çıkarmıştır. Zira teknolojik gelişmelerin (ve bu dolayımda dijitalleşmenin) yarattığı bu dönüşümün etkileri; tarımsal üretim, dolaşım ve yönetişim üzerinde giderek daha görünür hale gelmektedir. Dijital teknolojilerin tarım ve gıda alanında giderek yaygınlaşması, üretim süreçlerinden ürünlerin işlenmesine, finansmandan lojistiğe, perakendeden tüketici davranışlarının izlenmesine kadar gıda zincirinin farklı aşamalarını yeniden düzenlemektedir. Bu dönüşüm yalnızca yeni teknik araçların kullanıma girmesiyle sınırlı değildir; bilgi üretiminin, ekonomik koordinasyonun, karar alma süreçlerinin ve aktörler arasındaki güç ilişkilerinin yeni teknolojik örgütlenmeler aracılığıyla yeniden yapılandırılmasını da içermektedir. Dijitalleşmenin ekonomi-politik ilişkiler içerisindeki konumunun açıklığa

kavuşturulabilmesi için, dijital tarım literatürü ile gıda rejimi yaklaşımı arasında sistematik bir kuramsal bağlam kurulması gerekmektedir.

Bu bağlama dönük bağlantılar gıda ve tarıma dair sosyolojik literatürün içinde yok değildir. Örneğin gıda rejimi literatürü içinde Prause, Hackfort ve Lindgren (2021), gıda rejimi yaklaşımını doğrudan teorik çerçeve olarak alır ve dijitalleşmeyi yalnızca çiftlik düzeyinde kullanılan yeni bir üretim tekniği olarak değil, üçüncü gıda rejiminin bütün meta zincirini yeniden örgütleyen bir dönüşüm olarak değerlendirir. Yeni dijital teknolojilerin üçüncü gıda rejimi içindeki rolünün henüz yeterince incelenmediğini savundukları makalelerinde Prause ve diğerleri gıda rejimi literatürünün bilgi ve iletişim teknolojilerinin önemini genel olarak kabul ettiğini ifade eder.

Öte yandan dijital tarım literatürü çerçevesinde üretilen çalışmalar da söz konusu bağlam çerçevesinde belli katkılar üretmiştir. Dijital teknolojilerin tarımsal üretimin sınırlarını aşarak bütün gıda tedarik zincirinin örgütlenmesine müdahale ettiğini gösteren Wolfert, Verdouw ve Bogaardt (2017) bu dolayımda teknoloji ile güç ilişkileri arasındaki bağlantıyı ortaya serer. Analizlerinden çıkan sonuca göre büyük veri uygulamaları, yalnızca verimlilik ve karar desteği sağlayan teknik araçlar değildir. Bunun ötesinde bu uygulamalar, veri mülkiyetinin, iş modellerinin, karar haklarının ve zincirdeki aktörler arasındaki güç dağılımının biçimlenmesinde önemli bir rol oynamaktadır. Tarımın dijitalleşmesi teknik bilimlerde geniş biçimde incelenmesine rağmen bu konudaki sosyal bilim çalışmalarının dağınık kaldığını belirten Klerkx, Jakku ve Labarthe (2019), dijital tarım, akıllı tarım ve Tarım 4.0 hakkındaki sosyal bilim literatürünü sınıflandırmaktadır. Yazarlar, "dijital gıda rejimleri" kavramsallaştırmasını kullanmakta ve dijitalleşmenin ortaya çıkardığı güç ilişkilerinin politik ekonomi, politik ekoloji, toplumsal hareketler ve pratik kuramı gibi yaklaşımlarla incelenebileceğini ileri sürmektedir. Makale bu bağlamda Burch ve Lawrence'ın (2009) üçüncü gıda rejimi tartışmasına ve McMichael'ın kurumsal gıda rejimi çalışmasına doğrudan göndermede bulunur (2019, s.10). Eleştirel veri çalışmalarıyla gıda çalışmalarını bir araya getiren bir araştırma gündemi sundukları makalelerinde Bronson ve Knezevic ise, tarım ve gıda alanındaki büyük veri uygulamalarının gıda sistemindeki güç ilişkileri, veri mülkiyeti, çiftçi özerkliği ve egemen tarım modeli üzerindeki maddi sonuçlarına dikkat çekerler. Büyük verinin tarım ve gıda alanındaki etkilerinin, yalnızca teknolojinin kapasitesine değil, verinin üretildiği ve kullanıldığı toplumsal, ekonomik ve kurumsal bağlama bağlı olduğu sonucundan hareketle eleştirel veri çalışmaları ile gıda sistemi ve tarım sosyolojisi arasında bir diyalog kurulmasını önermektedirler.

Görüldüğü üzere, dijital tarımın kendi literatürü içinde bu olguyu yalnızca yeni teknolojilerin kullanıldığı bir üretim modeli olmaktan çıkaran ve tarım-gıda sistemindeki bilgi, mülkiyet ve iktidar ilişkilerini dönüştüren sosyo-teknik bir süreç olarak değerlendirilmeye başlayan bir damar belirmeye başlamıştır. Ancak gene de dijitalleşmeyi; sermaye birikimi, küresel meta zincirleri ve tarihsel kapitalizm bağlamında ele alan analizlerin oldukça sınırlı kaldığını kabul etmemiz gerekir.

Bu noktada belirtmek gerekir ki, teknik bilimlerin, teknoloji politikalarının, yenilik sistemlerinin veya işletme yönetimi perspektifinden incelediği dijitalleşme olgusunun sosyal bilimlere maledilmesi bağlamında gıda rejimi yaklaşımı önemli kuramsal olanaklara sahiptir. Bu pencere bize dijitalleşme ile gıda sistemi arasındaki ilişkiyi kavrama dolayımında teknik yeniliklerin kullanım alanlarını sıralayan betimleyici yaklaşımlardan çok daha fazlasını vaad etmektedir. Ancak bu kuramsal olanağın çalışabilmesi için çoğu zaman rejimlerin temel özelliklerini tamamlayan bir unsur olarak görülen teknolojilerin bu tarihsel ilişkiler ağı içerisinde nasıl özgül biçimler kazandığı ve kurumsallaştıktan sonra aynı ilişkiler ağının yeniden üretiminde nasıl bir rol oynadığı konusunda açık bir kuramsal çerçeveye ihtiyaç vardır. Peki bu sosyo-teknik alaşım nasıl üretilmelidir?

Kuramsal Çerçeve

Doğal olarak “gıda rejimi” yaklaşımı; literatürde son yıllarda kavramsallaştırılan “dijital tarım" (*digital agriculture*), "akıllı tarım" (*smart farming*) veya "Tarım 4.0" (*Agriculture 4.0*) gibi kavramlarda ifade bulan bu yeni terimler dağarcığını içermemektedir. Öte yandan “dijital tarım” literatüründe de kapitalizmin tarihsel kuruluşuna dönük bir kaygı öncelik taşımaz. Zaten sorun bu iki literatürü yan yana getirmek değildir. Asıl sorun dijitalleşme ile gıda rejimi arasındaki ilişkinin hangi nedensellik anlayışı içerisinde kurulacağına karar vermektir. Dijital teknolojileri gıda sistemindeki dönüşümlerin özerk ve birincil nedeni olarak ele almak teknolojik determinizme; onları yalnızca ekonomik çıkarların etkisiz araçları olarak değerlendirmek ise teknolojik örgütlenmenin özgül maddi etkililiğini gözden kaçıran ekonomik indirgemeciliğe yol açmaktadır. Bu çalışma, teknolojik ya da ekonomik özcülüğe sapmadan, dijitalleşme ile gıda rejimi arasındaki ilişkiyi Althusserci yapısal nedensellik anlayışı temelinde ele almaktadır (Althusser & Balibar, 1970, s. 186–189).

Althusser’in yapısal nedensellik anlayışını öne sürmesi Marksist epistemolojiyi “geçişli nedensellik” ve “ifadeci nedensellik” anlayışından arındırmak istemeyle ilişkilidir. Neden ile sonucu birbirinden bağımsızlaştıran geçişli nedensellikte neden, kendisinin dışında bulunan

sonuç üzerinde doğrusal biçimde etkide bulunur. Öte yandan toplumsal bütünün farklı öğelerini tek bir içsel özün ifadelerine indirgeyen ifadeci nedensellikte ise bütünün her parçası aynı basit özün fenomenal dışavurumu olarak kavranır. Yapısal nedensellikte ise yapı ne öğelerinin dışında bulunan bağımsız bir neden ne de onların arkasında yer alan içsel bir özdür. Yapı, öğelerin karşılıklı etkililiklerinin özgül örgütlenmesidir ve kendi etkilerinde var olur. Bu nedenle yapıyı teşkil eden düzeyler ne birbirlerinden bağımsız nedenlerdir ne de aynı özün eşdeğer ifadeleridir; göreli özerkliklerini koruyarak başatlık altında yapılanmış karmaşık bütün içerisinde farklı ve eşitsiz etkililikler gösterirler (Resch, 1992, ss. 46–57).

Althusser, "Contradiction and Overdetermination" makalesinin farklı ve eşitsiz etkililiklerin tarihsel sürecin genel yapısını nasıl belirlediğine dair tartışma yürüttüğü bölümünde (1969, 99-101) ekonomik determinizme ve Hegelci başat çelişki modeline karşı çıkar. Aynı zamanda bu tartışma esnasında toplumsal yapının çelişki üzerinden işleyişini açarken bir çoğulculuk da olmayan toplumsal bütünlüğü yapısal bir metonimi çerçevesinde tanımlar. Bu çerçeve, toplumu tarihsel olarak hareket ettiren temel birlik ve terimi olan somut belirlenimleri arasında bir koşutluk öngörür. Bu öngörü, ortodoks Marksist "genel çelişki" kavramındaki ikiliğin yeniden tanımlanması ile mümkün olmuştur. Bu tanımlama ile üretim güçlerinin üretim ilişkilerini belirlediğine dair geleneksel kabul sürdürülür. Ancak üretim ilişkilerinin de üretim güçlerinin varoluş koşullarını teşkil ettiği öne sürülür. Böylece çelişkinin terimi olan üretim ilişkileri, üretim güçlerinin çelişki yapısının karşısına metonimik bir ilişkilenme ile konmuş olur. Bu sayede Althusser düşüncesinde çelişki, "içinde bulunduğu toplumsal bedenin toplam yapısından, kendi biçimsel varoluş koşullarından ve hatta yönettiği kertelerden ayrılamaz; onlar tarafından köklü biçimde etkilenir. Aynı hareket içinde hem belirleyen hem de belirlenen olarak, canlandırdığı toplumsal formasyonun çeşitli düzeyleri ve kerteleri tarafından belirlenir" (1969, 101). Althusser'in "üstbelirlenim" kuramının da temeli olan bu mantığa göre çelişkili birlik (genel çelişki) somutlukları belirlerken somut belirlenimler, yani düzeyler, kerteler[1], yapıyı var eden koşulları oluşturur.[2]

[1] Elbette bunlar daha somut düşünüldüğünde her düzeyin kendi işleyişi içinde özgül kurumlar, sınıf ilişkileri, devlet aygıtları, formlar vb. olarak çeşitlenecektir. İdeolojik düzey örneği için bkz.: Althusser, L. (1971). Ideology and ideological state apparatuses: Notes towards an investigation. İçinde *Lenin and philosophy and other essays* (B. Brewster, Trans., pp. 127–186). New Left Books.

[2] Belirlenim–koşullandırma ayrımı da doğrudan ampirik olarak ölçülen iki ayrı nedensel mekanizma değil, yapı ile terimleri arasındaki ilişkiyi açıklamak için kullanılan kuramsal bir ayrımdır. Bu çalışma özelinde; belirlenim, gıda rejiminin teknolojik örgütlenmeye dışarıdan müdahale etmesini değil, teknolojik bölgenin kuruluş koşullarının rejimsel bütünlük içerisinde biçimlenmesini ifade etmektedir. Koşullandırma ise kurumsallaşmış teknolojik aygıtların üretim, dolaşım, finansman ve denetim ilişkilerinin gerçekleşme biçimlerini düzenleyen özgül maddi etkililiğini ifade etmektedir. Rejimin kendisi de zaten bu ve benzeri maddi etkinliklerde var olabilmektedir.

Bu doğrultuda gıda rejimi, çelişkili bir temel birlik olarak kavramsallaştırılmaktadır. Bu birlik, kendisini oluşturan terimlerin yani ekonomik, jeopolitik vb. düzeylerin/örgütlenmiş ilişki türlerinin/ilişki öbeklerinin üzerinde veya dışında bulunan ayrı bir bütün değildir; onların özgül eklemlenmesinde var olmaktadır. Bununla birlikte yapı, kurucu terimlerinden herhangi birine indirgenemez. Her düzeyin yapı içerisindeki konumu, sınırları ve etkililik biçimi, gıda rejiminin tarihsel bütünlüğü içerisinde belirlenmektedir. Dolayısıyla yapı ile terimleri arasındaki ilişki, birbirinden bağımsız değişkenlerin dışsal etkileşimi biçiminde değil, içkin bir belirlenim ilişkisi olarak anlaşılmalıdır (Althusser, 1969, ss. 133–136; Althusser & Balibar, 1970, s. 187–189).[3]

Bu çalışmada ekonomi, gıda rejiminin kurucu düzeylerinden biri olarak ele alınmaktadır. Teknolojik örgütlenme ise ekonomik düzeyle özdeş olmayan, fakat bu düzey içerisinde yer alan özgül bir bölge olarak tanımlanmaktadır. Nasıl ki ekonomik düzey içinde üretim, dolaşım vb. bölgeler ve ilişkiler varsa teknolojik örgütlenme de, araçlar, teknik bilgiler, maddi aygıtlar, standartlar ve koordinasyon biçimleri aracılığıyla ekonomik düzeyin bir bölgesini teşkil eder. Teknolojik örgütlenmenin ekonomik düzey içerisinde konumlandırılmasının temel gerekçesi, teknolojik örgütlenmenin özgül nesnesinin, ekonomik faaliyetlerin yürütülmesini mümkün kılan teknik kapasitenin toplumsal olarak üretilmesi, örgütlenmesi ve yeniden üretilmesi olmasıdır. Teknik bilgi ve becerilerin geliştirilmesi, araç ve makinelerin tasarlanması, altyapıların kurulması, teknik standartların belirlenmesi, yazılım ve donanımların uyumlaştırılması, teknik sistemlerin uygulanması, bakımı ve yenilenmesi bu bölgenin özgül ilişki ve pratiklerini oluşturmaktadır. İçerdiği araştırma-geliştirme faaliyetleri, şirket laboratuvarları, teknik eğitim kurumları, patentler, standart kuruluşları, makineler, yazılımlar, veri altyapıları, bakım sistemleri ve kullanım pratikleri ile teknolojik örgütlenme; kendine özgü nesnesi, aygıtları, pratikleri, çelişkileri ve zamansallığı bulunan görece özgül bir ekonomik bölge teşkil etmektedir. Teknolojik örgütlenme, ekonomik düzeyin üretim ve dolaşım gibi diğer bölgelerini; emek sürecini düzenlenmesi ve üretimin araçlarını, ölçeğini, işlenmesini, muhafazasını belirlenmesi vb. hususlarda belirlediği için diğer bölgelerle özdeşleştirmez. Teknolojik örgütlenme ait olduğu ekonomik düzeyin diğer düzeylerce üstbelirlenmesi dolayımında devlet politikaları, hukuki düzenlemeler, fikrî mülkiyet rejimleri, bilimsel kurumlar ve ideolojik yönelimler gibi unsurlarca da şekillenir. Ancak bu şekillenme teknolojiyi ekonomik düzeyin dışına taşımaz. Zira teknolojik pratiklerin özgül nesnesi ve

[3] Ayrıca bkz. [Yüksel], S.B. (2026). *Althusser'i okumak: Yapısalcı Marksizmin Ontolojisi Hakkında Bir Deneme* [Yayımlanmamış doktora tezi]. Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

başlıca etkililiği, ekonomik süreçlerin maddi ve bilgisel koşullarının örgütlenmesidir. Dijitalleşme ise teknoloji ile özdeş değildir. Teknolojik örgütlenme mekanikleşme, kimyasallaşma, biyoteknoloji, ulaştırma, soğutma, işleme ve bilgi altyapıları gibi farklı alt bölgeleri veya tarihsel örgütlenmeleri kapsayabilir. Dijitalleşme ise bu geniş teknolojik bölge içerisinde verinin üretilmesi ve işlenmesi, bağlantılı altyapılar kurulması ve kararların algoritmik sistemlerle yönlendirilmesi etrafında farklılaşan özgül alt bölge olarak tasarlanacaktır.

Bu kavramsal ayrım, gıda rejimi ve dijitalleşme arasındaki ilişkiyi katmanlı fakat mekanik olmayan bir biçimde kurmayı mümkün kılmaktadır. Gıda rejimi, ekonomik düzeyin yapı içerisindeki konumunu ve tarihsel biçimini belirlemekte; ekonomik düzeyin bu yapılanışı, kendi içerisindeki teknolojik örgütlenme bölgesinin kuruluş koşullarını yapılandırmaktadır. Dijitalleşmenin hangi sorunlara yöneltileceği, hangi aktörler tarafından geliştirileceği, hangi teknik standartlara dayanacağı ve hangi mülkiyet biçimleri içerisinde kurumsallaşacağı da teknolojik örgütlenmenin bu tarihsel yapılanışı içerisinde belirlenmektedir. Bu nedenle dijitalleşme, ekonomik ve toplumsal ilişkilerden bağımsız bir teknik gelişme süreci değildir; teknolojik değişimlerin şirketleşmiş gıda rejiminin ilişkileri içerisinde seçilmesi, yeniden işlevlendirilmesi ve kurumsallaştırılmasıyla oluşan özgül bir alandır.

Bununla birlikte belirlenim ilişkisi, teknolojik örgütlenmeyi (ve dijitalleşmeyi) basitçe gıda rejiminin (ve bu rejiminin ekonomik düzeyinin) edilgen yansıması kılmaz. Dijital araçlar belirli aygıtlar, altyapılar ve pratikler hâlinde kurumsallaştıklarında üretim, dolaşım, finansman, bilgi ve denetim ilişkilerinin gerçekleşme biçimini maddi olarak koşullandırmaktadır. Verilerin hangi faaliyetlerden üretileceği, ekonomik aktörlerin hangi platformlar üzerinden ilişki kuracağı ve üretim kararlarının hangi algoritmik ölçütlere göre yönlendirileceği, ekonomik düzeyin gündelik işleyişini etkilemektedir. Ekonomik düzeyin gıda rejiminin kurucu bir terimi olması nedeniyle dijitalleşmenin bu koşullandırıcı etkisi, teknolojik örgütlenme ve ekonomik düzey üzerinden rejimin yeniden üretimine dolayımlı biçimde katılmaktadır. Burada simetrik bir karşılıklı belirlenim değil; yapı, düzey ve bölge bağlantısı üzerinden her yapılaşmanın terimlerinde içkin olarak var olduğu metonimik bir ilişki söz konusudur.

Yapısalcı bir kuramsal çerçeveden yola çıkarak teknoloji ile gıda rejimi arasındaki ilişkinin niteliğini açıklığa kavuşturarak söz konusu kuramsal eksikliği gidermeyi amaçlayan bu makale iki temel soruya yanıt aramaktadır. Birincisi, teknolojik örgütlenme birinci, ikinci ve

şirketleşmiş gıda rejimlerinde hangi tarihsel biçimleri almıştır? İkincisi, şirketleşmiş gıda rejiminin mülkiyet, birikim, standartlaşma ve şirket yoğunlaşmasına dayalı yapısı dijital teknolojilerin gelişme yönünü nasıl belirlemektedir? Çalışma, bu soruları ampirik bir ülke veya şirket araştırması üzerinden değil, gıda rejimi ve eleştirel dijital tarım literatürünün kuramsal-tarihsel olarak yeniden okunması yoluyla ele almaktadır. Çalışmanın özgün katkısı, teknoloji ile gıda rejimi arasındaki ilişkinin Althusserci yapısal nedensellik anlayışı temelinde yeniden yorumlayarak gıda rejimini yapısal bir birlik, teknolojik örgütlenmeyi bu yapısal birliğin ekonomik düzeyinin görece özgül bir bölgesi ve dijitalleşmeyi bu bölgenin tarihsel olarak farklılaşmış bir alt bölgesi olarak kavramsallaştırmasında yatmaktadır.

Bu sorular bağlamında çalışma, söz konusu kuramsal çerçeveyi iki aşamada geliştirecektir. İlk olarak gıda rejimlerinin tarihsel dönüşümü içerisinde teknolojik örgütlenmenin konumu incelenmekte; farklı rejimlerde belirli üretim, taşıma, muhafaza, işleme, bilgi ve koordinasyon teknolojilerinin rejimsel ilişkiler içerisinde nasıl biçimlendiği ele alınmaktadır. Bu tarihsel inceleme, teknolojinin gıda rejimlerine dışarıdan eklenen bağımsız bir unsur olmadığını; her rejimin ekonomik ve toplumsal ilişkilerinin maddi işleyişine yerleşen özgül teknolojik örgütlenmeler oluşturduğunu göstermeyi amaçlamaktadır.

İkinci olarak şirketleşmiş gıda rejimindeki dijitalleşme, dijital tarım literatüründen hareketle çözümlenmektedir. Bu kapsamda dijitalleşme alanının işleyişi verileştirme, platformlaşma ve algoritmik yönetişim olmak üzere birbiriyle bağlantılı üç süreç üzerinden incelenmektedir. Verileştirme tarımsal faaliyetlerin hesaplanabilir veri nesnelerine dönüştürülmesini; platformlaşma aktörlerin, hizmetlerin, verilerin ve ekonomik işlemlerin özel dijital altyapılarda birbirine bağlanmasını; algoritmik yönetişim ise toplanan verilerin üretim, finansman, emek ve dolaşım kararlarını yönlendiren sınıflandırma, tahmin ve tavsiye araçlarına dönüştürülmesini ifade etmektedir. Dijitalleşmenin zorunlu ve doğrusal aşamaları olmayan bu üç süreç, aynı zamanda dijitalleşme olgusunu yapısallaştıran unsurlar olarak dijital teknolojik örgütlenmenin farklı bağlamlarda değişen biçimlerde eklemlenebilen işleyiş süreçleridir.

Çalışmanın temel savı, dijitalleşme, şirketleşmiş gıda rejimine dışarıdan eklenen özerk bir teknoloji değil; ekonomik düzey içerisindeki teknolojik örgütlenme bölgesinin veri, platform ve algoritmik sistemler temelinde farklılaşan, rejim tarafından belirlenirken ekonomik ilişkilerin maddi işleyişini koşullandıran tarihsel alt bölgesidir.

Teknoloji ile gıda rejimi arasındaki ilişkiye dair bütün literatürü kapsayan sistematik bir derleme niteliğinde olmayan bu çalışmanın literatür seçimi, araştırmanın kuramsal amacı doğrultusunda gerçekleştirilmiştir. Gıda rejimi yaklaşımında Friedmann ve McMichael'ın kurucu çalışmaları ile şirketleşmiş gıda rejiminin oluşumunu tartışan temel metinler; dijital tarım alanında ise gıda zincirinin farklı aşamalarını yeniden düzenlemesi ile beraber doğan sorunlara odaklanan eleştirel çalışmalar tercih edilmiştir. Öte yandan makalenin gıda rejimi literatürünü kullanımı da seçicidir. Birinci, ikinci ve şirketleşmiş gıda rejimleri, teknolojik örgütlenmenin tarihsel biçimlerini karşılaştırmaya imkân veren analitik dönemlendirmeler olarak ele alınsa da; rejimler kendi içinde homojen, bütün coğrafyalarda eş zamanlı olarak kurulan veya önceki ilişkileri tamamen ortadan kaldıran kapalı dönemler olarak değerlendirilmemektedir. Nasıl ki toplumsal formasyon yapısal Marksizmde birden fazla üretim tarzının başatlık ve tabiiyet ilişkileri içinde eklemlenmesi önermesi (Althusser & Balibar, 1970, s. 307) çerçevesinde düşünüyorsa gıdaya ilişki genel formasyon da bu şekilde düşünülmelidir. Birkaç gıda rejimi herhangi bir özgül modern-ulusal yapı içinde birlikte bulunabilir ve bu hiyerarşik birlikte varoluşta bunlardan biri diğeri üzerinde başatlık kurabilir. Bu dolayımda farklı teknolojik örgütlenmeler aynı tarihsel dönemde birlikte bulunabileceği gibi, rejimsel ilişkilerin etkileri ülkelere, ürün zincirlerine, sınıfsal konumlara ve kurumsal yapılara göre farklılaşabilir. Bu çalışma söz konusu farklılaşmaları ampirik olarak incelememekte, teknolojik örgütlenmenin rejimsel yapı içerisindeki genel konumunu açıklamaya yönelmektedir.

Kuramsal çerçevenin temel sınırı, Althusser'in teknoloji veya dijitalleşme konusunda doğrudan geliştirdiği tamamlanmış bir modelin bulunmamasıdır. Teknolojik örgütlenmenin ekonomik düzeyin görece özgül bir bölgesi, dijitalleşmenin ise bu bölgenin tarihsel bir alt bölgesi olarak kavramsallaştırılması Althusser'in kendi sınıflandırmasının aktarımı değildir. Bu kavramsallaştırma, onun başatlık altında yapılanmış bütün, görece özerklik, yapısal nedensellik ve içkin belirlenim anlayışının teknoloji sorununa doğru genişletilmesine dayanan bu çalışmaya özgü bir kuramsal öneridir. Bu nedenle makale, "Althusser'e göre teknoloji ekonomik düzeyin bir bölgesidir" iddiasını taşımamakta; Althusserci yapısal mantıktan hareketle böyle bir konumlandırmanın mümkün ve açıklayıcı olduğunu savunmaktadır.

Benzer biçimde verileştirme, platformlaşma ve algoritmik yönetim, dijital tarım literatüründeki bütün süreçleri kapsama iddiasında olan evrensel bir tipoloji değildir. Bu anlamda mutlak bir kategorizasyondan çok dijitalleşmenin yapısallığının serimlenmesi amacıyla kullanılan bir kombinasyon olarak üretilmiştir. Bu şekilde üretilmesinin nedeni

literatür tarama sürecinde bu süreçlerin, dijitalleşmede ilişkiselliğin yoğunlaştığı konumlar olarak tespit edilmelerinden kaynaklanmaktadır. Dijital tarım literatürü okuması genişletildikçe ya da çözümlenen zamanın niteliksel karakteri (kairos) özgülleştikçe daha farklı terimlerle de ifade edilebilir.

Gıda Rejimi ve Teknolojik Örgütlenme Arasındaki İlişki

Teknoloji olgusunu gıda rejimi çerçevesinde ele almak tarım makinelerini veya üretim tekniklerini sıralayarak gıda ile ilişkisini ortaya koymaktan fazlasıdır. Tekil teknik nesnelerin toplamı olarak teknolojiyi düşünmek yerine, bir ilişkiler ağı içinde etkilenen ve bu ilişkiler ağını etkileyen bir teknoloji anlayışı inşa etmek gerekir. Zira basitçe bir makinenin geliştirilmesi, yaygınlaştırılması ve kullanılabilmesi söz konusu olduğu andan itibaren bununla beraber araştırma kurumlarının, finansmanının, ilişkili hukuki angajmanların, bakım hizmetlerinin vb. düşünülmesi zorunluluk arz eder.[4]

Bu nedenle makalede teknoloji yerine bu yapısal ilişkiselliği karşılayacağı düşünülen daha geniş bir kavram olan teknolojik örgütlenme kullanılmaktadır. Teknolojik örgütlenme; üretim araçlarını, bilimsel ve teknik bilgi biçimlerini, araştırma-geliştirme süreçlerini, altyapıları, teknik standartları, ölçme ve sınıflandırma sistemlerini ve üretim zincirinin koordinasyonunu kapsamaktadır. Ancak bu kavram ile amaçlanan teknolojiye ekonomik veya siyasal ilişkilerden bağımsız bir alan kazandırmak, yani özerk bir düzey olarak teknolojiyi tasarlamak değil, teknik araçların ancak belirli ilişkiler ve kurumlar içerisinde işlev kazanabildiğini göstermektir.

Gıda rejiminin teknolojik örgütlenmeyi belirlemesi, belirli teknik sonuçların önceden ve eksiksiz biçimde tayin edilmesi anlamına gelmez. Belirlenim, teknolojik seçeneklerin ortaya çıktığı alanın eşitsiz biçimde yapılandırılmasıdır. Teknik müdahaleye uygun görülecek sonuçlar, devlet desteğini haiz olacak teknolojiler/firmalar, finansman bulabilecek araştırmalar ve piyasaya erişim koşulu hâline gelecek standartlar; dönemin mülkiyet ilişkileri, şirket stratejileri, politik dengeler, devlet politikaları ve hâkim üretim modeli tarafından şekillenir.

[4] Bir dijital platformu ele alalım: bu platform yalnızca yazılımdan oluşmaz; veri toplama altyapıları, mülkiyet hakları, abonelik sözleşmeleri, teknik standartlar, algoritmik modeller ve diğer hizmetlerle uyumluluk ilişkileriyle birlikte işler.

Teknolojik örgütlenmenin gıda rejimi tarafından belirlenmesi, teknolojinin ekonomik ilişkilerin ya da sermaye birikiminin doğrudan bir yansıması olduğu anlamına da gelmez. Teknik sistemler kurumsallaştıklarında belirli faaliyetleri kolaylaştırırken diğerlerini zorlaştırabilir; üretim ölçeklerini, bilgi akışını ve aktörlerin hareket seçeneklerini maddi olarak düzenleyebilir. Bir teknik standardın benimsenmesi belirli üreticilerin pazara erişimini kolaylaştırırken başkalarını dışarıda bırakabilir. Kapalı bir veri formatı üreticinin başka bir platforma geçmesini zorlaştırabilir. Büyük makineler için tasarlanmış üretim altyapısı, küçük ve çeşitlendirilmiş tarım modellerini ekonomik ve teknik bakımdan dezavantajlı hâle getirebilir.

Bu nedenle belirlenim ve koşullandırma birbirinden ayrılmalı, fakat birbirine karşıt hâle getirilmemelidir. Belirlenim, teknolojik örgütlenmenin hangi tarihsel ilişkiler içerisinde biçimlendiğini açıklar. Koşullandırma ise gıda rejiminin ancak belirli teknik sistemler (veya politik, ideolojik ya da başka ekonomik sistemler/aygıtlar/örgütlenmeler/düzenekler) aracılığıyla fiilen işleyebileceğini gösterir. Bir rejim (ya da bu çalışmada metodolojik olarak ele alınması bağlamında yapı), kendi teknolojik örgütlenmesinden önce tamamlanmış bağımsız bir oluşum değildir. Rejim, teknik örgütlenmenin de içinde bulunduğu ekonomik, siyasal, hukuki, kurumsal vb. ilişkilerin bağlantısında var olur.

Bu yaklaşım, gıda rejimlerinin tarihsel gelişimini teknolojilerin ardışık biçimde birbirinin yerini aldığı doğrusal bir modernleşme süreci olarak görmekten kaçınmayı gerektirir. Yeni bir rejim, önceki dönemin teknolojik mirasını bütünüyle ortadan kaldırmaz. İkinci rejimde merkezileşen mekanizasyon ve kimyasal girdiler üçüncü rejimde varlıklarını sürdürmüş; biyoteknoloji, özel standartlar, küresel lojistik ve dijital sistemlerle bütünleşmiştir. Rejimler arasındaki teknolojik dönüşüm, teknik araçların basit ikamesinden çok, eski ve yeni teknik kapasitelerin farklı güç ve mülkiyet ilişkileri içerisinde yeniden eklemlenmesidir.

Teknolojik Örgütlenmeyi Gıda Rejimlerine Eklemlemek

Gıda rejimi ve teknolojik örgütlenme arasındaki ilişkinin mahiyeti serimlendiğine göre bu bağlam üzerinden teknolojinin gıda rejimi yaklaşımındaki yeri kurulabilir. Bu bölümde sırasıyla gıda rejimi literatüründe üretilen üç dönem ele alınarak teknoloji bu dönemlere eklemlendirilecektir.

Birinci gıda rejimi: Sömürgeci ticaretin teknolojik altyapısı

Tesis edilen ilk gıda rejimi olarak nitelendirilebilecek kolonyal-diasporik gıda rejimi (1870-1914),[5] dünyada ilk olarak temel bir gıda maddesi için fiyat belirleyen bir tahıl borsası olarak ortaya çıkmıştır. Toplumsal huzursuzlukların bunalttığı Avrupa devletleri (en başta dönemin hegemon gücü İngiltere olmak üzere) yeni keşfedilen topraklara göçü teşvik ederek eski kıtadaki kentli işçi nüfusunun gıda ihtiyacını bu göçmenlerden yapılan ucuz gıda ithalatı ile giderme çözümüne gidecekti. Kolonilere yerleşen Avrupalı göçmenlerin vazifesi Avrupa'ya gereken buğday ve hayvan ithalatını sağlamaktı. Yeni kıtanın yükünü taşıdığı bu ilk gıda rejiminde Avrupa'nın gıda ihtiyaçlarına ve beklentilerine uygun bir biçimde büyük otlak ekosistemleri ortadan kaldırılacak ve mono kültürel bir üretim tarzına yönelinecekti. Bunun getireceği tahribat toprak ve su sorunlarını ortaya çıkartacak; 1930'larda tamamen çöken bu ilk gıda rejimi sadece ekonomik bunalımla değil aynı zamanda ekolojik felaketler yüzünden son bulacaktı (Friedman 2005; s. 236-41). Söz konusu bu ilk rejimin teknolojik örgütlenmesi rejimin varoluş sebebine koşut olarak öncelikle uzak üretim bölgeleriyle Avrupa pazarlarını birbirine bağlayan taşıma, depolama ve iletişim altyapıları ile ilişkiliydi. Avrupa kıtasını beslemeye dönük yüksek montanlı ithalat zorunluluğu sadece tarımsal üretim teknolojisini değil aynı zamanda üretim bölgelerinin limanlara bağlanmasını, ürünlerin sınıflandırılmasını ve uzun mesafelerde taşınmasını gerektiren bir lojistik/dolaşım teknolojisini de beraberinde getirecekti. Ancak belirli toprakları ve ürünleri uluslararası ticaret sistemine bağlamak üzere kurulan bu teknik altyapı, sömürgeci ve yerleşimci ilişkilerin dışında gelişen tarafsız modernleşme araçları değildi. Örneğin, demiryolları bağlamında bu ilişki hatların hangi bölgelere kurulacağı, hangi ürünlerin limanlara taşınacağı ve altyapının hangi mülkiyet ilişkilerini destekleyeceği olarak dünya pazarıyla bağlantılı olarak temayüz edecekti (Friedmann & McMichael, 1989, ss. 95–101; McMichael, 2009, s. 143). Ancak demiryolu, gemiler vb. lojistik teknolojiler gıda rejimini var etmese de gıda rejimi bu teknolojilerde var olacaktı. Zira yerleşimci bölgelerde üretilen tahılın Avrupa'ya sürekli ve büyük miktarlarda aktarılması da söz konusu taşıma sistemleri olmadan gerçekleştirilemezdi. Rejim taşıma

[5] McMichael'ın daha sonraki dönemlendirmesinde Avrupa'ya sömürgelerden gelen tropikal ürünlerle yerleşimci devletlerden gelen tahıl ve hayvansal ürün akışlarını birleştir bu rejimi 1930'lara kadar uzatır (McMichael, 2009).

altyapısının kuruluş yönünü yapılandırırken, altyapı rejimin uluslararası varoluşunu mümkün kılmıştı. En azından 1929 yılındaki "Büyük Bunalım"a kadar böyle olacaktı.

İkinci gıda rejimi: Mekanizasyon, kimyasal girdiler ve agro-endüstriyel bütünleşme

Büyük Bunalım sonrası yıllarda Krizden en fazla etkilenen ülke olan ABD'nin bunalıma çare olarak geliştirdiği tarım politikası gereğince; devlet tarımsal ürünleri hedef fiyatlara ulaşıncaya dek satın alacaktı. Ancak bu, devlete ait bir "üretim fazlası" yaratmıştı. Dahası Amerikan hükümetleri, yerel üreticilerin hedef piyasa fiyatını korumak için ithal kısıtlamaları yürürlüğe sokulmuştu. Bu sosyo-ekonomik altyapı çerçevesinde ABD'nin gıda stoklarını korumaya ve dağıtmaya dayanan yeni bir rejim kurulacaktı. 2. Gıda rejimi olarak adlandırılan bu sistemde; bir önceki gıda rejiminde gerçekleşen akış tersine çevrilecek; Avrupa tarımsal olarak kendine yeter bir hale getirilirken ABD temel gıda ihracatçısı konumuna yükseltecekti. Ancak bu rejimde gıda yardımları nedeniyle 3. Dünya ülkeleri tarımsal olarak kendine yeter yapısını kaybedip gıda ithalatçısı durumuna düşecekti. (Friedman 2005; s.230-42).

Bu dönemin tarımsal ekonominin devam ettirildiği bölgelerde ise en önemli özelliği yaşanacak Yeşil Devrimdi. İkinci gıda rejimi döneminde kaydedilen tarımsal üretim artışına işaret eden ve tarımda makineleşme, verimli ürünlere yöneliş, sulama teknikleri ve tohum teknolojisi gibi faktörlere dayanan bu fenomenin; her ne kadar milyonlarca insanı açlıktan kurtardığı iddia edilse de ("Dünya 11 milyar insanı", 2019), diğer yandan bu modernist açılım; doğal kaynakların yanlış değerlendirilmesine, kimyasal kullanımının başlangıcına ve erozyona neden olacak; ekosistemi tahrip ederek pek çok çevresel soruna yol açacaktı. Global olarak tarımın sanayileşmesi ve kimyasallaşması, tarımda sermayenin yoğunluğunun artışı; (gıda üretiminin biyolojik temellerinden kopması ve insanın doğasına yabancılaşması anlamına gelen) metabolik yarılmayı ortaya çıkaracaktı. Günümüze kadar etkisini ağırlaştırarak sürdüren metabolik yarılma olgusu özellikle kentleşme olgusu ile giderek derinleşecekti (Keyder ve Yenal 2014; s.22-3).

Bu dönemin itici teknolojileri olarak tanımlanabilecek mekanizasyon, bitki araştırmalarındaki ilerlemeler, kimyasal girdilerin kullanımı, tohumların değiştirilmesi ve fosil yakıta dayalı, büyük ölçekli ve sermaye yoğun endüstriyel üretim modeli (Prause ve diğerleri, 2021, ss.

643–644) ikinci gıda rejiminin teknolojik örgütlenmesi çerçevesinde düşünülmelidir.[6] Bu bakımdan ikinci rejimde gerçekleşen teknolojik dönüşüm, tek tek tarım araçlarının yaygınlaşmasından ziyade makine kullanımını, bilimsel bitki araştırmalarını, kimyasal girdileri ve değiştirilmiş tohumları aynı üretim modeli içerisinde birleştiren agro-endüstriyel bir örgütlenmenin kuruluşu olarak değerlendirilmelidir. Bu kuruluş büyük ölçekli ve sermaye yoğun endüstriyel üretim modeli üzerine inşa edilecekti zira bu dönem, gıda sorununda en önemli aktörlerden biri olacak çok uluslu firmaların ortaya çıkışına da sahne olacaktı. Firmalar ikinci gıda rejiminin sonlarına doğru kapitalizmin bayraktarlığını devletlerin elinden alarak dünya ekonomisinde önü alınamaz bir güç olarak yükselecekti.

Bu gelişme elbette ivmesi giderek artan tarımda sanayileşme ile ilişkiliydi. Fordist tüketim kapitalizmine özgü yoğun birikim modelinin parçası olarak gerçekleşen tarımın sanayileşmesi ve işlenmiş "dayanıklı gıdaların" geliştirilmesiyle şekillenen yeni gıda rejimi; (aynı birikim düzeni çerçevesinde) gelişmiş kapitalist ülkelerde yükselen ücretlerle birlikte hayvansal protein ve dayanıklı gıda tüketiminin genişlemesine de dayanmaktaydı (McMichael, 2009, s. 144; 154). Dolayısıyla burada tarım ürünlerinin yalnızca çiftlikte üretilen nihai tüketim malları olmaktan çıkarak işleme sanayilerinin girdileri hâline gelerek kitlesel tüketime sunulması; işleme, koruma, ambalajlama ve dağıtım kapasiteleri bakımında yeni teknik ve kurumsal aygıtlarla düzenlenmeleri getirecektir.[7]

Her ne kadar agro-endüstrileşme kalkınmacı bir ideal olarak ulusal olsa da gıda rejiminin yapılanması tarımsal girdileri, üretimi, işlemeyi, taşımayı ve ticareti küresel tedarik zincirleri içerisinde birbirine bağlayan ulusötesi bir ölçekte yapılanacaktır (Friedmann & McMichael, 1989, s. 103; McMichael, 2009, s. 141). Ulusal kalkınma modeli, tarım ile sanayinin bütünleşik bir üretim sistemi içerisinde karşılıklı olarak birbirini destekleyerek büyüyeceği varsayımına dayanıyordu. Bu bütünleşmenin teknolojik temeli; fosil yakıtla çalışan makineler, sentetik gübreler, pestisitler ve bilimsel yöntemlerle geliştirilmiş tohumlardan oluşuyordu. Tarımsal üretimdeki artışın sanayiye hem hammadde hem de pazar sağlaması; sanayinin ise tarıma makine, kimyasal girdi ve işleme kapasitesi sunması öngörülmekteydi

[6] Prause, Hackfort ve Lindgren, üçüncü gıda rejiminin, bu örgütlenmeyi ikinci rejimden devraldığını ve bu modelin Yeşil Devrim aracılığıyla Küresel Güney'e yayıldığını tespit eder (Prause ve diğerleri, 2021, s. 643).

[7] Bu düzenlemelerle koşullanan "dayanıklı gıda" kavramı tüketim ile üretim arasındaki zamansal bağlantıyı değiştirerek kitlesel perakende için homojen ve öngörülebilir ürün akışları meydana getirmiştir. Bu süreç, ürün çeşitlerinin ve kalite ölçütlerinin sanayi ihtiyaçlarına göre standartlaştırılmasını teşvik etmiştir.

(McMichael, 2009). Bu süreçte tarımsal üretim, sanayi girdilerine ve standartlaştırılmış üretim tekniklerine giderek daha fazla bağımlı hâle gelecek biçimde yeniden örgütlendi (Prause ve diğerleri, 2021). Ancak tarımsal üretimin bu teknik dönüşümü, önemli ölçüde büyük sermayeye ve ulusötesi şirketlerin uzmanlığına dayanması nedeniyle ulusal tarımların söz konusu şirketlere bağımlılığını da artırdı. Rejim merkantilist bir nitelik taşısa da tarımsal girdi, işleme ve ticaret alanlarında faaliyet gösteren firmalar giderek uluslararası bir mahiyet kazandı. Böylece çiftçinin karşısına hem girdi satıcısı hem de ürün alıcısı olarak çıkan kapitalist firmalar, tarımsal üreticileri dünya ölçeğinde kuşatan bir bağımlılık ilişkisi oluşturdu (Friedmann, 2005).

Bu firmalar mal zincirlerinin her yeni organizasyonunda çiftçiler karşısında ağırlıklarını artırdı; uluslararası ticarette de tercihlerini merkantil kurallar yerine serbest ticaretten yana koydular. Bu gelişmeler dünyada gıda politikalarının karakterini değiştirecekti. Ancak merkantil rejime en önemli darbe 70'lerin başında ABD ve Sovyetler Birliği arasında yaşanan politik yumuşama ile gelecekti. Bu yumuşama süreci (detanté) çerçevesinde ABD'nin Sovyetler ile ticarete başlaması 2. Gıda rejiminin yürütülmesini sağlayan ABD gıda stokunun elden çıkarılmasına yol açtı. Bu tahmin edilmeyen durum (ABD stoklarının aniden son bulması dolayısıyla) arz-talep dengesi çerçevesinde tüm dünyada hububat fiyatlarının üç katına çıkmasına yol açacaktı. İthalata bağımlı Güney ülkelerini artan maliyet karşısında kredi çekmeye zorlayan bu gelişme aynı zamanda büyük bir kıtlığa yol açtı. 1974 gıda krizi olarak adlandırılan bu durum 2. Gıda rejiminin de sonu anlamına geliyordu (Friedman 2005; s. 244-5).

Petrol krizinin eşlik ettiği bu gıda kıtlığı nedeniyle gıda yardımı adı altındaki sübvansiyonlu tarım fazlası ihracına dayanan sistem terk edilecek, çok uluslu firmaların istediği gibi çok taraflı ticaret anlaşmaları üzerinden tarım uluslararası ticarete dâhil edilmeye çalışılacaktı (Çaşkurlu 2012; s.177; Friedman 2005; s. 245). 70'li yıllarla beraber devlet merkezli gelişmeye yapılan saldırılar ulusötesi arz zincirlerinin ve global pazarların oluşumuna imkân sağlamıştı (Friedman 2005; s.256).

Şirketleşmiş Gıda Rejimi: Biyoteknoloji, Özel Standartlar ve Küresel Koordinasyon

Gelecek olan yeni rejimde düzenleyici ilke imparatorluklar ya da devletler değil, serbest piyasa olacaktı. Değer ilişkilerinin liberalleşme ve özelleşme üzerinden siyasallaştırılması ile şirketlerin imtiyazlandırılacağı bu sistemde devletler artık piyasanın hizmetine girecekti (McMichael 2009; s.285). İçine girilen bu yeni dönemi McMichael, "şirketleşmiş gıda rejimi"

kavramıyla açıklarken; Friedmann, çevresel taleplerin ve kalite politikalarının şirketler tarafından seçici biçimde içerilmesine dikkat çekerek oluşum hâlindeki bir "şirketleşmiş-çevreci gıda rejimi" kavramsallaştırmasını önerecekti (Friedmann, 2005, ss. 228, 249–253; McMichael, 2009, ss. 151–152). Üçüncü rejimi Dünya Ticaret Örgütünün 1995'te kurulmasıyla başlayan dönemle ilişkilendiren Prause, Hackfort ve Lindgren'e göre; neoliberal serbest piyasa politikaları, dünya piyasa fiyatlarının düzenleyici rolü, küresel gıda meta zincirlerinin genişlemesi, büyük perakendecilerin tedarik zincirleri ve özel standartlar üzerindeki artan denetimi, şirket birleşmeleri yoluyla yoğunlaşma ve finans sermayesinin tarım-gıda sistemi üzerindeki etkisi bu yeni dönemin başlıca nitelikleri olacaktı (Prause ve diğerleri, 2021, s. 643).

Bu dönemin temel kurucu unsuru olan ve küreselleşmeyi yedeğine alan neoliberal rüzgar ile Çevre (gelişmekte olan/3.dünya/Güney) ülkelerde klasik köylülükten pazara yönelik üreticiliğe geçiş hızlanacak, tarım dışı istihdam ve gelirin önemi artacak, köy ve kırsal ekonomi büyük bir dönüşüme girerek piyasa ilişkilerinin nüfuzu altına sokulacaktı (Keyder ve Yenal 2014; s.19-20). Nüfusa oranları azalan tarımsal işgücünün toplumsal tabanı gitgide azalıyor fiyat destekleri büyük firmalar lehine değişiyor ve çiftçi agro-gıda firmalarına bağımlı hale geliyordu (Friedman 2005; s. 246). Piyasayı ve rekabeti öncülleyen bu yönleniş gereği tüm dünyada ithalata karşı koruma duvarları kaldırılacak, fiyat destekleri ve devlet alımları azaltılacak, tarım sektörüne yabancı kapitalist sermayenin doğrudan ve dolaylı ortaklık yoluyla girmesi ile kırsal bölgelerde ticarileşme ve metalaşma artacaktı (Keyder ve Yenal 2014; s.19-20, 36). Önceki gıda rejiminin bir mirası olan kalkınma mitinin, neoliberalizm ile girdiği reaksiyon ile köylülüğün tasfiyesi artık kaçınılmazdı (Mcmichael 2009; s.284). Ve en nihayetinde köylülük ölecekti (Hobsbawm 2007).

Ancak "köylülüğün ölmesi" başlı başına en büyük gıda sorununu oluşturacaktır. McMichael'a göre üçüncü gıda rejiminin kuralları, örtük biçimde, Dünya Ticaret Örgütünün 1995'te kurulması ve çok taraflı Tarım Anlaşması'nın imzalanmasıyla belirlenmiştir. Bu düzenlemeler, ulusötesi tarım-gıda şirketlerinin dünya pazarlarındaki hareket alanını genişletmiştir. İlk aşamada düşük fiyatlı tarım ürünleri ithalatı, Küresel Güney'deki küçük üreticilerin rekabet gücünü zayıflatmıştır. Ardından bu piyasalarda hâkimiyet kuran ulusötesi şirketler, gıda fiyatlarını yükselterek yeni bir sömürü ve bağımlılık düzeni oluşturmuştur. Çiftçi tabanlı üretimden endüstriyel üretime geçilmesinin hedeflendiği bu düzende çok uluslu firmalar fiyat enflasyonu üzerinden kar maksimizasyonu sağlarken tarım sektöründen çıkış yapan köylülerin işçileşmesi emek ücretlerini ucuzlatarak sömürüyü arttırıyordu. Önceki gıda

rejimlerinde şehirli işçi kitlelerini dizginlemek amacıyla ve Soğuk Savaşın getirdiği rekabet gereğince düşük tutulan gıda fiyatları bu yeni dönemde dizginlenemez bir artış trendine girecek ve agroflasyon (tarım ürünleri enflasyonu) ortaya çıkacaktı (2009; s.284-5).

Gıda fiyatlarındaki artışın başka bir sorumlusu da yeni gıda rejiminde geçilen bio-yakıt teknolojisidir. Bu yeni teknoloji ile enerji ve gıda arasında bir mübadele hali ortaya çıkmıştır. Tarımsal üretimin beslenme yerine enerji üretimine tahsis edilmesi ile kendini gösterecek bu mübadele ile sadece gıda fiyatları artmamış aynı zamanda tarımın toprak ve su üzerinden besleyici geri dönüşümü azaltılarak tarımsal üretimi metalaştırılmış girdiler olarak enerji kaynaklarına aktarmakla "metabolik yarılma" arttırılmıştır (McMichael 2009; s.284, 286, 289-91). Üçüncü gıda rejiminin getireceği ve metabolik yarılmaya katkıda bulunan bir başka değişiklik de "2. Yeşil Devrim" olacaktır. (İkinci Dünya Savaşı sonrası dönemde yaşanan) birincisinden farklı olarak devletler eliyle değil fakat çok uluslu firmalar üzerinden yönlendirilen bu yeni devrim ile genetiği ile oynanmış tohumlar ve kimyasal katkılar ile doğal süreçlere müdahale edilip çiftçilerin tarımsal üretim üzerinde hâkimiyetleri ortadan kaldırılmaktadır. (Çaşkurlu 2012; s.182-3). Bu durum aslında karşımıza tıpkı mitolojik tanrı Janus'un iki yüzü gibi yorumlanabilecek bir ikilem çıkarmaktadır. Sermayenin doğal olandan (mekanizasyon, ikamecilik ve kimyasal girdiler üzerinden) uzaklaşması üretim sürecini öngörülebilir kılmak, doğadan kaynaklanan belirsizlikleri ortadan kaldırmak, verimliliği arttırmak ve üretimde istikrarı sağlamak gibi rasyonel kaygılar ile değerlendirilebilir (Keyder ve Yenal 2014; s.23). Ancak bu gidişat aynı zamanda GDO'lu tohumlardan başlayan bir gıda zinciri teşekkülü ve patentler yoluyla gıda üzerinde egemenliğin biyo-teknoloji alanını domine eden çok uluslu firmaların tekeline bırakılması olarak da yorumlanabilir (Aysu 2005; s.45; Çaşkurlu 2012; s.183).

Fakat hangi yorum benimsenecek olursa olsun ortada giderek artan bir gerçeklik vardır ki o da "bio-teknolojik müdahale"dir. Bu gerçek üçüncü gıda rejimi boyunca neoliberal düzenleyici yeniden yapılanmanın temel bir teknolojik bileşeni olacak; düzenleyici değişim ile genetik mühendisliği arasındaki ilişki beraber yürüyecektir (Pechlaner & Otero, 2008). Burada dikkate şayan husus; yeni rejimde genetik teknolojisi üzerinden tarımsal faaliyetin serbestisinin, fikri mülkiyet sahasına hapsedilmesidir. Tohum patentleri ve lisanslar, biyolojik materyalin teknik özellikleriyle fikrî mülkiyet ilişkilerini birbirine bağlayarak biyoteknolojiyi ürünlerin genetik özelliklerini değiştirmenin ötesinde bir araca dönüştürmektedir. Artık yukarıda değinilen "2. Yeşil Devrim" çerçevesinde hukuki sözleşmeler ve şirket politikaları

tarafından düzenlenebilen (tohumun saklanması, yeniden ekilmesi veya başka girdilerle birlikte kullanılması) tarımsal edimler; tarımsal üretimde teknolojiyle mülkiyet arasındaki ilişki teknik ürünün kullanım koşullarına yerleştirilerek çiftçinin üretim araçlarındaki mülkiyetini sınırlamaktadır. İkinci rejimde üretilen fosil yakıta, mekanizasyona, kimyasal girdiye dayalı; büyük ölçekli ve sermaye yoğun üretim modeli ile güçlenen ulusötesi şirketler üçüncü rejimdeki biyoteknolojik gelişmeler ile gücünü ve tahakkümünü daha da arttırmıştır (Prause ve diğerleri, 2021).

Friedman'ın tespit ettiği üzere insanlar bedeli ne olursa olsun gıda tüketmek zorunda oldukları için bu rejim, sistemi ve ticareti şekillendiren firmalara gıda kıtlığını muazzam karlara çevirme imkanı sunmuştur (2009; s.290). Genel olarak bakıldığında, İkinci Dünya Savaşı sonrasında başlayan modern tarımın, birinci Yeşil Devrim (endüstriyel tarım) ve günümüzde ikinci Yeşil Devrim (genetik tarım) olarak adlandırılan çağdaş üretim biçimleri aracılığıyla gıda rejimlerine koşut şekilde geliştiği görülmektedir. Bu gelişmeler sonucunda insan ve hayvan sağlığı açısından çeşitli riskler ortaya çıkmış, doğal denge ise bozulmuştur. (Aysu 2005; s.77). Kapitalizmin gerektirdiği mono üretimin ihtiyaç duyduğu ilaç, fosil yakıt ve gübre kullanımı, dünyanın birçok yerinde biyolojik çeşitliliği yok ederek küresel ısınmayı tetiklemektedir (Çakan ve Erol 2008). Neoliberal düşüncenin güdümündeki yeni kurumsal gıda rejiminde -1929 ve 1974 yılında patlak veren krizlerin çok ötesinde- gıda krizi artık anlık değil devamlı bir hal almıştır (McMichael 2009; s.289). Ancak bütün bu olumsuzluklara rağmen firmaların tüketici ve bireysel çiftçilik karşısında kaçınılmaz güçlenişinin altında elbette üretmeye muktedir oldukları teknik kapasite yatmaktadır. Zira meta zincirlerinin genişlemesi ancak belirli bir teknolojik altyapı ile realize edilebilmiştir.

Coğrafi olarak dağınık unsurlarını birbirine bağlayan teknolojik altyapıların gelişmesine dayanan bu genişlemenin kaynağı 1990'lardaki ticari serbestleşme ile dot-com patlaması sırasında kurulan yeni bilgi ve iletişim teknolojileri altyapısının birleşimi ile ilişkilendirilebilir. Karmaşık küresel ağlar içerisinde bilgi alışverişini ve üretim, tedarik ve dağıtım süreçlerinin koordinasyonunu mümkün kılan bu altyapının; soğutma, muhafaza ve taşıma teknolojilerindeki gelişmeler ile eklemlenmesiyle meta zincirlerinin kurulması mümkün olmuştur (Prause ve diğerleri, 2021, s. 643).

Bu üçüncü gıda rejimindeki örgütlenme kapasitesi ile yakından ilişkilidir. Coğrafi olarak dağınık üreticilerin sipariş, stok, teslimat ve kalite bilgilerinin merkezî biçimde koordine edilmesini gerektiren bu küresel girişimde karmaşık ürün akışlarının düzenli ve

standartlaştırılmış biçimde işleyebilmesi ancak kurumsal güç ile gerçekleştirilebilir. Bu kurumsal güç de ancak dijitalleşme ile sağlanabilir. Dijitalleşme, bu tarihsel örgütlenmenin dışında ortaya çıkan bağımsız bir dönüşüm değil, söz konusu teknik ve kurumsal zorunluluğun üzerinde gelişen yeni bir yapılanmadır.

Dijitalleşmeyi Yapısallaştırmak

Dijitalleşme analog bilgilerin sayısal biçime aktarılmasının ötesinde karmaşık bir yapılanmanın kavramıdır. Klerkx, Jakku ve Labarthe dijitalleşmenin tarım alanında büyük veri, nesnelerin interneti, artırılmış gerçeklik, robotik sistemler, sensörler, üç boyutlu baskı, sistem bütünleşmesi, yaygın bağlantı altyapıları, yapay zekâ, makine öğrenmesi, dijital ikizler ve blokzincir gibi farklı teknolojiler ve uygulamalar kapsadığını belirtmektedir. Yazarların gerçekleştirdiği literatür incelemesi, dijital tarıma ilişkin sosyal bilim çalışmalarının; teknoloji benimseme, emek ve beceri, güç ve mülkiyet, bilgi sistemleri ile değer zincirlerinin yönetimi gibi farklı farklı tematik kümelerde sınıflandığını göstermektedir (Klerkx ve diğerleri, 2019, s. 1).

Prause, Hackfort ve Lindgren'in 280 dijital ürün ve hizmet üzerine gerçekleştirdikleri ampirik inceleme, dijital teknolojilerin gıda meta zincirinin bütün aşamalarında kullanıldığını göstermektedir. Tarımsal girdi alanında genom düzenlenmiş tohumlar, kredi değerlendirme ve ödeme hizmetlerinde kullanılan finansal teknolojiler ile veriye dayalı sigorta uygulamaları öne çıkmaktadır. Çiftlik düzeyinde hassas tarım ekipmanları, tarım robotları, dijital makine paylaşım sistemleri, veriye dayalı agronomik danışmanlık hizmetleri ve çiftlik yönetim platformları kullanılmaktadır. Birincil tarımsal ürünlerin ticaretinde dijital pazar yerleri yaygınlaşırken, gıda işleme alanında işbirlikçi robotlar ve üç boyutlu gıda baskısı; ambalajlamada ise akıllı ambalajlama ve üç boyutlu baskı uygulamaları geliştirilmektedir. Taşıma ve depolama aşamalarında kalite sensörleri, veri analitiği, dijital yük ve lojistik yönetimi ile otomatik depolar kullanılmaktadır. Perakende ve tüketim alanında akıllı alışveriş uygulamaları ve e-ticaret platformları öne çıkarken, izlenebilirlik ve şeffaflık araçları gıda meta zincirinin bütününü kapsamaktadır (Prause ve diğerleri, 2021, ss. 645–6). Yazarlar bu bulgulardan hareketle dijitalleşmenin yalnızca tarımsal girdiler ve çiftlik faaliyetleriyle sınırlı olmadığını, üretimden işleme, taşıma, depolama, perakende ve tüketime kadar gıda meta zincirinin tamamına yayılarak rejimin işleyişini farklı aşamalarda etkilediğini belirtmektedir (Prause ve diğerleri, 2021, s. 651).

Elbette dijital teknolojilerin çeşitliliğini ve gıda zincirindeki yayılımını göstermenin ötesine geçen çalışmalara da ihtiyaç vardır. Özellikle dijitalleşmenin şirketleşmiş gıda rejimi içerisinde hangi mekanizmalar aracılığıyla işlediğini açıklamak bu dönüşümü kavramak için hayati önem taşır. Bu noktada Fraser'ın tarımsal verinin üretimi ve temellüküne ilişkin çözümlemesi literatürde göze çarpmaktadır. Fraser, hassas tarım uygulamalarının toprak, iklim, zararlılar, ürün gelişimi ve materyal akışları hakkında yeni veri noktaları oluşturduğunu; teknoloji şirketlerinin bu verileri toplayarak, birleştirerek ve işleyerek ekonomik değere dönüştürebildiğini ifade eder. Bunun doğal sonucu tarımsal faaliyetin gıda ile beraber bir veri üretim pratiğine dönüşmesidir. Sistem içinde çiftçiler yalnızca tarımsal ürün değil, aynı zamanda şirketler tarafından temellük edilebilen veri de üretmektedir (Fraser, 2019, s. 893).

Carolan ise dijital tarım platformlarını yalnızca hizmet sağlayan teknik araçlar olarak değil; çiftçileri, algoritmaları, makineleri, şirket ürünlerini ve üretim pratiklerini birbirine bağlayan sosyo-teknik bileşimler olarak ele almaktadır. Bu platformların üreticileri belirli veri formatlarına, yazılımlara, donanımlara ve şirket hizmetlerine bağlayabildiğini gösteren Carolan, dijital tarımın farklı bileşenlerinde ortaya çıkan bağımlılık ve kilitlenme eğilimlerine dikkat çekmektedir (2020, s. 1041).

Dijital tarım literatürünün genel olarak okunması ve çözümlenmesi dolayımında bu çalışmada "dijitalleşme" üç bağlantılı unsuru üzerinden çözümlenecektir: verileştirme, platformlaşma ve algoritmik yönetişim.[8] Her biri dijital tarım literatüründe farklı bağlamlarda tartışılan bu kavramlar üzerinden geliştirilen analitik çerçevenin amacı, Klerkx ve arkadaşlarının ortaya koyduğu teknolojik çeşitliliği, Prause ve arkadaşlarının gösterdiği zincir ölçeğindeki yayılımı, Fraser'ın veri temellüküne ilişkin çözümlemesini ve Carolan'ın platform bağımlılığına ilişkin yaklaşımını şirketleşmiş gıda rejiminin teknolojik örgütlenmesini açıklayacak biçimde bir araya getirmektir (Carolan, 2020; Fraser, 2019; Klerkx ve diğerleri, 2019; Prause ve diğerleri, 2021).

Bu yapısallaştırma ile kurulmak istenen; dijitalleşme ile şirketleşmiş gıda rejimi arasındaki ilişkiyi doğrudan ve simetrik bir karşılıklı etkileşim olarak değil, düzeyler ve yapı arasındaki

[8] Burada Forschung (araştırma süreci) aşamasında dijital tarıma ilişkin literatür analitik-semptomatik bir okumaya tabi tutulmuş; sonuç olarak burada sunulan (Darstellung) üç süreç/unsur belirlenmiştir. Bu mutlak bir kategorizasyondan çok dijitalleşmenin yapısallığının serimlenmesi amacıyla kullanılan şematik bir kategorizasyondur. Dijitalleşmede ilişkiselliğin yoğunlaştığı konumların topolojik olarak çözümlenmesi olan bu üçlü varoluş, dijital tarım literatürü okuması genişletildikçe ya da çözümlenen zamanın niteliksel karakteri (kairos) özgülleştikçe daha farklı terimlerle de ifade edilebilir.

eklemlenmiş bir belirlenim–koşullandırma ilişkisi olarak somutlaştırmaktır. Dijital teknolojik örgütlenme, yapısal mantık çerçevesinde gıda rejiminin ekonomik düzeyinden bağımsız bir düzey değil; bu düzey içerisinde özgül olarak oluşan teknolojik bölgenin bir unsurudur. Bu nedenle dijitalleşmenin kuruluş biçimi doğrudan doğruya kendi teknik özellikleri tarafından belirlenmez. Gıda rejimi, ekonomik düzeyin yapı içerisindeki konumunu, sınırlarını ve etkililik biçimini belirlerken; özel mülkiyet, sermaye birikimi, finansallaşma, şirket yoğunlaşması, özel standartlar ve küresel değer zincirleri gibi ekonomik ilişkilerin aldığı tarihsel biçimi de yapılandırmaktadır. Dijital teknolojik örgütlenme ise ekonomik düzeyin bu tarihsel yapılanışı içerisinde, söz konusu ilişkilerin belirli teknik aygıtlar, bilgi sistemleri, veri altyapıları ve koordinasyon biçimleri aracılığıyla örgütlendiği bir unsur/iç bölge/alan olarak ortaya çıkmaktadır. Dolayısıyla gıda rejiminin dijitalleşme üzerindeki belirlenimi, yapının dışarıdan teknolojiye müdahale etmesi biçiminde değil; ekonomik düzeyi ve bu düzey içerisindeki teknolojik örgütlenme bölgesinin kuruluş koşullarını yapılandırması yoluyla gerçekleşmektedir.

Bununla birlikte dijital teknolojik örgütlenme, (tıpkı ekonomik düzeyin ilişkili olduğu yapının edilgen bir yansıması olmaması gibi) ekonomik düzeyin edilgen bir yansıması değildir. Verilerin toplanması ve mülkiyet konusu hâline getirilmesi, işlemlerin şirket platformlarında merkezîleştirilmesi, üretim kararlarının algoritmik sistemler aracılığıyla yönlendirilmesi ve üreticilerin belirli teknik ekosistemlere bağlanması -doğal olarak- ekonomik ilişkilerin hangi maddi ve örgütsel biçimler içerisinde işleyeceğini koşullandırmaktadır. Dijital teknolojik örgütlenme, ekonomik düzeyin bir terimi olarak bu düzeyin işleyişini, koordinasyon kapasitesini ve yeniden üretim koşullarını düzenlemektedir. Ekonomik düzey de gıda rejiminin kurucu terimlerinden biri olduğundan, dijitalleşme rejimin bütününün yeniden üretimini dolaylı, ancak maddi biçimde koşullandırmaktadır.

Verileştirme, platformlaşma ve algoritmik yönetişim ayrımı, bu eklemlenmiş ilişkinin farklı uğraklarını görünür hâle getirmektedir. Verileştirme ekonomik faaliyetleri hesaplanabilir veri nesnelerine dönüştürmekte; platformlaşma aktörleri, hizmetleri ve işlemleri belirli şirket altyapıları içerisinde birleştirmekte; algoritmik yönetişim üretim ve dolaşım kararlarını belirli optimizasyon ölçütlerine göre yönlendirmektedir. Böylece bu üç unsur/süreç, şirketleşmiş gıda rejiminin ekonomik ilişkilerinin dijital teknolojik örgütlenme bölgesinde nasıl maddileştiğini ve bu bölgenin ekonomik düzey üzerinden rejimin yeniden üretimini nasıl koşulladığını açıklamaktadır.

Verileştirme

Dijital teknolojik örgütlenmenin ilk unsuru/süreci olarak ele alınan verileştirme, tarımsal üretim ve gıda dolaşımı içerisindeki faaliyetlerin kaydedilebilir, birleştirilebilir, karşılaştırılabilir ve hesaplanabilir veri noktalarına dönüştürülmesi olarak tanımlanabilir. Hassas tarım uygulamaları; ürün ve materyal akışları, toprak özellikleri, zararlıların yayılımı ve iklim koşulları hakkında daha önce mevcut olmayan veya sistematik biçimde toplanmayan yeni veri noktaları üretmektedir. Tarım teknolojisi sağlayıcıları ise bu verileri toplayabilmekte, bir araya getirebilmekte, hesaplayabilmekte ve ekonomik değere dönüştürebilmektedir (Fraser, 2019, s. 893). Bunun yanı sıra ürün gelişimi, girdi kullanımı, makine performansı, üretim süreçleri, taşıma ve depolama koşulları ile tüketici faaliyetleri de gıda meta zincirinin farklı aşamalarında kullanılan dijital araçlar aracılığıyla veri hâline getirilebilmektedir (Prause ve diğerleri, 2021, ss. 645–6, 649). Prause, Hackfort ve Lindgren bu farklı uygulamaların ortak eğilimini, gıda zincirinin tamamında büyük miktarda verinin çıkarılmasına ve analiz edilmesine yönelik artan bağımlılık olarak tanımlamaktadır (2021, s. 645-6).

Fraser'e göre hassas tarım uygulamaları aracılığıyla elde edilen veriler, tarım teknolojisi sağlayıcıları tarafından toplanabilmekte, birleştirilebilmekte, işlenebilmekte ve satış konusu hâline getirilebilmektedir. Böylece üreticiler tarımsal ürünle birlikte giderek artan miktarda veri de üretmektedir. Birden fazla çiftlikten elde edilen verilerin bir araya getirilmesi, söz konusu verileri tohum ve kimya şirketleri, makine üreticileri, agronomik danışmanlar, kooperatifler ve sigorta şirketleri bakımından ekonomik bir kaynağa dönüştürebilmektedir. Fraser'ın "veri kapma" kavramı, ise tarım teknolojisi sağlayıcılarının üreticilerin meydana getirdiği verileri toplama ve kullanma bakımından ayrıcalıklı bir konum kazanmasına, üreticilerin verileri üzerindeki denetimlerini kaybedebilmesine ve bu verilerden üretilen değer veya gelirin üreticilerle paylaşılmamasına dikkat çekmektedir (Fraser, 2019, ss. 893, 895–6, 899-900).

Verileştirme, tarımsal gerçekliğin nötr ve eksiksiz biçimde dijital ortama aktarılması olarak anlaşılmamalıdır. Bronson ve Knezevic, büyük verinin belirli toplumsal ve teknik bağlamlar içerisinde insanlar tarafından çerçevelendiğini ve yorumlandığını; verilerin kendiliğinden mevcut olmayıp üretilmesi gerektiğini vurgulamaktadır. Bu doğrultuda yazarlar, tarımsal verilerin üretim, depolama ve kullanım koşullarının belirlenmesine kimlerin katıldığı, hangi tür verilerin toplanacağına kimlerin karar verdiği ve bazı tarımsal sistemlerin maddi

gerçekliklerinin nicel veri toplama araçları ile temsil edilip edilemeyeceği sorularını gündeme getirmektedir (Bronson & Knezevic, 2016, ss. 2–3). Bu sorulardan hareketle verileştirme, yalnızca mevcut gerçekliği kaydeden teknik bir işlem değil, tarımsal gerçekliğin belirli yönlerini ölçülebilir ve müdahale edilebilir hâle getiren seçici bir süreç olarak değerlendirilebilir.

Bununla birlikte verileştirme, ekonomik düzeyin ya da gıda rejiminin edilgen bir yansıması olarak düşünülmemelidir. Fraser, hassas tarım uygulamalarının çiftlik faaliyetlerine ilişkin verilerin izlenmesini ve yönetilmesini kolaylaştırdığını; bu verilerin teknoloji sağlayıcıları tarafından toplanarak analiz edilebilir ve ekonomik değere dönüştürülebilir hâle getirildiğini göstermektedir (Fraser, 2019, ss. 898-9). Prause ve arkadaşları ise dijital finans uygulamalarında çiftçilerin kredi değerliliğinin çiftlik faaliyetleri ve çevresel veriler üzerinden hesaplandığını ve bu uygulamaların disipline edici sonuçlar doğurabildiğini belirtmektedir (Prause ve diğerleri, 2021, s. 648). Bu örnekler, verinin üretim, finansman ve denetim ilişkilerinin maddi bir bileşeni hâline gelerek ekonomik düzeyin işleyişini koşullandırdığını göstermektedir.

Verinin koşullandırıcı etkisi, tek başına yeni ekonomik ilişkiler yaratmasından değil; mülkiyet hakları, kullanıcı sözleşmeleri, platformlar, algoritmalar ve şirket stratejileriyle eklemlenmesinden kaynaklanmaktadır. Kullanıcı sözleşmeleri şirketlere çiftlik verilerini toplama ve kullanma imkânı verirken, veri sahipliği, erişim, mahremiyet ve güvenlik sorunlarını da gündeme getirmektedir (Fraser, 2019, ss. 895–6, 899–900). Tarım-gıda şirketleri bu verilerden ekonomik değer üretmekte ve üreticiler üzerindeki denetimlerini güçlendirmektedir (Prause ve diğerleri, 2021, ss. 651-2). Bu bağlamda gıda rejimini bağımsız olarak belirlemeyen verinin; ancak mülkiyet ve platform ilişkileri çerçevesinde örgütlendiğinde rejimi ilkesel olarak koşullandırdığı söylenebilir.

Ayrıca belirtmek gerekir ki verileştirme sadece ekonomik ilişkilerle değil, hukuki ve kurumsal düzenlemelere de bağlı olarak biçimlenir. Çiftlik yönetim sistemlerinin gıda güvenliği, sertifikasyon standartlarına ve sözleşme şartlarına uygun belgeleme işlevi taşıması, hukuki ve kurumsal ilişkilerin verileştirme bölgesinin kuruluşuna katıldığını; verileştirmenin de standartların uygulanmasını teknik olarak koşullandırdığını göstermektedir (Fraser, 2019, ss. 898-9; Prause ve diğerleri, 2021, s. 650).

Platformlaşma

Prause ve diğerleri ile Carolan tarafından güçlü bir şekilde üzerinde yoğunlaşılan "platformlaşma" kavramı ise bu çalışmada dijitalleşmenin bir diğer unsuru/süreci olarak belirlenmiş olup kavram; gıda zincirindeki aktörlerin, hizmetlerin, verilerin ve ekonomik işlemlerin dijital altyapılar aracılığıyla birbirine bağlanmasını ifade etmektedir. Çiftlik yönetimi, girdi satışı, agronomik danışmanlık, kredi, sigorta, ürün ticareti, lojistik ve perakende gibi farklı faaliyetler aynı platform ekosistemi içerisinde bütünleştirilebilmektedir. Prause, Hackfort ve Lindgren, dijital platformların tarımsal üretimden ticaret, taşıma, depolama ve perakendeye kadar gıda meta zincirinin farklı aşamalarında kullanıldığını göstermektedir (Prause ve diğerleri, 2021, ss. 645-6).

Platformlar yalnızca aktörler arasındaki iletişimi kolaylaştıran tarafsız aracılar değildir. Platformu işleten şirket, sisteme erişim koşullarını, hangi hizmetlerin birbiriyle ilişkilendirileceğini, hangi verilerin toplanacağını ve kullanıcıların hangi seçeneklerle karşılaşacağını düzenleyebilmektedir. Platformlaşma bu nedenle ekonomik ilişkilerin şirketlerin denetimindeki dijital altyapılarda merkezîleştirilmesini ve platform sahibinin koordinasyon kapasitesinin genişlemesini ifade etmektedir.

Platformlaşmanın aldığı biçim, şirketleşmiş gıda rejiminin şirket yoğunlaşması, finansallaşma ve dikey bütünleşme eğilimleri içerisinde belirlenmektedir. Büyük tarım-gıda şirketleri platformları yalnızca yazılım satışından gelir elde etmek için değil, tohum, pestisit ve tarım makineleri gibi temel ürünlerini desteklemek, kullanıcı verilerini toplamak ve üreticileri kendi ürün ekosistemlerine bağlamak amacıyla da geliştirmekte veya satın almaktadır. Böylece daha önce ayrı alanlarda gerçekleşen girdi satışı, üretim yönetimi, danışmanlık ve veri analizi aynı şirket altyapısı içerisinde bütünleşebilmektedir (Prause ve diğerleri, 2021, ss. 647-9).

Bununla birlikte platformlaşma, şirketleşmiş gıda rejiminin ekonomik ilişkilerinin edilgen bir yansıması değildir. Girdi satın alma, üretim planlama, kredi kullanma, ürün satma ve standartlara uyumu belgeleme gibi faaliyetler aynı platform üzerinden yürütüldüğünde, ekonomik işlemlerin gerçekleşme biçimi platformun teknik mimarisi tarafından koşullandırılmaktadır. Her tekil platform böylece yalnızca piyasadaki aktörlerden biri değil, aktörler arasındaki ilişkilerin gerçekleştiği altyapının düzenleyicisi hâline gelebilmektedir (Carolan, 2020, s. 1041; Prause ve diğerleri, 2021, ss. 648-9).

Carolan, dijital tarım platformlarını çiftçiler, algoritmalar, makineler, ürünler, mekânlar ve üretim pratikleri arasındaki ilişkileri örgütleyen sosyo-teknik bileşimler olarak ele almakta ve bu bileşimin farklı noktalarında ortaya çıkan kilitlenme eğilimlerine dikkat çekmektedir

(Carolan, 2020, s. 1041). Bu yaklaşım, platform gücünün yalnızca şirket mülkiyetine veya pazar payına dayanmadığını; veri formatları, yazılım ve donanım uyumlulukları ile platformun gündelik üretim pratiklerine yerleşmesi yoluyla da işlediğini göstermektedir. Böylece platformlar, üreticilerin başka bir sisteme geçmesini zorlaştırarak ekonomik bağımlılığı üretimin teknik örgütlenmesi içerisinde kurumsallaştırabilmektedir.

Dolayısıyla platformlar, ekonomik düzeyi veya gıda rejimini bağımsız olarak belirlememektedir. Platformların kuruluş biçimi; sermaye yatırımları, şirket stratejileri, fikrî mülkiyet ilişkileri ve veri düzenlemeleri ile belirlenirken; kurumsallaşan platformlar da ekonomik işlemlerin gerçekleştiği altyapıyı düzenlemektedir. Platformların veri akışlarına, teknik uyumluluklara ve gündelik üretim pratiklerine yerleşmesi, şirket yoğunlaşması, dikey bütünleşme ve üretici bağımlılığı gibi ilişkilerin yeniden üretimini koşullandırmaktadır.

Algoritmik yönetişim

Algoritmik yönetişim, bu çalışma bağlamında verileştirilen üretim ve dolaşım süreçlerinin algoritmik sistemler aracılığıyla sınıflandırılması, değerlendirilmesi, tahmin edilmesi ve yönlendirilmesi ifade etmektedir. Bu terim Prause ve diğerlerinde, finansallaşma bağlamında dijital teknolojilerin alabileceği bir form olarak Gruin (2019)'den alınarak kullanılmıştır. (2021, s.648) Ancak genel olarak düşünüldüğünde tarımsal faaliyete ilişkin her dijital sistem; ürün seçimi, ekim zamanı, sulama, gübreleme, pestisit kullanımı, hasat, depolama, fiyatlandırma, kredi tahsisi ve satış zamanı gibi konularda tavsiye veya otomatik karar üretebilmektedir. Algoritmik yönetişim bu nedenle verinin yalnızca saklanması ya da sadece finansal seçilim ile ilgili değildir; tarımsal faaliyetin bütününü ilgilendirir.

Algoritmik sistemlerin hangi amaçlara göre çalışacağı, şirketleşmiş gıda rejiminin ekonomik düzeyi içerisinde belirlenmektedir. Kapitalist üretimin kârlılık ilkesi dolayımında verimliliğin yükseltilmesi, girdi maliyetlerinin azaltılması, işgücü performansının ölçülmesi, riskin hesaplanması, tedarik sürelerinin kısaltılması ve satışların artırılması, algoritmik modellerin başlıca optimizasyon hedefleri olarak ortaya çıkmaktadır. Ekonomik ve kurumsal olarak algoritmaların teknik işleyişi tanımlanmaktadır. Bu tanımlama çerçevesinde örneğin (Prause ve arkadaşlarının değindiği) dijital finans uygulamaları, üreticilerin kredi değerliliğini (psikometrik veriler, çiftlik faaliyetleri ve çevresel koşullara ilişkin veriler üzerinden) hesaplamaktadır (2021, s.648). Böylece krediye erişim, yalnızca banka ile üretici arasında gerçekleştirilen bir değerlendirme olmaktan çıkarak, üreticinin davranışlarını ve çiftlik faaliyetlerini sayısal kategorilere dönüştüren tekno-algoritmik bir süreç hâline gelmektedir.

Algoritmik yönetişimin "dijital Taylorizm" bağlamında emek ve üretim süreçlerinde de ortaya çıkma potansiyeli, vardır. Çiftlik yönetim platformlarında işlerin ölçülmesi, standartlaştırılması ve sürekli gözetim altında tutulması, tarımsal emek üzerinde yeni denetim biçimleri yaratmaktadır. Bu durum da tarımsal emeğin vasıfsızlaşmasına ve yerel tarımsal bilginin ikincilleşmesine yol açabilecek bir tehlike taşımaktadır (Prause ve diğerleri, 2021, s. 649). Çiftçilerin deneyime, yerel ekolojik koşullara ve kuşaklar boyunca aktarılan bilgiye dayanan kararlar, şirketler tarafından geliştirilen veri modellerinin önerileriyle yer değiştikçe algoritma giderek doğrunun tek ve mutlak ölçütü haline gelebilecektir. Atasoy'a göre veriyle yönetişimin giderek artan egemenliğinde algoritmaya atfedilen "ahlaki güven" sayesinde çiftçiler kararlarını bireysel olarak değil, şirketlerin, danışmanların, platformların ve kamusal kurumların oluşturduğu ağlar içerisinde almaktadır (2025, 1299). Bu çerçevede teknik, tarafsız ve siyaset dışı olarak sunulan uzmanlık bilgisinin belirli hedefleri depolitize etmesinin (Atasoy 2025, 1304) algoritmik yönetişimin siyasal ve kurumsal boyutunu güçlendirdiği iddia edilebilir.

Ancak belirtmek gerekir ki algoritmaların tasarlanması, optimizasyonu, koşullanması; hukuki, ekonomik, siyasal ve kurumsal tercihlere bağlıdır. Atasoy algoritmik modellerin büyük veriyi tarafsız biçimde temsil etmediğini; hangi göstergelerin seçileceği, hangi bilgilerin sayısallaştırılacağı ve hangi verilerin model dışında bırakılacağı konusunda seçici olduğunu belirtir (2025, 1297-8). Prause ve arkadaşlarının gösterdiği gibi açık kaynaklı, üreticilerin veri üzerindeki denetimini koruyan veya agro-ekolojik üretimin ihtiyaçlarına göre geliştirilen sistemler farklı yönelimler taşıyabilmektedir. (Prause ve diğerleri, 2021, ss. 650). Algoritmik yönetişimin farklı kurumsal ve teknik düzenlemeler altında farklı etkiler üretebilmesi, dijital teknolojik örgütlenmenin yapısal olarak belirlendiğini; ancak somut teknik biçimlerinin ve sonuçlarının tek, zorunlu ya da kaçınılmaz olmadığını göstermektedir.

Dolayısıyla denilebilir ki tarihsel olarak belirlenen algoritmik yönetişim rejimin yeniden üretilmesi gereği ekonomik zorunluluklar ve politik ideolojik seçimler tarafından belirlenir. Ancak algoritmik sistemler de rejimin bu kendini varedişinde hangi üreticinin krediye erişeceğini, hangi ürünün yetiştirileceğini, ne miktarda girdi kullanılacağını ve emeğin nasıl denetleneceğini yönlendiren maddi bir kapasitesi ile ekonomik yapı dolayımında rejimi koşullar.

Değerlendirme

Verileştirme, platformlaşma ve algoritmik yönetişim, yapısallığın özgüllüğü gereği farklı ülkelerde, ürün zincirlerinde ve kurumsal bağlamlarda farklı yoğunluklarda ortaya çıkabilen özerk unsurların eklemlenmesi olarak düşünülmelidir. Bu unsurlar şirketleşmiş gıda rejiminin ekonomik düzeyi içerisinde işleyen dijital teknolojik örgütlenmenin farklı uğrakları olarak ele alınması gereken ekonomik üretim pratiğinin terimleridir. Bu pratik gereğince bu unsurlar hammaddelerini dönüştürürler. Verileştirme, tarımsal üretim ve gıda dolaşımı içerisindeki faaliyetleri kaydedilebilir, karşılaştırılabilir ve hesaplanabilir veri nesnelerine dönüştürmektedir. Platformlaşma, bu verileri üreten aktörleri, hizmetleri ve ekonomik işlemleri belirli dijital altyapılar içerisinde birbirine bağlamakta ve merkezileştirmektedir. Algoritmik yönetişim ise toplanan verileri sınıflandırma, puanlama, tahmin ve tavsiye üretimi aracılığıyla üretim, finansman, emek ve dolaşım kararlarına dönüştürmektedir.

Verileştirme, platformların işlemesi için gerekli bilgisel kaynağı üretmektedir. Platformlar, farklı çiftliklerden, makinelerden, ticari işlemlerden ve hizmetlerden elde edilen verileri ortak bir altyapıda bir araya getirerek algoritmik değerlendirmeyi mümkün kılmaktadır. Algoritmik sistemler de ürettikleri tavsiyeler, tahminler ve sınıflandırmalar aracılığıyla daha fazla üretim faaliyetinin ölçülmesini ve platform üzerinden yürütülmesini teşvik edebilmektedir. Bu unsurların eklemlenmesiyle dijitalleşme, teknolojik örgütlenmenin ekonomik düzey içerisindeki etkililiğini genişletebilmektedir. Üç sürecin eklemlenmesi, dijital teknolojik örgütlenme ile şirketleşmiş gıda rejimi arasındaki belirlenim ve koşullandırma ilişkisinin somutlaştırılmasını sağlamaktadır. Dijital teknolojik örgütlenme, gıda rejiminin ekonomik düzeyinden bağımsız bir düzey değildir; ekonomik düzey içerisinde oluşan özgül bir bölgedir. Bu bölgenin hangi amaçlara yöneltileceği, hangi aktörlerin denetiminde kurulacağı ve hangi teknik biçimleri alacağı; özel mülkiyet, sermaye birikimi, finansallaşma, şirket yoğunlaşması, fikrî mülkiyet ve küresel meta zincirleri gibi ekonomik ilişkiler tarafından yapılandırılmaktadır. Ekonomik düzey, gıda rejiminin diğer düzeyleriyle eklemlenmiş durumdadır. Bu nedenle dijital teknolojik örgütlenme yalnızca dar anlamdaki ekonomik gereksinimler tarafından belirlenmemektedir. Hukuki düzenlemeler, devlet politikaları, kurumsal standartlar, jeopolitik ilişkiler ve dijitalleşmeye yönelik ideolojik yönelimler de bu örgütlenmeyi üstbelirlemektedir. Bununla birlikte dijital teknolojik örgütlenme, kendisini belirleyen ekonomik ilişkilerin edilgen bir yansıması değildir. Verileştirme, ekonomik faaliyetlerin hangi yönlerinin ölçülebilir ve karşılaştırılabilir hâle geleceğini; platformlaşma, aktörler ve işlemler arasındaki ilişkilerin hangi altyapılar üzerinden yürütüleceğini; algoritmik yönetişim ise üretilen verilerin hangi ölçütlere göre ekonomik kararlara dönüştürüleceğini

düzenlemektedir. Böylece dijital teknolojik örgütlenme, bir bölgesi olduğu ekonomik düzeyin üretim, dolaşım, finansman, bilgi ve denetim ilişkilerinin gerçekleşme biçimini maddi olarak düzenlemektedir. Bir üstbelirlenim olarak düşünülmesi gereken bu düzenlenmişliği sayesinde ekonomik ilişkiler bütünü, kurucu bir terimi olduğu gıda rejiminin koşullayıcısı olarak işlev görür. Gıda rejimi, ekonomik düzeyin yapı içerisindeki konumunu ve tarihsel biçimini belirlemekte; ekonomik düzeyin bu yapılanışı da dijital teknolojik örgütlenmenin kuruluş koşullarını biçimlendirmektedir. Dijital teknolojik örgütlenme ise ekonomik ilişkilerin hangi aygıtlar, veri biçimleri ve koordinasyon mekanizmaları aracılığıyla işleyeceğini düzenlemektedir. Ekonomik düzey gıda rejiminin kurucu bir terimi olduğundan, dijital teknolojik örgütlenmenin ekonomik düzey üzerindeki koşullandırıcı etkisi rejimin bütününün yeniden üretimine dolayımlı olarak katılmaktadır. Dolayısıyla dijital teknolojiler, ne şirketleşmiş gıda rejimini dışarıdan dönüştüren özerk güçlerdir; ne de ekonomik ilişkilerin hiçbir özgül etkililiği bulunmayan basit araçlarıdır.

Sonuç

Tarımsal dijitalleşmeye dair literatürü gıda rejimi yaklaşımı çerçevesinde ele alan bu çalışma, teknolojiyi, rejime dışarıdan etki eden bağımsız bir neden veya ekonomik ilişkilerin edilgen bir sonucu olarak görmeden; gıda rejiminin içinde konumlandırmıştır. Bu doğrultuda gıda rejimi; yapısalcı bağlamda çelişkili bir temel birlik olarak varsayılmıştır. Teknolojik örgütlenme ise bu yapıyla aynı statüde bulunan bağımsız bir düzey olarak değil, üretim, mülkiyet, vb. ilişkiler gibi gıda rejiminin ekonomik düzeyi içerisinde ama ekonomik düzeyi tarihsel olarak kuran özgül bir bölge olarak tasarlanmıştır.

Bu bağlamda yapılan karşılaştırmalı tarihsel analiz göstermektedir ki, doğrusal bir teknik ilerleme güzergahı izlemeyen teknolojik örgütlenme her rejimin özgül birikim, mülkiyet, devletlerarası düzen ve emek ilişkileri içerisinde farklı bir biçim kazanmıştır. Birinci gıda rejiminde ulaştırma, depolama ve mekanikleşme teknolojileri kolonyal-yerleşimci tarım bölgelerini Avrupa sanayi merkezlerine bağlamış; ikinci rejimde mekanikleşme, kimyasallaşma ve Yeşil Devrim teknolojileri devlet destekli ulusal agro-endüstriyel yapıların kuruluşuna katılmıştır. Şirketleşmiş gıda rejiminde ise biyoteknolojik müdahale artmış, fikrî mülkiyet ve dijital altyapılarla eklemlenmiş ve üretim süreçlerinin ulusötesi şirketler tarafından daha yoğun biçimde koordine edilmesinin önü açılmıştır. Bu farklılaşma, teknolojinin rejimlerden bağımsız bir gelişme mantığına sahip olmadığını; rejimsel yapının

teknolojik örgütlenmenin kuruluş koşullarını belirlediğini, kurumsallaşan teknolojik örgütlenmenin de rejimin maddi işleyişini koşullandırdığını ortaya koymaktadır.

Paralel olarak dijital gelişme; şirketleşmiş gıda rejiminin ekonomik düzeyini meydana getiren özel mülkiyet, sermaye yoğunlaşması, finansallaşma, fikrî mülkiyet, şirket egemenliği ve küresel meta zincirlerinden bağımsız değildir. Dijital teknolojilerin hangi problemlere yöneltileceği, kimler tarafından geliştirileceği, verilerin kimlerin denetiminde bulunacağı ve dijital hizmetlerin hangi kurumsal biçimler altında sunulacağı bu ilişkiler içerisinde belirlenmektedir. Bununla birlikte, ekonomik düzey de gıda rejiminin diğer kurucu düzeylerinden bağımsız olmadığı için dijital teknolojik örgütlenme, hukuk, devlet politikaları, düzenleyici standartlar, ideolojik söylemler ve jeopolitik ilişkiler tarafından da belirlenmektedir.

Çalışmada dijital teknolojik örgütlenmenin işleyişi verileştirme, platformlaşma ve algoritmik yönetişim olmak üzere birbiriyle bağlantılı üç unsur/süreç üzerinden incelenmiştir. Bu unsurlar bir altyapılaşma mantığı içinde farklı bağlamlarda farklı biçimlerde eklemlenebilen analitik uğraklar olarak düşünülmelidir. Verileştirme, tarımsal faaliyetleri kaydedilebilir ve hesaplanabilir veri nesnelerine dönüştürmektedir. Platformlaşma, aktörleri, hizmetleri, verileri ve ekonomik işlemleri belirli dijital altyapılar içerisinde bir araya getirmektedir. Algoritmik yönetişim ise toplanan verileri üretim, finansman, emek ve dolaşım kararlarını yönlendiren sınıflandırma, tahmin, puanlama ve tavsiye araçlarına dönüştürmektedir.

Üç süreçli ayrımın temel işlevi, gıda rejimi ile dijital teknolojik örgütlenme arasındaki belirlenim–koşullandırma ilişkisini somutlaştırmaktır. Şirketleşmiş gıda rejimi ekonomik ilişkilerde var olurken, bu varoluş verileştirme, platformlaşma ve algoritmik yönetişim unsurları ile koşullanmaktadır. Ekonomik düzeyi belirleyen bağımsız bir neden olmayan dijital teknolojik örgütlenme bu yolla üretim, dolaşım, finansman, bilgi ve denetim ilişkilerinin işleyişini düzenleyen maddi bir kapasiteye sahiptir. Ekonomik düzeyin gıda rejiminin kurucu bir terimi olması nedeniyle bu koşullandırma, rejimin yeniden üretimine dolaylı olarak katılmaktadır.

Bu yaklaşımla temel amaç, dijitalleşme olgusunu kavrarken hem teknolojiyi mutlak belirleyici olarak sabitleyen teknolojik determinizmden hem de dijital aygıtları yalnızca sermayenin önceden kurulmuş amaçlarını uygulayan etkisiz araçlar olarak değerlendiren teknolojik indirgemecilikten uzak bir bakış açısı sunabilmektir. Bu bakış açısı çerçevesinde dijitalleşme (ve tabii teknoloji) bir ilişkisellik biçimi olarak toplumsallığın maddi işleyişine

yerleştirilerek ve onların gerçekleşme imkânlarını ve sınırlarını düzenleyen biçimde kavranmıştır. Bu anlamda teknolojik örgütlenme toplumun yeniden üretilmesinin/örgütlenmesinin bir parçasıdır. Bu yeniden üretimin bir aracı/parçası olarak dijital teknolojiler; özel mülkiyet, şirket yoğunlaşması, finansallaşma ve küresel meta zincirlerine dayalı temel ilişkileri büyük ölçüde sürdürmekte; aynı zamanda veri temellükü, platform denetimi ve algoritmik yönlendirme aracılığıyla bu ilişkilerin işleyiş biçimlerini gıda rejimininin hayatiyetini mümkün kılacak biçimde dönüştürmektedir.

Sonuç olarak teknoloji ile gıda rejimi arasındaki ilişki, iki bağımsız alan arasındaki karşılıklı etkileşim biçiminde değil; yapı, düzey ve bölge bağlantısı üzerinden yapının terimlerinde içkin olarak varoduğu bir metonimi ilişkisi içerisinde kavranmalıdır. Gıda rejimi ekonomik düzeyin tarihsel konumunu belirlemekte; ekonomik düzey içerisindeki dijital teknolojik örgütlenme de bu düzeyin maddi işleyişini düzenleyen bir yapı etkisi olarak rejimin yeniden üretimine katılmaktadır. Bu kavramsallaştırma, dijital tarımı yalnızca yeni araçların yaygınlaşması olarak değil, şirketleşmiş gıda rejiminin ekonomik ilişkilerinin teknik, bilgisel ve örgütsel biçimlerde yeniden düzenlenmesi olarak analiz etmeyi mümkün kılmaktadır.

Kaynakça

Althusser, L., & Balibar, É. (1970). *Reading capital* (B. Brewster, Trans.). New Left Books. (Original work published 1965).

Althusser, L. (1969). *For Marx* (B. Brewster, Trans.). Allen Lane. (Original work published 1965).

Atasoy, Y. (2025). Agriculture by algorithm: Big data, digitalization, and biotechnology under climate change. *Science, Technology, & Human Values, 50*(6), 1291–1333. https://doi.org/10.1177/01622439251321233

Aysu, A. (2005). Kırsal politika için yol haritası. In F. Özlüer, S. Yardımcı, & I. Özkaya (Eds.), *Kırda yoksulluk ve direniş: Ekolojik politika kitaplığı 1* (pp. 45–86). Külsanat.

Bronson, K., & Knezevic, I. (2016). Big data in food and agriculture. *Big Data & Society, 3*(1), 1–5. https://doi.org/10.1177/2053951716648174

Burch, D., & Lawrence, G. (2009). Towards a third food regime: Behind the transformation. *Agriculture and Human Values, 26*, 267–279.

Carolan, M. (2020). Acting like an algorithm: Digital farming platforms and the trajectories they (need not) lock-in. *Agriculture and Human Values, 37*(4), 1041–1053. https://doi.org/10.1007/s10460-020-10032-w

Çakan, E., & Erol, M. (2008). *Abdullah Aysu ile tarımın gidişatı üzerine: Şirketlere karşı bilge tarım*. Panel STGM. http://panel.stgm.org.tr/vera/app/var/files/s/i/sirketlere-karsi-bilge-tarim-abdullah-aysu-soylesisi.pdf

Çaşkurlu, S. (2012). Küresel gıda krizi: Üçüncü gıda rejimi, küresel sermaye ve gelişmekte olan ülkeler. *Ekonomik Yaklaşım, 23*(Special), 161–194.

Dünya 11 milyar insanı besleyebilir mi? (2019, 6 Haziran). *BBC News Türkçe*. https://www.bbc.com/turkce/haberler-dunya-48537255

Erbaş, H. (2017). Tarım-gıda etiği/politikası ve geleceğimiz: Ekonomi-politik ve ötesi sosyolojik bir çerçeve. *Türkiye Biyoetik Dergisi, 4*(1), 14–28.

Fraser, A. (2019). Land grab/data grab: Precision agriculture and its new horizons. *The Journal of Peasant Studies, 46*(5), 893–912. https://doi.org/10.1080/03066150.2017.1415887

Friedmann, H. (2005). From colonialism to green capitalism: Social movements and emergence of food regimes. In F. H. Buttel & P. McMichael (Eds.), *New directions in the sociology of global development* (Research in Rural Sociology and Development, Vol. 11, pp. 227–264). Elsevier. https://doi.org/10.1016/S1057-1922(05)11009-9

Friedmann, H., & McMichael, P. (1989). Agriculture and the state system: The rise and decline of national agricultures, 1870 to the present. *Sociologia Ruralis, 29*(2), 93–117. https://doi.org/10.1111/j.1467-9523.1989.tb00360.x

Gruin, J. (2019). Financializing authoritarian capitalism: Chinese fintech and the institutional foundations of algorithmic governance. *Finance and Society, 5*(2), 84–104. https://doi.org/10.2218/finsoc.v5i2.4135

Hobsbawm, E. J. (2007). *Kısa 20. yüzyıl, 1914–1991: Aşırılıklar çağı*. Everest.

Keyder, Ç., & Yenal, Z. (2013). *Bildiğimiz tarımın sonu: Küresel iktidar ve köylülük*. İletişim Yayınları.

Klerkx, L., Jakku, E., & Labarthe, P. (2019). A review of social science on digital agriculture, smart farming and Agriculture 4.0: New contributions and a future research agenda. *NJAS: Wageningen Journal of Life Sciences, 90–91*, Article 100315. https://doi.org/10.1016/j.njas.2019.100315

McMichael, P. (2009). Food regime analysis of the "world food crisis." *Agriculture and Human Values, 26*, 281–295.

McMichael, P. (2013). *Food regimes and agrarian questions*. Fernwood Publishing.

Pechlaner, G., & Otero, G. (2008). The third food regime: Neoliberal globalism and agricultural biotechnology in North America. *Sociologia Ruralis, 48*(4), 351–371. https://doi.org/10.1111/j.1467-9523.2008.00469.x

Prause, L., Hackfort, S., & Lindgren, M. (2021). Digitalization and the third food regime. *Agriculture and Human Values, 38*(3), 641–655. https://doi.org/10.1007/s10460-020-10161-2

Resch, R. P. (1992). *Althusser and the renewal of Marxist social theory*. University of California Press.

Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, M.-J. (2017). Big data in smart farming: A review. *Agricultural Systems, 153*, 69–80. https://doi.org/10.1016/j.agsy.2017.01.023

Yüksel, S.B. (2026). *Althusser'i okumak: Yapısalcı Marksizmin Ontolojisi Hakkında Bir Deneme* [Yayımlanmamış doktora tezi]. Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

OPINIONS / YORUMLAR

CYBER SECURITY IN THE AGE OF ARTIFICIAL INTELLIGENCE

Mehmet Emin ERENDOR*
ORCID ID: 0000-0002-8467-0743

Declaration*

With the acceleration of digitalization, cyberspace has become one of the most important areas of competition between states, economic conflicts of interest and social interactions. Especially when evaluated in the context of the developments in the last 10 years, the increase in the dependence of critical infrastructures on digital networks, the transfer of public services to online platforms and the fact that artificial intelligence (AI)-supported technologies have become an integral part of daily life have revealed that cyber security is not only a technical issue, but rather one of the basic components of national and international security. Today's cyber attacks are no longer considered only as isolated incidents targeting information systems, but also as multidimensional security problems that directly affect economic stability, democratic processes, critical infrastructures and national security strategies of states.

AI has brought about a paradigm shift in the field of cybersecurity in recent years. While rapid advances in machine learning, deep learning, and especially generative AI applications have significantly increased defense capacity in threat detection, anomaly analysis, incident response, and malware analysis, they have also brought new risks such as automating cyberattacks, preparing advanced phishing campaigns, synthetic media production, and rapid exploitation of vulnerabilities. Therefore, AI should be considered not only as a protective technology or a new threat source in terms of cyber security, but also as a dual-use strategic technology that transforms the nature of competition between attack and defense.

However, it would be an incomplete approach to evaluate the impact of AI on cyber security only through technological developments. The real transformation lies in the fact that AI is changing the functioning of the international security environment by increasing the speed, scale, level of autonomy and uncertainties of cyber conflicts. Many cyber operations, which traditionally required high technical expertise, significant financial resources and long preparation processes, can be carried out at lower costs, in less time and on a larger scale

* Prof. Dr. At International Relations, ATÜ, merendor@atu.edu.tr
* The opinions expressed belong to the authors only and do not reflect the official position of the institutions they are affiliated with.

thanks to AI. This situation facilitates the access of not only states but also organized crime organizations, terrorist organizations, private companies and individual actors to advanced cyber capacities, thus reshaping the distribution of cyber power.

In this context, the main issue in the age of AI is not whether the technology will be used in the field of cyber security. The main question is how this technology will be managed in a way that supports international peace and security, in line with which normative principles it will be limited, and with which governance mechanisms will new risks be controlled. The widening gap between the pace of development of technological innovations and the compliance capacity of international law, ethical principles and institutional regulations constitutes one of the most important security problems of today. Therefore, the relationship between AI and cybersecurity should be considered not only as a technical transformation but also as a structural issue that shapes the future of international governance, strategic stability, and global security architecture.

How is AI Changing the Character of Cyber Conflicts?

The transformation in the field of cyber security is often explained through new attack techniques or advanced defense tools. However, the impact of AI is much deeper than adding a new dimension to existing cyber threats. The real change is manifesting in the way cyber conflicts are conducted, in the capacity of the actors and in the nature of strategic calculations. In other words, AI transforms the speed, scale, autonomy and accessibility of existing threats rather than creating an entirely new threat landscape in cyberspace.

In the past, carrying out an advanced cyber operation required high technical expertise, long preparation processes, strong financial resources and qualified human resources. State-sponsored advanced persistent threat groups have therefore been at the top of the cyber power hierarchy for many years. Today, generative AI and large language models significantly facilitate the processes of generating code, analyzing security vulnerabilities, preparing phishing content, and developing malware, even for actors with a certain amount of technical knowledge. This indicates a new trend that can be expressed as the democratization of cyber operations. Of course, AI alone does not create an advanced attack capacity, but it lowers the barriers to entry by reducing the need for technical knowledge and makes it possible for a wider group of actors to access advanced cyber tools.

This transformation not only increases the diversity of actors, but also radically changes the pace of cyber operations. AI-powered systems can analyze network traffic in real-time, automatically detect security vulnerabilities, and manage attack or defense processes without human intervention under certain conditions. Thus, the time between decision-making and implementation is getting shorter and shorter, and interactions that take place in seconds or even milliseconds push the limits of human control. This increases the risk of false alarms, erroneous judgments or involuntary escalation, especially in times of crisis. In this new environment where speed gains strategic importance, the capacity of decision-makers to evaluate events and develop appropriate reactions is gradually narrowing.

Another element that AI is transforming is the scale of cyber operations. While phishing attacks carried out with traditional methods are prepared for a certain number of targets, generative AI can produce messages that can be sent to millions of people in a short time, grammatically correct and tailored to the target. Similarly, synthetic audio and video technologies increase the persuasiveness of social engineering attacks and make disinformation campaigns aimed at manipulating public opinion more effective. Therefore, AI strengthens not only attacks targeting technical systems but also cognitive security threats centered on the human factor. This development demonstrates that cybersecurity is no longer merely a matter of safeguarding networks and information systems, necessitating a broader understanding of security that encompasses the preservation of the information ecosystem and societal trust.

However, the impact of AI is not limited to its attack capacity alone. The same technologies also provide significant advantages in the field of defense. Analyzing large datasets, detecting anomalous network behavior, processing threat intelligence, and automating incident response processes allow defenders to achieve significant gains in speed and accuracy. Especially in the protection of critical infrastructures, AI-supported early warning systems can identify patterns that human operators may have difficulty noticing and enable faster reactions to possible attacks.

Yet, this does not mean that there is a definite superiority between attackers and defenders. On the contrary, AI emerges as a technology that constantly increases the tempo of competition instead of making one of the parties permanently advantageous. As defense systems become stronger with AI, attackers develop more complex and adaptable methods using the same technology. Thus, a constantly renewed and accelerating technological

competition cycle is formed in the field of cyber security. This cycle dictates that security can no longer be achieved through static measures, necessitating defense approaches that continuously learn, adapt, and innovate.

As a result, the most important impact of AI on cyber security is not that it gives the offensive or defense side an absolute superiority. The real transformation lies in changing the strategic logic of cyber conflicts. The fact that operations are becoming faster, more autonomous, more scalable and more uncertain raises new questions in a wide range of areas, from threat perceptions of states to crisis management, from deterrence strategies to international cooperation mechanisms. Therefore, understanding the impact of AI on cybersecurity requires not only following technological developments but also analyzing how these developments are reshaping the international security order.

Governance Gap, Attribution Problem, and the Future of Cyber Deterrence

The effects of AI in the field of cyber security are often evaluated through the increase in technical capacity. However, the real importance of this technology in terms of international security stems from the difficulty of existing governance mechanisms in adapting to the new dynamics created by AI-supported cyber operations. In other words, the main problem we face today is not the technological progress itself, but the inability of the legal, institutional and normative framework to regulate this progress to develop at the same pace. This situation creates a "governance gap" that is getting deeper.

Cyberspace is an environment that inherently extends beyond national borders and in which numerous non-state actors operate. AI makes this structure even more complex. Today, not only governments but also technology companies, organized crime organizations, private security firms, open source developer communities, and individual actors can access AI-based tools and use them for different purposes. In such an environment, it is becoming increasingly difficult to ensure security only with state-centered approaches. Cybersecurity is no longer just a military or technical issue, but a multidimensional security area at the intersection of public policy, international law, private sector management, and digital governance.

One of the most important consequences of AI-supported cyber operations is that it further complicates the citation problem, which has been one of the main problems of cyber security literature for many years. It is already technically and politically difficult to determine the exact identity of the attacker in cyber attacks. Attacks are routed through servers located in

different countries, using third-party infrastructure, or conducted through proxy actors, making it difficult to determine responsibility. AI takes this uncertainty to a new level. Adaptive malware, attack systems that can make automatic decisions, and algorithms that can generate synthetic digital traces can make it possible to deliberately hide the source of the attack or produce false evidence that makes different actors look guilty. This situation directly affects not only technical analysis processes but also political decision-making mechanisms.

The deepening of the citation problem has important consequences in terms of cyber deterrence. The classical understanding of deterrence is based on the ability to identify the potential attacker, increase the cost of the attack, and provide a reliable response when necessary. Yet, when there is a high level of uncertainty about the perpetrator of the attack, the credibility of the threat of retaliation weakens and the deterrence mechanism loses its effectiveness. The speed, automation, and anonymity provided by AI-powered cyber operations make this issue even more pronounced. States are often forced to make political decisions without being able to definitively identify the actor behind the attack, which can lead to either unnecessarily harsh reactions or passive approaches that weaken deterrence.

More importantly, the increasing use of AI in decision support systems poses new risks in terms of crisis management. Today, many governments use AI-based analysis systems in the detection, prioritization and evaluation processes of cyber threats. Although these systems are capable of processing large amounts of data in a short amount of time, algorithmic errors, incomplete data sets, or deliberate manipulations can result in inaccurate threat assessments. Especially in times of international crisis, the unquestioned acceptance of an erroneous warning generated by AI by human decision-makers can increase the risk of miscalculation. In such a scenario, the issue is not merely a technical error but a vulnerability that could directly impact strategic stability.

For this reason, cyber security discussions in the age of AI cannot be carried out only on attack and defense capacity. The real issue is how to develop the institutional and normative capacity to manage the effects of AI on the international security architecture. Today, although the rules of international law regulating the behavior of states, norm development studies carried out within the United Nations, and various regional initiatives are important steps, they are far from comprehensively solving the problems posed by AI-supported cyber operations. In particular, issues such as algorithmic responsibility, accountability of AI

systems, the limits of autonomous cyber operations, and the role of the private sector in international security remain significantly unclear.

Therefore, maintaining strategic stability in the age of AI is not only possible by developing more advanced defense technologies. At the same time, it is necessary to strengthen confidence-building measures between states, establish common norms, develop information sharing mechanisms, and institutionalize multi-stakeholder governance models involving the private sector. Otherwise, the gap between technological developments and governance capacity will gradually widen, which will deepen the uncertainty in cyberspace instead of reducing it. The main challenge faced in the age of AI-supported cyber security is not to achieve technological superiority, but to manage technological transformation with common rules and institutions that will support international stability.

The Future of Cybersecurity in the Age of AI: Bridging the Governance Gap

While AI-powered cybersecurity discussions focus on the pace of technological innovations, they often push the institutional and political consequences of this transformation to the background. However, the factor that will be decisive in terms of international security is not how much AI will develop, but within the framework of which rules, principles and governance mechanisms this technology will be used. The main problem experienced today is that technological capacity has surpassed international governance capacity. Therefore, the top priority of the coming period is to develop an inclusive and applicable governance framework that will reduce the risks posed by AI-powered cyber operations.

The first element of such a framework is the updating of international norms. While the principles developed to date regarding responsible state behavior in cyberspace provide an important foundation, they fall short of covering new problem areas such as the autonomy of AI-powered systems, algorithmic decision-making processes, and synthetic content generation. In particular, clearer international principles need to be developed regarding the conditions under which states will assume responsibility in AI-based cyber operations, the legal nature of AI-supported decisions, and the limits of autonomous attacks on critical infrastructure. In this context, rather than a new and comprehensive international treaty, updating the existing normative framework according to the needs of the AI age seems to be a more realistic and feasible approach.

Secondly, it is inevitable to strengthen the understanding of multi-stakeholder governance. Technology companies, cloud service providers, cybersecurity firms, and open-source software communities play critical roles in the development and operation of AI technologies. Therefore, the future of cyber security cannot be shaped solely by diplomatic negotiations between states. Multi-stakeholder mechanisms that increase information sharing between public institutions, the private sector, academia and civil society, develop common standards and ensure coordination in times of crisis will be one of the basic elements of security in the age of AI.

Third, the international community needs to expand confidence-building measures to include the AI dimension. Communication channels and crisis management mechanisms similar to those developed in the nuclear field during the Cold War are becoming increasingly important for cyberspace. Especially considering the potential of AI-powered cyber operations to lead to misunderstandings, misattribution, or involuntary escalation, communication channels that enable rapid information sharing between states, joint white review processes, and crisis management protocols can contribute to maintaining strategic stability.

In addition, the security of AI systems should become an integral part of cybersecurity discussions. While today's attention is largely focused on how AI is used in cybersecurity, AI systems themselves are exposed to various cyber threats, including data poisoning, model manipulation, prompt injection, and model theft. For this reason, in the future, the "cyber security of AI" approach will become one of the basic components of national security strategies as well as "cyber security with AI".

Lastly, policymakers need to adopt a balanced approach between technological optimism and security concerns. AI is an important technology that, when used correctly, strengthens cyber defenses, increases the resilience of critical infrastructures, and enables public institutions to respond faster to threats. However, the same technology can increase the impact of cyberattacks, make disinformation more convincing, and complicate the management of international crises if adequate control mechanisms are not established. Therefore, the main purpose of security policies should not be to limit the use of AI, but to ensure that this use takes place in accordance with the principles of transparency, accountability, human control and international law.

Conclusion

AI is not only a technology that develops new tools in the field of cybersecurity but is also at the cent**re** of a structural transformation that is reshaping the functioning of international security, the distribution of power and the dynamics of strategic stability. The most distinctive feature of this transformation is that it makes cyber operations faster, more scalable, and more autonomous, while at the same time increasing uncertainty. In particular, the deepening of the attribution problem, the increasing influence of algorithmic systems in decision-making processes, and the ease of access to advanced AI tools by non-state actors necessitate a re-evaluation of existing security approaches.

The biggest challenge posed by AI for international security is not the technology itself, but the growing mismatch between technology and governance capacity. In other words, the main problem of today is not a "technology gap", but a "governance gap". If this gap cannot be closed, AI may become a factor that increases strategic uncertainty and weakens international stability, rather than a tool that strengthens cybersecurity.

Therefore, success in the age of AI will be possible not only by producing more advanced algorithms, but also by developing common norms that will guide the use of these algorithms, strengthening international cooperation, and integrating technological innovations with a governance approach that prioritizes human safety. The future of cyberspace will largely depend on the ability of the international community to manage this capacity within the framework of common rules and shared responsibility, rather than the technical capacity of AI.

DIGITAL IDENTITY AND STATE OF CITIZENS' PRIVACY IN PAKISTAN

Fahad NABEL[*]
ORCID ID: 0000-0003-1446-2399

Declaration[*]

In March this year, the National Database and Registration Authority (NADRA), which is responsible for regulating government databases in Pakistan and managing the registration records of the citizens, clarified that the digital national identity card has the same legal status as the physical identity card (Radio Pakistan, 2026). The digital identity card is seen as a sign of modernisation. However, in Pakistan, data breaches continue to occur periodically. The absence of a comprehensive personal data protection law further compounds the situation. This opinion piece explains how the Pakistani government's gradual adoption of digital authoritarian practices is converting the digital identity infrastructure into a political architecture of visibility.

The Constitution of Pakistan recognises the right to privacy as a fundamental right under Article 14(1). The text refers to the privacy of the home. However, legal judgments in Pakistan have made it clear that 'home' should not be taken in the literal sense (Amin & Hassan, n.d.). Therefore, the concept of the right to privacy under the Constitution has been broadened to places beyond the home where a person is presumed to be free from invasion. However, the right to privacy under the Constitution is not an absolute right. Various court judgements have given a specific and limited interpretation to the phrase "subject to law" as mentioned alongside the right to privacy under Article 14(1).

In Pakistan, there are primarily four stakeholders who are directly related to the privacy of citizens in one way or another. The four stakeholders are state actors, local firms, the public, and foreign actors. The government is considered the most important stakeholder in ensuring citizens' privacy owing to its political dominance. It is also the principal driving force in promoting policy and legal developments regarding citizens' privacy. By possessing the main decision-making power, the government controls the pace of policy and law implementation. Therefore, the government is primarily responsible for formulating personal data protection law to protect citizens' privacy.

[*] Fahad Nabeel is the Chief Executive Officer of Geopolitical Insights, a Pakistan-based research consultancy firm. fahadnabeelfn@gmail.com.
[*] Artificial intelligence (AI) was not used in this study. All responsibility rests with the author.

Local firms are also considered stakeholders in safeguarding citizens' privacy. The local firms primarily focus on economic growth using digital means. However, it has limited influence compared to foreign firms in shaping the policy or legal measures the government takes to protect citizens' privacy. On the other hand, foreign forces generally consist of governments, corporations, non-governmental organisations, civil society, and influential individuals. EU officials have highlighted the importance to regulating digital spaces in Pakistan by ensuring the right to privacy and other human rights (European External Action Service, 2021). The US Chamber of Commerce have commented on Pakistan's latest personal data protection bill by objecting to provisions affecting data transfers, localisation, government access, and business compliance. Digital rights organisations and other foreign entities regularly offer their perspectives on Pakistan's approach towards formulation of personal data protection and securing citizens' privacy and remind Pakistani officials of their international commitments to rights to privacy and other fundamental rights coupled with the right to privacy.

The public is the fourth major stakeholder and the weakest one. The public is relatively powerless in influencing the setting of the legislative agenda. The absence of a personal data protection law in the country means that citizens have no legal protection if their personal data is unlawfully processed or breached. There is generally a limited understanding of privacy and personal data protection awareness among the public. Likewise, there is no prominent influencing actor, either in legacy or social media, who talks about personal data rights protection. People have generally come to know of the importance of privacy and personal data protection through news coverage of data breaches. Local digital rights organisations and civil society regularly highlighted the issues in Pakistan's proposed data protection framework and how it is inconsistent with Pakistan's commitments to the right to privacy under the international human rights regime (Digital Rights Foundation, 2023).

According to Surfshark, Pakistan currently ranks 48th globally in the ranking of global personal data breaches. Since 2004, more than 28.2 million email accounts have been breached, and nearly 83 million data points, e.g., full names, genders, etc., have also been compromised. There is a 103 per cent increase in the first quarter of this year compared with the last quarter of 2025. This indicates the urgency that needs to be demonstrated to protect the personal data of Pakistani citizens. Personal data breaches, occurring periodically, contribute to a surge in cybercrime across the country. Last year alone, more than 150,000 cybercrime-related complaints were made, and citizens suffered financial losses of about Rs. 2.7 billion (about US$9.7 million). Every third educated Pakistani has become a victim of

cybercrime. Educated Pakistanis are observed to have mainly become victims of hacking, cyber bullying, and cyber harassment. 58 per cent educated Pakistanis believed that the state should be involved in surveilling every citizen for social security. However, 72 per cent educated Pakistanis are not in favour of state authorities having unfettered access to citizens' data.

In the past two decades, five personal data protection bills have been prepared. The first such attempt was made in 2005 when a bill was prepared. However, the bill was never tabled in parliament, and no reason was given for not doing so. Some believe that the draft was too weak (Digital Rights Foundation, 2020). After 13 years, another similar effort was made in the form of the 'Personal Data Protection Bill 2018'(Ministry of Information Technology and Telecommunication, 2018). However, the bill was largely plagiarised from the Malaysian Personal Data Protection Act 2010 (Personal Data Protection Act 2010, 2010). Revised bills were presented again in 2020 (Ministry of Information Technology and Telecommunication [MoITT], 2020) and 2021 (National Telecom Computer Emergency Response Team, 2021). The latest bill draft was presented in 2023 (Ministry of Information Technology and Telecommunication, 2023) and continues to remain under discussion for parliamentary approval. The recently released 'Data Governance Policy 2026' draft does not give a timeframe for when a personal data protection law will be introduced. While a comparative analysis of personal data protection bills is beyond the scope of this piece, it is important to note that, from the 2021 bill onwards, the proposed data protection law's relationship with other laws is of a 'bare minimum' standard. In other words, if there exists another applicable law on the subject, then the provisions with the stricter impact shall prevail.

Pakistan's journey towards a proposed personal data protection law is largely rooted in its colonial past. The framing of privacy in various personal data protection bills is largely inspired by the Government of India Act, 1935. Under the 1935 Act, the colonial state was entitled to keep its intelligence, deliberations, and records confidential. At the same time, the citizens were given no right to protection from state information-gathering or surveillance (Government of India Act, 1935). Beyond the 1935 Act, Pakistan's approach to a proposed personal data protection law has a colonial genealogy and draws inspiration from various other colonial-era laws.

The current data protection bill draft reveals that it will substantially elevate the level of personal data protection by laying out a basic regulatory framework with only minimally

acceptable enforceability, primarily driven by national security concerns and the needs of digital economic growth. However, the state prefers a lenient personal data protection strategy, as it remains the leading power in regulating personal data protection. It will continue to treat 'national security' as a paramount priority.

References

Amin, M. H., & Hassan, M. (n.d.). *Digital privacy in Pakistan: Ending the era of self-regulation*. Shaikh Ahmad Hassan School of Law, Lahore University of Management Sciences. https://sahsol.lums.edu.pk/node/17036

Digital Rights Foundation. (2020, May 5). *Personal data protection bill 2020: Civil society submission to the Ministry of Information Technology and Telecommunications*. https://digitalrightsfoundation.pk/wp-content/uploads/2020/05/PDPB-2020_-Final-Analysis_05.05.2020-1.pdf

Digital Rights Foundation. (2023, July 18). *Analysis: Personal data protection bill 2023*. https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf

European External Action Service. (2021, February 12). *Press release: European Union hosts webinar to explore the economic potential of digitalisation*. https://www.eeas.europa.eu/delegations/pakistan/press-release-european-union-hosts-webinar-explore-economic-potential-digitalisation_en

Government of India Act 1935, 26 Geo. 5 & 1 Edw. 8 c. 2 (UK). https://www.legislation.gov.uk/ukpga/1935/2/pdfs/ukpga_19350002_en.pdf

Ministry of Information Technology and Telecommunication. (2018, July). *Personal data protection bill 2018*. https://moitt.gov.pk/SiteImage/Legislations/PERSONAL-DATA-PROTECTION-BILL-July-18-Draft.pdf

Ministry of Information Technology and Telecommunication. (2020, April 9). *Personal data protection bill 2020*. https://moitt.gov.pk/SiteImage/Legislations/Personal%20Data%20Protection%20Bill%202020.pdf

National Telecom Computer Emergency Response Team. (2021, August 25). *Personal data protection bill 2021*. https://ntcert.pta.gov.pk/sops/Personal_Data_Protection_Bill_2021.pdf

Personal Data Protection Act 2010 (Act 709) (Malaysia). https://www.investmalaysia.gov.my/media/3x4fsqum/personal-data-protection-act-2010.pdf

Radio Pakistan. (2026, March 13). *Digital CNIC legally equivalent to physical CNIC: NADRA*. https://radio.gov.pk/13-03-2026/digital-cnic-legally-equivalent-to-physical-cnic

GELENEKSEL İSTİHBARATIN SINIRINDA SİBER OPERASYONLAR: MOSSAD'IN HİZBULLAH'A YÖNELİK ÇAĞRI CİHAZI SALDIRISI

Necati YILDIZ[*]

ORCID ID: 0009-0005-6023-396X

Declaration[*]

Özet

Bu çalışma, geleneksel istihbarat yöntemleri ile siber operasyonlar arasındaki etkileşimi incelemeyi amaçlamakta olup, temel araştırma sorusuna odaklanmaktadır: Fiziksel ve dijital unsurları bünyesinde barındıran hibrit siber operasyonlar, geleneksel istihbarat uygulamalarını ne ölçüde dönüştürmekte ve bu dönüşüm uluslararası güvenlik dinamiklerini nasıl yeniden şekillendirmektedir? Bu soruyu yanıtlamak üzere çalışmada, nitel vaka analizi yöntemi benimsenmiş; Mossad'ın Hizbullah'a yönelik gerçekleştirdiği çağrı cihazı saldırısı, açık kaynak istihbaratı (OSINT) verileri, güvenlik raporları ve ilgili akademik çalışmalar çerçevesinde incelenmiştir. Analiz sonucunda ulaşılan temel bulgu, siber operasyonların artık yalnızca istihbarat toplama veya elektronik gözetleme aracı olmaktan çıktığı; tedarik zinciri zafiyetlerinin istihbarat örgütleri tarafından operasyonel bir silah olarak kullanılmasıyla, doğrudan fiziksel ve stratejik sonuçlar doğuran bir güç unsuru haline geldiği incelenmektedir. Çalışmanın özgün katkısı ise, çağrı cihazı saldırısını yalnızca teknik bir vaka olarak ele almanın ötesinde hem geleneksel istihbaratın hem de siber operasyonların hibrit model olarak bütünleştirilmiş bir yapı haline geldiğini analiz etmektedir. Bu bağlamda çalışma, siber operasyonlar ile geleneksel istihbaratın kesişiminde ortaya çıkan ikilemler ve stratejik belirsizlikler tartışarak, gelecekteki araştırmalar için kavramsal zemin hazırlamayı hedeflemektedir.

Anahtar Kelimeler: Geleneksel İstihbarat, Siber Operasyonlar, Mossad, Hizbullah, Güvenlik Dinamikleri, Çağrı Cihazı Saldırısı

[*] Adana Alparslan Türkeş Bilim ve Teknoloji Üniversitesi Lisanüstü Eğitim Enstitüsü Uluslararası İlişkiler Anabilim Dalı Yüksek Lisans Öğrencisi. nctyldzz@gmail.com

[*] Bu çalışmanın hazırlanma sürecinde, ilgili literatürün taranması ve potansiyel kaynakların tespit edilmesi aşamasında yapay zekâ destekli bir dil modelinden (Claude, Anthropic) faydalanılmıştır. Bütün sorumluluk yazarın kendisine aittir.

Abstract

This study aims to conduct an in-depth examination of the interaction between traditional intelligence methods and cyber operations, focusing on the following central research question: To what extent are hybrid cyber operations which incorporate both physical and digital elements—transforming traditional intelligence practices, and how is this transformation reshaping international security dynamics? To answer this question, the study employs a qualitative case study methodology; the Mossad's pager attack against Hezbollah was examined within a comprehensive framework through a critical discourse analysis of open-source intelligence (OSINT) data, security reports, and relevant literature. The key finding resulting from the analysis is that cyber operations have moved beyond serving merely as tools for intelligence gathering or electronic surveillance; by exploiting supply chain vulnerabilities as an operational weapon, they have become a power factor that directly produces physical and strategic consequences. The study's original contribution lies in analyzing how, beyond treating the pager attack merely as a technical case, both traditional intelligence and cyber operations have merged into an integrated hybrid model. In this context, the study aims to lay the groundwork—both conceptual and methodological for future research by discussing the dilemmas and strategic uncertainties that arise at the intersection of cyber operations and traditional intelligence.

Keywords: Traditional Intelligence, Cyber Operations, Mossad, Hezbollah, Security Dynamics, Pager Attack.

Giriş

Geleneksel istihbarat, bilgi toplama ve düşmanın faaliyetlerini önceden tespit etme faaliyetleridir. Bu nedenle istihbarat örgütleri uzun zamandır gizli ve doğrudan insan kaynakları yahut teknik yöntemlerle operasyonlar yapmaktadır (Lowenthal M. M., 2020). Fakat teknoloji hızla gelişirken, siber alanlar yeni bir operasyon bölgesi olmaya başlamıştır. Siber operasyonlar; bilgiye erişim, veri değişikliği, iletişim kesintisi gibi amaçlarla yapılmaktadır. Bunlar, geleneksel yöntemlere göre daha ucuzdur, daha az fiziksel tehlike barındırır ve daha gizli şekilde gerçekleştirilebilir. Bu durum, istihbarat faaliyetlerini genişletmiş ve operasyonların şeklini değiştirmiştir. Ayrıca, istihbarattaki bu değişim, kamu ve özel sektör arasındaki iş birliklerinin artmasına da neden olmuştur (Daricili & Erendor, 2021). Bu iş birlikleri, kaynakların daha verimli kullanılmasını ve siber tehditlere karşı daha

etkili önlemler alınmasını sağlamaktadır. Yeni yaklaşımlar, istihbarat toplama süreçlerini dönüştürmekte ve siber alanlarda daha fazla veri analizi yapılmasına olanak tanımaktadır.

Siber istihbarat operasyonlarının geleneksel istihbarattan farkı, fiziksel müdahale yerine dijital müdahale ve manipülasyonların tercih edilmesidir. Ayrıca, siber ortamlar genişleme ve anonimlik açısından avantaj sağlamakta; bu da operasyonların kim tarafından gerçekleştirildiğini tespit etmeyi zorlaştırmaktadır. Ancak, bu yeni ortam aynı zamanda uluslararası hukuk ve etik kurallar açısından çeşitli tartışmaları da beraberinde getirmektedir. Geleneksel istihbarat yöntemleri genellikle açıkça tanımlanabilir sınırlar ve kurallar çerçevesinde yürütülürken, siber operasyonlar bu sınırların ötesine geçerek etik ve hukuki kuralların sorgulanmasına neden olmaktadır (Cohen, 2024).

Buna karşılık, geleneksel yöntemlerin sınırları karmaşık ve erişim güçlüğü arz eden hedeflerde yetersiz kalabilmekte olup, siber operasyonlar bu noktada önemli bir alternatif olarak görülmektedir. Dolayısıyla hem geleneksel hem de siber istihbarat faaliyetleri, ulusal güvenlik politikalarının vazgeçilmez unsurları haline gelmiş, birbirleriyle etkileşimi ve sınırları sürekli olarak yeniden tanımlanmıştır (Lowenthal M. M., 2016). Bu süreçte teknolojik altyapıya ve hukuki çerçeveye uygun hareket etmek, operasyonların başarıyla sonuçlanması açısından önem arz etmektedir.

Araştıma sorusunda belirtildiği üzere hibrit siber saldırılar, geleneksel istihbarat metodlarını değiştirmektedir. Fakat bu tamamen yeni teknolojiler geleneksel istihbaratın yerini almış demek değildir. Çağrı cihazı saldırılarında, insan istihbaratı, karşı istihbarat, paravan şirketler, tedarik zincirine sızma, teknik mühendislik ve uzaktan tetikleme tek bir operasyon içinde bütünleşmiştir.

Çalışmada, nitel vaka analizi yöntemi benimsenmiştir. Örnek olay olarak, Mossad'ın Hizbullah'a yönelik gerçekleştirdiği çağrı cihazı saldırısı seçilmiştir. Bu vakanın tercih edilmesinin nedeni, siber müdahale ile fiziksel sonuç arasındaki doğrudan bağı en çarpıcı şekilde sergileyen yakın dönem istihbarat operasyonu olmasıdır. Veri toplama sürecinde açık kaynak istihbaratı (OSINT) verileri, akademik çalışmalar ve uluslararası güvenlik raporları kullanılmıştır.

Bu çalışma, mevcut literatürden farklı olarak, siber operasyonları sadece bir araç olarak değil, geleneksel istihbaratın ayrılmaz parçası olarak kabul etmekte ve çağrı cihazı saldırısı özelinde siber istihbarat operasyonlarının kavramsal çerçevesini istihbarat disiplinine kazandırmayı

hedeflemektedir. Çalışmanın özgün katkısı, bu tür hibrit saldırıların sadece teknik bir müdahale değil; aynı zamanda geleneksel istihbaratın gizlilik, güvenilirlik ve istihbarat döngüsü aşamalarını nasıl yeniden tanımladığını sistematik olarak ortaya koymasıdır. Böylece, gelecekteki akademik çalışmalara siber istihbarat faaliyetlerinin değerlendirilebilmesine katkı sağlamayı amaçlamaktadır.

Geleneksel İstihbarat ve Siber İstihbaratın Etkileşimi ile Farklılıkları

Modern çatışma ortamında istihbarat disiplini, jeopolitik rekabetin evrimiyle birlikte yapısal bir dönüşüm geçirmektedir. Tarihsel olarak şekillenen geleneksel istihbarat, ulusal güvenliği tehdit eden unsurları tespit etmek için insan istihbaratı (HUMINT), sinyal istihbaratı (SIGINT) ve coğrafi istihbarat (GEOINT) gibi belirli fiziksel ve beşeri kanallara dayanmaktadır (Troy Mattern, 2014). Geleneksel istihbarat faaliyetleri genellikle sınırlı insani ve teknik araçlar kullanarak belirli bölgesel veya ulusal tehditleri tespit etmek ve karşı önlemler geliştirmek amacıyla yürütülmektedir. Bu yöntemler, uzun yıllara dayanan güvenlik geleneklerine dayanmakta olup, genellikle somut istihbarat toplama, insan kaynağıyla operasyonlar ve teknik izleme gibi temel unsurlara odaklanmaktadır (Johnson, 2010).

Siber istihbarat ise modern teknolojinin sunduğu dijital altyapıyı kullanarak gizlilik ve hızlılık avantajı sağlamaktadır (Gioe, 2020). Siber alan, geleneksel yöntemlere kıyasla daha geniş çaplı ve karmaşık tehditleri tespit edip engellemeye imkan tanımakta olup, operasyonların sanal ortamlarda yürütülmesi, fiziksel sınırların ötesine geçme esnekliği sunmaktadır. Geleneksel ve siber istihbarat arasındaki temel farklardan biri, siberin bir “amaç” mı yoksa “araç” mı olduğu tartışmasında yatmaktadır. Mark Lowenthal’a (2020) göre siber, başlı başına yeni bir istihbarat disiplini (INT) değil; tıpkı uydular gibi çeşitli istihbarat türlerini mümkün kılan ve bütün toplama disiplinlerinin ortak paydası olan bir teknolojidir (Austin, 2025).

Bu iki alan arasındaki temel farklar, uygulama biçimleri ve araç setleriyle ilişkilidir. Geleneksel istihbarat genellikle fiziki takip ve iletişim dinleme gibi yöntemlerle çalışırken, siber operasyonlar dijital izleri kullanır ve çok daha hızlı iletişim ve bilgi akışına olanak sağlar. Ayrıca, siber operasyonlar, genellikle anonimlik ve sızma kabiliyetleriyle öne çıkar; bu da geleneksel istihbarat yöntemlerine kıyasla daha az görünür ve daha az doğrudan müdahale gerektirir (Devanny, 2021). Bu bağlamda, siber alanın doğası, geleneksel istihbaratın sınırlarını aşmasına ve yeni nesil tehditlerle karşı karşıya kalmasına neden olmaktadır (Cunliffe, 2021).

Bununla birlikte, her iki yaklaşımın da amaç ve hedefleri benzerdir; ulusal güvenliği sağlamak, potansiyel tehditleri önceden tespit etmek ve karşı önlemler geliştirmektir (Bonfanti, 2018). Ancak, siber operasyonların hızlı gelişimi ve teknolojik karmaşıklıkları, geleneksel yöntemlerin üstünlüklerini ve sınırlarını yeniden sorgulamaya yol açmaktadır. Bu nedenle, modern güvenlik yapıları, her iki alanın entegrasyonunu ve uyumunu sağlayarak, karşı karşıya kalınan tehditlere karşı daha etkili ve esnek stratejiler geliştirmektedir. Birlikte kullanım hem fiziksel hem de dijital tehdit ortamını kapsayan bütünsel bir güvenlik yaklaşımını mümkün kılmaktadır (Kravetz, 2025).

Mossad ve Hizbullah: Tarihsel Gelişmeler ve Operasyonel Bağlamda Önemli Noktalar

Mossad ve Hizbullah arasındaki ilişki, bölgesel güvenlik dinamikleri ve istihbarat faaliyetleri açısından oldukça karmaşık ve köklüdür (Hazbun, 2026). Mossad, İsrail'in istihbarat kurumu olarak, 1949 yılında kurulduktan sonra, bölgedeki güvenlik çıkarlarını koruma ve tehditleri önleme amacıyla çeşitli operasyonlar yürütmüştür. Mossad'ın özellikle Hizbullah ile olan mücadelesi, tarihsel süreç içinde önemli bir yer tutmaktadır. Hizbullah, Lübnan'da 1980'lerin başında özellikle, 1982 İsrail'in Lübnan'ı işgali sonrası Şii direniş hareketi olarak ortaya çıkmış ve hızla bölgesel etkisini artırarak İran tarafından desteklenen güçlü bir yapı haline gelmiştir. İran'ın direniş ekseni doktrininde önemli yer tutan Hizbullah, İran'ın direniş eksenindeki vekil gücüdür (Gök, 2021). "Direniş Ekseni, İran liderliğindeki devlet ve devlet dışı aktörlerin bir koalisyonudur. ABD, İsrail ve müttefiklerine güçlü bir şekilde karşı çıkan aktörlerden oluşur (Cingöz, 2024)." Bu yapının faaliyetleri, İsrail'in güvenliğine doğrudan tehdit teşkil etmektedir ve bu nedenle Mossad'ın askeri ve istihbarat operasyonları bu bölgede yoğunlaşmıştır.

İki taraf arasındaki ilişkiler, zaman zaman gizli operasyonlar ve karşı saldırılar şeklinde seyretmiş; Mossad, Hizbullah'ın hassas bölgelerine sızmayı ve istihbarat toplamayı amaçlayan çeşitli misyonlar gerçekleştirmiştir (Heavy Nala Estriani, 2023). Zaman içerisinde istihbarat mücadelesi sadece bilgi toplama sınırını aşmış, aynı zamanda teknik operasyonlar ve siber saldırılarla yeni bir boyut kazanmıştır (Bonfanti, 2018). Özellikle, Hizbullah'ın iletişim altyapılarına karşı gerçekleştirilen siber operasyonlar ve özel cihazlar kullanımı, karşılıklı gizli savaşların bir parçası olmuştur (Sobelman, 2025). Bu bağlamda, Mossad'ın bölgedeki faaliyetleri, politik ve askeri hesapların yanı sıra teknolojik gelişmeleri de yakından takip ederek, düşman unsurların iletişim ve komuta süreçlerini bozmak üzere tasarlanmıştır.

Sonuç olarak, Mossad ve Hizbullah arasındaki tarihî ve operasyonel bağlam, bölge güvenliği ve istihbarat taktikleri açısından dikkat çekici bir örnek teşkil etmektedir. Her iki taraf da karşı tarafı zayıflatmak adına çeşitli taktiklere ve teknolojik araçlara başvurmuş, bu da bölgedeki çatışmaların sınırlarını hem fiziksel hem de siber alanlarda genişletmiştir. Bu ilişkiler, geleneksel üslerin ötesine geçerek yeni savaş alanlarını ve teknikleri içermekte olup, bölgedeki güç dengelerine yön vermeye devam etmektedir.

Çağrı Cihazı Saldırısının Teknik Özellikleri

Lübnan'da 2024 yılında yaşanan çağrı cihazı patlamaları, siber-fiziksel güvenlik alanında eşi benzeri görülmemiş bir saldırı olarak değerlendirilmektedir. Bu olay, günlük hayatta kullanılan elektronik cihazların fiziksel birer silaha dönüştürülerek toplumsal paniğe ve ciddi zayiatlara yol açabileceğini göstermiştir. Saldırılar, 17 ve 18 Eylül 2024 tarihlerinde iki dalga halinde gerçekleşmiştir. İlk dalgada Hizbullah üyeleri tarafından kullanılan binlerce çağrı cihazı (pager) eş zamanlı olarak patlatılmış; ertesi gün ise ikinci bir dalgada telsizler ve diğer bazı elektronik cihazlar hedef alınmıştır (AlBadawi, 2025) . Olaylar sonucunda 42 kişi hayatını kaybetmiş, 3500'den fazla kişi yaralanmıştır. (C. Sheng, 2024).

2024 Lübnan saldırılarının operasyonel başarısı, geleneksel siber saldırıların ötesine geçerek donanım ve yazılımın eş zamanlı manipüle edildiği karmaşık bir teknik tasarıma dayanmaktadır (Crypto Museum, 2024). Çalışmanın bu kısmında, Hizbullah tarafından kullanılan Gold Apollo AR-924 model çağrı cihazlarının nasıl birer kinetik silaha dönüştürüldüğü açıklanmaya çalışılacaktır. Çağrı cihazı saldırısının tasarımı ve teknik özellikleri, operasyonun başarıyla gerçekleştirilmesi adına detaylı ve hassas mühendislik çalışmaları gerektirmiştir. Bu tür saldırılar genellikle hedefin iletişim altyapısındaki zayıf noktaları istismar ederek, gizlilik ve sızma kabiliyetlerini artırmayı amaçlar. Saldırıda kullanılan çağrı cihazı, sıradan bir iletişim aracından farklı olarak, özel olarak tasarlanmış ve manipüle edilmiş yazılım ve donanım unsurlarını içermektedir (Cohen, 2024). Saldırıda hedef alınan ana donanım, Tayvan merkezli Gold Apollo firmasının lisansıyla üretilen ancak paravan şirketler (BAC Consulting ve Norta Global) aracılığıyla tedarik zincirine sokulan AR-924 model alfanümerik çağrı cihazlarıdır (Sarker, 2025). Teknik incelemeler, bu cihazların standart donanımının milimetrik bir hassasiyetle modifiye edildiğini ortaya koymuştur:

Batarya Modifikasyonu: Cihazların içerisine yerleştirilen LI-BT783 model özel tasarım lityum-iyon bataryaların katmanları arasına, yaklaşık 3 ila 6 gram miktarında askeri sınıf PETN (Pentaeritritol tetranitrat) patlayıcı dolgusu yerleştirilmiştir (Crypto Museum, 2024).

Fiziksel Gizleme: Patlayıcı düzeneği, standart X-ray taramaları veya görsel denetimlerle fark edilemeyecek şekilde batarya ünitesinin içine ve Koruma Devre Modülü (PCM) ile entegre biçimde gizlenmiştir. PETN gibi plastik patlayıcıların düşük atom numarası, yoğunluk tabanlı tarama sistemlerinde kontrast farkı yaratmayarak tespit edilmesini neredeyse imkansız kılmıştır (Crypto Museum, 2024).

Teknik anlamda, cihazın tasarımında minimal bileşen kullanımı ve yüksek taşınırlık ön plandadır. Çalışma esnasında fark edilme riskini azaltmak adına, düşük güç tüketimi ve sessiz iletişim modları tercih edilmiştir. Ayrıca, saldırıda kullanılan çağrı cihazı, şifrelenmiş ve anlık veri aktarım yeteneklerine sahip olacak şekilde geliştirilmiştir. Aynı zamanda, cihazın uzaktan kontrol edilebilmesi ve güncellenebilmesi, operasyonel esneklik sağlamaktadır (AlBadawi, 2025).

Saldırıda kullanılan cihazların üretiminde yüksek uzmanlık seviyeleri ve özel malzemeler kullanılır. Bu malzemeler, gizlilik ve dayanıklılık açısından yüksek standartlara sahiptir. Ayrıca, iletişim sırasında oluşturulan sinyallerin tespiti ve engellenmesi için anti-dinleme ve anti-tespit mekanizmaları entegre edilmiştir. Bu teknik özellikler, operasyonun ileri düzey elektronik karıştırma ve müdahale teknikleriyle desteklenmesini mümkün kılar (Sarker, 2025). Sonuç olarak, çağrı cihazı saldırısının tasarımı ve teknik bileşenleri, hedef alınan yapıda ciddi hasarlara yol açmıştır. Elektronik cihazların da fiziksel bir silaha dönüşebileceği gerçeği, siber güvenlik ve istihbarat alanında son derece önemli bir gelişme olmuştur.

Çağrı cihazı operasyonu yalnızca bir siber saldırı değildir; insan istihbaratı, hedef analizi, aldatma, tedarik zincirine sızma, donanım manipülasyonu ve fiziksel sabotajın bütünleştiği hibrit bir istihbarat operasyonudur.

Sorunlar ve Sınırlılıklar

Eylül 2024'te Lübnan'da yaşanan çağrı cihazı patlamaları, modern güvenlik anlayışlarının bilgi temellerini ve teknolojik aletlerin özne-nesne ilişkisi içindeki yerini köklü bir biçimde sorgulayan, karmaşık ve çok taraflı bir kriz olarak tanımlanmaktadır. Bu olayı besleyen en derin teknik ve sistemik sorun, küresel üretim sistemlerinin giderek daha fazla modüler hale gelmesi ve coğrafi olarak dağılmış alt yüklenici ağlarına bağlanmasıyla ortaya çıkan tedarik

zincirinde kontrol dengesizliğidir. Çünkü günümüz üretim ortamlarında tasarım, prototip oluşturma, parça tedariki, montaj ve lojistik süreçleri arasındaki neden-sonuç bağı, araya giren çok katmanlı taşeron ilişkileri yüzünden giderek daha belirsiz bir hale gelmekte; bu da kontrol mekanizmalarının etkisizleşmesine ve ulusal güvenlik açısından önemli olan teknolojik ürünlerin bütünlüğünün doğrulanamamasına neden olmaktadır (Buchar, 2024). Bu durum, geleneksel siber güvenlik yaklaşımlarının sadece yazılım tehditlerine odaklanan dar kapsamını aşarak, donanım düzeyinde ve üretim aşamasında önleyici müdahaleyi zorunlu kılan yeni bir güvenlik anlayışının inşasını gündeme getirmektedir.

Operasyonel riskler arasında yanlış hedefleme, siber saldırının yayılması ve beklenmedik sonuçların ortaya çıkması yer alır. Yanlış tespitler, hassas bölgelerde sivil altyapıyı veya masum bireyleri hedef alma riski taşır; bu da hem etik hem de hukuki açıdan ciddi sorunlara yol açar. Ayrıca, siber saldırıların izlerinin kaybolması veya saldırganın kimliğinin tespiti zorluğu, operasyonun sürdürülebilirliğini ve sorumluluğun belirlenmesini güçleştirir (Kravetz, 2025).

Sonuç

Geleneksel istihbarat ve siber operasyonlar arasındaki sınırların belirsizliği, modern güvenlik ortamında yeni bir anlayış gerektirmiştir. Bu bağlamda, teknik ve operasyonel yaklaşımların entegrasyonu, istihbarat toplama ve müdahale süreçlerinde artan bir önem kazanmıştır. Mossad'ın Hizbullah'a karşı yürüttüğü çağrı cihazı saldırısı, bu entegrasyonun somut bir örneğini teşkil etmektedir. Bu operasyon hem geleneksel yöntemlerin hem de siber araçların kullanılmasıyla, bilgi edinme ve karşı tarafın iletişim altyapısını hedef alma açısından yeni standartlar belirlemiştir. Saldırının tasarımında, yüksek hassasiyetli teknikler ve detaylı planlamalar öne çıkarken, operasyonun başarısı risk yönetimi ve uyum konularında dikkatli bir denge kurulmasını zorunlu kılmıştır. Güvenlik önlemleri ve savunma stratejilerinin geliştirilmesi ise, olası saldırıların önünü kesmek ve ulusal çıkarları korumak amacıyla sürekli güncellenen bir süreçtir. Sonuç olarak, geleneksel istihbaratın sınırlarını genişleten ve siber alanın sunduğu imkanları en iyi şekilde kullanan operasyonlar, modern güvenlik paradigmasının temel unsurlarını oluşturmaktadır. Bu gelişmeler hem ulusal hem de uluslararası güvenlik ortamında yeni denge ve dengeli politikaların tesis edilmesine ihtiyaç olduğunu göstermektedir.

Çalışmanın temel bulguları, Mossad'ın Hizbullah'a yönelik çağrı cihazı saldırısı özelinde, hibrit operasyonların iki stratejik sonuç doğurduğunu göstermektedir. Tedarik zincirinin

yalnızca bir lojistik unsur değil, doğrudan operasyonel bir silah olarak kullanılabileceğini, siber müdahale ile geleneksel insan istihbaratının iç içe geçmesinin, stratejik etkisini artırdığını kanıtlamıştır.

Çalışma tek bir vaka analizine (Mossad-Hizbullah çağrı cihazı saldırısı) dayanmakta olup, operasyonun perde arkasındaki istihbarat karar alma süreçlerine ve gizli teknik detaylara doğrudan erişim imkânı bulunmadığından, bulgular büyük ölçüde açık kaynak verileri, güvenlik raporları ve ikincil literatürle sınırlıdır. Netice olarak, geleneksel istihbaratın sınırlarını genişleten ve siber alanın sunduğu imkanları birleştiren operasyonlar, modern güvenlik anlayışının önemli parçalarını oluşturmaktadır; bu gelişmeler hem ulusal hem de uluslararası güvenlik ortamında yeni denge ve dengeli politikaların kurulması ihtiyacını zorunlu kılmaktadır.

Kaynakça

AlBadawi, Habib. "Hezbollah's Military Setback: From Strategic Strength to Political Dilemma—A Comprehensive Analysis." *The Journal of Social Encounters* 9.2 (2025): 107-123.

Austin, J. (2025). Exploring the Evolution of Cyber Intelligence (CYINT): A Disciplinary Debate and Practical Implications. National Intelligence University - Intelligence Studies Summit 2025.

Bonfanti, M. E. (2018). Cyber Intelligence: in pursuit of a better understanding for an emerging practice. *Cyber, Intelligence, and Security*, 2(1), 105-121.

Buchar, J. (2024). Lessons from exploding pagers in Lebanon: The West must protect its supply chains. Defense Magazine. Retrieved from: https://www.defensemagazine.com/ (Accessed time: 10 July 2026)

Sheng, C., Ma, W., Han, Q. L., Zhou, W., Zhu, X., Wen, S., ... & Wang, F. Y. (2024). Pager explosion: Cybersecurity insights and afterthoughts. *IEEE/CAA Journal of Automatica Sinica*, 11(12), 2359-2362.

Cingöz, M., Özkan, F., Alkan, Y. S., & İzol, R. (2024). Iran's axis of resistance through the lens of ontological security. *Third World Quarterly*, 45(13), 1963-1980.

Cohen, A. &. (2024). “Well, it depends”: The explosive pagers attack revisited. Lieber Institute West Point. Retrieved from: https://lieber.westpoint.edu/well-it-depends-explosive-pagers-attack-revisited/ (Accessed Time: 10 July 2026)

Crypto Museum. (2024). Retrieved from: https://www.cryptomuseum.com/covert/radio/apollo/ar924/ (Accessed Time: 03 July 2026)

Cunliffe, K. S. (2021). Hard target espionage in the information era: new challenges for the second oldest profession. Intelligence and National Security, 36(7), 1018-1034.

Daricili, A. B., & Erendor, M. E. (2021). The cyber security strategy of Israel. *Voprosy Istorii,* *11*(3), 233–246.

Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy,* 6(3), 429-450.

Gioe, D. V., Goodman, M. S., & Stevens, T. (2020). Intelligence in the cyber era: Evolution or revolution?. *Political Science Quarterly,* 135(2), 191-224.

Gök, A. (2021). Vekâlet Savaşlarında İstihbarat Örgütlerinin Rolü: Kudüs Gücü Örneği. *Ekonomi Politika ve Finans Araştırmaları Dergisi*, 6(3), 728-747.

Hazbun, W. (2026). Israel, the Axis of Resistance, and the end of deterrence. Project on Middle East Political Science. Retrieved from: https://pomeps.org/israel-the-axis-of-resistance-and-the-end-of-deterrence (Accessed Time: 02 July 2026)

Estriani, H. N., Dewanto, P. A., & Asyidiqi, H. (2023). Asymmetric and Hybrid Warfare in Postmodern Times: Lesson from Hezbollah-Israeli War 2006. *Andalas Journal of International Studies (AJIS),* 12(1), 27-37.

Johnson, L. (2010). Evaluating “Humint”: The role of foreign agents in US security. *Comparative Strategy*, 29(4), 308-332.

Kravetz MSc, J. R. (2025). The Cyber Deterrence Dilemma: Parallels Between Cyber and Intelligence Special Operations. *Joint Force Quarterly*, 119(4), 72-81.

Lowenthal, M. M., & Clark, R. M. (Eds.). (2015). The five disciplines of intelligence collection. Sage.

Lowenthal, M. M. (2025). Intelligence: From secrets to policy. CQ press.

Force, C. I. T. (2013). Operational levels of cyber intelligence. The Intelligence and National Security Alliance (INSA), Tech. Rep, 9.

Sarker, P. P. (2025). When everyday devices become weapons: A closer look at the pager and walkie-talkie attacks. arXiv preprint arXiv:2501.17405.

Sobelman, D. (2025). Axis of Resistance: Asymmetric deterrence and rules of the game in contemporary Middle East conflicts. SUNY Press.

Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and CounterIntelligence*, 27(4), 702-719

ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ

CYBER SECURITY IN THE AGE OF ARTIFICIAL INTELLIGENCE AND AUTONOMOUS WEAPONS

Müfide Onur[*]
ORCID ID: 0009-0004-4444-0443

Edited by Mehmet Emin Erendor, *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons (CRC Press: Boca Raton, 2025, 1st Edition), 216 Pages,* ISBN: 978-1-032-57939-9 (hbk, ISBN: 978-1-032-57938-2 (pbk), ISBN: 978-1-003-44170-0 (ebk), DOI: 10.1201/9781003441700

Declaration[*]

The work titled "Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons" is an academic study that aims to examine the concepts of artificial intelligence (AI) and autonomous weapon systems, two critical dimensions that often remain in the background of the field of cyber security from a distinct perspective. While evaluating these phenomena through an interdisciplinary approach, the book aims to achieve an international character by incorporating contributions from academics from various countries and geographic regions. The first edition of the work was published by CRC Press in 2025. The book's editor, Mehmet Emin Erendor, is an academic whose work is centered on the field of International Relations; his research interests include cyber security, terrorism, the Turkic world, Turkish foreign policy, and international organizations.

General Framework Of The Study

This study primarily employs an interdisciplinary approach to address the impacts of artificial intelligence (AI), autonomous weapon systems, cyber warfare, intelligence technologies, and new modes of warfare on international security, law, and ethics. The book does not limit itself to explaining technological advancements; rather, it aims to discuss how AI is transforming the nature of warfare and redefining the role of humans within it.

The compilation of chapters by various authors provides the work with a rich and multidimensional content, allowing for a comprehensive evaluation of the subject from

[*] ATÜ, Lisansüstü Enstitüsü, Uluslararası İlişkiler Bölümü, Adana, Türkiye, mufideonr@gmail.com.
[*] In this study, artificial intelligence was used solely to assist with language editing and the refinement of writing. The research and analysis were conducted entirely by the author, and she assumes full responsibility for the content of this work.

diverse perspectives. One of the work's prominent arguments is the analysis of the transformation created by AI technologies in the security and defense sectors. It reveals that the wars of the future will be shaped not merely by human will, physical force, and traditional military capacity, but also by data, algorithms, autonomous systems, and digital infrastructures. In this context, the study evaluates the use of AI in the military sphere not solely as a technological progression, but as a multidimensional security issue with strategic, legal, ethical, and political consequences.

Contributing significantly to the literature, the work offers the reader both a critical perspective and promising suggestions on how technology can be utilized in the interest of the public. It contains important implications for professionals working in public institutions, law enforcement, and the technology sector, as well as for academics and students researching international relations, security studies, and law. The study comprehensively addresses how AI-supported autonomous weapon systems shape the future of warfare, how these systems transform human decision-making processes, and the new dynamics they create for international security. By including examples related to current trends and technological developments, the work enriches the narrative, allowing for the evaluation of subjects based on concrete events.

In the work, the ethical, legal, and accountability dimensions regarding the use of autonomous weapon systems are highlighted. The debates arising from the authority of machines to make decisions on the battlefield in terms of human rights, international humanitarian law, and the ethics of war are examined in detail. Furthermore, the role of AI in data management, algorithmic decision-making, threat analysis, and strategic planning is evaluated, emphasising that the wars of the future will be shaped by information, data, and technological superiority rather than just physical power and traditional military capacity.

Overall, the work demonstrates that AI and autonomous systems are transforming the understanding of security in international relations, reshaping the actors, methods, and decision-making mechanisms of war. Within this framework, the study provides a comprehensive and critical analysis of how the future security environment might evolve by evaluating the military advantages of AI alongside its ethical, legal, and strategic consequences.

Evaluation of The Study

When evaluated within its general framework, the work provides a robust and interdisciplinary contribution to security studies by demonstrating that AI and autonomous systems are transforming the nature of warfare. By addressing different fields such as cybersecurity, intelligence operations, data management, strategic planning, international law, and ethics within a common theoretical framework, the study shows that modern warfare is shaped not only in physical conflict zones but also in digital and algorithmic planes. In this regard, the work fills a significant gap in the literature by examining the phenomenon of AI, which is gaining increasing importance in security studies through a comprehensive perspective.

The chapters specifically dedicated to autonomous weapon systems, cyber warfare, and AI-supported intelligence mechanisms offer in-depth analyses of the future of warfare at both technical and conceptual levels. The work convincingly demonstrates that these technologies are not merely tools to increase military capacity; they have become fundamental elements that reshape decision-making processes, accountability relations, and the international security architecture. Furthermore, the emphasis on the role of AI in strategic planning and operational processes significantly enhances the study's analytical power.

Moreover, the work does not settle for explaining the transformation of war solely through technological developments; it also comprehensively evaluates the ethical and legal dimensions. The problems arising from autonomous weapon systems regarding international humanitarian law, the ethics of war, and principles of accountability are addressed with a systematic approach. Thus, the study successfully merges technical analysis with normative evaluation.

Additionally, relating the approaches of classical war theorists, such as Clausewitz, to today's AI-based technological transformation increases the work's theoretical depth and contributes to the evaluation of war studies within a historical continuity. This approach establishes a meaningful bridge between classical security theories and contemporary technological developments, strengthening the conceptual richness of the study. In conclusion, the work is extremely valuable for its multidimensional approach to the transformation of war in the age of AI, its ability to bring different disciplines together within a common analytical framework, and its holistic evaluation of technical, strategic, legal, and ethical dimensions. In

this respect, the book not only makes a significant contribution to the existing academic literature but also provides a strong theoretical and analytical framework that can guide future security and war studies.

Conclusion

The issues addressed in this study artificial intelligence, autonomous weapon systems, cyber security, intelligence technologies, and ethical and legal debates offer a broad and multi-layered perspective on understanding the transformation of the contemporary international security environment. In this sense, the work provides an interdisciplinary analysis that goes beyond merely examining technological developments to encompass the political, legal, and ethical dimensions of war.

In this context, the book first provides a strong theoretical infrastructure for undergraduate and graduate students studying international relations, political science, security studies, and law. At the same time, for professionals working in military strategy, defense policy, cyber security, and intelligence, it serves as an important reference source for understanding the impacts of AI-based technological transformation on security policies. Furthermore, for researchers working on AI and data technologies, the work provides the opportunity to evaluate these technologies from a holistic perspective not just as engineering components, but as factors affecting international politics, security, law, and society. For academics, it serves as an important reference by encouraging interdisciplinary research, bringing together different theoretical approaches, and providing a comprehensive perspective on current security debates.

Ultimately, the work appeals to a wide readership in both theoretical and practical aspects; it stands out as a valuable reference for students, researchers, academics, and policymakers who wish to understand the transformation of the concept of security and war in the age of artificial intelligence. From a personal evaluation perspective, the work is highly eye-opening due to its comprehensive content and interdisciplinary approach. One of its strongest attributes is its treatment of AI's role in security not merely as a technological development but as a strategic element affecting the functioning of the international system and the security architecture. The sections regarding autonomous weapon systems, cyber warfare, and AI-supported intelligence technologies are both explanatory and thought-provoking for understanding current security debates. The authors' ability to link technological

developments with international relations theories, security policies, and strategic analyses increases the work's academic value. Moreover, the fact that ethical and legal dimensions are not overlooked comprehensively addressing the problems of accountability, human oversight, and international humanitarian law regarding autonomous systems gives the study a balanced and critical perspective. Overall, the work is a significant academic study that examines the multidimensional transformation of war and the understanding of security in the age of AI, successfully integrating theoretical and practical discussions. In this respect, the book can be considered a guiding reference for researchers, students, and practitioners who wish to understand the future security environment.

THE ETHICS OF INFORMATION

Saliha Nur KÖŞGER*
ORCID ID: 0009-0003-4836-1032

Edited by Luciano Floridi, *The Ethics of Information (Oxford University Press: United Kingdom, 2013, 1st Edition)* 353 Pages, Online ISBN: 9780191760938, Print ISBN: 9780199641321, https://doi.org/10.1093/acprof:oso/9780199641321.001.0001.

Declaration*

Introduction

The Italian philosopher Luciano Floridi, regarded as the founder of the fields of philosophy of information and digital ethics, is a pioneering thinker who has redefined the relationship between technology, artificial intelligence and ethics throughout his academic career. After completing his education at La Sapienza University in Rome and the University of Warwick, he spent many years at the University of Oxford, where he founded the Digital Ethics Laboratory. He currently continues his work as director of the Digital Ethics Centre (DEC), which he established at Yale University, and as a professor at the University of Bologna. Floridi not only develops philosophical theories but also advises institutions such as the European Union on technology policy; in 2022, he was honoured with Italy's highest state honour in recognition of his immense contributions to the literature and to global AI ethics.

Human history has undergone—and continues to undergo—profound shifts in mindset driven by scientific and technological revolutions. Nicolaus Copernicus ushered in a cosmological shift by removing humanity from the center of the universe; Charles Darwin established an evolutionary continuum by dethroning humanity from the pinnacle of the biological kingdom; and Sigmund Freud sparked a psychoanalytic revolution by shaking the belief in the transparency of the purely rational mind. In his work *The Ethics of Information (2013)*, Luciano Floridi characterizes the revolution in information and communication technologies (ICT)—pioneered by Alan Turing—as the Fourth Revolution, one that redefines humanity's place in the universe and its very nature. The transformative effects of Information and Communication Technologies (ICT) on the human condition, social structure, and perception of reality constitute one of the most fundamental philosophical issues of the twenty-first

* kosger346@gmail.com
* The author acknowledges the use of Gemini for proofreading and language editing purposes during the preparation of this manuscript. The final content was reviewed and approved by the author.

century. Luciano Floridi's work The Ethics of Information offers a comprehensive, systematic, and innovative macroethical framework to address the ethical challenges posed by this technological and ontological transformation. As the second volume of the four-volume Principia Philosophiae Informationis series—which lays the foundations of the philosophy of information—the work begins with the thesis that classical anthropocentric (human-centered) or biocentric (life-centered) ethical theories fall short in resolving the complex problems of the information age.

Floridi argues that humanity is currently in a hyperhistorical phase. In this phase, social well-being and development are directly dependent on the successful management of information cycles. In this era, in which technology is restructuring the world not only epistemologically but also ontologically (re-ontologization), Floridi develops an "e-nvironmental" approach, arguing that all information entities possess an intrinsic moral value. In assessing the historical process, the author notes that we have moved beyond the historical era that began with the recording and transmission of information; in this period, referred to as the zettabyte era, people now experience an "onlife" (online life) in which digital and analog boundaries have dissolved. This study examines Floridi's work by first providing a detailed summary of all sixteen chapters, followed by a thorough book review of the work's philosophical architecture.

This work aims to achieve certain objectives in order to systematize the conceptual foundations of information ethics. The meta-theoretical objective defines the nature, methods, and issues of information ethics, while the introductory objective helps the reader understand concepts related to computer ethics. The analytical objective, meanwhile, focuses on addressing theoretical questions regarding the philosophical and ethical implications of information and communication technologies. To achieve these objectives, the work presents a broad scope of analysis, ranging from the philosophy of being to complex global ethical issues.

Abstract

If a classification is to be made, the first five chapters of the book begin by laying an ontological foundation for the problem of situating ethics in the wake of the information revolution. The book features a first chapter that examines the information revolution—the fourth revolution in humanity's understanding of its own nature, following the Copernican, Darwinian, and Freudian revolutions—which emerged with Alan Turing. The author argues

that humans are not beings who stand motionless at the center of the universe (pre-Copernican), are completely detached from other living beings (pre-Darwinian), or are transparent, purely rational entities (pre-Freudian). On the contrary, he contends that they have become interconnected "inforgs" within a global information ecosystem called the "Infosphere." By ontologically restructuring our environment and erasing the boundary between the digital and analog worlds, ICTs create a hyper-historical state of existence. In the zettabyte age—reached as a result of the accumulation of information—concepts such as ownership, virtual entities, and autonomous systems have emerged.

In the second chapter, the author examines the development of the concept of Information Ethics within the framework of the Source, Product, Target, and Macroethics model. This evolution, illustrated through the example of Alice—an ethical failure—demonstrates how the nature of information is perceived. Arguing that the first three stages (Source, Product, and Target) are reductionist, the author positions Information Ethics in the fourth stage as a holistic macroethical theory in its own right. This transformation requires accepting information as an ontological entity.

To deepen his philosophical analysis, Floridi introduces the concept of Levels of Abstraction (LoA) in the third chapter, borrowing it from the formal methods of computer science. The analysis of a system and the properties attributed to it are directly dependent on the set of observable variables selected—that is, the LoA. Floridi uses this method to redefine the concept of telepresence. He rejects the standard model, which defines telepresence as an epistemic failure—the inability to distinguish between the real and the virtual. Instead, he defines telepresence as the successful observation of an entity in a distant field of view at a specific LoA. Furthermore, by distinguishing between forward and backward telepresence based on the direction of the action, it enables a clearer understanding of privacy issues in situations such as the use of CCTV cameras.

In the fourth chapter, Floridi establishes Information Ethics as an ontocentric (entity-centered) and patient-oriented (focused on those affected by actions rather than the agent) macroethical theory that views all entities as information systems. He explains the homogeneity of entities by referring to the state of Nothingness or the corruption of being as metaphysical entropy. By extending his ecological approach to the information universe, he introduces the principle of ontological equality, which states that every entity deserves respect, even at the most minimal level. Finally, by evaluating the relationships between information ethics and virtue ethics,

deontology, and consequentialism, issues such as vandalism, bioengineering, and death are examined through an e-environmental analysis.

In the fifth chapter, the author addresses the ongoing foundationalist debates regarding the academic status of Computer Ethics. While some approaches view Computer Ethics as a temporary pedagogical method or an adaptation of existing philosophical theories to new problems (applied ethics), Floridi adopts a radical approach. He argues that the problems created by ICTs are unique; therefore, there is a need for a new philosophical discipline with ontological foundations—namely, Information Ethics as a branch of macroethics.

In the sixth chapter of the book, Floridi harshly criticizes Kantian axiology, which confines ethical debates to human reason. He emphasizes that approaches which accept rationality as the sole criterion of moral respect are insufficient for grasping the wholeness of the Infosphere and that well-being. The fundamental axiom of the Ethics of Information is as follows: Everything that exists—whether natural or artificial—possesses a minimum intrinsic moral value and holds the right to development simply by virtue of being an object of knowledge. This ontocentric approach expands the horizons of environmental ethics beyond biological life to include inanimate digital entities as well.

The class of moral agents is expanded beyond its traditional boundaries to include autonomous artificial intelligence systems (Artificial Agents—AA) that lack consciousness or free will. Floridi and Sanders state that for an entity to be considered an agent, it must meet three criteria at a specific Level of Abstraction (LoA): interactivity, autonomy, and adaptability. Consciousness, mental states, or intent are not absolute prerequisites for moral agency. This non-mental conception of ethics acknowledges that artificial systems can be the source of actions that produce morally good or bad outcomes, while drawing a clear line between the concepts of intent-based responsibility and accountability based on causal impact.

If the world is an ontologically restructured Infosphere and we, too, are inforgs, what is humanity's moral role here? Finding the classical models of Homo Faber (Tool-Making Man) or Homo Oeconomicus (Economic Man) inadequate, Floridi argues that humans are creative agents who shape the world—that is, Homo Poieticus (Creator Man). While traditional virtue ethics focuses on the individual's construction of their own character, the information age necessitates the moral construction of the goals of our actions and our environment—that is, ecopoiesis. Movements such as the internet and open-source software serve as examples of

poietically empowering ecosystems and maximize humanity's potential as both an epistemic agent and a moral constructor.

Understanding the nature of evil lies at the heart of the ethics of knowledge. Floridi adopts an interpretation that does not define evil as a positive, essential entity. Just as in the Augustinian tradition, evil is the absence of good or the corruption of being; in a computational context, this corresponds to metaphysical entropy. The unjust destruction or corruption of knowledge structures, data, and relationships constitutes fundamental evil. This concept allows us to understand the phenomenon of artificial evil—harm caused to the environment by the interaction of machines without human intent, yet without a malevolent agent behind it.

The Information Age creates a paradoxical state of moral anguish. Thanks to global communication networks, people are constantly and instantly aware of evils, disasters, and injustices taking place all over the world. However, when this high flow of information is not supported by a commensurate capacity for intervention, good intentions—as a moral agent—experience a profound tragedy. Floridi explains this situation by drawing parallels to the character of Miranda in Shakespeare's "The Tempest", who helplessly watches a distant shipwreck, and to Cassandra of Troy, who knew of impending disasters but lacked the power to prevent them. While ICTs constantly confront us with evils we cannot resolve, creating a sense of moral exhaustion and helplessness, initiatives such as the Copenhagen Consensus are presented as strategies for coping with information through information itself. The author examines human identity and the self through a computational architecture. Drawing on Plato's metaphor of the charioteer, Floridi questions how the self holds together multiple layers and proposes the "Three Membranes" model.

Floridi offers a revolutionary approach to privacy debates. He notes that theories defending privacy through classical property rights or spatial boundary violations fail to resolve the problems created by data collected in public spaces (such as via CCTV cameras). Instead, he argues that a person's personal data is an ontological part of the individual and a building block of the information architecture. Consequently, a privacy violation is not theft or a boundary violation, but an attack on a person's ontological integrity—a form of bodily abduction or cloning. The frictionlessness of the infosphere leads to an uncontrolled flow of data, directly threatening the construction of identity.

In networked hyper-societies, moral actions increasingly transcend the boundaries of the individual agent. The concept of distributed ethics refers to the phenomenon where small

actions—each of which might be considered morally neutral or insignificant on its own—cumulatively combine through the network to produce massive macro-level consequences, whether good or bad. In this context, Floridi develops the concept of "infraethics." Infraethics refers to mechanisms in society—such as trust, transparency, design, and communication infrastructure—that are morally neutral in and of themselves; these elements act as systemic catalysts that either facilitate or hinder the occurrence of distributed moral actions. Examples of this include online crowdfunding and algorithmic systemic biases.

Institutions and businesses are considered macro-actors within the Infosphere. Floridi presents the WHI (What, How, Impact) framework to facilitate the ethical analysis of institutional structures. A company's products or services (What), the methods and processes used to produce them (How), and the ontological and ecological traces of these activities within the Infosphere (Impact) must be evaluated together. This intersection of business ethics and information ethics offers a new perspective on the distribution of responsibility within the multi-actor network structures of the modern information economy.

The globalizing, increasingly interconnected, and synchronized information society raises the issue of the universality of moral values. Floridi argues that simple communication ethics will prove insufficient in this complex structure and that a transition to a profound global information ethics is necessary. However, this does not imply the imposition of a hegemonic universality. To ensure that cultural differences are preserved to the greatest extent possible—unlike the necessary relationship between a lion and a gazelle—an ontological foundation of trust must be established in which agents voluntarily agree not to destroy one another.

In the book's concluding chapter, Floridi tests his philosophical system by providing methodological responses to 20 fundamental criticisms directed at his theory over the past decade. Among these criticisms are claims that the Ethics of Knowledge is a naturalistic fallacy, that attributing value to all entities implies pantheism, that it confuses moral value with moral respect, and that it is inapplicable because it dehumanizes. The author demonstrates that the protection of entities in the Infosphere is not a mystical belief but a logical and ecological necessity, and that his macroethical system is resilient against such skeptical attacks.

Analysis

Luciano Floridi's "The Ethics of Information" is a monumental intellectual endeavor that pushes the boundaries by treating information not merely as a communication process, a data set, or semantic content, but as the fundamental ontological fabric of reality. The book does not merely offer a practical prescription for resolving current debates in Computer Ethics or Cyber Ethics (such as software ownership, artificial intelligence biases, or spam messages); rather, it constructs a macro-structure that reinterprets Kantian ethics, Spinozist philosophy, and Platonic epistemology in light of the information age.

The book's greatest philosophical strength lies in its innovative ontology of technology. While technology is often viewed as an artificial construct set in opposition to nature, Floridi dismantles this classic dichotomy by equating the status of information entities. New terms coined by the author—such as the Infosphere, Inforg, Metaphysical Entropy, Ontic Trust, and Homo Poieticus—are the product of an effort to construct not merely a descriptive but also a normative world.

In particular, the discussions on privacy in Chapter 12 make a significant contribution to the existing literature. By shifting the focus of privacy away from a property-based foundation and grounding it in the context of personhood, bodily integrity, and ontological identity, the book offers legal and policy makers a much stronger line of defense against big data collectors and technology companies in the public sphere. Similarly, the concept of distributed ethics is vital for understanding the moral accountability gaps caused by today's multi-actor, simultaneous, and algorithm-driven networks of action. The analysis of how structures that appear neutral can act as catalysts for major moral catastrophes or social good is one of the sharpest observations of the social media age.

While the work possesses strong internal consistency, the conceptual barrier for the reader is quite high. As Floridi himself states in the preface, this book is not a quick or easy read. For readers with a weak philosophical background, the adaptation of mathematical/computational terminology—such as Levels of Abstraction (LoA) and computational structural realism—to philosophy is challenging. Furthermore, the issue of practical applicability arises in Floridi's ontocentric approach. While arguing that every entity of knowledge—be it an algorithm, an inanimate stone, or a fictional text—possesses intrinsic value at a specific LoA may be theoretically comprehensive, in practice it complicates moral prioritization during moments of crisis marked by conflicting interests.

To help readers overcome this challenge, the author has sought to enhance the text's flow by adding summaries at the beginning of each chapter and conclusions at the end, aiming to bridge the traditional divide between analytics and philosophy.

This book serves as a foundational resource, particularly for philosophers, professionals in the field of information technology, students with a high level of academic knowledge and strong interest in the subject, and researchers interested in the social impacts of technology. It develops a philosophical approach not only to practical technological issues but also to the ethical challenges posed by the digital age. In addition, it offers theoretical responses to some of today's most debated topics (privacy and the accountability of artificial intelligence systems). Although the book is not written in an easy-to-read style or with straightforward content, it possesses the depth to be recommended to anyone curious about the fundamentals of computer technology, big data, and artificial intelligence—as well as the topic of information ethics—in our increasingly digital world.

In conclusion, Luciano Floridi's The Ethics of Information is a monumental conceptual framework designed to address the social, ethical, and existential issues shaped by technology in the twenty-first century. The text does not merely establish practical legal rules to manage the side effects of current technologies (such as data theft, artificial intelligence autonomy, and censorship); it defines the very knowledge of reality, its environmental protection, and its ethical construction as an ontological task.

By successfully synthesizing methodological abstractions derived from computer science (LoA) with the metaphysical depth of classical Western philosophy (Spinoza, Kant, Heidegger, Moore), Floridi provides a single, integrated perspective of the Ethics of Knowledge to address a wide range of issues, from cybersecurity to artificial intelligence, and from digital privacy to the climate crisis. Although his work faces harsh criticism in academic debates—such as accusations of excessive inclusivity, the elimination of anthropocentrism, or the fallacy of naturalism—it serves as a visionary guide for Homo Poieticus (the creative human) existing within a digital ecosystem. The survival of the infosphere, the protection of information entities from entropy, and the management of distributed ethics through appropriate infrastructures are presented as both a moral responsibility and an ontological destiny for humanity. Given that generative artificial intelligence, big data, and autonomous systems will become even more prevalent in daily life in the coming decades—as the "onlife" experience becomes the norm—the theoretical foundations laid by Floridi will continue to be

one of the indispensable mainstream paradigms not only of technology ethics but of general philosophical ethics as well.

References

Floridi, Luciano. *The Ethics of Information*. Oxford University Press: United Kingdom, 2013, 1st Edition.

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.